

Протокол RS232 для настольного считывателя PW-Desktop

Ревизия 1.03

Оглавление

Описание устройства	3
Драйвер USB ↔ COM.....	3
Параметры подключения по COM порту	3
Общие информационные команды	4
Информация об устройстве.....	4
Режим работы считывателя (разрешенные типы идентификаторов)	4
Получение текущего режима работы считывателя.....	4
Установка нового режима работы считывателя	4
Получение информации об оставшемся количестве мобильных идентификаторов	4
Чтение кодов идентификаторов	5
Установка тестового формата вывода кодов.....	5
Установка бинарного формата вывода кодов	5
Процедура чтения существующего мобильного идентификатора с помощью ProxWay Desktop	6
Повторное чтение кода идентификатора в поле считывателя	6
Ограничение длины кода	6
Выпуск мобильных идентификаторов.....	7
Локальная выдача идентификаторов.....	7
Выдача идентификаторов по e-mail	7
Дополнительная защита систем доступа (персонификация идентификаторов).....	9
Определение, включен ли режим шифрования идентификаторов ProxWay BLE ID.....	9
Установка режима шифрования мобильных идентификаторов.....	9
Включение режима шифрования и установка пароля шифрования	9
Выключение режима шифрования и очистка пароля.....	10
Установка режима шифрования Mifare®	11
Определение, включен ли режим шифрования идентификаторов Mifare	11
Установка режима шифрования карт Mifare Classic, Mifare Plus в режиме SL1 (алгоритм шифрования Crypto1)	12
Отключение режима шифрования карт Mifare Classic, Mifare Plus в режиме SL1 (алгоритм шифрования Crypto1)	12
Установка режима шифрования карт Mifare Plus в режиме SL3 (алгоритм шифрования AES)	13
Отключение режима шифрования карт Mifare Plus в режиме SL3 (алгоритм шифрования AES)	13
Установка стартового номера персонифицированного идентификатора	14
Выпуск зашифрованной карты.....	15
Очистка зашифрованной карты	16

Описание устройства

Настольный считыватель ASK / FSK / Mifare / Mifare Plus и поддержкой BLE с USB интерфейсом и открытым текстовым протоколом предназначен для максимально простой интеграции в любую систему СКУД.

Может использоваться для выдачи мобильных идентификаторов из выделенного списка мобильных идентификаторов.

Характеристики

RF ID ASK, FSK, ASK+FSK (125 кГц)
Mifare, Mifare Plus SL1, Mifare Plus SL3 (ISO 14443A - 13,56 МГц)
Чтение мобильных идентификаторов PROXWAY BLE ID.
Выдача мобильных идентификаторов PROXWAY BLE ID из выделенного списка мобильных идентификаторов. Переход в режим выдачи PROXWAY BLE ID по мастер-карте.
Обмен данными со смартфонами по Bluetooth Low Energy (Bluetooth Smart, BLE)
Используется зашифрованный 256-битным ключом и стойкий к саботажу протокол для обмена данными со смартфонами
Программирование ProxWay Desktop по BLE со смартфона с Android с помощью ПО ProxWay Config по BLE - устанавливается размерность (битность) идентификаторов, загружаются лицензии на мобильные идентификаторы.

Драйвер USB ↔ COM

Для эмуляции COM порта в системе используется SyLabs CP210x USB to UART мост.

Драйвера можно скачать по следующей ссылке:

<http://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers>

Параметры подключения по COM порту

Скорость – 9600 бод

8 бит информации в пакете

Без бита проверки четности (N)

1 стоп-бит

Внимание!!! Символы <cr><lf> обозначают перевод строки:

<CR> - 0x0D, 13 в десятичной системе, '\r'

<LF> - 0x0A, 10 в десятичной системе, '\n'

Общие информационные команды

Информация об устройстве

С помощью данной команды можно получить информацию об устройстве - его серийном номере и версии микропрограммы

Запрос:

```
i
```

Ответ:

```
MODEL DESKTOP READER<cr><lf>  
SERIAL 00:32:00:00:01:8B<cr><lf>  
VERSION 11.23<cr><lf>  
BLE VER 02.26<cr><lf>
```

Режим работы считывателя (разрешенные типы идентификаторов)

С помощью данной команды можно включить или отключить работу (чтение и запись) с определенными типами идентификаторов. Таблица значений возможных режимов приведена ниже.

Получение текущего режима работы считывателя

Запрос:

```
t<cr><lf>
```

Ответ:

```
TYPE 15<cr><lf>
```

Установка нового режима работы считывателя

Запрос:

```
t12<cr><lf>
```

Ответ:

```
TYPE 12<cr><lf>
```

		BLE ID	Mifare	FSK	ASK
15	1111	+	+	+	+
14	1110	+	+	+	
13	1101	+	+		+
12	1100	+	+		
11	1011	+		+	+
10	1010	+		+	
9	1001	+			+
8	1000	+			
7	0111		+	+	+
6	0110		+	+	
5	0101		+		+
4	0100		+		
3	0011			+	+
2	0010			+	
1	0001				+

Получение информации об оставшемся количестве мобильных идентификаторов

Устройство используется для выдачи мобильных идентификаторов из выделенного списка. Базовая поставка включает 5 бесплатных идентификаторов.

С помощью данной команды можно посмотреть количество неиспользованных лицензий в списке мобильных идентификаторов.

Запрос:

```
q<cr><lf>
```

Ответ:

```
Quantity 274<cr><lf>
```

Чтение кодов идентификаторов

После поднесения идентификатора к считывателю его код будет считан и передан в COM порт автоматически.

Если установлен текстовый режим, то данные о коде карточки будут выводиться следующим образом:

Получение данных:

```
Mifare[E4009A14] 000,39444 1K (0004,08)<cr><lf>
Mifare[04B62AE1BB0280] 182,10977 UL (0044,00)<cr><lf>
Mifare[C2ECA99C] 236,43420 4K (0002,18)<cr><lf>
Mifare[04210D21B21C80] 033,03361 DF (0344,20)<cr><lf>
CryptedMifare[01EB931000] 147,04096 1K (0004,08)<cr><lf>
Em-Marine[565A] 123,16044<cr><lf>
FSK[00120040] 08111<cr><lf>
FSK[0010029A] 38193<cr><lf>
MobileID[1122334455667788]<cr><lf>
```

Внимание!!! В текстовом режиме, при вынесении карты из поля действия считывателя будет выведено:

```
No card<cr><lf>
```

Mifare	– карточки Mifare® стандарта ISO14443a,
CryptedMifare	– персонализированная карта (доп. защищенная) с индивидуальным кодом,
Em-Marine	– карточки с амплитудной модуляцией (ASK),
FSK	– карточки с частотной модуляцией
MobileID	– мобильный идентификатор, полученный от смартфона.

Если установлен бинарный режим, то данные о коде карточки будут выводиться следующим образом:

Получение данных:

```
#4300>3;;>:><cr><lf>
#005=5<92=61<cr><lf>
```

Длина - 12 символов: заголовок, затем 10 символов собственно 5 байт кода, а последний символ – crc8.

Символы в коде соответствуют:

#	– заголовок
0...9	– цифры 0...9
:	– A (hex)
;	– B (hex)
<	– C (hex)
=	– D (hex)
>	– E (hex)
?	– F (hex)

Внимание!!! Обычно бинарный режим используется только в вспомогательной утилите.

Установка тестового формата вывода кодов

Запрос:

```
bt<cr><lf>
```

Ответ:

```
Set Text Prot<cr><lf>
```

Установка бинарного формата вывода кодов

Запрос:

```
bb<cr><lf>
```

Ответ:

```
Set Binary Prot<cr><lf>
```

Процедура чтения существующего мобильного идентификатора с помощью ProxWay Desktop

1. Пользователь подносит смартфон к ProxWay Desktop, и запускает или активирует мобильное приложение PROXWAY ID
2. Настольный считыватель получает код от смартфона
3. Код полученного мобильного идентификатора выводится в COM порт (передается в СКУД и т.д.)

Повторное чтение кода идентификатора в поле считывателя

Используется для проверки наличия карточки в поле считывателя. Если карточка в поле, ее код будет считан и передан в COM порт автоматически, если нет – выведено сообщение об её отсутствии. Например:

Запрос:

```
r
```

Ответ:

```
Em-Marine[7F03] 037,65535<cr><lf>
```

или

```
No card<cr><lf>к
```

Ограничение длины кода

С помощью данной команды можно ограничить длину кода идентификатора до соответствующего формата Wiegand, с заполнением старшей части кода нулями. Например, при установке Wiegand 42 код мобильного идентификатора будет следующим:

```
MobileID[000000D36B2638CD]<cr><lf>
```

Получить текущее значение параметра

Запрос:

```
w<cr><lf>
```

Ответ:

```
Wiegand 3<cr><lf>
```

Установка Wiegand

Запрос:

```
w1<cr><lf>
```

Ответ:

```
Wiegand 1<cr><lf>
```

Интерфейс	Параметр
Wiegand Auto	0
Wiegand 26	1
Wiegand 37	2
Wiegand 42	3
TouchMemory 40	4
RS232	5
Wiegand 34	6
Wiegand 40	7
Wiegand 56	8
Wiegand 58	9
Wiegand 64	10
Wiegand 32	11
RS PRO	12
TouchMemory 26	13

Выпуск мобильных идентификаторов

Устройство используется для выдачи мобильных идентификаторов из выделенного списка. Базовая поставка включает 5 бесплатных идентификаторов.

Локальная выдача идентификаторов

При использовании команд протокола RS232 возможна только локальная выдача идентификаторов.

Процедура локальной выдачи нового идентификатора с помощью ProxWay Desktop

1. Администратор системы переводит настольный считыватель в режим выдачи идентификаторов – размещает на считывателе мастер-карту.
2. Пользователь подносит смартфон к ProxWay Desktop, и в настройках приложения PROXWAY ID нажимает кнопку "Получить от Desktop"- приложение соединяется и получает мобильный идентификатор из выделенного списка мобильных идентификаторов.
3. Код полученного мобильного идентификатора выводится в COM порт (передается в СКУД и т.д.)

После получения мобильного идентификатора его код будет передан в COM порт автоматически.

Получение данных:

```
NewMobileID[5CF0CF54BE81EAD2]<cr><lf>
```

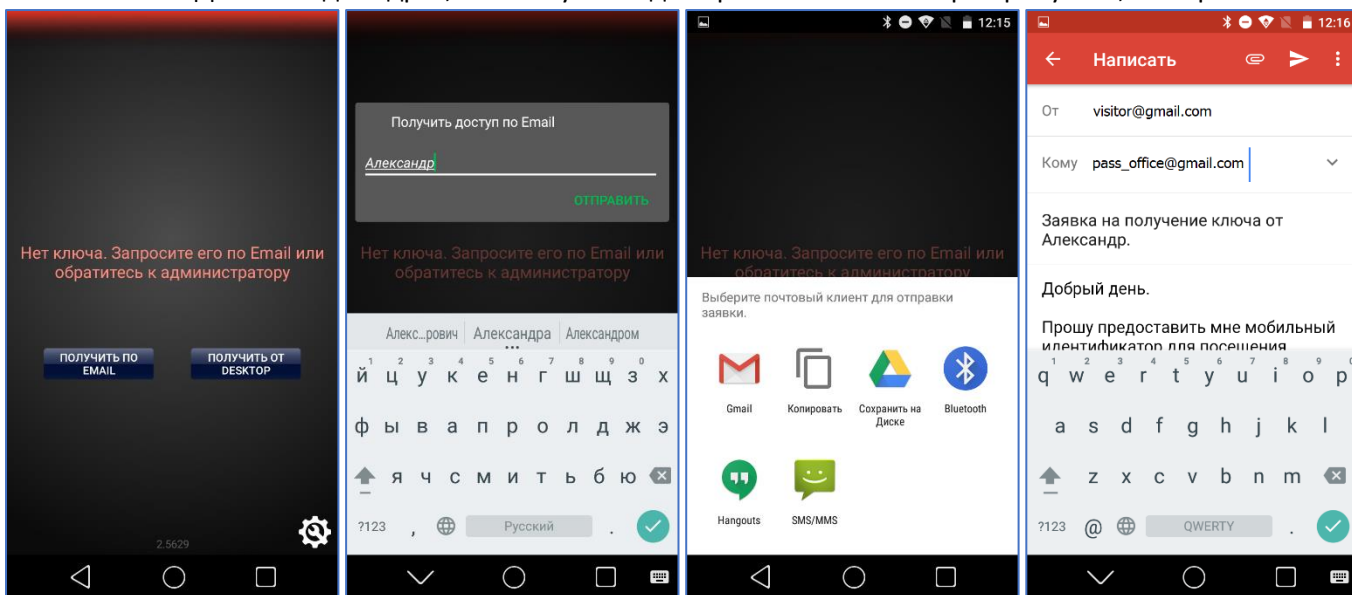
Выдача идентификаторов по e-mail

С помощью мобильного приложения и ProxWay Desktop возможна выдача мобильных идентификаторов по e-mail (удаленно)

Процедура нового идентификатора по e-mail с помощью ProxWay Desktop и ProxWay Config

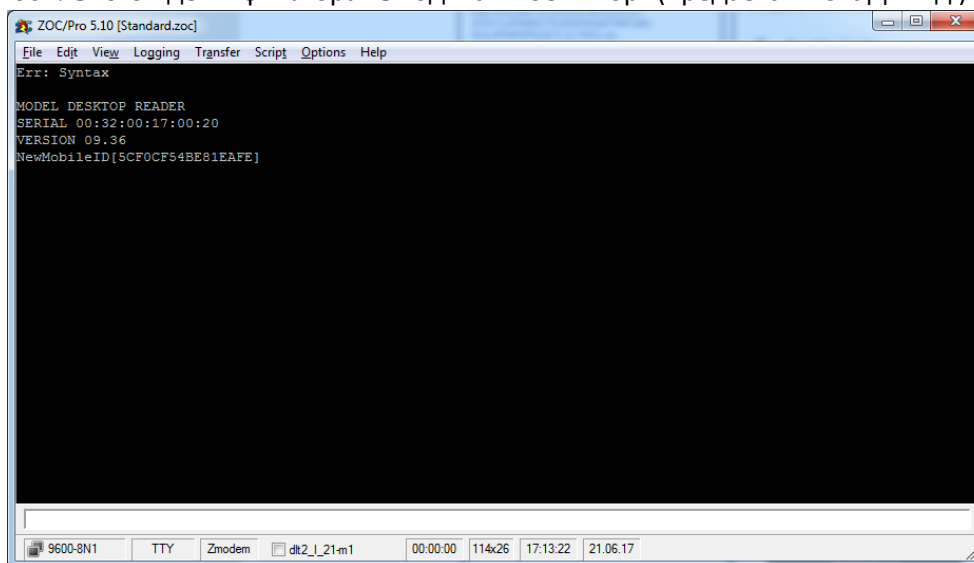
1. Если у посетителя еще нет приложения ProxWay ID, он его устанавливает на своем смартфоне
2. В приложении ProxWay ID пользователь нажимает кнопку "Получить по e-mail" (или в настройках приложения использует форму "Запрос сетевого ключа"), вводит свое имя и выбирает программу почты для отправки заявки.

Далее вводит адрес, используемый для приема заявок в бюро пропусков, и отправляет письмо

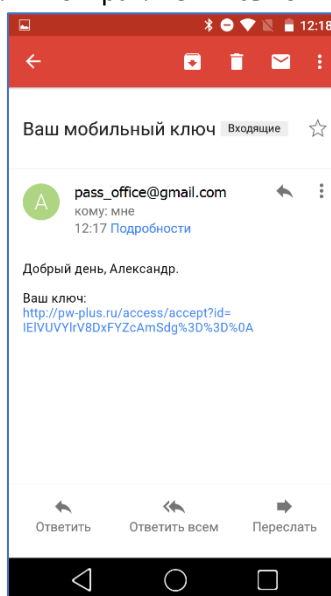


3. Получив почту с заявкой, сотрудник бюро пропусков открывает её на смартфоне с установленным приложением ProxWay Config. После нажатия на ссылку в письме будет запущено приложение и сохранена заявка.

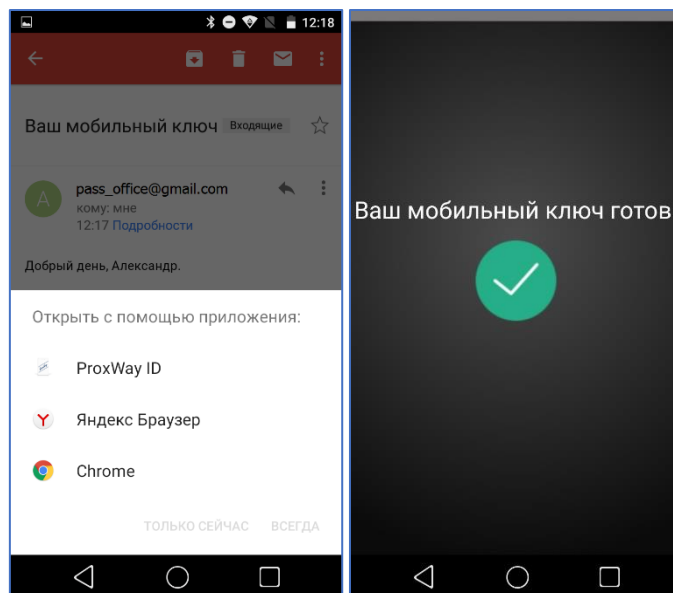
4. Сотрудник бюро пропусков переводит настольный считыватель в режим выдачи идентификаторов – размещает на считывателе мастер-карту.
5. Сотрудник бюро пропусков с помощью ProxWay Config подключается к настольному считывателю, переходит в меню "Доступ" и нажимает "Подтвердить"
6. Приложение получает мобильный идентификатор из выделенного списка, код полученного мобильного идентификатора выводится в СОМ порт (передается в СКУД и т.д.)



7. В то же время приложение ProxWay Config формирует e-mail подтверждение. Сотрудник бюро пропусков вводит адрес посетителя и отправляет письмо.



8. Получив почту с заявкой, посетитель открывает её на смартфоне с помощью приложения ProxWay ID. После нажатия на ссылку в письме, будет запущено приложение и сохранен код идентификатора.



Дополнительная защита систем доступа (персонализация идентификаторов)

Считыватели ProxWay поддерживают режим, в котором они принимают код только тех мобильных идентификаторов, которые зашифрованы известными им ключом шифрования (паролем).

Чтобы создать закрытую систему достаточно выполнить программирование считывателей задав им секретный пароль, а с помощью ProxWay Desktop выдавать закрытые уникальным ключом шифрования идентификаторы.

Персонализация поддерживается для идентификаторов BLE ID, Mifare® и Mifare® Plus. При использовании Mifare® и Mifare® Plus есть возможность хранить свой номер идентификатора в зашифрованных секторах данных.

Так как идентификаторы Mifare® Plus в режиме SL3 обладают большим уровнем защиты, то для записи данных используется только один сектор, а при работе с идентификатором Mifare® в режиме SL1 (Mifare Classic и т.д) шифруются все свободные сектора данных, чтобы исключить возможность взлома подбором. Если до этого на карточке были сектора с данными другой программы, то они пропускаются.

Определение, включен ли режим шифрования идентификаторов ProxWay BLE ID

С помощью данной команды можно информацию о том, включен ли режим шифрования мобильных идентификаторов в устройстве.

По умолчанию – значение 0, выключено. Если режим шифрования включен – значение 1.

Запрос:

```
bconf<cr><lf>
```

Ответ:

```
bconf 0<cr><lf>
```

Установка режима шифрования мобильных идентификаторов

Включение режима шифрования и установка пароля шифрования

Запрос:

```
p123456AA<cr><lf>
```

пароль - 4 байта (8 символов hex)

Ответ:

```
MOBILEPASS 1<cr><lf>
```

Внимание!!! Шифрованные и нешифрованные идентификаторы хранятся в различных областях памяти мобильного приложения PROXWAY ID.

Выключение режима шифрования и очистка пароля

Запрос:

```
p<cr><lf>
```

Ответ:

```
MOBILEPASS 0<cr><lf>
```

Для тонкой настройки правил шифрования Mifare® рекомендуем использовать конфигуратор ProxWay Config.

Определение, включен ли режим шифрования идентификаторов Mifare

С помощью данной команды можно информацию о том, включен ли режим шифрования мобильных идентификаторов в устройстве и его параметров.

Запрос:

```
mconf<cr><lf>
```

Ответ:

```
SL1Crypto 1<cr><lf>
SL1Revers 0<cr><lf>
SL1Internal 1<cr><lf>
SL1Diversity 0<cr><lf>
SL1Sector 00-15<cr><lf>
SL1Address 00-06<cr><lf>
SL3Crypto 1<cr><lf>
SL3Revers 0<cr><lf>
SL3Internal 0<cr><lf>
SL3Diversity 0<cr><lf>
SL3Sector 00-31<cr><lf>
SL3Address 00-00<cr><lf>
```

Описание параметров:

Карты Mifare Classic, Mifare Plus в режиме SL1 (алгоритм шифрования Crypto1)

SL1Crypto	1 - шифрование включено, 0 - выключено
SL1Revers	1 - вывод инвертированного кода идентификатора включен, 0 - выключен
SL1Internal	1 - вывод персонифицированного кода идентификатора (записанного в сектор карты) включен, 0 - выключен
SL1Diversity	1 – диверсификация, алгоритм привязки шифрования к карте включен, 0 - выключен
SL1Sector	Секторы данных, используемые для чтения/записи данных.
SL1Address	Блоки данных в секторе, используемые для чтения/записи данных

Карты Mifare Plus в режиме SL3 (алгоритм шифрования AES)

SL3Crypto 1	1 - шифрование включено, 0 - выключено
SL3Revers	1 - вывод инвертированного кода идентификатора включен, 0 - выключен
SL3Internal	1 - вывод персонифицированного кода идентификатора (записанного в сектор карты) включен, 0 - выключен
SL3Diversity	1 – диверсификация, алгоритм привязки шифрования к карте включен, 0 - выключен
SL3Sector	Секторы данных, используемые для чтения/записи данных
SL3Address	Блоки данных в секторе, используемые для чтения/записи данных

Установка режима шифрования карт Mifare Classic, Mifare Plus в режиме SL1 (алгоритм шифрования Crypto1)

С помощью данной команды можно включить только шифрование карт Mifare®.

Запрос:

```
m1234567890AA, diversification<cr><lf>
```

пароль - 6 байт (12 символов hex)

Где diversification – параметр включения режима диверсификации: 1 – включен.

Запрос:

```
m1234567890AA <cr><lf>
```

Ответ:

```
SL1Crypto 1<cr><lf>  
SL1Revers 0<cr><lf>  
SL1Internal 0<cr><lf>  
SL1Diversity 0<cr><lf>  
SL1Sector 00-15<cr><lf>  
SL1Address 00-06<cr><lf>
```

Запрос:

```
m1234567890AA,1 <cr><lf>
```

Ответ:

```
SL1Crypto 1<cr><lf>  
SL1Revers 0<cr><lf>  
SL1Internal 0<cr><lf>  
SL1Diversity 1<cr><lf>  
SL1Sector 00-15<cr><lf>  
SL1Address 00-06<cr><lf>
```

Отключение режима шифрования карт Mifare Classic, Mifare Plus в режиме SL1 (алгоритм шифрования Crypto1)

Будет отключен режим шифрования и очищен пароль

Запрос:

```
m<cr><lf>
```

Ответ:

```
SL1Crypto 0<cr><lf>  
SL1Revers 0<cr><lf>  
SL1Internal 0<cr><lf>  
SL1Diversity 0<cr><lf>  
SL1ForSL3 0<cr><lf>  
SL1Sector 00-15<cr><lf>  
SL1Address 00-06<cr><lf>
```

Установка режима шифрования карт Mifare Plus в режиме SL3 (алгоритм шифрования AES)
С помощью данной команды можно включить только шифрование карт Mifare® Plus в режиме SL3.

Запрос:

```
mp00112233445566778899AABBCCDDEEFF,diversification<cr><lf>
```

пароль - 16 байт (32 символа hex)

Где diversification – параметр включения режима диверсификации: 1 – включен.

Запрос, без включения диверсификации:

```
mp00112233445566778899AABBCCDDEEFF<cr><lf>
```

Ответ:

```
SL3Crypto 1<cr><lf>  
SL3Revers 0<cr><lf>  
SL3Internal 0<cr><lf>  
SL3Diversity 0<cr><lf>  
SL3Sector 00-31<cr><lf>  
SL3Address 00-00<cr><lf>
```

Запрос, включение диверсификации:

```
mp00112233445566778899AABBCCDDEEFF,1 <cr><lf>
```

Ответ:

```
SL3Crypto 1<cr><lf>  
SL3Revers 0<cr><lf>  
SL3Internal 0<cr><lf>  
SL3Diversity 1<cr><lf>  
SL3Sector 00-31<cr><lf>  
SL3Address 00-00<cr><lf>
```

Отключение режима шифрования карт Mifare Plus в режиме SL3 (алгоритм шифрования AES)
Будет отключен режим шифрования и очищен пароль

Запрос:

```
mp<cr><lf>
```

Ответ:

```
SL3Crypto 0<cr><lf>  
SL3Revers 0<cr><lf>  
SL3Internal 0<cr><lf>  
SL3Diversity 1<cr><lf>  
SL3Sector 00-31<cr><lf>  
SL3Address 00-00<cr><lf>
```

Установка стартового номера персонифицированного идентификатора

С помощью данной команды можно просмотреть и задать стартовый номер для записи индивидуальных идентификаторов Mifare и Mifare Plus. После каждого выпуска карты номер будет увеличиваться на единицу.

Запрос для просмотра стартового номера:

```
ms<cr><lf>
```

Ответ:

```
MSTART 0000000000<cr><lf>
```

Запрос для установки стартового номера:

```
ms01EB931000<cr><lf>
```

где 01EB931000 (5 байт, 10 символов hex) - стартовый номер для записи индивидуальных идентификаторов

Ответ:

```
MSTART 01EB931000<cr><lf>
```

Выпуск зашифрованной карты

Выпуск карт производится в пакетном режиме, для остановки выпуска следует отправить команду останова.

Запрос для остановки выпуска карт:

```
stop<cr><lf>
```

Ответ:

```
Stop Issue Card<cr><lf>
```

Запрос для выпуска карт Mifare Classic, Mifare Plus в режиме SL1 (алгоритм шифрования Crypto1):

```
sl1<cr><lf>
```

Ответ:

```
Start Issue Card<cr><lf>
```

Запрос для выпуска карт Mifare Plus в режиме SL3 (алгоритм шифрования AES):

```
sl3<cr><lf>
```

Ответ:

```
Start Issue Card<cr><lf>
```

Ответ:

```
MifareBlock[+++++]  
Mifare[E4009A14] 000,39444 1K (0004,08)<cr><lf>
```

Или, если включен индивидуальный номер карты

```
MifareBlock[+++++]  
CryptedMifare[01EB931000] 147,04096 1K (0004,08)<cr><lf>
```

Карты Mifare Classic, Mifare Plus в режиме SL1 (алгоритм шифрования Crypto1) имеют объём памяти, который разделен на 16 секторов. Каждый сектор имеет свои ключи доступа, что позволяет разграничивать доступ к различным приложениям. Для предотвращения атаки подбором все 16 секторов должны быть закрыты. Индикация записи и шифрования сектора отображается в сообщении MifareBlock[+++++].

Процедура выдачи нового идентификатора

1. Администратор размещает на считывателе новую (чистую) карту Mifare®.
2. Администратор дает команду на выпуск новой карты – выполняется шифрование.
3. По завершению шифрования код полученного идентификатора считывается и выводится в СОМ порт (передается в СКУД и т.д.)
4. Администратор размещает на считывателе следующую чистую карту Mifare®
5. Администратор дает команду на останов выпуска карт

Возможные варианты выпуска карты:

Выпущено успешно, зашифрованы все 16 секторов

```
MifareBlock[+++++]
```

Выпущено успешно, зашифровано 5 секторов, остальные недоступны для шифрования, так как используются в другом ПО

```
MifareBlock[-++++-]
```

Выпуск не удался, все 16 секторов недоступны для шифрования

```
MifareBlock[-----]
```

Карта была убрана со считывателя, последние 4 сектора не зашифрованы (потенциальная брешь для атаки, следует перевыпустить этот идентификатор)

```
MifareBlock[+++++++!!!!]
```

Очистка зашифрованной карты

Будут очищены и снято шифрование с секторов данных, которые были зашифрованы известным паролем.

Запрос:

```
z<cr><lf>
```

Ответ:

```
MifareBlock[+++++++]  
Mifare[E4009A14] 000,39444 1K (0004,08)<cr><lf>
```