

Работа с картами Mifare Classic мобильного приложения BioSmart Mobile Reader

Работа в незащищенном режиме, чтение UID

Для карт Mifare Classic поддерживается функция считывания их открытого уникального идентификатора – UID.

Для настройки мобильного приложения на чтение UID карты, выполните следующие действия:

1. Откройте приложение BioSmart Mobile Reader.
2. Нажмите кнопку  в правом верхнем углу экрана, введите пин-код (по умолчанию 0000) и нажмите **Вход**.
3. Выберите пункт **Настройки**, затем **Система**.
4. В выпадающем списке **Режим чтения карты** выберите **Открытый UID**.
5. Сохраните изменения.

Работа в защищенном режиме



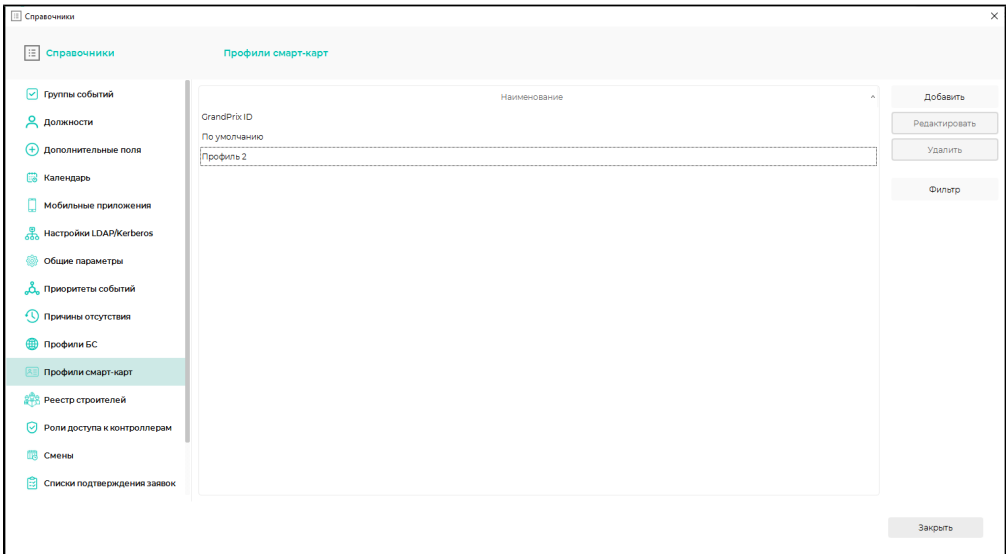
При работе с профилем смарт-карт запрещено изменять настройки в меню приложения.

Считывателем поддерживается защищённый режим работы для карт Mifare Classic.

Для работы с картами Mifare Classic в защищенном режиме выполните следующие действия:

Для создания [профиля смарт-карт](#) выполните вход в [ПО Biosmart-Studio v6](#).

- Перейдите в **Основное меню** в раздел **Справочники** → **Профили смарт-карт**.



- Нажмите кнопку **Добавить**, чтобы создать новый профиль смарткарт.
- В поле **Формат данных** установите одно из значений приведённых в таблице ниже.

Значение	Описание
----------	----------

Номер карты	Настройка определяет количество информации, которое может быть записано в защищенную область карты, и в каком порядке будет считываться информация из памяти карты. Для данной настройки можно выбрать следующие параметры: • порядок байт – в каком порядке будет считываться информация из памяти карты, записанная в байтах. От старшего к младшему – считывается прямой порядок байт информация из памяти карты. От младшего к старшему – считывается реверсивный порядок байт информация из памяти карты. • длина номера карты (байт) – количество информации, которое может быть записано в защищенную область карты (4 байта или 8 байт).
Schlumberger	Настройка определяет порядок работы с картами Schlumberger.

- Выберите вкладку **Mifare Classic**.

Профиль настроек смарт-карт

Название*

Профиль 2

✕

Формат данных

Номер карты

▼

Параметры

Порядок байт

От старшего к младшему

▼

Длина номера карты (байт)

4 байта

▼

Общее

Mifare Classic

Mifare Plus

Mifare DESFire

BioSmart ID

Ключ А

••••••••

↺

Ключ В

••••••••

☐
Использовать разные ключи

Доступ

Блоки данных

По умолчанию

▼

Системные блоки

По умолчанию

▼

Блоки

9

▲▼

-

0

▲▼

☒
Без ограничений размера

Смещение

0

▲▼

ОК

Отмена

- Заполните следующие поля в зависимости от используемого режима безопасности:

Название поля	Описание
Ключ А	Поле для указания мастер-ключа карты для доступа к защищенной области.
Ключ В	Ключ состоит из 6 байт, представленных в виде строки из 12 шестнадцатеричных символов.

Использовать разные ключи	Отметка в чек-боксе позволяет использовать различные ключи (ключ А и ключ В) для чтения и записи информации в память карты.  В настоящее время данная функция недоступна. Для чтения и записи информации могут использоваться только одинаковые ключи А и В.
Доступ	• Чтение AIB, запись AIB - для чтения и записи информации в память карты может использоваться ключ А или ключ В; • Чтение AIB, запись В - для чтения информации может использоваться ключ А или ключ В, для записи только ключ В; • Чтение В, запись В - для чтения и записи информации может использоваться только ключ В.  В настоящее время данная функция недоступна.
Блоки	• В первом переключателе с помощью стрелок указывается номер блока памяти, с которого начинается запись информации в память карты. Номер блока указывается в шестнадцатеричном формате. Указываемый блок не должен быть нулевым блоком нулевого сектора. • Во втором переключателе с помощью стрелок указывается номер блока памяти, на котором должна завершиться запись информации в память карты. Если значение задано, запись выполняется до указанного блока включительно. Переключатель активен, если в чек-боксе Без ограничений размера не проставлена отметка. В таком случае, длина идентификатора, записываемого на карту, ограничивается ("обрезается") в соответствии с выбранным значением. Если в чек-боксе проставлена отметка, то в память карты будет записываться идентификатор без ограничений по длине. Также во все блоки будут записаны заданные выше ключи, начиная с указанного в первом окне Блоки.

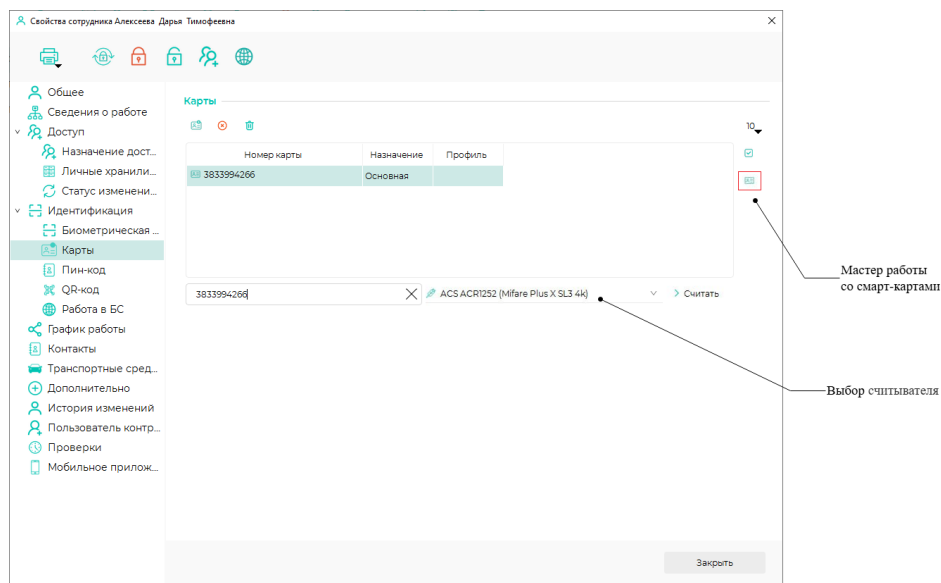


При выборе формата данных **Schlumberger** доступно только заполнение **ключа А**.

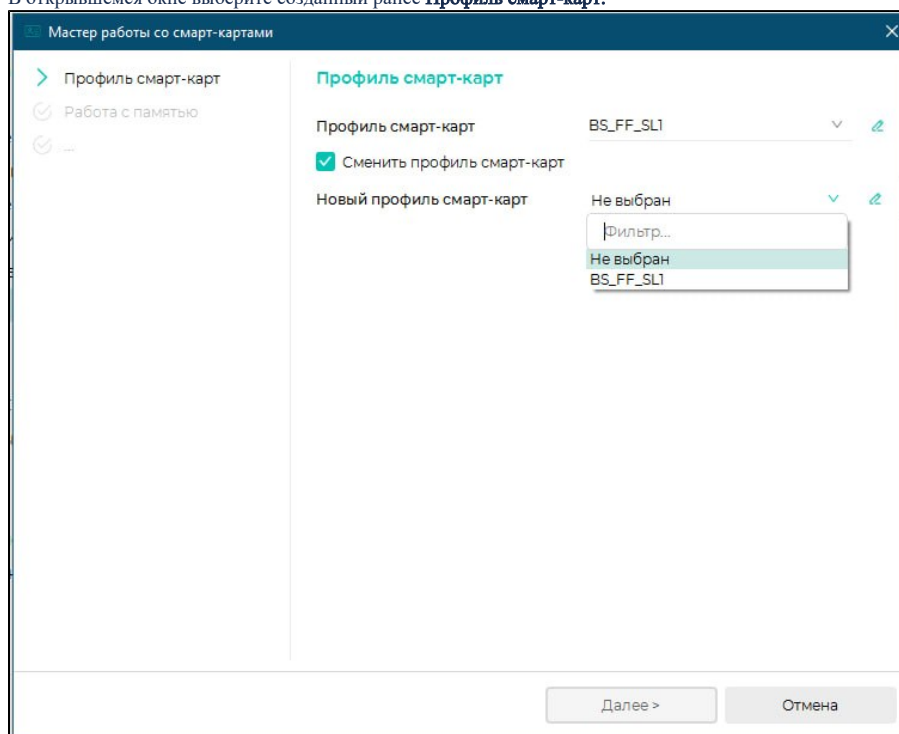
- Нижне приведен пример настроек профиля смарткарт, используемого для перевода карты защищенный режим, с помощью настройки **Номер карты**.

Для записи информации в зашифрованную область памяти карты выполните следующие действия:

- Подключите к ПК считыватель, с помощью которого будет производиться занесение карт в базу данных ПО Biosmart-Studio v6.
Для перевода карт Mifare Classic в безопасный режим должен использоваться USB-считыватель ACR1252U.
- Перейдите в раздел **Сотрудники** → выберите **Предприятие** → выберите сотрудника в списке → нажмите кнопку **Свойства** на панели инструментов.
- Перейдите в раздел **Карты** → нажмите кнопку **Добавить новую карту сотруднику** → выберите считыватель ACR1252U.



- Нажмите на кнопку **Мастер работы со смарт-картами**.
- В открывшемся окне выберите созданный ранее **Профиль смарт-карт**.



- Нажмите **Далее** и выберите, какие данные будут записаны в память RFID-карты.

The screenshot shows a software window titled "Мастер работы со смарт-картами" (Master of smart cards). On the left is a sidebar with three items: "Профиль смарт-карт" (Smart card profile) with a checkmark, "Работа с памятью" (Work with memory) with a right-pointing arrow, and a third item with a checkmark and an ellipsis. The main area is titled "Работа с памятью" (Work with memory) and contains three radio button options: "Записать шаблон сотрудника на карту" (Record employee template on card) which is selected, "Записать открытый UID на карту" (Record open UID on card), and "Очистить карту" (Erase card). At the bottom right are two buttons: "Далее >" (Next >) and "Отмена" (Cancel).

- Нажмите **Далее** и завершите работу с **Мастером работы со смарт-картами**.
- После этого в зашифрованную область памяти карты будет записан идентификатор сотрудника и ключ доступа к зашифрованной области.