MПротокол обмена считывателя Mifare Plus

Параметры соединения

Считыватель Mifare Plus имеет следующие параметры соединения: скорость обмена по умолчанию 57600, 1 стоп бит, проверка на чётность. Скорость обмена может быть изменена, см. ниже.

Формат сообщений

Формат сообщений между ведущим устройством и считывателем:

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Стартовый байт, код 02h | 1 |
| 2 | Длина данных N. Учитывается только поле 3 | 1 |
| 3 | Данные | N |
| 4 | Контрольная сумма сообщения, от поля 2 до 3 включительно.  Вычисляется путём сложения байт по XOR. | 1 |

Минимальная длина сообщения 1 байт.

В сообщения от ведущего устройства первый байт сообщения содержит код команды.

По умолчанию в ответах считывателя первый байт содержит код ошибки. При включении режима ответа с кодом команды (см. команду F4h), первый байт код команды и второй байт код ошибки. Т.е. в ответ добавляется код команды, длина сообщения при этом увеличивается на 1 байт.

В полях сообщений содержащих значения разрядностью больше 1байта, первым всегда идёт младший байт.

Если код ошибки не равен MI\_OK (00h), то другие данные содержащиеся в ответе не валидны.

Терминология

PICC - карта Mifare Classic, Mifare Ultralight, Mifare Ultralight C, Mifare Plus или My-D Move.

PCD – считыватель.

PICC UID – уникальный номер карты. Возможны UID длиной в 4, 7, 10 байт.

AtqA - Answer to Request Type A. Ответ карты на запрос. Описание AtqA см. в ISO/IEC 14443-3 или AN10833 Mifare Type Identification Procedure.

SAK - Select Acknowledge. Ответ карты на выбор. Описание SAK см. в ISO/IEC 14443-3 или AN10833 Mifare Type Identification Procedure.

SL0 – режим работы чистой Mifare Plus карты (болванки).

SL1 – режим совместимости Mifare Plus карты с картами Mifare Classic.

SL2 – SL1 + авторизация по AES к карте.

SL3 – режим с авторизацией к карте по AES ключу, авторизацией по AES к блокам, подпись передаваемых данных, шифрование передаваемых данных.

RATS (Request for Answer to Select) – команда запроса ATS у PICC и переключающая PICC на протокол ISO14443-4.

PPS (Protocol and Parameter Selection) – команда установления параметров обмена между PICC и PCD. Выполняется после RATS.

SAM AV2 модуль – модуль хранящий ключи для авторизации к PICC и для оффлайн криптографии.

Команды протокола

В данном разделе перечислены команды работы со считывателем.

**Команда 02h “Проверка связи”**

Проверка связи со считывателем.

Включает поле радиополе считывателя, если оно было выключено.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 02h | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 04h “Запрос карт”**

Запрос карт находящихся в радиополе считывателя.

Сообщение к считывателю

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 04h | 1 |
| 2 | Параметр запроса.  PICC\_REQALL(52h) – запрос всех карт.  PICC\_REQIDL (26h) – запрос карт находящихся в режиме ожидания. | 1 |

Ответ от считывателя

Длина сообщения: 3 байта.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Ответ карты Answer to Request Type A (AtqA).  Описание AtqA см. в ISO/IEC 14443-3. | 2 |

**Команда 05h “Антиколлизия”**

Запрос номера PICC UID карты находящейся в радиополе считывателя.

Считыватель получает номер одной из приложенных карт и возвращает его в ответе.

Сообщение к считывателю

Длина сообщения: 7 - 15 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 05h | 1 |
| 2 | Параметр запроса. Код антиколлизии.  SELECT\_CASCADE\_LEVEL\_1(93h) – первый уровень.  SELECT\_CASCADE\_LEVEL\_2 (95h) – второй уровень.  SELECT\_CASCADE\_LEVEL\_3 (97h) – третий уровень. | 1 |
| 3 | Число известных бит UID | 1 |
| 4 | Массив, содержащий известные биты номера карты | 4 - 12 |

Ответ от считывателя

Длина сообщения: 5, 8 или 11 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | PICC UID – уникальный номер карты.  Содержит 4 байта UID для “Single Size UID PICC”, 7 байт UID для “Double Size UID PICC”, 10 байта UID для “Triple Size UID PICC” | 4, 7, 10 |

**Команда 06h “Выбор карты”**

Выбор карты PICC с заданным номером.

Считыватель выбирает карту номер которой задан.

Сообщение к считывателю

Длина сообщения: 6 или 9 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 06h | 1 |
| 2 | Параметр запроса. Код антиколлизии.  SELECT\_CASCADE\_LEVEL\_1(93h) – первый уровень.  SELECT\_CASCADE\_LEVEL\_2 (95h) – второй уровень.  SELECT\_CASCADE\_LEVEL\_3 (97h) – третий уровень. | 1 |
| 3 | PICC UID – номер карты. | 4, 7 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | PICC UID – уникальный номер карты.  Содержит 4 байта UID для “Single Size UID PICC”, 7 байт UID для “Double Size UID PICC”, 10 байта UID для “Triple Size UID PICC” | 4, 7, 10 |
| 3 | Select Acknowledge (SAK). Ответ карты на выбор.  Описание SAK см. в ISO/IEC 14443-3. | 1 |

**Команда 07h “Активация карты в режиме ожидания”**

Активация карты PICC находящейся в режиме ожидания.

Происходит запрос, получение (антиколлизия) номера и выбор карты находящейся в режиме ожидания.

Сообщение к считывателю

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 07h | 1 |
| 2 | Зарезервировано. Всегда 0. | 1 |

Ответ от считывателя

Длина сообщения: 9, 12, 14 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Ответ карты Answer to Request Type A (AtqA).  Описание AtqA см. в ISO/IEC 14443-3. | 2 |
| 3 | Select Acknowledge (SAK). Ответ карты на выбор.  Описание SAK см. в ISO/IEC 14443-3. | 1 |
| 4 | Длина номера карты. 4 байта UID для “Single Size UID PICC”, 7 байт UID для “Double Size UID PICC”, 10 байта UID для “Triple Size UID PICC” | 1 |
| 5 | PICC UID – уникальный номер карты. | 4, 7, 10 |

**Команда 09h “Активация карты в режиме остановки”**

Активация карты PICC находящейся в режиме остановки.

Происходит запрос, получение (антиколлизия) номера и выбор карты находящейся в режиме ожидания.

Сообщение к считывателю

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 09h | 1 |
| 2 | Зарезервировано. Всегда 0. | 1 |

Ответ от считывателя

Длина сообщения: 9, 12, 14 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Ответ карты Answer to Request Type A (AtqA).  Описание AtqA см. в ISO/IEC 14443-3. | 2 |
| 3 | Select Acknowledge (SAK). Ответ карты на выбор.  Описание SAK см. в ISO/IEC 14443-3. | 1 |
| 4 | Длина номера карты. 4 байта UID для “Single Size UID PICC”, 7 байт UID для “Double Size UID PICC”, 10 байта UID для “Triple Size UID PICC” | 1 |
| 5 | PICC UID – уникальный номер карты. | 4, 7, 10 |

**Команда 0Ah, 12h “Авторизация к блоку карты”**

Авторизация с блоку карты PICC по заданному ключу.

Происходит авторизация к карте по ключу Crypto-1. Используется для работы с картами Mifare Classic и Mifare Plus в режиме SL1.

Рекомендуется использовать команду 32h.

Сообщение к считывателю

Длина сообщения: 4 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 0Ah или 12h | 1 |
| 2 | Тип ключа.  Для ключа A значение 60h.  Для ключа B значение 61h. | 1 |
| 3 | Номер записи (Key Entry) с ключом, используемым для авторизации и хранящегося на SAM AV2 модуле.  Значение от 0 до 254. | 1 |
| 4 | Номер блока, к которому производится авторизация. | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 0Bh “Запись ключа авторизации Crypto-1”**

Реализована для обеспечения совместимости с предыдущими считывателями Mifare.

Записывает один ключ в SAM AV2 модуль, только A или только B.

Рекомендуется использовать команду 31h.

Сообщение к считывателю

Длина сообщения: 9 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 0Bh | 1 |
| 2 | Тип ключа.  Для ключа A значение 60h.  Для ключа B значение 61h. | 1 |
| 3 | Номер записи (Key Entry) в которую будет записан ключ.  Значение от 0 до 254. | 1 |
| 4 | Ключ | 6 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 0Dh “Чтение блока карты”**

Считывает 16 байт блока данных с карты.

Сообщение к считывателю

Длина сообщения: 4 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 0Dh | 1 |
| 2 | Не используется. Оставлено для совместимости. Всегда 0. | 1 |
| 3 | Номер читаемого блока. | 1 |
| 4 | Не используется. Оставлено для совместимости. Всегда 0. | 1 |

Ответ от считывателя

Длина сообщения: 17 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Данные считанные из заданного блока | 16 |

**Команда 0Eh “Запись блока карты”**

Записывает 16 байт данных в заданный блок с карты.

Сообщение к считывателю

Длина сообщения: 20 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 0Eh | 1 |
| 2 | Код операции записи. Всегда A0h | 1 |
| 3 | Номер записываемого блока. | 1 |
| 4 | Число записываемых байт данных. Всегда 16. | 1 |
| 5 | Записываемые данные. | 16 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 0Fh “Изменение блок значения с сохранением”**

Изменение блок значения (Value блока) с выполнением команды Transfer.

Сообщение к считывателю

Длина сообщения: 8 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 0Fh | 1 |
| 2 | Код операции.  Декремент PICC\_DECREMENT (C0h). Инкрементирует значение данных из блока источника и сохраняет его во временном регистре. Затем данные сохраняются в блоке получателе.  Инкремент PICC\_INCREMENT (0xC1) . Декрементирует значение данных из блока источника и сохраняет его во временном регистре. Затем данные сохраняются в блоке получателе.  Восстановление значения во временном регистре PICC\_RESTORE (C2h). Происходит запись значения в регистр из блока источника. Затем данные сохраняются в блоке получателе.  Сохранение значения в Value блоке PICC\_TRANSFER (0xB0). Записывает значение из временного регистра в Value блоке. | 1 |
| 3 | Номер блока источника. Из него считываются данные перед операцией. | 1 |
| 4 | Номер блока получателя. В него сохраняются данные. | 1 |
| 5 | Значение. | 4 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 10h “Изменение блок значения”**

Изменение блок значения (Value блока).

Сообщение к считывателю

Длина сообщения: 8 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 10h | 1 |
| 2 | Код операции.  Декремент PICC\_DECREMENT (C0h). Инкрементирует значение данных из блока источника и сохраняет его во временном регистре.  Инкремент PICC\_INCREMENT (0xC1) . Декрементирует значение данных из блока источника и сохраняет его во временном регистре.  Восстановление значения во временном регистре PICC\_RESTORE (C2h). Происходит запись значения в регистр из блока источника. Затем  Сохранение значения в Value блоке PICC\_TRANSFER (0xB0). Записывает значение из временного регистра в Value блоке. | 1 |
| 3 | Номер блока источника. Из него считываются данные перед операцией. | 1 |
| 4 | Номер блока получателя. В него сохраняются данные. | 1 |
| 5 | Значение. | 4 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 11h “Чтение блок значения”**

Считывает 4 байта блок значения с карты и его адрес.

Сообщение к считывателю

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 11h | 1 |
| 2 | Номер читаемого блока. | 1 |

Ответ от считывателя

Длина сообщения: 6 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Данные считанные из заданного блока | 4 |
| 3 | Адрес блока. См. описание Value Block у Mifare | 1 |

**Команда 13h “Останов выбранной карты”**

Переводит выбранную карту в Halt состояние.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 13h | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 14h “Запись блок значение”**

Записывает 4 байта блок значения с карты и его адрес.

Сообщение к считывателю

Длина сообщения: 7 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 14h | 1 |
| 2 | Номер записываемого блока. | 1 |
| 3 | Записываемые данные. | 4 |
| 4 | Адрес блока | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 15h “Запрос серийного номера считывателя”**

Возвращает 4 байта серийного номера считывателя.

Команда оставлена для совместимости с предыдущими считывателями Mifare.

См. новую команду 36h, которая возвращает 16 байт.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 15h | 1 |

Ответ от считывателя

Длина сообщения: 5 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Серийный номер. | 4 |

**Команда 16h “Запрос описания считывателя”**

Возвращает ASCII строку с названием считывателя и версий прошивки.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 16h | 1 |

Ответ от считывателя

Длина сообщения: различна для разных версий.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Описание |  |

**Команда 17h “Запрос версии RIC”**

Оставлено для совместимости.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 17h | 1 |

Ответ от считывателя

Длина сообщения: 6 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | RIC, всегда 11h, 02h, A7h, 10h, ABh | 5 |

**Команда 1Ah “Сброс радиополя”**

Сброс радиополя на заданное время.

**Для безопасности рекомендуется всегда сбрасывать поле после работы с картой. Для сброса авторизации.**

Сообщение к считывателю

Длина сообщения: 3 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 1Ah | 1 |
| 2 | Время сброса в мс. | 2 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 1Сh “Переключение карты на протокол ISO14443-4”**

Выполняет команды RATS (Request for Answer to Select) и команду PPS (Protocol and Parameter Selection).

**Необходима для работы с картами в режиме SL2 и SL3, для смены режима, для выполнения команд персонализации.**

Карта перед выполнением команды должна быть активирована (выбрана).

Выполняется однократно после активации карты.

Сообщение к считывателю

Длина сообщения: 3 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 1Ch | 1 |
| 2 | Скорость передачи данных от PCD к PICC.  Значения:  PHPAL\_I14443P4A\_DATARATE\_106 (00h) – 106 кбит/сек.  PHPAL\_I14443P4A\_DATARATE\_212 (01h) – 212 кбит/сек.  PHPAL\_I14443P4A\_DATARATE\_424 (02h) – 424 кбит/сек.  PHPAL\_I14443P4A\_DATARATE\_848 (03h) – 848 кбит/сек. | 1 |
| 3 | Скорость передачи данных от PICC к PCD.  Значения:  PHPAL\_I14443P4A\_DATARATE\_106 (00h) – 106 кбит/сек.  PHPAL\_I14443P4A\_DATARATE\_212 (01h) – 212 кбит/сек.  PHPAL\_I14443P4A\_DATARATE\_424 (02h) – 424 кбит/сек.  PHPAL\_I14443P4A\_DATARATE\_848 (03h) – 848 кбит/сек. | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 1Dh “Подтверждение персонализации”**

Переводит карту из режима SL0 в режим SL1.

**Перед выполнением команды необходимо записать на карту все ключи, биты доступа, настройки карты, начальные значения данных.**

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 1Dh | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 1Eh “Запись данных при персонализации”**

Запись блоков данных при персонализации карты.

Блоки данных по 16 байт содержат ключи, настройки, начальные значения.

**При персонализации карты категорически нельзя оставлять ключи со значениями по умолчанию. Особенно это касается AES ключей**

Сообщение к считывателю

Длина сообщения: 19 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 1Eh | 1 |
| 2 | Адрес для записи блока данных. См. описание карты. | 2 |
| 3 | Данные. См. описание карты. | 16 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 1Fh “Сброс считывателя”**

Проверка связи со считывателем.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 1Fh | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 20h “Звуковой сигнал”**

Проверка связи со считывателем.

Сообщение к считывателю

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 20h | 1 |
| 2 | Номер проигрываемого звукового сигнала | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 21h “Чтение страницы с карты Ultraligth”**

Считывает данные с карты Ultralight или Ultralight C.

Сообщение к считывателю

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 21h | 1 |
| 2 | Номер читаемой страницы | 1 |

Ответ от считывателя

Длина сообщения: 17 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | 16 байт считанных данных. 4 первых байта для заданной страницы.  12 байт со следующих 3-х страниц. | 16 |

**Команда 22h “Запись страницы на карту Ultraligth”**

Записывает данные на карту Ultralight или Ultralight C.

Сообщение к считывателю

Длина сообщения: 6 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 22h | 1 |
| 2 | Номер записываемой страницы | 1 |
| 3 | Записываемые данные | 4 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 23h “Запись страницы на карту Ultraligth в режиме совместимости”**

Записывает данные на карту Ultralight или Ultralight C в режиме совместимости с Mifare Classic.

Сообщение к считывателю

Длина сообщения: 18 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 23h | 1 |
| 2 | Номер записываемой страницы | 1 |
| 3 | Записываемые данные. 4 первых байта должны содержать записываемые данные. 12 следующих байт игнорируются, в них рекомендуется записывать 0. | 16 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 24h “Запись 2K3DES ключа для карт Ultralight C в SAM AV2 модуль”**

Записывает ключ авторизации к карте Ultralight в SAM AV2 модуль.

**В одной записи можно хранить 3 ключа с разными версиями, в разных позициях.**

Сообщение к считывателю

Длина сообщения: 20 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 24h | 1 |
| 2 | Номер записи (Key Entry) в которую будет записан ключ.  Значение от 0 до 254. | 1 |
| 3 | Позиция ключа. Значение 0 – 2. | 1 |
| 4 | Версия ключа. Значение 0 - 255. | 1 |
| 5 | Ключ 2K3DES. Два ключа по 8 байт. | 16 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 25h “Авторизация к карте Ultralight C 2K3DES ключом”**

Производит авторизацию к карте Ultralight C 2K3DES ключом.

Сообщение к считывателю

Длина сообщения: 3 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 25h | 1 |
| 2 | Номер записи (Key Entry) в которую записан ключ.  Значение от 0 до 254. | 1 |
| 3 | Версия используемого ключа. Значение 0 - 255. | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 30h “Запрос информации производителя SAM AV2 модуля”**

Запрашивает у SAM AV2 модуля информацию производителя и возвращает ведущему устройству. Информация производителя содержит: ID производителя (04h для NXP), тип, подтип, версию, размер памяти, тип протокола (01h для T1), уникальный серийный номер, номер продукта, дата производства. Более подробно см. в описании SAM AV2 модуля.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 30h | 1 |

Ответ от считывателя

Длина сообщения: зависит от SAM AV2 модуля, но на момент описания протокола 32 байта.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Информация производителя | X, 31 |

**Команда 31h “Запись ключей авторизации Crypto-1, A и B”**

Одновременно записывает пару ключей A и B в SAM AV2 модуль.

**В одной записи можно хранить 3 пары ключей с разными версиями, в разных позициях.**

Сообщение к считывателю

Длина сообщения: 16 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 31h | 1 |
| 2 | Номер записи (Key Entry) в которую будет записана пара ключей.  Значение от 0 до 254. | 1 |
| 3 | Позиция ключей для записи | 1 |
| 4 | Версия ключей | 1 |
| 5 | Ключ A | 6 |
| 6 | Ключ B | 6 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 32h “Авторизация к блоку карты”**

Авторизация к блоку карты PICC по заданному ключу.

Происходит авторизация к карте по ключу Crypto-1. Используется для работы с картами Mifare Classic и Mifare Plus в режиме SL1.

Сообщение к считывателю

Длина сообщения: 5 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 32h | 1 |
| 2 | Тип ключа.  Для ключа A значение 60h.  Для ключа B значение 61h. | 1 |
| 3 | Номер записи (Key Entry) с ключом, используемым для авторизации и хранящегося на SAM AV2 модуле.  Значение от 0 до 254. | 1 |
| 4 | Версия используемого ключа. | 1 |
| 5 | Номер блока, к которому производится авторизация. | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 34h “Запись AES ключа авторизации к SAM AV2 модулю”**

Записывает в SAM AV2 модуль ключ для авторизации к нему.

Используется для персонализации SAM AV2 модуля. Считыватель перед началом работы должен авторизоваться к SAM AV2 модулю этим ключом.

**Необходимо внимательно отнесись к записи этого ключа. Ошибка приведёт к невозможности использовать модуль.**

Сообщение к считывателю

Длина сообщения: 19 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 34h | 1 |
| 2 | Ключ авторизации. | 16 |
| 3 | CRC ключа авторизации. Используется CCITT-CRC16.  Полином X^16 + X^12 + X^5 + 1. Начальное значение 0000h.  См. Приложение 1. | 2 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 35h “Чтение параметров ключей”**

Читает параметры ключей (тип и версию) в ключевой записи.

Сообщение к считывателю

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 35h | 1 |
| 2 | Номер записи (Key Entry) с ключами.  Значение от 0 до 254. | 1 |

Ответ от считывателя

Длина сообщения: 11 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Тип ключей.  00h – AES128.  01h – AES192.  02h – AES256.  03h – DES.  04h – 2K3DES.  05h – 3K3DES.  06h – MIFARE (Crypto-1). | 2 |
| 3 | Длина списка версий ключей. Содержит число ключей в записи и сообщает сколько полей версий ключей заполнено.  Значение от 0 до 3.  3 – для Crypto-1, AES128, 2K3DES. | 2 |
| 4 | Версия ключа в позиции 0. | 2 |
| 5 | Версия ключа в позиции 1. | 2 |
| 6 | Версия ключа в позиции 2. | 2 |

**Команда 36h “Получить полный серийный номер считывателя”**

Возвращает полный серийный номер считывателя. Может использоваться для привязки SAM AV2 модуля к считывателю.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 36h | 1 |

Ответ от считывателя

Длина сообщения: 17 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Полный серийный номер. | 16 |

**Команда 37h “Включить привязку SAM AV2 модуля к считывателю”**

Привязывает SAM AV2 модуль установленный в считыватель к этому считывателю.

При этом в SAM AV2 модуль записывается ключ авторизации полученный на основе серийного номера модуля и серийного номера считывателя.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 37h | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 38h “Включить привязку SAM AV2 модуля к считывателю с заданным серийным номером”**

Привязывает SAM AV2 модуль, установленный в считыватель к считывателю, серийный номер которого задается в команде.

При этом в SAM AV2 модуль записывается ключ авторизации полученный на основе серийного номера модуля и серийного номера считывателя.

Используется для выпуска SAM AV2 модулей.

Сообщение к считывателю

Длина сообщения: 19 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 38h | 1 |
| 2 | Серийный номер считывателя | 16 |
| 3 | CRC серийного номера. Используется CCITT-CRC16.  Полином X^16 + X^12 + X^5 + 1. Начальное значение 0000h.  См. Приложение 1. | 2 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 39h “Сброс авторизации к карте Mifare Plus”**

Сбрасывает авторизацию к карте. Используется при необходимости авторизации другим ключом.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 39h | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 3Ah “Запись блока данных на карту Mifare Plus”**

Записывает блок данных на карту Mifare Plus, находящуюся в режиме SL2 или SL3.

Сообщение к считывателю

Длина сообщения: 21 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 3Ah | 1 |
| 2 | Номер блока. | 2 |
| 3 | Настройка обмена, шифрование  1 – включено.  0 – выключено. | 1 |
| 4 | Настройка обмена, подпись ответа  1 – включено.  0 – выключено. | 1 |
| 5 | Записываемые данные. | 16 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 3Bh “Чтение блока данных с карты Mifare Plus”**

Читает блок данных с карты Mifare Plus, находящейся в режиме SL2 или SL3.

Сообщение к считывателю

Длина сообщения: 6 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 3Bh | 1 |
| 2 | Номер блока. | 2 |
| 3 | Настройка обмена, шифрование  1 – включено.  0 – выключено. | 1 |
| 4 | Настройка обмена, подпись ответа  1 – включено.  0 – выключено. | 1 |
| 5 | Настройка обмена, подпись команды  1 – включено.  0 – выключено. | 1 |

Ответ от считывателя

Длина сообщения: 17 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Прочитанные данные. | 16 |

**Команда 3Ch “Запись блока значения на карту Mifare Plus”**

Записывает блок значение (value блок) на карту Mifare Plus, находящуюся в режиме SL2 или SL3.

Сообщение к считывателю

Длина сообщения: 9 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 3Ch | 1 |
| 2 | Номер блока. | 2 |
| 3 | Настройка обмена, шифрование  1 – включено.  0 – выключено. | 1 |
| 4 | Настройка обмена, подпись ответа  1 – включено.  0 – выключено. | 1 |
| 5 | Записываемые данные. | 4 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 3Dh “Чтение блока значения с карты Mifare Plus”**

Читает блок значение (value блок) с карты Mifare Plus, находящейся в режиме SL2 или SL3.

Сообщение к считывателю

Длина сообщения: 6 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 3Dh | 1 |
| 2 | Номер блока. | 2 |
| 3 | Настройка обмена, шифрование  1 – включено.  0 – выключено. | 1 |
| 4 | Настройка обмена, подпись ответа  1 – включено.  0 – выключено. | 1 |
| 5 | Настройка обмена, подпись команды  1 – включено.  0 – выключено. | 1 |

Ответ от считывателя

Длина сообщения: 5 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Прочитанные данные. | 4 |

**Команда 3Eh “Инкремент блока значения на карте Mifare Plus”**

Инкрементирует блок значение (value блок) на карте Mifare Plus, находящейся в режиме SL2 или SL3. Результат сохраняется во временном регистре.

Сообщение к считывателю

Длина сообщения: 8 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 3Eh | 1 |
| 2 | Номер блока. | 2 |
| 3 | Настройка обмена, подпись ответа  1 – включено.  0 – выключено. | 1 |
| 4 | Величина инкремента. | 4 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 3Fh “Декремент блока значения на карте Mifare Plus”**

Декрементирует блок значение (value блок) на карте Mifare Plus, находящейся в режиме SL2 или SL3. Результат сохраняется во временном регистре.

Сообщение к считывателю

Длина сообщения: 8 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 3Fh | 1 |
| 2 | Номер блока. | 2 |
| 3 | Настройка обмена, подпись ответа  1 – включено.  0 – выключено. | 1 |
| 4 | Величина декремента. | 4 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 40h “Сохранение блок значения на карте Mifare Plus”**

Пересылает данные из временного регистра в блок значение.

Сообщение к считывателю

Длина сообщения: 4 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 40h | 1 |
| 2 | Номер блока. | 2 |
| 3 | Настройка обмена, подпись ответа  1 – включено.  0 – выключено. | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 41h “Восстановление блок значения с карты Mifare Plus”**

Пересылает данные из блок значения во временный регистр.

Сообщение к считывателю

Длина сообщения: 4 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 41h | 1 |
| 2 | Номер блока. | 2 |
| 3 | Настройка обмена, подпись ответа  1 – включено.  0 – выключено. | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 42h “Инкремент блока значения на карте Mifare Plus с сохранением”**

Инкрементирует блок значение (value блок) на карте Mifare Plus, находящейся в режиме SL2 или SL3. Результат сохраняется в том же блоке.

Сообщение к считывателю

Длина сообщения: 8 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 42h | 1 |
| 2 | Номер блока. | 2 |
| 3 | Настройка обмена, подпись ответа  1 – включено.  0 – выключено. | 1 |
| 4 | Величина инкремента. | 4 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 43h “Декремент блока значения на карте Mifare Plus с сохранением”**

Декрементирует блок значение (value блок) на карте Mifare Plus, находящейся в режиме SL2 или SL3. Результат сохраняется в том же блоке.

Сообщение к считывателю

Длина сообщения: 8 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 43h | 1 |
| 2 | Номер блока. | 2 |
| 3 | Настройка обмена, подпись ответа  1 – включено.  0 – выключено. | 1 |
| 4 | Величина декремента. | 4 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 44h “Авторизация к карте Mifare Plus в режиме SL3”**

Производит авторизация к карте Mifare Plus находящуюся в режиме SL3 по ключу AES128, находящемуся в SAM AV2 модуле.

Сообщение к считывателю

Длина сообщения: 6 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 44h | 1 |
| 2 | Тип авторизации.  FOLLOWING\_AUTH (00h) – повторная авторизация.  FIRST\_AUTH (01h) – первичная авторизация. | 1 |
| 3 | Номер блока. | 2 |
| 4 | Номер ключа в SAM AV2 модуле. | 1 |
| 5 | Версия ключа в SAM AV2 модуле. | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 45h “Запись нескольких блоков данных на карту Mifare Plus”**

Записывает несколько блоков данных на карту Mifare Plus, находящуюся в режиме SL2 или SL3. Ключ авторизации для записываемых блоков должен быть или один или ключи должны совпадать.

Сообщение к считывателю

Длина сообщения: зависит от числа записываемых блоков.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 45h | 1 |
| 2 | Номер блока, начиная с которого производится запись. | 2 |
| 3 | Число записываемых блоков N. Значение должно быть не более 15. Ограничение протокола | 1 |
| 4 | Настройка обмена, шифрование  1 – включено.  0 – выключено. | 1 |
| 5 | Настройка обмена, подпись ответа  1 – включено.  0 – выключено. | 1 |
| 6 | Записываемые данные. Один блок данных содержит 16 байт. | 16\*N |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 46h “Чтение нескольких блоков данных с карту Mifare Plus”**

Читает несколько блоков данных с карты Mifare Plus, находящейся в режиме SL2 или SL3. Ключ авторизации для читаемых блоков должен быть или один или ключи должны совпадать.

Сообщение к считывателю

Длина сообщения: 7.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 46h | 1 |
| 2 | Номер блока, начиная с которого производится чтение. | 2 |
| 3 | Число записываемых блоков N. Значение должно быть не более 15. Здесь ограничение протокола. | 1 |
| 4 | Настройка обмена, шифрование  1 – включено.  0 – выключено. | 1 |
| 5 | Настройка обмена, подпись ответа  1 – включено.  0 – выключено. | 1 |
| 6 | Настройка обмена, подпись команды  1 – включено.  0 – выключено. | 1 |

Ответ от считывателя

Длина сообщения: зависит от числа читаемых блоков.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Считанные данные. Один блок данных содержит 16 байт. | 16\*N |

**Команда 47h “Авторизация к карте Mifare Plus в режиме SL1”**

Производит авторизация к карте Mifare Plus находящуюся в режиме SL1 по ключу AES128, находящемуся в SAM AV2 модуле.

Команда нужна для перевода карты из режима SL1 в режим SL2 или SL3. Требует предварительного перевода карты в режим ISO14443-4 (см. команду 1Ch).

Так же используется для проверки карты на уровне SL1 (протокол ISO14443\_3), используя AES128 ключ (см. описание карты, ключ 0x9004). Позволяет отличить карту Mifare Plus работающую на уровне SL1, от карт Mifare Classic.

Сообщение к считывателю

Длина сообщения: 7 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 47h | 1 |
| 2 | Тип авторизации.  FOLLOWING\_AUTH (00h) – повторная авторизация.  FIRST\_AUTH (01h) – первичная авторизация. | 1 |
| 3 | Протокол  ISO14443\_3 (00h) – для авторизации к карте (не сектору) на уровне SL1.  ISO14443\_4 (01h) – для переключения на следующий уровень. | 1 |
| 4 | Номер блока. | 2 |
| 5 | Номер ключа в SAM AV2 модуле. | 1 |
| 6 | Версия ключа в SAM AV2 модуле. | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 48h “Запись AES128 ключа для карт Mifare Plus в SAM AV2 модуль”**

Записывает ключ авторизации к карте Mifare Plus в SAM AV2 модуль.

**В одной записи можно хранить 3 ключа с разными версиями, в разных позициях.**

Сообщение к считывателю

Длина сообщения: 20 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 48h | 1 |
| 2 | Номер записи (Key Entry) в которую будет записан ключ.  Значение от 0 до 254. | 1 |
| 3 | Позиция ключа. Значение 0 – 2. | 1 |
| 4 | Версия ключа. Значение 0 - 255. | 1 |
| 5 | Ключ AES128. | 16 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 49h “Авторизация к сектору карты Mifare Plus в режиме SL2, ключом AES”**

Производит авторизация к карте Mifare Plus находящуюся в режиме SL2 по ключу AES128, находящемуся в SAM AV2 модуле.

Команда нужна для перевода карты из режима SL2 в режим SL3. Требует предварительного перевода карты в режим ISO14443-4 (см. команду 1Ch).

Так же используется для авторизации к секторам карты находящейся на уровне SL2, ключом AES128. Затем требуется авторизация к сектору ключом Crypto-1, командой 0x4A. При этом ключи AES128 для секторов начинаются по адресам с 0x4000. Cм. приложение 2.

Сообщение к считывателю

Длина сообщения: 7 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 49h | 1 |
| 2 | Тип авторизации.  FOLLOWING\_AUTH (00h) – повторная авторизация.  FIRST\_AUTH (01h) – первичная авторизация. | 1 |
| 3 | Протокол  ISO14443\_3 (00h) – для авторизации к карте (к сектору) на уровне SL2.  ISO14443\_4 (01h) – для переключения на следующий уровень. | 1 |
| 4 | Номер блока. | 2 |
| 5 | Номер ключа в SAM AV2 модуле. | 1 |
| 6 | Версия ключа в SAM AV2 модуле. | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 4Ah “Авторизация к сектору карты Mifare Plus в режиме SL2, ключом Crypto-1”**

Производит авторизация к сектору карты Mifare Plus, находящуюся в режиме SL2 по ключу Crypto-1. Предварительно требует авторизацию ключом AES128 по команде 0x49.

Сообщение к считывателю

Длина сообщения: 10, 13, 16 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 4Ah | 1 |
| 2 | Номер блока | 1 |
| 3 | Тип ключа.  Для ключа A значение 60h.  Для ключа B значение 61h. | 1 |
| 4 | Номер ключа в SAM AV2 модуле. | 1 |
| 5 | Версия ключа в SAM AV2 модуле. | 1 |
| 6 | Длина UID карты (4, 7 или 10). | 1 |
| 7 | UID карты | 4, 7, 10 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 4Bh “Запись нескольких блоков данных на карту Mifare Plus”**

Записывает несколько блоков данных на карту Mifare Plus, находящуюся в режиме SL2. Ключ авторизации для записываемых блоков должен быть или один или ключи должны совпадать.

Сообщение к считывателю

Длина сообщения: зависит от числа записываемых блоков.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 4Bh | 1 |
| 2 | Номер блока, начиная с которого производится запись. | 1 |
| 3 | Число записываемых блоков N. Значение должно быть не более 3. Ограничение карты. | 1 |
| 4 | Записываемые данные. Один блок данных содержит 16 байт. | 16\*N |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 4Ch “Чтение нескольких блоков данных с карты Mifare Plus”**

Читает несколько блоков данных с карты Mifare Plus, находящейся в режиме SL2. Ключ авторизации для читаемых блоков должен быть или один или ключи должны совпадать.

Сообщение к считывателю

Длина сообщения: 3.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 4Ch | 1 |
| 2 | Номер блока, начиная с которого производится чтение. | 1 |
| 3 | Число читаемых блоков N. Значение должно быть не более 3. Ограничение карты. | 1 |

Ответ от считывателя

Длина сообщения: зависит от числа читаемых блоков.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Считанные данные. Один блок данных содержит 16 байт. | 16\*N |

**Команда C0h “Генерация пары RSA ключей”**

Выполняет генерацию RSA ключа (пары) с его сохранением в SAM AV2 модуле.

Всего в SAM AV2 модуле есть 3 ключевых записи для RSA ключей. Эти ключи хранятся отдельно от симметричных ключей.

Каждый ключ может иметь модуль от 256 бит (32 байта) до 2048 бит (256 байт) и с экспонентой от 32 бит (4 байта) до 2048 бит (256 байт). Для модуля размер кратен 64 битам (8 байт), для экспоненты 32 битам (4 байта). Модуль должен быть больше или равен экспоненте.

Ключевая запись с номером 2 может хранить только открытый ключ и не может использоваться при генерации пары ключей.

Ключи после генерации могут быть получены командами экспорта.

Формат хранения ключей в SAM AV2 модуле приведён в Приложении 5.

Сообщение к считывателю

Длина сообщения: 11.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: C0h | 1 |
| 2 | Номер ключевой записи: [0:1] | 1 |
| 3 | Конфигурационные биты:  0 – наличие приватного ключа: 0 нет приватного ключа (не будет сгенерирован), но будет публичный; 1 есть.  1 – разрешение экспорта приватного ключа: 0 запрещён, 1 разрешён.  2 – запретить ключ: 0 запись разрешена, 1 запись запрещена.  3 – запрет использования ключа для шифрования и дешифрования: 0 разрешено, 1 –запрещено.  4 – запрет на использование ключа при работе с ЭЦП: 0 разрешено, 1 запрещено.  5 – разрешение использовать ключ для обновления ключей работы с картами. 0 запрещено, 1 разрешено.  6 – использовать CRT представление при хранении ключа: всегда 1.  7 – 15 – неиспользуемые биты, всегда 0. | 2 |
| 4 | Номер ключа (симметричного) авторизация по которому требуется для изменения этого ключа. Значение по умолчанию 0. | 1 |
| 5 | Версия ключа (симметричного) авторизация по которому требуется для изменения этого ключа. Значение по умолчанию 0. | 1 |
| 6 | Счётчик использования ключа. По умолчании 0xFF – без ограничений. | 1 |
| 7 | Модуль | 2 |
| 8 | Экспонента | 2 |

Ответ от считывателя

Длина сообщения: 1.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда C1h “Экспорт приватного RSA ключа”**

Выполняет экспорт приватной части RSA ключа (пары).

Приватная часть сохраняется в памяти считывателя (буфер) и затем может быть оттуда считана.

Реализация вызвана ограничением протокола считывателя: максимальная длина сообщения 255 байт.

Формат экспортируемого ключа приведён в Приложении 6.

Сообщение к считывателю

Длина сообщения: 2.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: C1h | 1 |
| 2 | Номер ключевой записи: [0:1] | 1 |

Ответ от считывателя

Длина сообщения: 5.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Объём данных полученных от SAM AV2 модуля и сохранённых в памяти считывателя. | 2 |
| 3 | Размер блоков буфера. Т.е. максимальный размер блока, который может быть считан за один раз. | 1 |
| 4 | Число блоков буфера. | 1 |

**Команда C2h “Экспорт публичного RSA ключа”**

Выполняет экспорт публичной части RSA ключа (пары).

Приватная часть сохраняется в памяти считывателя (буфер) и затем может быть оттуда считана.

Реализация вызвана ограничением протокола считывателя: максимальная длина сообщения 255 байт.

Формат экспортируемого ключа приведён в Приложении 7.

Сообщение к считывателю

Длина сообщения: 2.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: C2h | 1 |
| 2 | Номер ключевой записи: [0:2] | 1 |

Ответ от считывателя

Длина сообщения: 5.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Объём данных полученных от SAM AV2 модуля и сохранённых в памяти считывателя. | 2 |
| 3 | Размер блоков буфера. Т.е. максимальный размер блока, который может быть считан за один раз. | 1 |
| 4 | Число блоков буфера. | 1 |

**Команда C3h “Чтение буфера считывателя”**

Выполняет чтение буфера считывателя.

Сообщение к считывателю

Длина сообщения: 3.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: C3h | 1 |
| 2 | Адрес читаемого блока | 1 |
| 3 | Число N читаемых из блока байт. При значении 0, может быть использована для получения параметров буфера | 1 |

Ответ от считывателя

Длина сообщения: зависит от параметров.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Число N считанных байт | 2 |
| 3 | Размер блоков буфера. Т.е. максимальный размер блока, который может быть считан за один раз. | 1 |
| 4 | Число блоков буфера. | 1 |
| 5 | Считанные данные | N |

**Команда C4h “Запись буфера считывателя”**

Выполняет запись буфера считывателя.

Сообщение к считывателю

Длина сообщения: зависит от параметров.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: C4h | 1 |
| 2 | Адрес записываемого блока | 1 |
| 3 | Число N записываемых байт. При значении 0, может быть использована для получения параметров буфера | 1 |
| 4 | Записываемые данные | N |

Ответ от считывателя

Длина сообщения: 5.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Число N записанных байт | 2 |
| 3 | Размер блоков буфера. Т.е. максимальный размер блока, который может быть считан за один раз. | 1 |
| 4 | Число блоков буфера. | 1 |

**Команда C5h “Вычисление цифровой подписи”**

Выполняет вычисление цифровой подписи с использованием приватного RSA ключа.

Сообщение к считывателю

Длина сообщения: 23, 31, 35.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: C5h | 1 |
| 2 | Используемый алгоритм вычисления хеш.  0 – SHA1  1 – SHA2-224  3 – SHA2-256 | 1 |
| 3 | Номер используемого ключа: [0, 1] | 1 |
| 4 | Значение хеш.  Длина 20 байт для SHA1, 28 для SHA2-224, 32 для SHA2-256 | 20, 28, 32 |

Ответ от считывателя

Длина сообщения: 1.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда C6h “Получить вычисленную цифровую подпись”**

Считывает из вычисленную (0xC5) цифровую подпись из SAM AV2 модуля в память считывателя.

Сообщение к считывателю

Длина сообщения: 1

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: C6h | 1 |

Ответ от считывателя

Длина сообщения: 5.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Объём данных полученных от SAM AV2 модуля и сохранённых в памяти считывателя. Т.е. размер полученной подписи. Равен длине ключа | 2 |
| 3 | Размер блоков буфера. Т.е. максимальный размер блока, который может быть считан за один раз. | 1 |
| 4 | Число блоков буфера. | 1 |

**Команда C7h “Проверка цифровой подписи”**

Проверяет цифровую подпись.

Проверяемая подпись должна быть записана в буфер считывателя.

Формат импортируемого ключа приведён в Приложении 8.

Сообщение к считывателю

Длина сообщения: зависит от параметров команды

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: C7h | 1 |
| 2 | Номер используемого ключа: [0, 2] | 1 |
| 3 | Используемый алгоритм вычисления хеш.  0 – SHA1  1 – SHA2-224  3 – SHA2-256 | 1 |
| 4 | Число N байт передаваемого хеша: 20, 28, 32 | 1 |
| 5 | Число байт передаваемой на проверку подписи | 2 |
| 6 | Передаваемый хеш | N |

Ответ от считывателя

Длина сообщения: 1.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда C8h “Импорт RSA ключа”**

Производит запись RSA ключа в SAM AV2 модуль или обновление его параметров.

Сообщение к считывателю

Длина сообщения: 3

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: C8h | 1 |
| 2 | Номер используемого ключа: [0, 2] | 1 |
| 3 | Опции импорта.  При значении 0 происходим импорт ключа, при значении 1 происходит обновление настроек ключа | 1 |

Ответ от считывателя

Длина сообщения: 1.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда С9h “Шифрование данных, используя Offline Crypto”**

Производит шифрование данных активированным ключом (команда 0xDC). Объём данных ограничен размером буфера считывателя.

Данные должны быть предварительно записаны в буфер.

Сообщение к считывателю

Длина сообщения: 3

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: C9h | 1 |
| 2 | Размер шифруемых данных | 2 |

Ответ от считывателя

Длина сообщения: 5.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Размер зашифрованных данных | 2 |
| 3 | Размер блоков буфера. Т.е. максимальный размер блока, который может быть считан за один раз. | 1 |
| 4 | Число блоков буфера. | 1 |

**Команда СAh “Дешифрование данных, используя Offline Crypto”**

Производит дешифрование данных активированным ключом (команда 0xDC). Объём данных ограничен размером буфера считывателя.

Данные должны быть предварительно записаны в буфер.

Сообщение к считывателю

Длина сообщения: 3

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: CAh | 1 |
| 2 | Размер шифруемых данных | 2 |

Ответ от считывателя

Длина сообщения: 5.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Размер дешифрованных данных | 2 |
| 3 | Размер блоков буфера. Т.е. максимальный размер блока, который может быть считан за один раз. | 1 |
| 4 | Число блоков буфера. | 1 |

**Команда CBh “Вычисление хэш для данных в буфере”**

Вычисляет хеш для данных находящихся в буфере считывателя.

Сообщение к считывателю

Длина сообщения: 4

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: CBh | 1 |
| 2 | Алгоритм вычисления хеш:  0 – SHA1  1 – SHA2-224  3 – SHA2-256 | 1 |
| 3 | Размер данных | 2 |

Ответ от считывателя

Длина сообщения: 21, 29, 33.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Хеш. 20 байт для SHA1, 28 байт для SHA2-224, 32 байт для SHA2-256 | 20, 28, 32 |

**Команда CCh “Активация Offline Crypto ключа”**

Производит активацию ключа, который будет использован для Offline Crypto. Ключ должен быть предварительно записан командой DBh.

Команда аналог команды DCh, но добавлен параметр диверсификации.

Сообщение к считывателю

Длина сообщения: 4 + N байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: CCh | 1 |
| 2 | Номер записи (Key Entry) в которую записан ключ.  Значение от 0 до 254. | 1 |
| 3 | Версия ключа. Значение 0 - 255. | 1 |
| 4 | Длина данных для диверсификации ключа N | 1 |
| 5 | Данные для диверсификации ключа | N |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда СDh “Вычисление MAC, используя Offline Crypto”**

Производит вычисление подписи MAC активированным ключом (команда 0xDC). Данные должны быть предварительно записаны в буфер.

Сообщение к считывателю

Длина сообщения: 3

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: CDh | 1 |
| 2 | Длина (усечение) вычисленной подписи MAC | 1 |
| 3 | Размер данных в буфере | 1 |

Ответ от считывателя

Длина сообщения: 2 + N.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Размер вычисленного MAC N | 1 |
| 3 | Подпись MAC | N |

**Команда СEh “Верификация MAC, используя Offline Crypto”**

Производит проверку подписи MAC активированным ключом (команда 0xDC).

Данные должны быть предварительно записаны в буфер.

Команде надо передать данные, для которых вычислена подпись MAC и саму подпись MAC. В итоге поле 3 должно содержать N байт данных и M байт подписи.

Сообщение к считывателю

Длина сообщения: 3

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: CEh | 1 |
| 2 | Длина подписи MAC M | 1 |
| 3 | Размер данных в буфере N + M.  Сначала идут байты данных, затем байты подписи | 1 |

Ответ от считывателя

Длина сообщения: 1.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда D0h “Чтение страниц с карты My-D Move”**

Считывает данные с карты My-D Move компании Infineon.

Сообщение к считывателю

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: D0h | 1 |
| 2 | Номер читаемой страницы | 1 |

Ответ от считывателя

Длина сообщения: 17 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | 16 байт считанных данных. 4 первых байта для заданной страницы.  12 байт со следующих 3-х страниц. | 16 |

**Команда D1h “Чтение двух страниц с карты My-D Move”**

Считывает данные с карты My-D Move компании Infineon.

Сообщение к считывателю

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: D1h | 1 |
| 2 | Номер читаемой страницы | 1 |

Ответ от считывателя

Длина сообщения: 9 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | 8 байт считанных данных. 4 первых байта для заданной страницы.  4 байта со следующей страницы. | 8 |

**Команда D2h “Запись страницы на карту My-D Move”**

Записывает данные на карту My-D Move.

Сообщение к считывателю

Длина сообщения: 6 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: D2h | 1 |
| 2 | Номер записываемой страницы | 1 |
| 3 | Записываемые данные | 4 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда D3h “Запись двух страниц на карту My-D Move”**

Записывает данные на карту My-D Move.

Сообщение к считывателю

Длина сообщения: 10 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: D3h | 1 |
| 2 | Номер записываемой страницы | 1 |
| 3 | Записываемые данные | 8 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда D4h “Запись страницы на карту My-D Move в режиме совместимости”**

Записывает данные на карту My-D Move в режиме совместимости с Mifare Classic.

Сообщение к считывателю

Длина сообщения: 18 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: D4h | 1 |
| 2 | Номер записываемой страницы | 1 |
| 3 | Записываемые данные. 4 первых байта должны содержать записываемые данные. 12 следующих байт игнорируются, в них рекомендуется записывать 0. | 16 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда D5h “Запись пароля на карту My-D Move”**

Записывает 4-х байтный пароль на карту My-D Move.

Сообщение к считывателю

Длина сообщения: 5 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: D5h | 1 |
| 2 | Записываемый пароль | 4 |

Ответ от считывателя

Длина сообщения: 5 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Записанный пароль | 4 |

**Команда D6h “Авторизация по паролю к карте My-D Move”**

Производит авторизацию к карте My-D Move.

Сообщение к считывателю

Длина сообщения: 5 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: D6h | 1 |
| 2 | Пароль | 4 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда D7h “Декремент счётчика карты My-D Move”**

Производит декремент счётчика на карте My-D Move.

Сообщение к считывателю

Длина сообщения: 3 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: D7h | 1 |
| 2 | Значение декремента | 2 |

Ответ от считывателя

Длина сообщения: 3 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Значение счётчика после выполнения декремента | 2 |

**Команда D8h “Вычисление хэш функции SHA256”**

Производит вычисление hash значения для переданных данных.

Сообщение к считывателю

Длина сообщения: 3 - 255 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: D8h | 1 |
| 2 | Данные | 0 - 252 |
| 3 | CRC16 | 2 |

Ответ от считывателя

Длина сообщения: 33 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Вычисленное значение hash | 32 |

**Команда D9h “Вычисление хэш функции SHA224”**

Производит вычисление hash значения для переданных данных.

Сообщение к считывателю

Длина сообщения: 3 - 255 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: D9h | 1 |
| 2 | Данные | 0 - 252 |
| 3 | CRC16 | 2 |

Ответ от считывателя

Длина сообщения: 29 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Вычисленное значение hash | 28 |

**Команда DAh “Вычисление хэш функции SHA-1”**

Производит вычисление hash значения для переданных данных.

Сообщение к считывателю

Длина сообщения: 3 - 255 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: DAh | 1 |
| 2 | Данные | 0 - 252 |
| 3 | CRC16 | 2 |

Ответ от считывателя

Длина сообщения: 21 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Вычисленное значение hash | 20 |

**Команда DBh “Запись ключа для Offline Crypto в SAM AV2 модуль”**

Записывает ключ Offline Crypto в SAM AV2 модуль.

**В одной записи можно хранить 2/3 ключа с разными версиями, в разных позициях.**

Сообщение к считывателю

Длина сообщения: 21/29 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: DBh | 1 |
| 2 | Тип ключа:  0 – AES128,  1 – AES192,  2 – 2K3DES,  3 – 3K3DES | 1 |
| 3 | Номер записи (Key Entry) в которую будет записан ключ.  Значение от 0 до 254. | 1 |
| 4 | Позиция ключа.  Значение 0 – 2 для AES128 и 2K3DES.  Значение 0 – 1 для AES192 и 3K3DES. | 1 |
| 5 | Версия ключа. Значение 0 - 255. | 1 |
| 6 | Ключ:  AES128 – 16 байт,  AES192 – 24 байт,  2K3DES – 16 байт,  3K3DES – 24 байт | 16/24 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда DCh “Активация Offline Crypto ключа”**

Производит активацию ключа, который будет использован для Offline Crypto. Ключ должен быть предварительно записан командой DBh.

Сообщение к считывателю

Длина сообщения: 3 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: DCh | 1 |
| 2 | Номер записи (Key Entry) в которую записан ключ.  Значение от 0 до 254. | 1 |
| 3 | Версия ключа. Значение 0 - 255. | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда DDh “Шифрование данных, используя Offline Crypto”**

Производит шифрование данных активированным ключом.

Сообщение к считывателю

Длина сообщения: зависит от данных.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: DDh | 1 |
| 2 | Данные (размер должен быть кратен 16 байтам) | до 240 |

Ответ от считывателя

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Размер данных | 1 |
| 3 | Зашифрованные данные | до 240 |

**Команда DEh “Дешифрование данных, используя Offline Crypto”**

Производит дешифрование данных активированным ключом.

Сообщение к считывателю

Длина сообщения: зависит от данных.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: DEh | 1 |
| 2 | Данные (размер должен быть кратен 16 байтам) | до 240 |

Ответ от считывателя

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Размер данных | 1 |
| 3 | Дешифрованные данные | до 240 |

**Команда DFh “Деактивация авторизации к SAM AV2 модулю”**

Деактивирует авторизацию считывателя к SAM AV2 модулю.

После этой команды считыватель не может работать с SAM AV2 модулем. Требуется сброс для повторной авторизации. Команда может быть использована в целях безопасности, при вскрытии изделия.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: DFh | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда F0h “Управление светодиодами и чтение состояния кнопки”**

Управление светодиодами, установленными в считывателе и чтение состояния кнопки.

См. конкретную реализацию аппаратной части считывателя. От неё зависит число светодиодов и наличие кнопки.

Сообщение к считывателю

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: F0h | 1 |
| 2 | Биты управления светодиодами.  Значения битов: 1 – зажечь, 0 – погасить.  Бит 0 – синий, бит 1 – красны, бит 2 – зелёный, бит 3 – жёлтый. | 1 |

Ответ от считывателя

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 1 | Состояние кнопки.  0 –не была нажата.  > 0 – была нажата.  Состояние сбрасывается после выполнения команды.  Всегда 0, если кнопка не установлена в считывателе. | 1 |

**Команда F1h “Переход в режим программирования”**

Передача управления Bootloader-у.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: F1h | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда F2h “Управление светодиодами”**

Управление светодиодами, установленными в считывателе.

См. конкретную реализацию аппаратной части считывателя. От неё зависит число светодиодов.

Сообщение к считывателю

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: F2h | 1 |
| 2 | Биты управления светодиодами.  Значения битов: 1 – зажечь, 0 – погасить.  Бит 0 – синий, бит 1 – красны, бит 2 – зелёный, бит 3 – жёлтый. | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда F3h “Чтение состояния кнопки”**

Чтение состояния кнопки.

См. конкретную реализацию аппаратной части считывателя. От неё зависит наличие кнопки.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: F3h | 1 |

Ответ от считывателя

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Состояние кнопки.  0 –не была нажата.  > 0 – была нажата.  Состояние сбрасывается после выполнения команды.  Всегда 0, если кнопка не установлена в считывателе. | 1 |

**Команда F4h “Включение режима ответа с кодом команды”**

Включает режим работы при котором в ответ от считывателя добавляется код команды.

Код команды добавляется после кода ошибки. Длина ответа при этом увеличивается на 1.

Режим сбрасывается после сброса считывателя.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: F4h | 1 |

Ответ от считывателя

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Код команды F4h. | 1 |

**Команда F5h “Установить скорость обмена”**

Устанавливает скорость обмена с ведущим устройством, используемая считывателем.

Установленное значение сохраняется в энергонезависимой памяти.

Сообщение к считывателю

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: F5h | 1 |
| 2 | Скорость обмена.  0 – 2400 бод.  1 – 4800 бод.  2 – 9600 бод.  3 – 14400 бод.  4 – 19200 бод.  5 – 28800 бод.  6 – 38400 бод.  7 – 57600 бод. **Значение по умолчанию.**  8 – 115200 бод. | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда F6h “Чтение настроек считывателя”**

Чтение настроек считывателя из энергонезависимой памяти.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: F6h | 1 |

Ответ от считывателя

Длина сообщения: 9 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Скорость обмена, см. команду 0xF5 | 1 |
| 3 | Параметр REG\_RFCFG | 1 |
| 4 | Параметр REG\_RXSEL | 1 |
| 5 | Параметр REG\_MODE | 1 |
| 6 | Параметр REG\_GSN | 1 |
| 7 | Параметр REG\_CWGSP | 1 |
| 8 | Параметр REG\_MODGSP | 1 |
| 9 | Зарезервировано | 1 |

**Команда F7h “Запись настроек считывателя”**

Запись настроек считывателя в энергонезависимую память.

Команда позволяет записать скорость обмена и параметры приёмо-передатчика считывателя (глубину модуляции, амплитуду сигнала).

Сообщение к считывателю

Длина сообщения: 9 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: F7h | 1 |
| 2 | Скорость обмена, см. команду 0xF5 | 1 |
| 3 | Параметр REG\_RFCFG | 1 |
| 4 | Параметр REG\_RXSEL | 1 |
| 5 | Параметр REG\_MODE | 1 |
| 6 | Параметр REG\_GSN | 1 |
| 7 | Параметр REG\_CWGSP | 1 |
| 8 | Параметр REG\_MODGSP | 1 |
| 9 | Зарезервировано | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда F8h “Запрос расширенного кода ошибки”**

Команда служит для получения расширенного кода ошибки последней ошибочно выполненной команды.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: F8h | 1 |

Ответ от считывателя

Длина сообщения: 3 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Старший байт кода ошибки | 1 |
| 3 | Младший байт кода ошибки | 1 |
| 4 | Код ошибки возникшей при старте ридера  0x00 Нет ошибки  0x01 Не отвечает TDA8026  0x02 Не SAM модулей  0x03Не отвечает приёмопередатчик PN512  0x04 Ошибка авторизации к SAM модулю  0x05 Не отвечает SAM модуль  0x06 Не отвечает моторизованный считыватель  0x09 Перегрузка по питания SAM AV2 модуля (модулей). КЗ.  0x0A Слишком низкое питание SAM AV2 модуля. |  |

**Команда F9h “Запись ключа авторизации к SAM AV2 модулю в память считывателя”**

Команда служит для записи ключа AES128 в память считывателя. После перезагрузки считывателя он будет авторизоваться к SAM AV2 модулю этим ключём.

Для записи ключа в SAM AV2 модуль служит команда 0x34h.

Сообщение к считывателю

Длина сообщения: 20 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: F9h | 1 |
| 2 | Параметр, указывающий на использование ключа.  0 – ключ не используется для авторизации при включении считывателя  Больше 0 - ключ используется для авторизации при включении считывателя | 1 |
| 3 | Ключ авторизации AES128 | 16 |
| 4 | CRC полей 2 и 3. Используется CCITT-CRC16.  Полином X^16 + X^12 + X^5 + 1. Начальное значение 0000h.  См. Приложение 1. | 2 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда FAh “Запись UID считывателя в память”**

Запись 16-ти байтного UID в память считывателя. Не путать с серийным номером считывателя.

Сообщение к считывателю

Длина сообщения: 19 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: FAh | 1 |
| 2 | UID считывателя | 16 |
| 3 | CRC поля 2. Используется CCITT-CRC16.  Полином X^16 + X^12 + X^5 + 1. Начальное значение 0000h.  См. Приложение 1. | 2 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда FBh “Чтение UID считывателя из памяти”**

Чтение 16-ти байтного UID из памяти считывателя. Не путать с серийным номером считывателя.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: FBh | 1 |

Ответ от считывателя

Длина сообщения: 9 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | UID | 16 |

**Команда FCh “Ротация светодиодов”**

Управление режимом работы светодиодов считывателя.

Включает или выключает “ротацию” светодиодов: красный-зелёный, синий-жёлтый.

Нужно для плат SME10158\_387\_01 и SME10158\_384\_01.

Сообщение к считывателю

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: FCh | 1 |
| 2 | Режим:  0 – выключено  1 - включено | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда FFh “Снижение энергопотребления ”**

Выключает радиополе считывателя и светодиоды.

Для включения радиополя необходимо подать команду 02h.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: FFh | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

Команды протокола для работы с 3K5

В данном разделе перечислены команды работы считывателя с моторизованным считывателем 3K5.

**Команда E0h “Разрешение/запрет приёма карт”**

Команда разрешения или запрета приёма карт.

После разрешения приёма карт, моторизованный считыватель переходит в режим при котором самостоятельно принимает карты.

Сообщение к считывателю

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: E0h | 1 |
| 2 | Параметр команды.  0x30 – разрешить приём карт.  0x31 – запретить приём карт. | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки  0x00 – нет ошибок.  MI\_WRONG\_PARAMETER\_VALUE (-60) – ошибка в парметрах команды  0xFF – моторизованный считыватель занят предыдущей командой | 1 |

**Команда E1h “Запросить статус считывателя”**

Команда запроса статус считывателя. Используется для определения наличия карты в считывателе.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: E1h | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки  0x00 – нет ошибок.  0xFF – моторизованный считыватель занят предыдущей командой | 1 |

**Команда E2h “Выдать карту”**

Команда выдачи карты клиенту.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: E2h | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки  0x00 – нет ошибок.  0xFF – моторизованный считыватель занят предыдущей командой | 1 |

**Команда E3h “Захватить карту”**

Команда захвата карты.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: E3h | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки  0x00 – нет ошибок.  0xFF – моторизованный считыватель занят предыдущей командой | 1 |

**Команда E4h “Получить ответ на последнюю поданную команду”**

Команда возвращает ответ от считывателя на последнюю поданную команду.

Сообщение к считывателю

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: E4h | 1 |

Ответ от считывателя

Длина сообщения: 2 + N байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки  Всегда 0x00 | 1 |
| 2 | Код ответа считывателя   1. ACK 2. NAK 3. STX - данные 4. STX – данные, но ошибка CRCC 5. DLE 6. EOT 7. таймаут закончился, но считыватель не ответил | 1 |
| 3 | Данные от считывателя. Актуально при коде ответа равном 3. | N |

**Команда E5h “Управление светодиодом”**

Команда управления светодиодом.

Сообщение к считывателю

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: E0h | 1 |
| 2 | Параметр команды.  0x30 – погасить.  0x31 – зажечь зелёный.  0x32 – зажечь красный.  0x33 – зажечь желтый. | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки  0x00 – нет ошибок.  MI\_WRONG\_PARAMETER\_VALUE (-60) – ошибка в парметрах команды  0xFF – моторизованный считыватель занят предыдущей командой | 1 |

Команды протокола для работы считывателя в турникете

Команды действительны только для прошивки считывателя турникета.

Операции чтения и записи атомарные, т.е. не разделяемы. Содержат в себе авторизацию к карте и чтение/запись.

**Команда 09h “Активация карты в режиме остановки”**

Активация карты PICC находящейся в режиме остановки.

Происходит запрос, получение номера и выбор карты находящейся в режиме ожидания. При этом если перед командой карта уже была выбрана, она будет предварительно остановлена.

Сообщение к считывателю

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 09h | 1 |
| 2 | Зарезервировано. Всегда 0. | 1 |

Ответ от считывателя

Длина сообщения: 9, 12, 14 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Ответ карты Answer to Request Type A (AtqA).  Описание AtqA см. в ISO/IEC 14443-3. | 2 |
| 3 | Select Acknowledge (SAK). Ответ карты на выбор.  Описание SAK см. в ISO/IEC 14443-3. | 1 |
| 4 | Длина номера карты. 4 байта UID для “Single Size UID PICC”, 7 байт UID для “Double Size UID PICC”, 10 байта UID для “Triple Size UID PICC” | 1 |
| 5 | PICC UID – уникальный номер карты. | 4, 7, 10 |

**Команда 0Dh “Чтение блока/блоков карты”**

Считывает 16 байт блока или блоков данных с карты.

Сообщение к считывателю

Длина сообщения: 7 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 0Dh | 1 |
| 2 | Номер читаемого блока. | 1 |
| 3 | Необходимость авторизации (0 – не нужна, 1 – нужна авторизация Crypto-1, нужна авторизация 3DES).  Авторизация не нужна для карт Ultralight. | 1 |
| 4 | Номер записи (Key Entry) с ключом, используемым для авторизации и хранящегося на SAM AV2 модуле. Значение от 0 до 254. | 1 |
| 5 | Версия используемого ключа. | 1 |
| 6 | Тип ключа.  Для ключа A значение 60h.  Для ключа B значение 61h. | 1 |
| 7 | Число читаемых блоков N. Значение от 0 до 4. 0 и 1 эквивалентны и приводят к чтению одного блока. |  |

Ответ от считывателя

Длина сообщения: 1 + 16\*N байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Данные считанные из заданного блока | 16\*N |

**Команда 0Eh “Запись блока карты”**

Записывает 16 байт данных в заданный блок с карты.

Сообщение к считывателю

Длина сообщения: 7 + 16\*N байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 0Eh | 1 |
| 2 | Номер записываемого блока. | 1 |
| 3 | Необходимость авторизации (0 – не нужна, 1 – нужна авторизация Crypto-1, нужна авторизация 3DES).  Авторизация не нужна для карт Ultralight. | 1 |
| 4 | Номер записи (Key Entry) с ключом, используемым для авторизации и хранящегося на SAM AV2 модуле. Значение от 0 до 254. | 1 |
| 5 | Версия используемого ключа. | 1 |
| 6 | Тип ключа.  Для ключа A значение 60h.  Для ключа B значение 61h. | 1 |
| 7 | Число записываемых блоков N. Значение от 0 до 4. 0 и 1 эквивалентны и приводят к чтению одного блока. | 1 |
| 8 | Записываемые данные. | 16\*N |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 0Fh “Изменение блок значения с сохранением”**

Изменение блок значения (Value блока) с выполнением команды Transfer.

Сообщение к считывателю

Длина сообщения: 12 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 0Fh | 1 |
| 2 | Код операции.  Декремент PICC\_DECREMENT (C0h). Инкрементирует значение данных из блока источника и сохраняет его во временном регистре. Затем данные сохраняются в блоке получателе.  Инкремент PICC\_INCREMENT (0xC1) . Декрементирует значение данных из блока источника и сохраняет его во временном регистре. Затем данные сохраняются в блоке получателе.  Восстановление значения во временном регистре PICC\_RESTORE (C2h). Происходит запись значения в регистр из блока источника. Затем данные сохраняются в блоке получателе.  Сохранение значения в Value блоке PICC\_TRANSFER (0xB0). Записывает значение из временного регистра в Value блоке. | 1 |
| 3 | Номер блока источника. Из него считываются данные перед операцией. | 1 |
| 4 | Номер блока получателя. В него сохраняются данные. | 1 |
| 5 | Необходимость авторизации (0 – не нужна, 1 – нужна авторизация Crypto-1, нужна авторизация 3DES).  Авторизация не нужна для карт Ultralight. | 1 |
| 6 | Номер записи (Key Entry) с ключом, используемым для авторизации и хранящегося на SAM AV2 модуле. Значение от 0 до 254. | 1 |
| 7 | Версия используемого ключа. | 1 |
| 8 | Тип ключа.  Для ключа A значение 60h.  Для ключа B значение 61h. | 1 |
| 9 | Значение. | 4 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 10h “Изменение блок значения”**

Изменение блок значения (Value блока).

Сообщение к считывателю

Длина сообщения: 11 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 10h | 1 |
| 2 | Код операции.  Декремент PICC\_DECREMENT (C0h). Инкрементирует значение данных из блока источника и сохраняет его во временном регистре.  Инкремент PICC\_INCREMENT (0xC1) . Декрементирует значение данных из блока источника и сохраняет его во временном регистре.  Восстановление значения во временном регистре PICC\_RESTORE (C2h). Происходит запись значения в регистр из блока источника. Затем  Сохранение значения в Value блоке PICC\_TRANSFER (0xB0). Записывает значение из временного регистра в Value блоке. | 1 |
| 3 | Номер блока. | 1 |
| 5 | Необходимость авторизации (0 – не нужна, 1 – нужна авторизация Crypto-1, нужна авторизация 3DES).  Авторизация не нужна для карт Ultralight. | 1 |
| 6 | Номер записи (Key Entry) с ключом, используемым для авторизации и хранящегося на SAM AV2 модуле. Значение от 0 до 254. | 1 |
| 7 | Версия используемого ключа. | 1 |
| 8 | Тип ключа.  Для ключа A значение 60h.  Для ключа B значение 61h. | 1 |
| 9 | Значение. | 4 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

**Команда 11h “Чтение блок значения”**

Считывает 4 байта блок значения с карты и его адрес.

Сообщение к считывателю

Длина сообщения: 2 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 11h | 1 |
| 2 | Номер читаемого блока. | 1 |
| 3 | Необходимость авторизации (0 – не нужна, 1 – нужна авторизация Crypto-1, нужна авторизация 3DES).  Авторизация не нужна для карт Ultralight. | 1 |
| 4 | Номер записи (Key Entry) с ключом, используемым для авторизации и хранящегося на SAM AV2 модуле. Значение от 0 до 254. | 1 |
| 5 | Версия используемого ключа. | 1 |
| 6 | Тип ключа.  Для ключа A значение 60h.  Для ключа B значение 61h. | 1 |

Ответ от считывателя

Длина сообщения: 6 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |
| 2 | Данные считанные из заданного блока | 4 |
| 3 | Адрес блока. См. описание Value Block у Mifare | 1 |

**Команда 14h “Запись блок значение”**

Записывает 4 байта блок значения с карты и его адрес.

Сообщение к считывателю

Длина сообщения: 7 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 14h | 1 |
| 2 | Номер записываемого блока. | 1 |
| 3 | Необходимость авторизации (0 – не нужна, 1 – нужна авторизация Crypto-1, нужна авторизация 3DES).  Авторизация не нужна для карт Ultralight. | 1 |
| 4 | Номер записи (Key Entry) с ключом, используемым для авторизации и хранящегося на SAM AV2 модуле. Значение от 0 до 254. | 1 |
| 5 | Версия используемого ключа. | 1 |
| 6 | Тип ключа.  Для ключа A значение 60h.  Для ключа B значение 61h. | 1 |
| 7 | Записываемые данные. | 4 |
| 8 | Адрес блока | 1 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

Команды протокола для эмиссии карт

**Команда 26h “Запись зашифрованных AES128 ключом данных на карты”**

Записывает на карту блок данных, предварительно расшифровав его указанным AES ключом.

Сообщение к считывателю

Длина сообщения: 22 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код команды: 26h | 1 |
| 2 | Протокол, используемый для записи:  0x00 – ISO14443-3 (для карт Mifare Classic)  0x01 – ISO14443-4 (для карт Mifare Plus) | 1 |
| 3 | Номер блока для записи | 2 |
| 4 | Номер записи (Key Entry) с ключом AES для дешифрования блока | 1 |
| 5 | Версия ключа | 1 |
| 6 | Данные | 16 |

Ответ от считывателя

Длина сообщения: 1 байт.

| **№** | **Описание** | **Размер, байт** |
| --- | --- | --- |
| 1 | Код ошибки | 1 |

Приложение 1

Реализация алгоритма вычисление CCITT-CRC16.

uint16\_t crc\_ccitt\_update (uint16\_t crc, uint8\_t data)

{

data ^= (uint8\_t) (crc & 0xff);

data ^= (uint8\_t) (data << 4);

return ((((uint16\_t)data << 8) | ((crc & 0xff00) >> 8))

^ (uint8\_t)(data >> 4)

^ ((uint16\_t)data << 3));

}

uint16\_t CRC16(uint8\_t \*data, uint16\_t sizedata)//Подсчёт CRC

{

uint16\_t i;

uint16\_t crc = 0x0000;//CRC

for(i = 0; i < sizedata; i++)

{

crc = crc\_ccitt\_update(crc, \*(data + i));

}

return crc;

}

Приложение 2

Вычисление адресов AES128 ключей для режимов SL2 и SL3.

/\*\*

\* calculate the coresponding AES key Address

\* Key A even and Key B odd at the Physical AES start address 0x4000U

\*/

#define AES\_SECTOR\_KEYS\_A(sectorNr) (((sectorNr)\*2) + PHYSICAL\_AES\_START\_ADDRESS)

#define AES\_SECTOR\_KEYS\_B(sectorNr) ((((sectorNr)\*2) + 1) + PHYSICAL\_AES\_START\_ADDRESS)

Приложение 3

Ключи AES128 карт Mifare Plus.

/\*\*

\* Block Addresses

\*/

#define CARD\_MASTER\_KEY 0x9000U /\*\*< Card Master Key Address \*/

#define CARD\_CONFIGURATIOM\_KEY 0x9001U /\*\*< Card Configuration Key Address \*/

#define LEVEL\_2\_SWITCH\_KEY 0x9002U /\*\*< Level 2 Switch Key Address \*/

#define LEVEL\_3\_SWITCH\_KEY 0x9003U /\*\*< Level 3 Switch Key Address \*/

#define SL\_1\_CARD\_AUTHENTICATION\_KEY 0x9004U /\*\*< SL1 Card Authentication Key Address \*/

#define SELECT\_VC\_KEY 0xA000U /\*\*< Select VC Key Address \*/

#define PROXIMITY\_CHECK\_KEY 0xA001U /\*\*< Proximity Check Key Address \*/

#define VC\_POLLING\_ENC\_KEY 0xA080U /\*\*< VC Polling ENC Key Address \*/

#define VC\_POLLING\_MAC\_KEY 0xA081U /\*\*< VC Polling MAC Key Address \*/

#define MFP\_CONFIGURATION\_BLOCK 0xB000U /\*\*< MIFARE Plus Configuration block Address \*/

#define INSTALLATION\_IDENTIFIER 0xB001U /\*\*< Installation Identifier Address \*/

#define FIELD\_CONFIGURATION\_BLOCK 0xB003U /\*\*< Field Configuration block Address \*/

#define PHYSICAL\_AES\_START\_ADDRESS 0x4000U /\*\*< physical start address of AES key location Address \*/

Приложение 4

Описание поведения индикации считывателя при включении:

//Всегда: зажглись и погасли 4 светодиода. Если не так то или нет питания, или неисправен/непропаян стабилизатор питания, или неисправен/непоропаян микроконтроллер SMT32F103RCT6

//Всё в порядке: ридер проиграл мелодию (мелодия только когда нет ошибок), не горит светодиодов

//Не отвечает TDA8026 (не пропай на маленькой плате SM11006.07.0x), нет мелодии, загорается синий светодиод

//Нет SAM модулей (не пропай на маленькой плате SM11006.07.0x, нет модулей реально, не исправный модуль), нет мелодии, загорается красный светодиод

//Не отвечает приёмопередатчик PN512 (не пропай), нет мелодии, загораются синий и красный светодиоды

//Ошибка авторизации к SAM модулю (там или записан какой то ключ авторизации, которого нет у ридера или модуль не исправен), нет мелодии, загорается зелёный светодиод

//Не отвечает SAM модуль (в слот установлен не SAM AV2 модуль), нет мелодии, загораются синий и зелёный светодиоды

//Не исправен кварцевый резонатор на 8 МГц (или не пропай), нет мелодии, загорается жёлтый светодиод

Приложение 5

Формат хранения ключей RSA в SAM AV2 модуле.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Длина, байт | Формат | Параметр | Описание |
|  | 1 | unsigned byte | PKI\_KeyNo | Номер записи с ключом |
|  | 2 | bit mask | PKI\_Set | Конфигурационные биты |
| Публичный  ключ | 2 | unsigned byte | PKI\_NLen | Длина ключа в байтах. От 32 до 256 байт, т.е. от 256 до 2048 бит.  Это длина PKI\_N |
| 2 | unsigned byte | PKI\_eLen | Длина публичной экспоненты в байтах. От 4 до 256 байт. Это длина PKI\_e.  Не может быть больше PKI\_N |
| 256 | string | PKI\_N | Модуль RSA (N = p\*q) |
| 256 | string | PKI\_e | Публичная экспонента |
| Приватный  ключ | 248 | string | PKI\_p | Простое число. Длиной PKI\_NLen/2 |
| 248 | string | PKI\_q | Простое число. Длиной PKI\_NLen/2 |
| 248 | string | PKI\_dP | Приватная экспонента dp. Длиной PKI\_NLen/2. CRT представление приватного ключа |
| 248 | string | PKI\_dQ | Приватная экспонента dq. Длиной PKI\_NLen/2. CRT представление приватного ключа |
| 248 | string | PKI\_ipq | Инверсия p-1 mod q. CRT представление приватного ключа |
|  | 1 | unsigned byte | PKI\_KeyNoCEK | Ключ, к которому необходимо авторизоваться перед работой с этой записью.  Значение 0xFE выключает необходимость авторизации |
|  | 1 | unsigned byte | PKI\_KeyVCEK | Версия ключа |
|  | 1 | unsigned byte | PKI\_RefNoCUK | Номер счётчика использования ключа.  Если счётчик не используется пишется значение 0xFF |

Конфигурационные биты:

0 – наличие приватного ключа: 0 нет приватного ключа (не будет сгенерирован), но будет публичный; 1 есть.

1 – разрешение экспорта приватного ключа: 0 запрещён, 1 разрешён.

2 – запретить ключ: 0 запись разрешена, 1 запись запрещена.

3 – запрет использования ключа для шифрования и дешифрования: 0 разрешено, 1 –запрещено.

4 – запрет на использование ключа при работе с ЭЦП: 0 разрешено, 1 запрещено.

5 – разрешение использовать ключ для обновления ключей работы с картами. 0 запрещено, 1 разрешено.

6 – использовать CRT представление при хранении ключа: всегда 1.

7 – 15 – неиспользуемые биты, всегда 0.

Приложение 6

Формат экспортируемого приватного ключа RSA.

|  |  |  |
| --- | --- | --- |
| Параметр | Описание | Размер |
| PKI\_Set | Конфигурационные биты | 2 |
| PKI\_KeyNoCEK | Ключ, к которому необходимо авторизоваться перед работой с этой записью | 1 |
| PKI\_KeyVCEK | Версия ключа | 1 |
| PKI\_RefNoCUK | Номер счётчика использования ключа | 1 |
| PKI\_NLen | Длина ключа в байтах | 2 |
| PKI\_eLen | Длина публичной экспоненты в байтах | 2 |
| PKI\_pLen | Длина простого числа P | 2 |
| PKI\_qLen | Длина простого числа Q | 2 |
| PKI\_N | Модуль RSA (N = p\*q) | PKI\_NLen |
| PKI\_e | Публичная экспонента | PKI\_eLen |
| PKI\_p | Простое число | PKI\_pLen |
| PKI\_q | Простое число | PKI\_qLen |
| PKI\_dP | Приватная экспонента dp | PKI\_pLen |
| PKI\_dQ | Приватная экспонента dq | PKI\_qLen |
| PKI\_ipq | Инверсия p-1 mod q | PKI\_qLen |

Приложение 7

Формат экспортируемого публичного ключа RSA.

|  |  |  |
| --- | --- | --- |
| Параметр | Описание | Размер |
| PKI\_Set | Конфигурационные биты | 2 |
| PKI\_KeyNoCEK | Ключ, к которому необходимо авторизоваться перед работой с этой записью | 1 |
| PKI\_KeyVCEK | Версия ключа | 1 |
| PKI\_RefNoCUK | Номер счётчика использования ключа | 1 |
| PKI\_NLen | Длина ключа в байтах | 2 |
| PKI\_eLen | Длина публичной экспоненты в байтах | 2 |
| PKI\_N | Модуль RSA (N = p\*q) | PKI\_NLen |
| PKI\_e | Публичная экспонента | PKI\_eLen |

Приложение 8

Формат импортируемого RSA ключа.

|  |  |  |
| --- | --- | --- |
| Параметр | Описание | Размер |
| PKI\_Set | Конфигурационные биты | 2 |
| PKI\_KeyNoCEK | Ключ, к которому необходимо авторизоваться перед работой с этой записью | 1 |
| PKI\_KeyVCEK | Версия ключа | 1 |
| PKI\_RefNoCUK | Номер счётчика использования ключа | 1 |
| PKI\_NLen | Длина ключа в байтах. Значение от 32 до 256 байт.  Имеет значение 0 при обновлении настроек ключа. | 2 |
| PKI\_eLen | Длина публичной экспоненты в байтах. Значение от 4 до 256 байт. Не должно быть больше PKI\_NLen.  Имеет значение 0 при обновлении настроек ключа. | 2 |
| PKI\_pLen | Длина простого числа P. Значение от 6 до 252 байт.  Поле отсутствует при обновлении настроек ключа или при импорте публичного ключа. Присутствует только при импорте приватного ключа | 2 |
| PKI\_qLen | Длина простого числа Q. Значение от 6 до 252 байт.  Поле отсутствует при обновлении настроек ключа или при импорте публичного ключа. Присутствует только при импорте приватного ключа | 2 |
| PKI\_N | Модуль RSA (N = p\*q).  Поле отсутствует при обновлении настроек ключа | PKI\_NLen |
| PKI\_e | Публичная экспонента.  Поле отсутствует при обновлении настроек ключа | PKI\_eLen |
| PKI\_p | Простое число.  Поле отсутствует при обновлении настроек ключа или при импорте публичного ключа. Присутствует только при импорте приватного ключа | PKI\_pLen |
| PKI\_q | Простое число.  Поле отсутствует при обновлении настроек ключа или при импорте публичного ключа. Присутствует только при импорте приватного ключа | PKI\_qLen |
| PKI\_dP | Приватная экспонента dp.  Присутствует только при импорте приватного ключа | PKI\_pLen |
| PKI\_dQ | Приватная экспонента dq.  Присутствует только при импорте приватного ключа | PKI\_qLen |
| PKI\_ipq | Инверсия p-1 mod q.  Присутствует только при импорте приватного ключа | PKI\_qLen |

История версий прошивки и протокола

1.56 – добавлена команда 0xF8.

1.58 – добавлен байт кода ошибки (ошибки старта) в команде 0xF8.

1.58 for 3K5 – добавлены команды работы с моторизованным считывателем Sankyo 3K5.

1.59 – добавлены команды работы с My-D Move.

1.60 – изменены команды записи, чтения, инкремента, декремента, пересылки для Mifare Plus. Добавлены параметры шифрования данных и подписи ответа.

1.61 – 1.65 – латание багов.

1.66 – добавлена команда 0x48 – запись ключа AES128, изменена команда 0x47. Добавлены команды 0x49, 0x4A, 0x4B, 0x4C. Изменение команд 0x3A – 0x43, добавлены параметры шифрования и подписи.

1.67 – изменение в командах 0x3A, 0x3C – добавлен контроль длины сообщения. Исправил описание команд 0x45, 0x46. Исправил команды 0x45, 0x46.

1.69 – добавлены команды для вычисления хэш и для оффлайн криптографии.

1.70 – 1.75 – добавлены команды для генерации, экспорта и импорта RSA ключей.

1.77 – добавлено вычисление хэш для блоков до 2048 байт.

1.78 – исправлена работа с картами с 7-ми байтными UID.

1.80 – изменение адреса старта, для работы с BootLoader.

1.81 – добавлена команда записи UID считывателя.

1.83 – изменения в хранении настроек. Учтено выравнивание структур памяти.

1.84 – 1.86 – добавление команд MIFARE Ultralight EV1.

1.87 – добавление настройки ротации светодиодов, для исправления бага платы антенны.

1.88 – 1.90 – добавление команд работы с KUC и CEK.

1.91 – исправлена ошибка авторизации к картам с 7-и байтным UID и исправлена запись ключей.

1.92 – добавлены команды вычисления MAC.

1.93 – исправлена работа с защитой (авторизацией) SAM AV2 модуля. Теперь выставляются биты запрещающие не только записывать ключи без авторизации, но и использовать их.

1.95 – добавлена диагностика КЗ и Supervisor по питанию SAM AV2 модулей через TDA8026.

1.96 – добавлены команды турникета. Увеличен порог напряжения супервизора микроконтроллера с 2.8 до 2.9 В.

1.97 – реализация списания поездок в турникете с карт Ultralight C.

1.98 – изменение порядка инициализации считывателя.

1.981 – добавление повторных попыток инициализации SAM AV2 модуля. 10 попыток с паузой 200 мс.

1.982 – добавление возможности энергосбережения в прошивку. Выключение поля когда нет карты. Включается директивой условной компиляции.

1.983 – добавлены команды для турникета.