

PW Config

Обзор функциональных возможностей софта
на примере программирования считывателя
PW-mini MF BLE



Скачайте и установите мобильное приложение «PW Config»

С его помощью выполняется полная настройка считывателя.

СКАЧАТЬ
PW CONFIG



Поддерживаются устройства с Android 5.0 и выше, имеющие Bluetooth 4.0 с поддержкой BLE (Bluetooth Low Energy).

Переведите считыватель в режим программирования

Замкните выводы D0 (зеленый) и D1 (белый) между собой и подайте питание.

Внимание!!! При попытке соединения, без авторизации в окне программы будет выведено сообщение о невозможности доступа.

Запустите PW Config

Нажмите кнопку «Поиск» (рис.1-1), начнется поиск устройств. Если Bluetooth не включен, программа выдаст запрос на его включение, нажмите «Да» (рис.1-2).

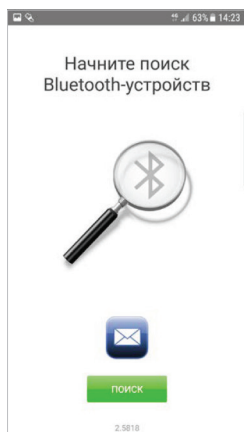


Рис.1-1

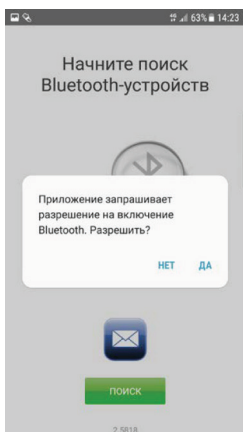


Рис.1-2

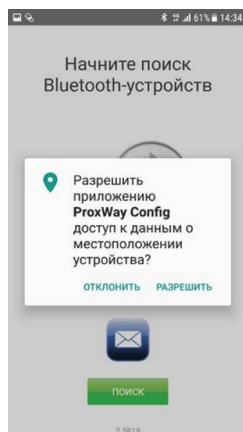


Рис.1-3

Внимание!!! Для работы BLE выше должны быть включены службы местоположения (рис.1-3).

Вычитка конфигурации

При сканировании будет выведено имя считывателя, выбираем считыватель и нажимаем кнопку «Подключить» (рис.2). Будет выполнена вычитка конфигурации (рис.3).

После успешной вычитки будет доступно основное меню, в котором можно **настроить** считыватель, **сохранить или восстановить** его конфигурацию (шаблон) и **обновить** микропрограмму считывателя (прошивку) (рис.4).



Рис.2

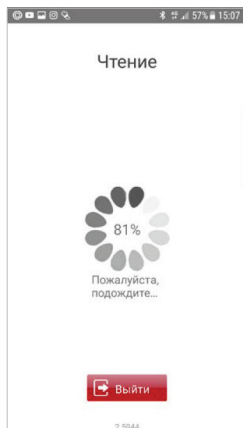


Рис.3

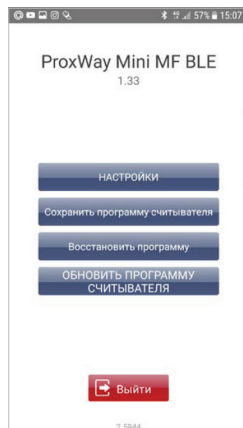


Рис.4

Если внесены изменения в конфигурацию, становится доступен пункт меню «Записать в устройство» (рис.5). По его нажатию конфигурация будет записана в считыватель.

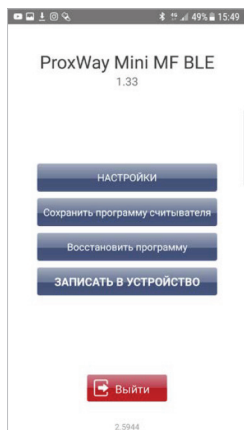


Рис.5

Для того, чтобы разъединиться со считывателем, нажмите кнопку «Выйти».

Внимание!!!

Если разъединиться без записи конфигурации, все изменения будут утеряны.

Пункт меню «Настройки»

Здесь доступны поля групп настроек считывателя: «Устройство», «Доступ», «Индикация» и «Mobile ID».

Группа настроек «Устройство»

«Серийный номер устройства» (рис.6-1) - информационное поле, содержащее информацию о серийном номере считывателя.

«Версия микропрограммы» (рис.6-2) - содержит информацию о текущей версии прошивки считывателя, а также позволяет обновить прошивку считывателя.

После выбора данного пункта меню, будет отображен список доступных файлов в формате *.bin. Выберите один из них – начнется процесс обновления микропрограммы.

Внимание!!! Все микрограммы должны размещаться в папке “Загрузки” (Download) в основной памяти мобильного устройства.

«Код инженера» (рис.6-3) - смена кода инженера для доступа в считыватель.

При установке кода инженера пропадет необходимость замыкать выводы D0 (зеленый) и D1 (белый), что позволяет настраивать считыватели ProxWay с помощью мобильного телефона, используя технологию BLE. Это наиболее быстрый и удобный способ изменения конфигурации считывателя без его демонтажа.

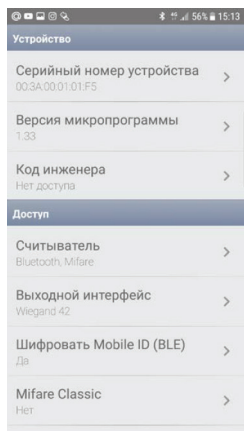


Рис.6-1

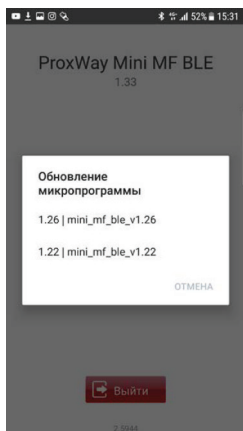


Рис.6-2

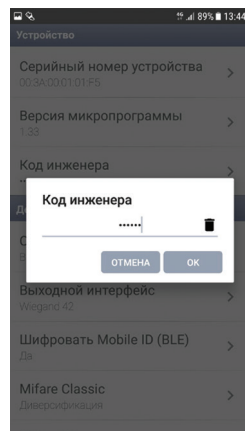


Рис.6-3

Группа настроек «Доступ»

«Считыватель» (рис.7-1) - выбор типа используемых идентификаторов.

Чтение только Mifare, только Bluetooth или Mifare и Bluetooth. (рис.7-2)

«Выходной интерфейс» (рис.8) - можно задать тип выходного интерфейса для связи с контроллером.

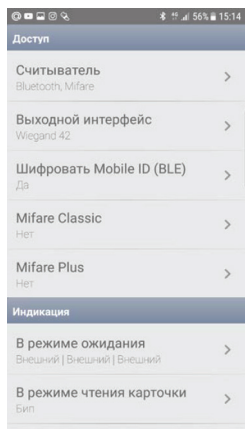


Рис.7-1

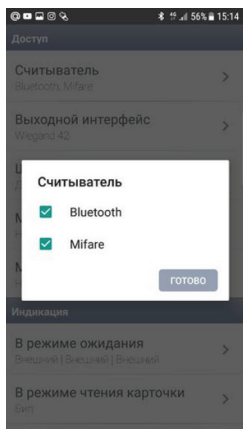


Рис.7-2

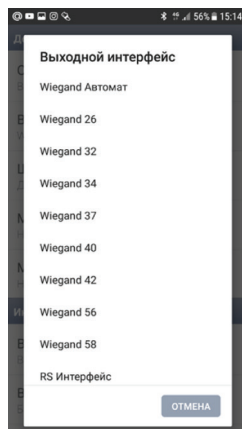


Рис.8

«Шифровать Mobile ID (BLE)» (рис.9) - можно задать пароль шифрования мобильных идентификаторов: до 8 шестнадцатеричных символов.

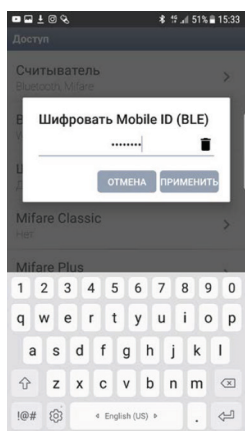


Рис.9

Алгоритм шифрования канала передачи данных соответствует ГОСТ 28147-89, согласно которому максимальная длина криптографического ключа составляет 256 бит. (Это означает, что идентификаторы защищены от копирования по воздуху, создания клона и взлома).

Группа настроек «Mifare Classic»

«Mifare Classic» - при использовании карт доступа типа Mifare Classic, содержит в себе ряд настроек безопасности.

Технология Mifare используется, как правило, в сложных системах, где вопросы конфиденциальности и защиты данных имеют большое значение.

Именно для обеспечения защиты и безопасности в технологии MIFARE реализована обработка данных с использованием ключей и криптографических алгоритмов.

Считыватели, используемые для записи и чтения данных в чип Mifare, должны также поддерживать защиту и безопасность данных со своей стороны. Это означает, что считыватель должен также хранить в своей памяти ключи доступа для каждого сектора Mifare Classic.

Если считыватель не обладает такой возможностью, то такой считыватель не следует использовать, так как защищенность всей системы в целом будет на низком уровне.

Если шифровать карты не требуется:

«**Безопасность**» → «**Нет**» (рис.10-1, 10-2). В этом случае будет передаваться в контроллер только UID и информация завода-изготовителя чипа.

В этом режиме дополнительно можно настроить:

«**Порядок байт кода карточки**» → «**Прямой**» или «**Обратный**» (рис.11). Данная функция предусмотрена для интеграции в различные системы СКУД в которых может требоваться такая инверсия.

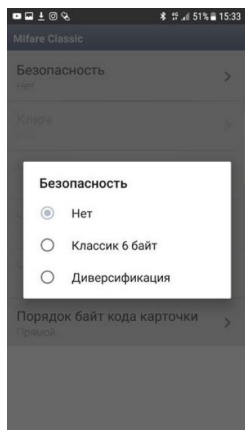


Рис.10-1

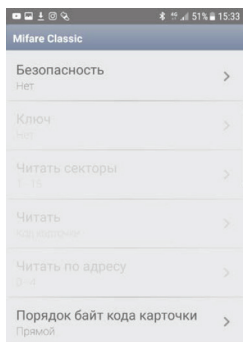


Рис.10-2

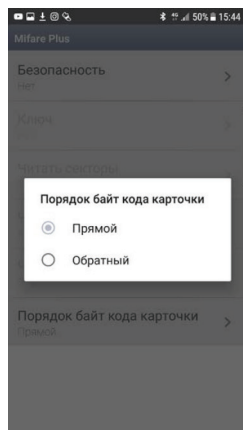


Рис.11

Если карты Mifare Classic будут зашифрованы

Требуется чтение данных из защищенного блока Mifare. Для этого в поле «Безопасность» есть два варианта – «Классик 6 байт» и «Диверсификация»

«Безопасность» → «Классик 6 байт» (рис.12-1, 12-2). Режим шифрования SL1 (CRYPTO-1).

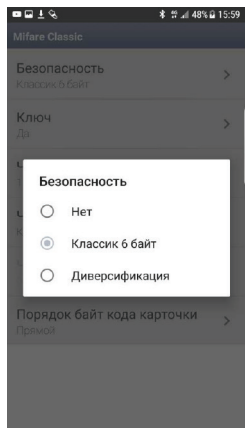


Рис.12-1

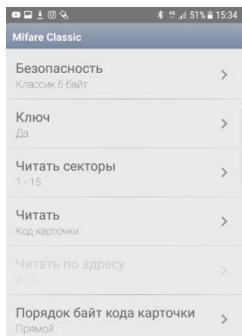


Рис.12-2

«Ключ» - в этом поле можно задать ключ шифрования для идентификаторов Mifare: 12 шестнадцатеричных символов (рис. 13-1, 13-2).

При инициализации чипа Mifare Classic заказчик (владелец объекта) должен сам сгенерировать значения ключей и надежно хранить эту информации. Это организационный момент, значение которого нельзя недооценивать.

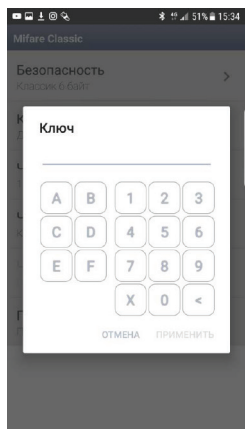


Рис.13-1

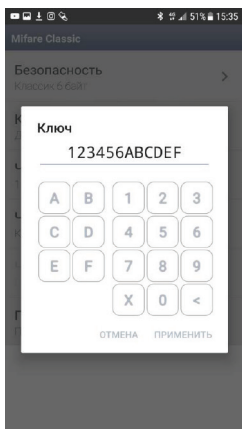


Рис.13-2

«**Читать секторы**» (рис.14). В этом поле можно задать значения секторов, которые нам необходимо читать.

Каждый сектор Mifare Classic может иметь свои собственные ключи доступа и условия записи / чтения данных.

«**Читать**» → «**Код карточки**» (рис.15). Если ключ шифрования записанной ячейки в карте совпадает с ключом шифрования в считывателе, то на выходе в контроллер будет передаваться код карты (UID).

«**Читать**» → «**По адресу**» (рис.16). Выбирая этот пункт, мы получаем на выходе со считывателя информацию, записанную в определенный блок памяти карты.

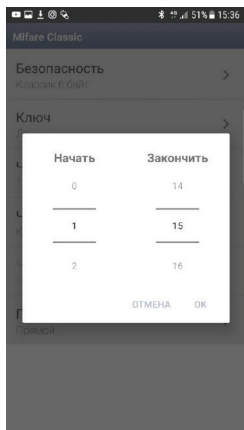


Рис.14

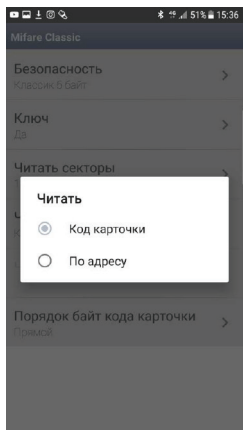


Рис.15

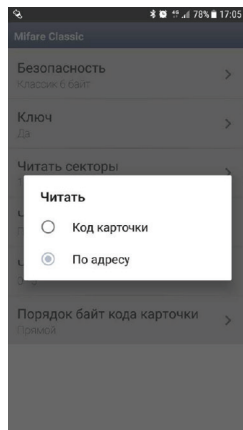


Рис.16

После выбора пункта меню **«По адресу»** становится доступной команда **«Читать по адресу»**. Здесь мы можем указать смещения в битах для чтения в блоках (рис.17).

«Порядок байт кода карточки» → **«Прямой»** или **«Обратный»** (рис.18).

Данная функция предусмотрена для интеграции в различные системы СКУД в которых может требоваться такая инверсия.



Рис.17

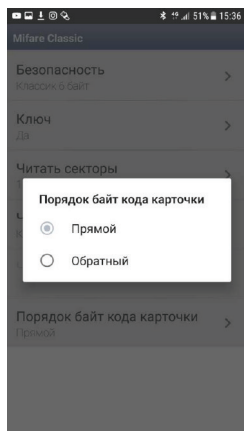


Рис.18

«Безопасность» → **«Диверсификация»** (рис.19-1, 19-2).

Более защищенный прикладной алгоритм шифрования «Диверсифицированные ключи» на любом, выбранном уровне шифрования (SL1, SL3). Принцип алгоритма заключается в том, что каждый идентификатор имеет свой индивидуальный ключ шифрования.

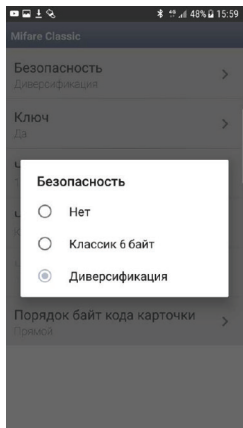


Рис.19-1

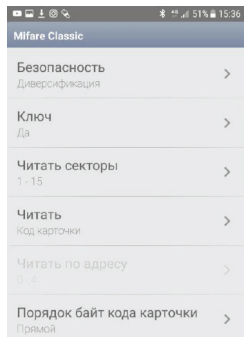


Рис.19-2



Рис.20

«Ключ» - в этом поле можно задать ключ шифрования для идентификаторов Mifare Classic в режиме диверсифицированных ключей: 16 шестнадцатеричных символов (8 байт) (рис.20).

При инициализации чипа Mifare Classic заказчик (владелец объекта) должен сам сгенерировать значения ключей и надежно хранить эту информацию. Это организационный момент, значение которого нельзя недооценивать.

«Читать секторы» (рис.21). В этом поле можно задать значения секторов, которые нам необходимо читать.

Каждый сектор Mifare Classic может иметь свои собственные ключи доступа и условия записи / чтения данных.

«Читать» → «Код карточки» (рис.22). Если ключ шифрования записанной ячейки в карте совпадает с ключом шифрования в считывателе, то на выходе в контроллер будет передаваться код карты (UID).

«Читать» → «По адресу» (рис.23). Выбирая этот пункт, мы получаем на выходе со считывателя информацию, записанную в определенный блок памяти карты.

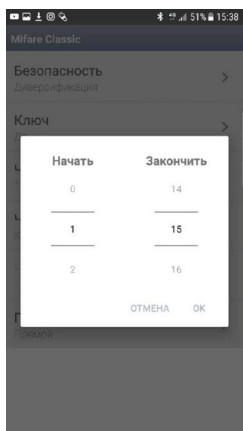


Рис.21

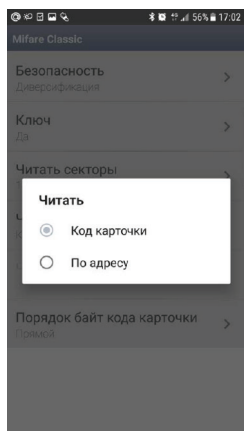


Рис.22

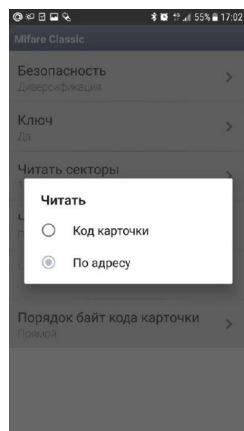


Рис.23

После выбора пункта меню «По адресу» становится доступной команда «Читать по адресу». Здесь мы можем указать смещения в битах для чтения в блоках (рис.24).

«Порядок байт кода карточки» → «Прямой» или «Обратный» (рис.25).

Данная функция предусмотрена для интеграции в различные системы СКУД в которых может требоваться такая инверсия.



Рис.24

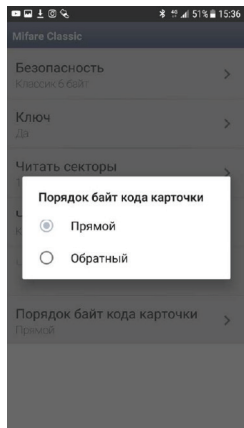


Рис.25

Группа настроек «Mifare Plus»

«Mifare Plus» - при использовании карт доступа типа Mifare Plus, содержит в себе ряд настроек безопасности.

Технология Mifare используется, как правило, в сложных системах, где вопросы конфиденциальности и защиты данных имеют большое значение.

В свою очередь продукты Mifare Plus призваны повысить существующий уровень безопасности при использовании бесконтактных смарт-карт карт.

Mifare Plus обеспечивает полную совместимость снизу-вверх с продуктами Mifare Classic 1K и Mifare Classic 4K.

Карты Mifare Plus могут легко интегрироваться в существующие системы, где уже используются карты Mifare Classic.

Уровень защищенности карт Mifare Plus может быть повышен в любой момент по мере развития системы путем активизации алгоритма AES (Advanced Encryption Standard), обеспечивающего высокий уровень безопасности, целостности данных, аутентификации и шифрования.

Если шифровать карты не требуется:

«**Безопасность**» → «**Нет**» (рис.26-1, 26-2). В этом случае будет передаваться в контроллер только UID и информация завода-изготовителя чипа.

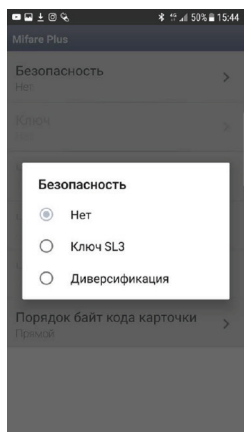


Рис. 26-1

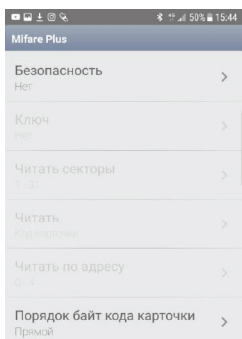


Рис. 26-2

В этом режиме дополнительно можно настроить:

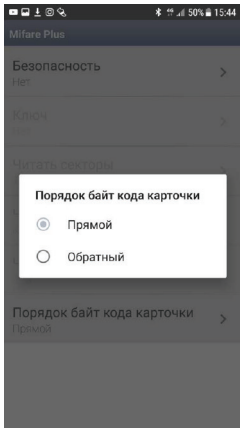


Рис.27

«Порядок байт кода карточки» → «Прямой» или «Обратный» (рис.27). Данная функция предусмотрена для интеграции в различные системы СКУД в которых может требоваться такая инверсия.

Если карты Mifare Plus будут зашифрованы

Требуется чтение данных соответствующего шифрованию режима. Для этого в поле «Безопасность» есть два варианта – «Ключ SL3» и «Диверсификация»

«Безопасность» → «Ключ SL3» (рис. 28-1, 28-2). Используется для аутентификации, обмена и шифрования данных, для работы с памятью, а также для выявления удаленных атак по радиоканалу. Используется крипто-алгоритм AES.

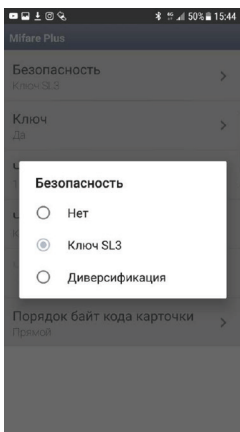


Рис.28-1

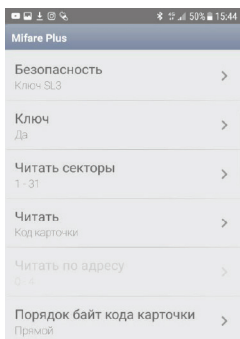


Рис.28-2

«Ключ» - в этом поле можно задать ключ шифрования для идентификаторов Mifare: 32 шестнадцатеричных символов.
(рис. 29-1, 29-2)

С завода-изготовителя чипы Mifare Plus (в картах, метках, браслетах и т.п.) поступают на уровне безопасности SL-0.

Использовать в прикладной системе карты на уровне SL-0 нельзя, чип Mifare Plus должен быть проинициализирован, т.е. переведен на уровень SL-1, SL-2 или SL-3.

При инициализации чипа Mifare Plus заказчик (владелец объекта) должен сам сгенерировать значения ключей и надежно хранить эту информации. Это организационный момент, значение которого нельзя недооценивать.



Рис. 29-1



Рис. 29-2

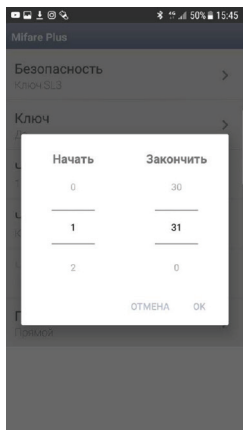


Рис. 30

«Читать секторы» (рис.30)

В этом поле можно задать значения секторов, которые нам необходимо читать.

Каждый сектор Mifare Plus может иметь свои собственные ключи доступа и условия записи / чтения данных

«**Читать**» → «**Код карточки**» (рис.31). Если ключ шифрования записанной ячейки в карте совпадает с ключом шифрования в считывателе, то на выходе в контроллер будет передаваться код карты (UID).

«**Читать**» → «**По адресу**» Выбирая этот пункт, мы получаем на выходе со считывателя информацию, записанную в определенный блок памяти карты.

После выбора пункта меню «**По адресу**» становится доступной команда «**Читать по адресу**». Здесь мы можем указать смещения в битах для чтения в блоках (рис.32).

«**Порядок байт кода карточки**» → «**Прямой**» или «**Обратный**» (рис.33).

Данная функция предусмотрена для интеграции в различные системы СКУД в которых может требоваться такая инверсия.

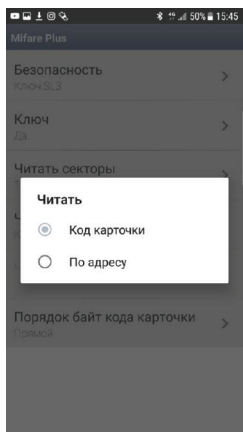


Рис.31



Рис.32

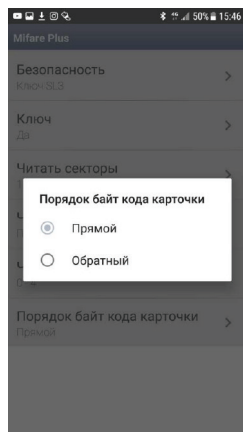


Рис.33

«Безопасность» → «Диверсификация» (Mifare Plus)
(рис.34-1, 34-2). Более защищенный прикладной алгоритм шифрования «Диверсифицированные ключи» на любом, выбранном уровне шифрования (SL1, SL3).

Принцип алгоритма заключается в том, что каждый идентификатор имеет свой индивидуальный ключ шифрования.

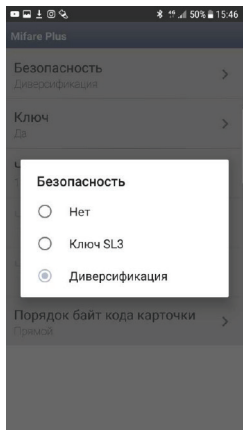


Рис.34-1

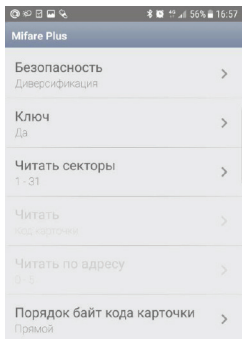


Рис.34-2

«Ключ» - в этом поле можно задать ключ шифрования для идентификаторов Mifare Plus в режиме диверсифицированных ключей: 16 шестнадцатеричных символов (8 байт). (рис. 35-1, 35-2).

При инициализации чипа Mifare Plus заказчик (владелец объекта) должен сам сгенерировать значения ключей и надежно хранить эту информации. Это организационный момент, значение которого нельзя недооценивать.



Рис. 35-1



Рис. 35-2

«Читать секторы» (рис.36).

В этом поле можно задать значения секторов, которые нам необходимо читать.

Каждый сектор Mifare Plus может иметь свои собственные ключи доступа и условия записи / чтения данных

«Порядок байт кода карточки» → «Прямой» или «Обратный» (рис.37).

Данная функция предусмотрена для интеграции в различные системы СКУД в которых может требоваться такая инверсия.

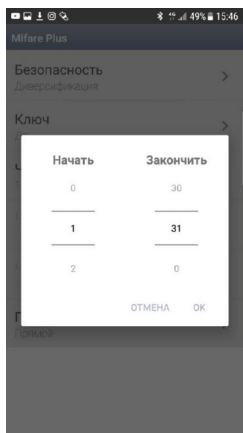


Рис. 36

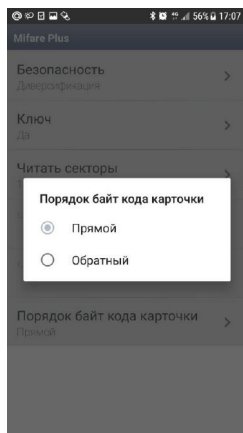


Рис. 37

Группа настроек «Индикация»

«В режиме ожидания» (рис. 38).

- Выбираем режим (цвет) индикации в режиме ожидания.

«В режиме чтения карточки» (рис. 39).

- Выбираем индикацию считывателя в режиме чтения карты (цвет и бипер).

«Продолжительность» (рис.40).

- выбираем продолжительность индикации считывателя.

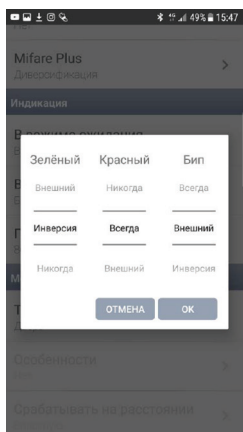


Рис. 38

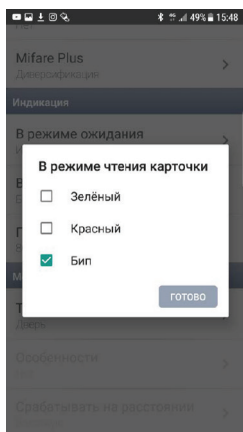


Рис.39

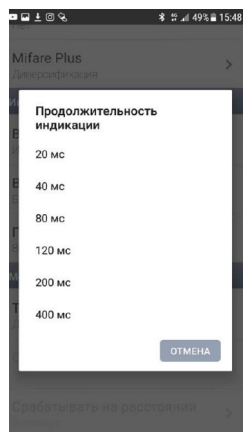


Рис.40

Группа настроек «Mobile ID»

«Точка прохода» (рис. 41) - Выбираем режим, в котором будет работать считыватель по каналу BLE. Этот выбор влияет на дальность работы.

В считывателе **PW-mini MF BLE** в этом меню доступно для выбора 2 режима: «Дверь» и «Ворота|Шлагбаум»

«Точка прохода» → «Дверь» (рис.42) - По умолчанию выбран этот режим, дальность работы до 80 см. Другие настройки в данном режиме не активны.

«Точка прохода» → «Ворота | Шлагбаум» (рис.43)

- При выборе этого режима, дальность работы увеличивается до 20м. Также становятся доступными дополнительные настройки.

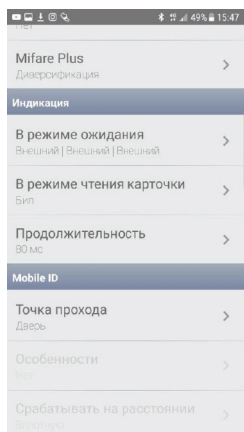


Рис. 41

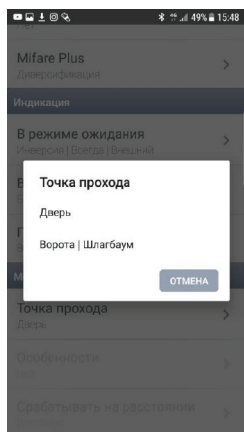


Рис. 42

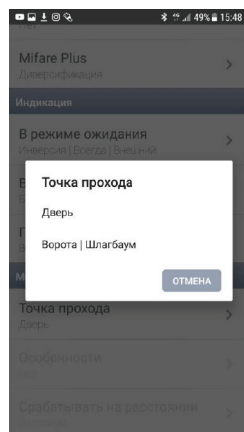


Рис. 43

«**Особенности**» - Для выбора доступен пункт в меню «Доступ только из приложения». Активация данного пункта помогает предостеречь от ложных сработок («по включению экрана» и «по разблокировке»), т.к. расстояние считывания увеличено.

«**Срабатывать на расстоянии**» (рис.44-1, 44-2) - Ползунком в настройках мы можем регулировать расстояние, что очень удобно для точной юстировки по месту установки считывателя.

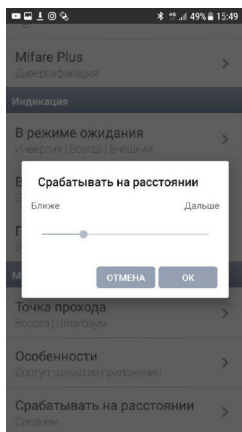


Рис. 44-1

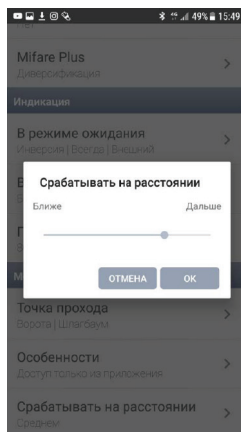


Рис.44-2

Сохранение настроек считывателя

Важно!!! Не забудьте записать настройки в считыватель после его конфигурирования

В главном меню выбираем пункт –
«Сохранить программу считывателя» (рис.45-1, 45-2)

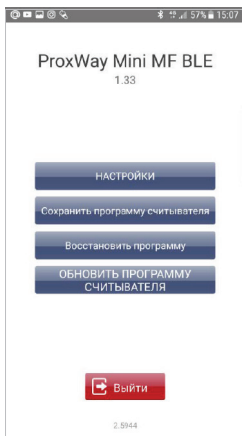


Рис. 45-1

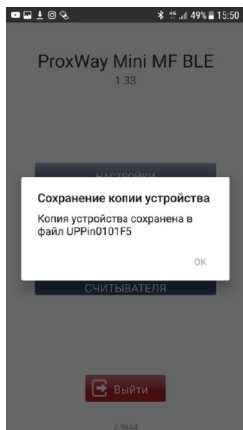


Рис.45-2

«Восстановить программу» (рис.46) - позволяет нам восстановить все настройки которые ранее были сохранены, а также через данное меню мы можем записать эти настройки в другие считыватели, где требуется работа с точно такими же настройками, что позволяет существенно сэкономить время.

«Обновить программу считывателя» (рис.47) - позволяет нам обновить микропрограмму (прошивку) считывателя.

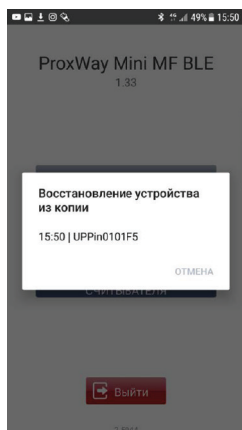


Рис. 46

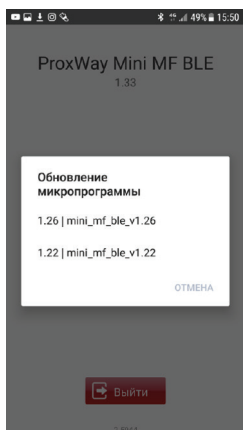


Рис.47