

Считыватели бесконтактные контроля доступа UEM Mifare/NFC SKD reader, UEM Mifare/NFC SKD BT reader

Руководство по конфигурированию карт

Версия 1.5.5



© 2025 Акционерное общество "МикроЭМ"

Москва

Содержание

1 Принцип работы считывателя контроля доступа	4
1.1 Настройки по умолчанию	4
1.2 Режимы работы считывателя	4
1.2.1 Автономный режим.....	4
1.2.2 Подчиненный режим	5
1.3 Индикация.....	5
2 Виды бесконтактных карт.....	5
2.1 Карта-ключ.....	6
2.2 Мастер-карта	6
2.3 Карта-пропуск.....	7
2.4 Смартфоны с интерфейсами NFC и Bluetooth.....	7
3 Конфигурирование бесконтактных карт	8
3.1 Считыватель настольный рабочего места администратора.....	9
3.2 Конфигурирование	9
3.2.1 Подключение к считывателю	9
3.2.2 Работа с картой-ключом.....	11
3.2.2.1 Изготовление карты-ключа	12
3.2.2.2 Применение карты-ключа	13
3.2.2.3 Стирание карты-ключа	14
3.2.3 Работа с мастер-картой	14
3.2.3.1 Изготовление мастер-карты	15
3.2.3.2 Применение мастер-карты.....	16
3.2.3.3 Стирание мастер-карты	17
3.2.3.4 Копирование мастер-карты	17
3.2.3.5 Изменение настроек мастер-карты	17
3.2.4 Работа с картой-пропуском	24
3.2.4.1 Пропуска в виде бесконтактных карт	25
3.2.4.1.1 Изготовление карты-пропуска	25
3.2.4.1.2 Чтение и изменение настроек карты-пропуска.....	27
3.2.4.2 Пропуска в виде виртуальных карт на смартфонах с интерфейсом NFC	28
3.2.4.2.1 Изготовление виртуальной карты-пропуска.....	28
3.2.4.2.2 Чтение и изменение настроек виртуальной карты-пропуска	29

3.2.4.3	Пропуска в виде виртуальных карт на смартфонах с.....	31
	интерфейсом Bluetooth.....	31
3.2.4.3.1	Изготовление виртуальной карты-пропуска.....	32
3.2.4.3.2	Чтение и изменение настроек виртуальной карты-пропуска	34
3.2.5	Завершение работы с программой.....	36
4	Доступ по картам-пропускам и смартфонам	37
4.1	Вычитывание идентификатора по интерфейсу RS-485	38
4.1.1	Использование протокола UEM	38
4.1.2	Использование протокола MODBUS.....	39
4.1.3	Использование протокола OSDP	40

1 Принцип работы считывателя контроля доступа

После подачи питания считыватель излучает вблизи себя высокочастотное электромагнитное поле, частотой 13.56 МГц. Пассивная бесконтактная карта получает от него энергию, достаточную для работы внутренней электронной схемы, и в простейшем случае в ответ на специфическую команду считывателя передает свой уникальный идентификационный номер (UID).

Далее считыватель передает полученный идентификатор управляющему контроллеру СКУД по интерфейсу Wiegand или 1-Wire. Начиная с версии микропрограммы 0x98 и выше, доступен интерфейс RS485 с протоколом OSDP.

1.1 Настройки по умолчанию

Считыватель поставляется с настройками по умолчанию:

- автономный режим работы;
- связь с контроллером СКУД осуществляется по интерфейсу Wiegand-58;
- идентификатором пропуска является открытый UID карты (или данные от смартфона);
- входные сигналы управления индикацией включают ее низким уровнем;
- при получении идентификатора считыватель независимо от контроллера издает короткий звуковой сигнал и кратковременно зажигает зеленый светодиод.

1.2 Режимы работы считывателя

Считыватель предназначен для работы в двух режимах.

1.2.1 Автономный режим

В автономном режиме считыватель самостоятельно определяет наличие транспондера (смарт-карты) в непосредственной близости от антенны и передает прочитанный идентификатор по интерфейсу Wiegand, 1-Wire или OSDP.

При работе в формате Wiegand длительность одного бита равна 2000 мкс, длительность импульса - 200 мкс.

Новый считыватель изначально настроен выдавать полный UID карты в формате Wiegand-58 в автономном режиме. В случае 4-байтового UID старшие три байта идентификатора заполняются нулями.

1.2.2 Подчиненный режим

В подчиненном режиме считыватель не производит никаких самостоятельных действий, а выполняет только команды от управляющего устройства.

Формат команд для работы в подчиненном режиме, а также описание библиотеки разработчика находятся в отдельном документе - PgmGuide_SAM.pdf

Для работы со считывателем в подчиненном режиме используйте специализированное проверочное программное обеспечение - CLESCAR_SAM.EXE, документация по которому размещена в файле Test_UEM_SAM.pdf

1.3 Индикация

Считыватель снабжен звукоизлучателем, а также красным и зеленым светодиодами.

По умолчанию при обнаружении карты считыватель издает короткий звуковой сигнал и кратковременно зажигает зеленый светодиод.

Данная индикация никак не связана с правами карты в системе, в которой установлен считыватель.

2 Виды бесконтактных карт

Система контроля доступа на основе считывателей МикроЭМ построена на следующих компонентах:

- устройства ограничения доступа (двери, турникеты, шлагбаумы и т.п);
- контроллеры управления устройствами ограничения доступа;
- бесконтактные считыватели рабочих мест администраторов системы контроля доступа;
- бесконтактные считыватели пунктов пропуска;
- бесконтактные карты для настройки параметров считывателей (мастер-карта);
- бесконтактные карты для авторизации выпуска мастер-карт (карта-ключ);
- бесконтактные карты для пропусков (карта-пропуск).

В работе системы контроля доступа участвуют 3 типа бесконтактных карт стандарта ISO14443A, работающих на частоте 13.56 МГц:

- Mifare Classic для карты-ключа, мастер-карты и карты-пропуска (длина ключа 48 бит);
- Mifare Plus для карты-ключа, мастер-карты и карты-пропуска (длина ключа в режиме SL3 128 бит);
- Mifare Ultralight C для карты-ключа и карты-пропуска (длина ключа 128 бит).

Кроме того, в качестве карт-пропусков, работающих в открытом режиме, можно использовать карты стандартов ISO 14443B и ISO 15693.

В поле считывателя всегда следует подносить только одну карту любого из поддерживаемых типов.

2.1 Карта-ключ

Карта-ключ применяется для доступа администратора к конфигурированию мастер-карт.

Хранит мастер-ключи А и В для доступа к Мастер-карте, необходимые для чтения и записи данных на мастер-карту. Эти ключи предварительно генерируются администратором СКУД и используются для защиты от несанкционированного доступа.

Считывателю заранее известны мастер-ключи, необходимые для доступа к ключ-карте, поэтому он может считать с неё данные и получить доступ к мастер-ключам для дальнейшей настройки.

Карта-ключ строго привязана к системе СКУД и создаётся один раз. Она хранится у администратора СКУД и никому не передаётся. Только администратор может с её помощью создавать валидные мастер-карты, пригодные для конфигурирования считывателей и создания карт-пропусков.

Администратор СКУД лично проводит персонализацию каждого нового считывателя.

2.2 Мастер-карта

Мастер карта предназначена для бесконтактной настройки конфигурации считывателей контроля доступа, а также для настройки параметров рабочего места администратора системы контроля доступа с целью серийного выпуска карт-пропусков.

Хранит мастер-ключи А и В для доступа к Карте-пропуску, а также параметры конфигурации считывателя и профилей пропусков, которые создает администратор СКУД.

Мастер-ключи для доступа к этой карте считывателю изначально не известны, они хранятся в карте-ключе и записываются в защищенную (только для записи) память считывателя в процессе его персонализации (конфигурирования).

Во время конфигурирования считывателя мастер-карта прикладывается к нему, и хранящиеся в ней ключи автоматически передаются в защищённую область памяти считывателя. Так как эта область предназначена только для записи, считать данные из неё невозможно, что обеспечивает безопасность ключей.

После записи мастер-ключей считыватель может распознавать и работать с картами-пропусками, защищёнными этими ключами. Это позволяет ограничить доступ только для тех карт, которые были выпущены с использованием нужных ключей, и исключает возможность использования посторонних или случайных карт.

Мастер-карта хранится у администратора СКУД и выдается работникам службы установки для конфигурации считывателя.

2.3 Карта-пропуск

Карта-пропуск предназначена для идентификации пользователя.

Считыватель при поднесении карты считывает идентификатор и передает его контроллеру по интерфейсу Wiegand, 1-Wire или OSDP.

Контроллер принимает решение об открытии двери в зависимости от наличия идентификатора в своей базе данных.

Идентификатор может быть открытый (UID карты) или закрытый (вычитываемый из защищённой области памяти карты).

Закрытый идентификатор создает администратор СКУД с помощью ключ-карты и мастер-карты.

2.4 Смартфоны с интерфейсами NFC и Bluetooth

В настоящий момент система поддерживает смартфоны на базе Android 4.4 и выше с поддержкой технологий бесконтактного обмена Near Field Communication (NFC) в режиме Host Card Emulation (HCE)* и Bluetooth Low Energy (BLE)**, а также смартфоны iPhone.

Смартфон может быть использован в качестве карты-пропуска: для этого в приложении для смартфонов реализован механизм "виртуальных карт".

Уникальный открытый идентификатор для виртуальных карт создается случайным образом и сохраняется в памяти смартфона.

Закрытый идентификатор может быть добавлен к виртуальной карте и сохраняется в памяти смартфона в зашифрованном виде.

Открытый или закрытый идентификаторы передаются по радиоканалу считывателю и далее - по интерфейсу Wiegand, 1-Wire или OSDP отправляются на контроллер (хост).

Для работы требуется установленное на смартфон специализированное приложение MicroEM Virtual Card.

* Интерфейс NFC (HCE - Host Card Emulation) поддерживают обе модельные линейки считывателей СКД: UEM Mifare/NFC SKD reader и UEM Mifare/NFC SKD BT reader.

** Интерфейс Bluetooth (BLE - Bluetooth Low Energy) поддерживает только модельная линейка UEM Mifare/NFC SKD BT reader.

3 Конфигурирование бесконтактных карт

В случае, если для хранения уникального идентификатора карты-пропуска система подразумевает использование ее защищенной области памяти, требуется предварительно сконфигурировать (изготовить) такие карты.

Если же в качестве идентификатора будет использоваться собственный публичный UID карты (согласно стандарта ISO14443A), то использование карт-ключей, мастер-карт и дополнительного программного обеспечения для их конфигурирования не обязательно, а настройки считывателей могут быть выполнены при помощи переключателей, согласно документации Wiegand-Installation-Guide.pdf, и раздел "Конфигурирование" можно проигнорировать.

Если возможность смены настроек считывателей при помощи переключателей не удобна, то можно использовать карты-ключи и мастер-карты без персонализации карт-пропусков.

Для изготовления карты-ключа подходят следующие типы карт:

- MIFARE Classic (EV1) объемом памяти не менее 1K
- MIFARE Ultralight C
- MIFARE Plus (EV1) объемом памяти не менее 1K

Для изготовления мастер-карты подходят следующие типы карт:

- MIFARE Classic (EV1) объемом памяти не менее 1K
- MIFARE Plus (EV1) объемом памяти не менее 1K

Для изготовления карты-пропусков подходят следующие типы карт:

- MIFARE Classic (EV1) любого объема памяти
- MIFARE Ultralight C
- MIFARE Plus (EV1) любого объема памяти

3.1 Считыватель настольный рабочего места администратора

Для конфигурирования карт администратором системы контроля доступа могут применяться настольные считыватели компании "МикроЭМ":

- UEM Mifare/ICode/NFC USB reader
- UEM Mifare/ICode/NFC RS reader
- UEM MifareNFC SKD reader (версии V4.0 и выше) в подчиненном режиме

Настольный считыватель подключается к персональному компьютеру (ноутбуку) посредством интерфейса USB/RS.

Управляется при помощи специализированного программного обеспечения рабочего места администратора СКУД (приложение WiegandTool.exe).

3.2 Конфигурирование

Приложение WiegandTool.exe предназначено для обслуживания смарт-карт системы контроля и управления доступом (СКУД), в которой уникальный идентификатор пропуска хранится в защищенной области памяти карты, а обмен данными осуществляется с помощью считывателей производства АО "МикроЭМ" UEM Mifare/ NFC SKD reader.

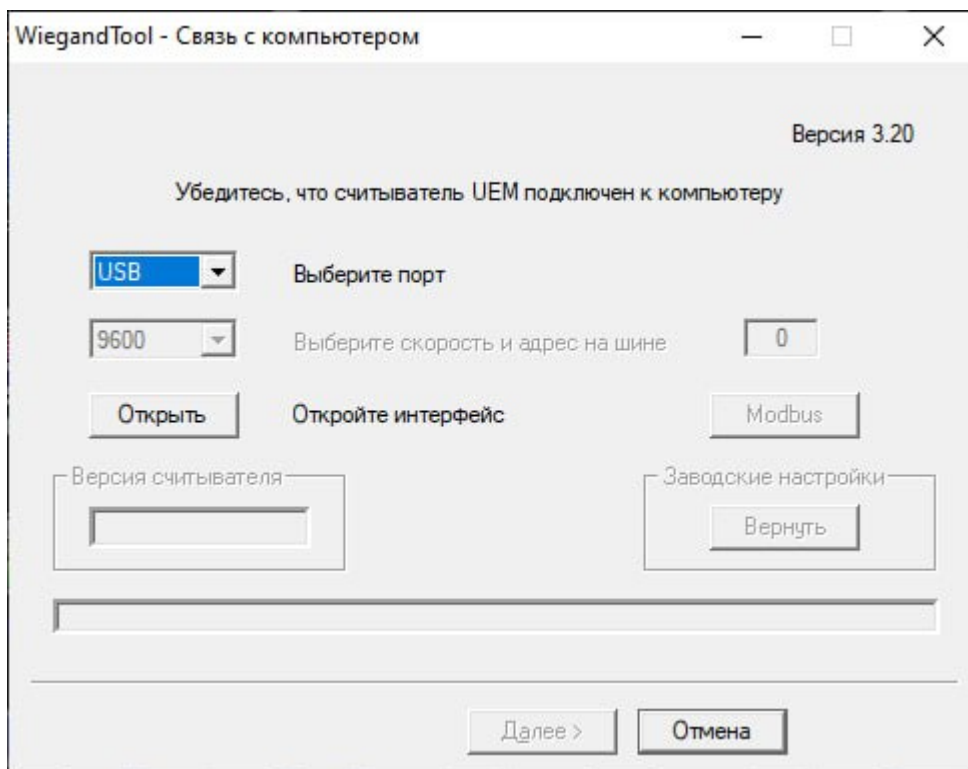
Для подготовки и обслуживания смарт-карт СКУД утилита поддерживает любые считыватели производства АО "МикроЭМ" (в том числе и UEM Mifare/NFC SKD reader) с версией микропрограммы 0x80 и выше.

Работа с утилитой построена в стиле слайд-шоу (мастера).

В любой момент работу с утилитой можно прервать, нажав кнопку "Отмена" или с помощью комбинации клавиш Alt-F4.

3.2.1 Подключение к считывателю

Внешний вид стартового окна утилиты приведен на рисунке ниже.



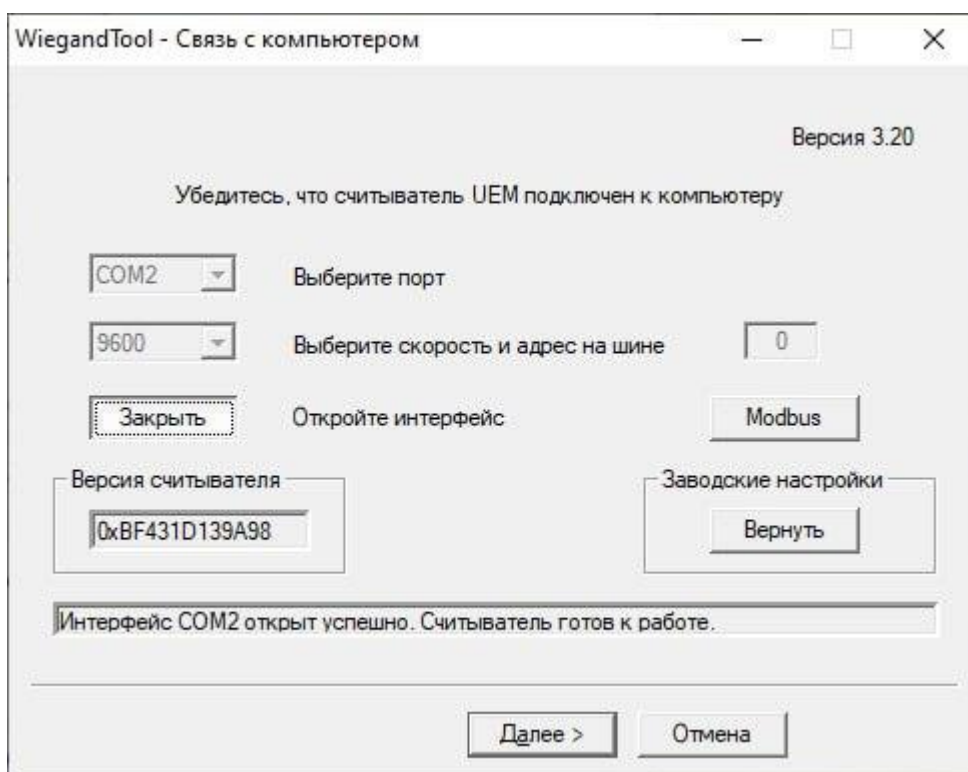
Здесь можно выбрать интерфейс, с помощью которого считыватель подключен к компьютеру. Это может быть USB или COM-порт (RS232 или RS485).

Для COM-порта выберите скорость обмена.

В случае интерфейса RS485 укажите ненулевой адрес на шине, если на ней более одного считывателя.

Нажмите кнопку "Открыть".

Если операция прошла без ошибок, внизу появится "Считыватель готов к работе".



Нажмите кнопку "Далее".

3.2.2 Работа с картой-ключом

Карта-ключ хранит ключи для доступа к мастер-карте.

Эта карта является основным ключом вашей системы доступа. При её утрате вы лишитесь возможности обновлять существующие и создавать новые мастер-карты. Вы также не сможете стереть ключи из СКД-считывателя без необходимости отправки устройства производителю.

WiegandTool - Карта-ключ

☒ Карта-ключ еще не изготовлена

☐ Карта-ключ уже имеется

Уберите со считывателя все карты и поместите чистую карту

Задайте ключи, вручную или с помощью [генератора](#)

Ключ для чтения

(ключ - это последовательность из 32 шестнадцатеричных цифр)

Ключ для записи

[Записать](#)

[< Назад](#) [Далее >](#) [Отмена](#)

3.2.2.1 Изготовление карты-ключа

WiegandTool - Карта-ключ

☒ Карта-ключ еще не изготовлена

☐ Карта-ключ уже имеется

Уберите со считывателя все карты и поместите чистую карту

Задайте ключи, вручную или с помощью [генератора](#)

Ключ для чтения

E896EFA95922ED0A699ACDD5060507F1

(ключ - это последовательность из 32 шестнадцатеричных цифр)

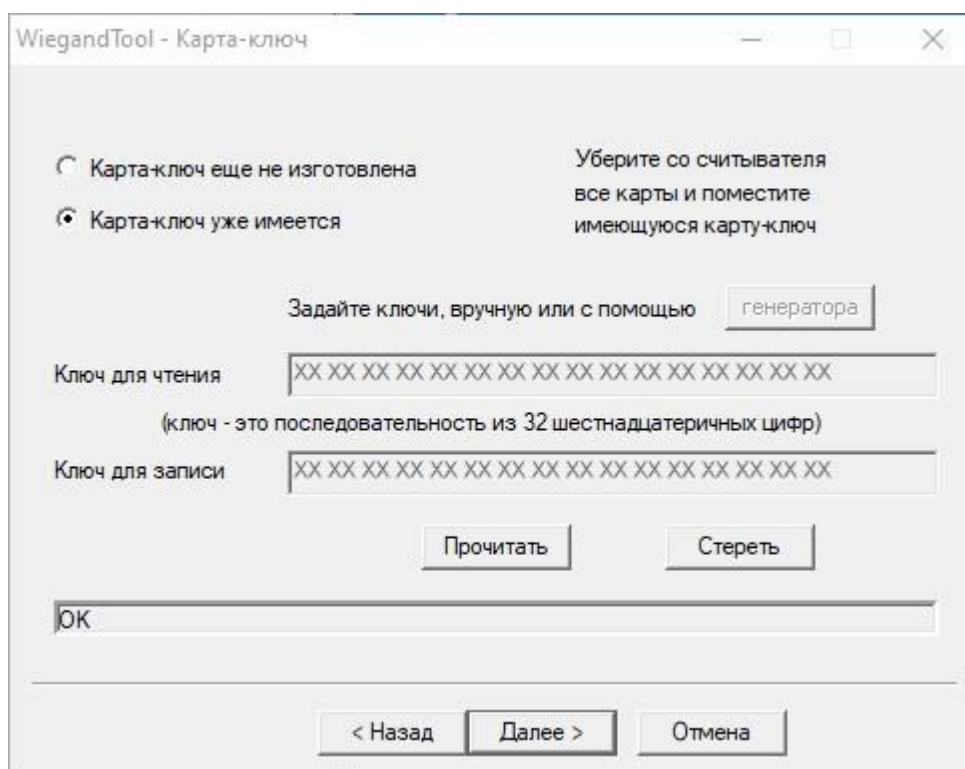
Ключ для записи

910E2DFD3407D67F762FDC3E0C30C7EC

[Записать](#)

[< Назад](#) [Далее >](#) [Отмена](#)

Если карта-ключ еще не изготовлена, необходимо:



Если операция прошла без ошибок, нажмите кнопку "Далее".

3.2.2.3 Стирание карты-ключа

Если требуется полностью очистить карту-ключ, то после ее чтения, нажмите на кнопку "Стереть".

Внимание! Данная операция приведет к утрате основного ключа вашей системы доступа, построенной на стираемой карте-ключе.

3.2.3 Работа с мастер-картой

Мастер-карта хранит ключи для доступа к картам-пропускам, а также настройки считывателя UEM Mifare NFC SKD reader и профилей пропусков.

В пределах одного профиля у всех карт-пропусков единые ключи доступа. В связи с этим дополнительные профили с новыми мастер-ключами могут быть созданы только с целью образования подгрупп доступа в организации. Допускается также копирование созданных мастер-карт с последующим изменением параметров - тогда копии можно будет использовать в отдельных подгруппах доступа.

Для работы с мастер-картой предварительно требуется использовать карту-ключ.

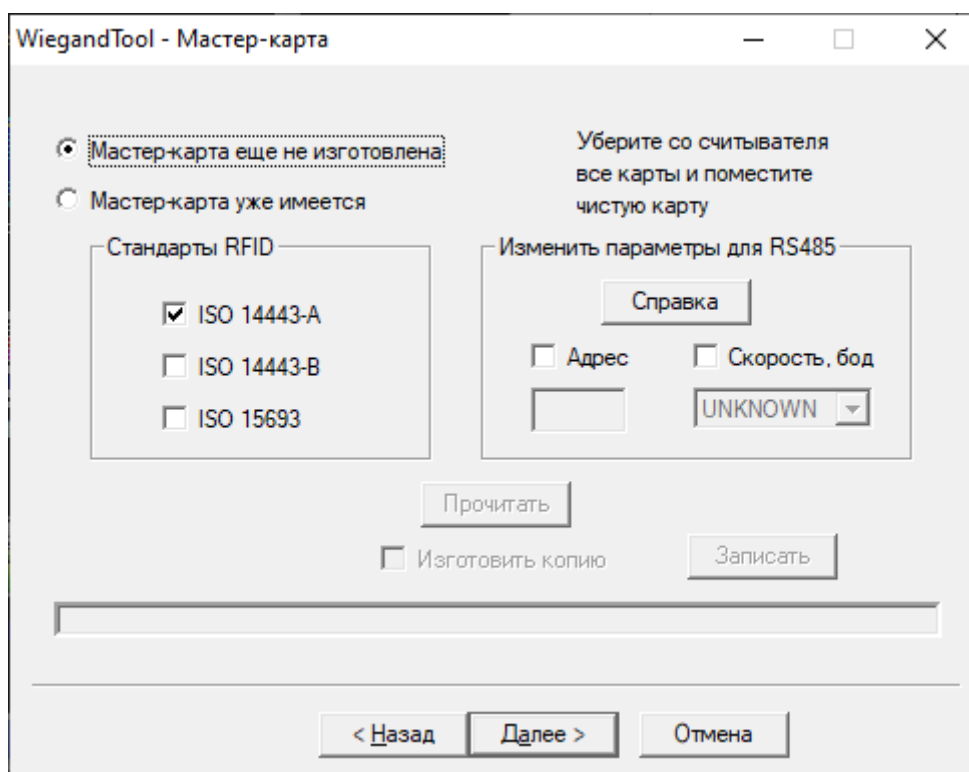
Если карты-ключа у вас нет, сперва ее нужно создать, выполнив действия из раздела "Изготовление карты-ключа".

Если карта-ключ у вас имеется, ее нужно прочесть, выполнив действия из раздела "Применение карты-ключа".

После выполнения этих действий уберите карту-ключ со считывателя.

Следующие четыре окна предназначены для работы с мастер-картой.

3.2.3.1 Изготовление мастер-карты



Если мастер-карта еще не изготовлена, необходимо:

- поместить на считыватель чистую карту типа MIFARE Plus или MIFARE Classic;
- установить стандарты карт, с которыми должны будут работать настраиваемые мастер-картой считыватели;
- при необходимости выбрать адрес и скорость (бод) и выбрать соответствующие галочки (если считыватель будет работать по RS-485). По умолчанию, считыватель работает на скорости 9600 и имеет адрес 0.
- после выбора необходимых настроек нажать «Записать»;
- нажать "Далее".

Замечание. Если установлена галочка «Адрес», то при первом прикладывании мастер-карты к считывателю будет выдан указанный адрес. При каждом последующем прикладывании этой карты адрес будет увеличиваться на 1,

независимо от того, к какому считывателю она приложена. Например, если указать адрес «1» и последовательно приложить карту к 10 разным считывателям, они получат адреса от 1 до 10. Если после этого снова приложить карту к первому считывателю, он получит уже следующий адрес — 11, а не 2.

Дальнейшие шаги описаны в разделе "Изменение настроек мастер-карты".

3.2.3.2 Применение мастер-карты

Если мастер-карта уже существует, необходимо:

- поместить ее на считыватель;
- нажать кнопку "Мастер-карта уже имеется";
- нажать кнопку "Прочитать".

WiegandTool - Мастер-карта

☐ Мастер-карта еще не изготовлена

☒ Мастер-карта уже имеется

Уберите со считывателя все карты и поместите имеющуюся мастер-карту

Стандарты RFID

- ☒ ISO 14443-A
- ☐ ISO 14443-B
- ☐ ISO 15693

Изменить параметры для RS485

Справка

☐ Адрес

☐ Скорость, бод

UNKNOWN

Прочитать

☐ Изготовить копию

Записать

< Назад Далее > Отмена

Если операция прошла без ошибок, внизу вы увидите «ОК».

Теперь можно при необходимости изменить настройки стандартов и типов карт, настройки адреса и скорости (бод), сохраненные в этой мастер-карте, изготовить копию карты или нажать кнопку "Далее" для уточнения параметров.

Дальнейшие шаги описаны в разделе "Изменение настроек мастер-карты" (или "Копирование мастер-карты", если также нужно изготовить ее копии).

3.2.3.3 Стирание мастер-карты

Если требуется полностью очистить мастер-карту, то после ее чтения нажмите на кнопку "Стереть".

Внимание! Данная операция приведет к утрате мастер-ключей вашей системы доступа, построенной на стираемой мастер-карте. После стирания ключей мастер-карты вы утратите возможность обновлять существующие и создавать новые карты-пропуска, если у вас нет дополнительных копий стираемой мастер-карты.

3.2.3.4 Копирование мастер-карты

Для копирования мастер-карты необходимо:

- пройти операции в пункте "Изготовление мастер-карты" или "Применение мастер-карты", если мастер-карта уже изготовлена;
- установить флаг "Изготовить копию";
- нажать кнопку "Записать".

Если операция прошла без ошибок, то в только что изготовленном дубликате мастер-карты можно изменить настройки. Для этого необходимо нажать на кнопку "Далее".

Дальнейшие шаги описаны в разделе "Изменение настроек мастер-карты".

3.2.3.5 Изменение настроек мастер-карты

Перед изменением настроек мастер-карту нужно создать согласно разделу "Изготовление мастер-карты", либо применить уже созданную, согласно разделу "Применение мастер-карты".

Следующее окно предназначено для изменения параметров интерфейса передачи идентификатора.

Для интерфейса Wiegand возможен выбор из популярных вариантов: Wiegand-26, 33, 34, 37, 40, 42 или 58.

Кроме того, предоставлена возможность реализовать свой собственный вариант, задавая такие параметры, как количество битов данных, наличие и тип битов четности, период сигнала и длительность импульса.

У интерфейса 1-Wire (по-другому он еще называется "Touch memory" или Dallas) все параметры фиксированы.

При выборе OSDP, имеется возможность выбрать галочки «повторять идентификатор, пока приложена карта». Если галочка не выбрана, то считыватель отправит идентификатор один раз. Чтобы отправить идентификатор второй раз, необходимо убрать карту со считывателя и приложить снова.

Примечание. Настройка может быть полезна для различных конфигураций контроллеров, которые могут реагировать на длительность прикладывания карты.

В следующем окне уточняются параметры индикации, блютуза и задержки.

Считыватель снабжен двумя светодиодами (красным и зеленым) и звукоизлучателем.

Если контроллер СКУД имеет возможность управлять этими средствами, то необходимо задать уровень сигнала (низкий или высокий), которым включается то или иное средство индикации.

Кроме того, надо уточнить, для каких средств индикации включено автоматическое сопровождение прикладывания карты к считывателю.

В группе управления "Блютуз" задаются идентификатор (ID) инфраструктуры, символьное имя считывателя, мощность передатчика Bluetooth.

ID инфраструктуры используется для того, чтобы приложения на смартфонах могли подобрать нужную виртуальную карту для работы с конкретным считывателем, он генерируется на основе главного ключа, хранящегося в ключ-карте. Однако вы можете задать свой идентификатор в формате HEX, 4 байта.

Мощность передатчика Bluetooth в считывателе может быть установлена вручную в диапазоне от -40 дБм (наименьшая мощность, самое короткое расстояние срабатывания приложения на смартфонах, примерно 10-30 см.) до 4 дБм (наибольшая мощность, позволяющая активировать считыватель на максимальном расстоянии в несколько метров, зависящем также от модели смартфона). Установка

мощности считывателей позволяет конфигурировать их либо для контроля доступа к двери в помещение, либо для проезда транспорта через ворота.

Имя считывателя позволяет идентифицировать считыватель в приложении на смартфонах, что нужно как для ручной, так и для автоматической активации считывателя смартфоном и может применяться совместно с активацией считывателей по идентификатору инфраструктуры. Длина Имени считывателя не должна превышать 18 символов. Пауза после обнаружения карты Mifare Plus ребуется для запитывания карты энергией.

Далее открывается окно для работы с профилями.

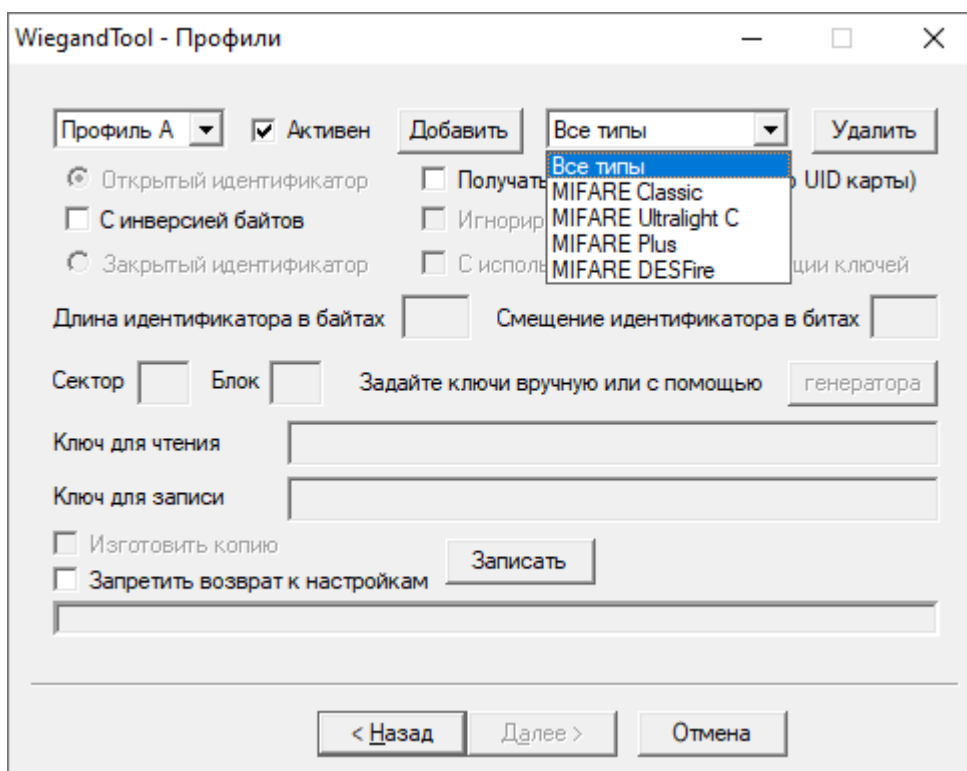
В новом окне можно задать до 12 профилей, которые представляют собой различные конфигурации способов получения уникального идентификатора из карты пропуска.

При поднесении карты-пропуска, СКД-считыватель перебирает запрограммированные в нем профили до тех пор, пока с одним из них карточка не аутентифицируется успешно и не вернет свой уникальный номер.

Допустимо использование только одного профиля с открытым идентификатором.

При создании мастер-карты, в ней автоматически прописывается всего один профиль - открытый идентификатор. Этот профиль позволяет вычитывать заводские уникальные идентификаторы чипов бесконтактных карт для любого типа карт.

Чтобы задать конкретный тип карты, используйте выкидной список с перечнем поддерживаемых типов.



Если вы при автономном режиме работы считывателя используете открытый идентификатор (открытый режим), то вы можете выбрать опцию получения идентификатора на основе EMV. Если эта опция активна, то при поднесении к считывателю смартфона с включенным NFC или банковской карты, считыватель будет создавать уникальный открытый идентификатор (UID) карты/смартфона на основании статических уникальных данных карты/смартфона в поле, которые считыватель получит автоматически. И только при неудачной попытке такого считывания, будет использоваться обычный открытый идентификатор согласно используемому протоколу. *На начало 2021 года это единственная возможность использовать iPhone в качестве NFC пропуска, без нашего мобильного приложения, использующего на iPhone только Bluetooth.* Важно: полученный таким образом открытый идентификатор не несет в себе никаких персональных, в том числе платежных, данных пользователя системы: идентификатор обезличивается программно, а считыватель и система в целом не сохраняют и не передают такие данные. Тем не менее, если вы планируете использовать данный метод создания открытого идентификатора в своей системе доступа, то вы как организатор/владелец системы доступа обязаны предварительно получить согласие всех ее пользователей на обработку их персональной информации, поскольку считыватель будет обращаться к системным приложениям на картах/

смартфонах, но только для чтения статической информации, находящейся там в открытом доступе: никаких финансовых операций, никаких операций записи/изменений в банковских картах или платежных приложениях на смартфонах считыватель самостоятельно не выполняет.

Профили можно добавлять (до 12 штук) при помощи кнопки "Добавить". При этом новый профиль получит свободную латинскую букву обозначения и будет добавлен в конец выкидного списка.

Если вы добавите профиль с использованием закрытого (защищенного) идентификатора/режима, то для такого вида профиля нужно будет задать номер сектора и блока карты-пропуска для хранения уникального идентификатора пропуска, тип используемой карты, а также ключи доступа к сектору.

Инверсия байтов означает, что байты идентификатора будут передаваться в обратном порядке, сохраняя порядок передачи битов для выбранного интерфейса.

Для карт Ultralight C абсолютный номер блока переводится в адрес следующим образом:

$$Mf_UL_Page = (AbsBlockNo \% 9 + 1) << 2.$$

Кроме того, в настройках профиля вы можете выбрать, диверсифицировать или нет ключи карт-пропусков. Если выбрана диверсификация, то ключи доступа к секторам карт-пропусков будут разными для каждой отдельной карты-пропуска, и будут вычисляться на основании общего мастер-ключа и уникальных открытых идентификаторов пропусков.

Для удаления предварительно выберите ненужный профиль в выкидном списке, например, Профиль А.

The screenshot shows the 'WiegandTool - Профили' window. At the top, 'Профиль А' is selected in a dropdown menu. Below it, 'Профиль А' is highlighted in a list. The 'Активен' checkbox is checked. To the right are 'Добавить' and 'Удалить' buttons. Further right is a dropdown menu set to 'Все типы'. Below these are several checkboxes: 'Получать на основе EMV (вместо UID карты)', 'Игнорировать младший байт', 'С инверсией байтов', 'Закрывать идентификатор', and 'С использованием диверсификации ключей'. There are also input fields for 'Длина идентификатора в байтах' and 'Смещение идентификатора в битах'. Below these are 'Сектор' and 'Блок' input fields, and a button 'Задайте ключи вручную или с помощью генератора'. There are two text input fields for 'Ключ для чтения' and 'Ключ для записи'. At the bottom are checkboxes for 'Изготовить копию' and 'Запретить возврат к настройкам', and a 'Записать' button. At the very bottom are navigation buttons: '< Назад', 'Далее >', and 'Отмена'.

Нажмите «Удалить» и убедитесь, что теперь Профиль А в списке отсутствует.

The screenshot shows the 'WiegandTool - Профили' window after Profile A has been removed. 'Профиль В' is now selected in the dropdown menu and highlighted in the list. The 'Активен' checkbox is checked. The 'Удалить' button is still present. The dropdown menu now shows 'MIFARE Plus'. The checkboxes for 'Получать на основе EMV (вместо UID карты)', 'Игнорировать младший байт', 'С инверсией байтов', 'Закрывать идентификатор', and 'С использованием диверсификации ключей' are still there. The input fields for 'Длина идентификатора в байтах' (now 7) and 'Смещение идентификатора в битах' (now 0) are updated. The 'Сектор' and 'Блок' input fields are now 1 and 2 respectively. The 'Задайте ключи вручную или с помощью генератора' button is still there. The 'Ключ для чтения' and 'Ключ для записи' text input fields now contain hexadecimal values: '8A A1 4A 30 CD 3A 9C 28 5A 6F A1 6E D1 75 8A F8' and '99 26 9F 86 C7 51 3C 91 42 55 1A 7E 24 EE D0 18'. The 'Изготовить копию' and 'Запретить возврат к настройкам' checkboxes are still there, along with the 'Записать' button. The navigation buttons at the bottom are the same: '< Назад', 'Далее >', and 'Отмена'.

Если все настройки заданы, а ненужные профили удалены, нажмите кнопку "Записать".

Общие параметры, а также обновленный список профилей доступа к картам-пропускам будут сохранены в мастер-карту.

При последующем нажатии на кнопку "Далее" откроется окно работы с картами-пропусками для профиля, выбранного в выкидном списке в окне Профили.

WiegandTool - Карта-пропуск

Профиль В

☒ Изготовить новый пропуск ☐ Прочитать/Изменить ☐ Работа со смартфонами при помощи QR-кодов

Прочитать

Карты и смартфоны с NFC
Уберите со считывателя все карты и поместите чистую карту или смартфон

Задайте идентификатор, вручную или с помощью генератора

Integrated code (LSB) Facility code Card number (MSB)

00 00 00 00 00 00 00 Hex 00 000000000000

0 Dec 0 0

☐ Авто- ☐ Инкремент Записать Стереть

< Назад Далее > Отмена

3.2.4 Работа с картой-пропуском

Карта-пропуск используется при непосредственном проходе через двери.

В качестве карты-пропуска также может быть использован смартфон, поддерживающий технологию NFC HCE (эмуляция карт NFC), либо BLE (Bluetooth Low Energy)

Для работы с картой-пропуском предварительно требуется прочитать карту-ключ и мастер-карту, последовательно пройдя все предыдущие окна, даже не производя в них никаких изменений.

Если карты-ключа у вас нет, сперва ее нужно создать, выполнив действия из раздела "Изготовление карты-ключа".

Если мастер-карты у вас нет, сперва ее нужно создать, выполнив действия из раздела "Изготовление мастер-карты".

Перед началом работы с пропусками уберите мастер-карту со считывателя.

Здесь можно изготовить бесконтактную карту-пропуск, либо виртуальную карту-пропуск на смартфоне, а также прочитать или изменить идентификатор в уже имеющейся карте-пропуске.

Если в предыдущем окне был выбран профиль с открытым идентификатором, то идентификатор можно лишь прочитать.

3.2.4.1 Пропуска в виде бесконтактных карт

3.2.4.1.1 Изготовление карты-пропуска

Для изготовления карты-пропуска на основе карт типа MIFARE Plus и MIFARE Classic допускается использование бывшей в употреблении карты со свободным сектором, имеющим ключи по умолчанию (все единицы), при этом единственное ограничение - все карты-пропуска в данном профиле должны иметь один и тот же номер сектора для хранения уникального идентификатора.

Ограничения в использовании б/у карт MIFARE Plus SL3 и MIFARE Classic:

- необходимо наличие свободного сектора с единичными ключами и чтением/записью по ключу A;
- номер свободного сектора должен совпадать с номером сектора в данном профиле.

Дополнительно для карт MIFARE Plus в SL3:

- после перевода карты в T=CL аутентификация используемого сектора должна быть доступна без каких-либо дополнительных операций.

Дополнительно для карт MIFARE Plus EV1:

- карта должна иметь ATS, где T0 = 0x78.

Для изготовления карты-пропуска с UID, хранящимся в защищенной области памяти карты:

- поместите на считыватель чистую карту типа MIFARE Plus, MIFARE Ultralight C или MIFARE Classic; выберите пункт "Изготовить новый пропуск";
- убедитесь, что галочка "Работа со смартфонами при помощи QR-кодов" НЕ установлена;
- в поле "Integrated code" слева от слова "Hex" укажите уникальный идентификатор карты в формате HEX:

- для Wiegand-26: 3 байта;
- для Wiegand-33: 4 байта;
- для Wiegand-34: 4 байта;
- для Wiegand-37: 5 байт;
- для Wiegand-40: 5 байт;
- для Wiegand-42: 5 байт;
- для Wiegand-58: 7 байт;
- для 1-Wire: 6 байт.

Вы также можете задать идентификатор путем вписывания по отдельности значений Facility Code (код подразделения) и Card number (номер карты).

Как альтернатива, вы можете задать значения полей в десятичном формате, воспользовавшись дублирующими полями ввода, расположенными под полями ввода значения в шестнадцатеричном формате Hex.

Можно разово увеличить значение на 1 при помощи кнопки "Инкремент", либо увеличивать автоматически при помощи галочки "Авто".

- нажмите на кнопку "Записать".

3.2.4.1.2 Чтение и изменение настроек карты-пропуска

Для чтения идентификатора карты-пропуска с UID, хранящимся в открытой или защищенной области памяти карты: поместите на считыватель карту-пропуск;

- выберите пункт "Прочитать/Изменить";
- убедитесь, что галочка "Работа со смартфонами при помощи QR-кодов" НЕ установлена;
- нажмите на кнопку "Прочитать".

WiegandTool - Карта-пропуск

Профиль В

☐ Изготовить новый пропуск ☒ Прочитать/Изменить ☐ Работа со смартфонами при помощи QR-кодов

Прочитать

Карты и смартфоны с NFC
Уберите со считывателя все карты и поместите карту-пропуск или смартфон

Задайте идентификатор, вручную или с помощью генератора

Integrated code (LSB)	Facility code	Card number (MSB)
Hex 00	Hex 00	000000000000
Dec 0	Dec 0	0

☐ Авто-

< Назад Далее > Отмена

Для изменения идентификатора карты-пропуска с UID, хранящимся в защищенной области памяти карты:

- поместите на считыватель карту-пропуск;

- выберите пункт "Прочитать/Изменить";
- убедитесь, что галочка "Работа со смартфонами при помощи QR-кодов" НЕ установлена; нажмите на кнопку "Прочитать";
- измените уникальный идентификатор карты (можно разово увеличить значение на 1 при помощи кнопки "Инкремент", либо увеличивать автоматически при помощи галочки "Авто");
- нажмите на кнопку "Записать".

3.2.4.2 Пропуска в виде виртуальных карт на смартфонах с интерфейсом NFC

Для работы в качестве бесконтактного пропуска в системе, на Android-смартфоне через функцию NFC:

- 1) должно быть установлено специализированное приложение по ссылке (в разделе программного обеспечения):

<https://www.uemdesign.ru/>

- 2) в настройках смартфона должен быть активирован модуль NFC.

3.2.4.2.1 Изготовление виртуальной карты-пропуска

С точки зрения работы с приложением WiegandTool процедура изготовления виртуальной карты-пропуска на смартфоне, в случае применения технологии NFC, аналогична процедуре изготовления бесконтактной карты-пропуска:

WiegandTool - Карта-пропуск

Профиль В

☒ Изготовить новый пропуск ☐ Прочитать/Изменить ☐ Работа со смартфонами при помощи QR-кодов

Прочитать

Карты и смартфоны с NFC
Уберите со считывателя все карты и поместите чистую карту или смартфон

генератора

Задайте идентификатор, вручную или с помощью

Integrated code (LSB)	Facility code	Card number (MSB)
90 91 92 93 94 95 96	Hex 25	96959493929190
42385711870153104	Dec 37	42385711870153104

☐ Авто ☐ Инкремент

ОК

< Назад Далее > Отмена

Для изготовления защищенного идентификатора виртуальной карты пропуска:

- создайте новую виртуальную карту или выберите уже существующую виртуальную карту в настройках приложения MicroEM Virtual Card на смартфоне;
- положите смартфон на считыватель; в WiegandTool выберите пункт
- "Изготовить новый пропуск";
- убедитесь, что галочка "Работа со смартфонами при помощи QR-кодов" НЕ установлена;
- в поле "Integrated code" слева от слова "Hex" укажите уникальный идентификатор карты в формате HEX:
 - для Wiegand-26: 3 байта;
 - для Wiegand-33: 4 байта;
 - для Wiegand-34: 4 байта;
 - для Wiegand-37: 5 байт;
 - для Wiegand-40: 5 байт;
 - для Wiegand-42: 5 байт;
 - для Wiegand-58: 7 байт;
 - для 1-Wire: 6 байт.

Вы также можете задать идентификатор путем вписывания по отдельности значений Facility Code (код подразделения) и Card number (номер карты).

Как альтернатива, вы можете задать значения полей в десятичном формате, воспользовавшись дублирующими полями ввода, расположенными под полями ввода значения в шестнадцатеричном формате Hex.

Можно разово увеличить значение на 1 при помощи кнопки "Инкремент", либо увеличивать автоматически при помощи галочки "Авто".

- нажмите на кнопку "Записать".

3.2.4.2.2 Чтение и изменение настроек виртуальной карты-пропуска

С точки зрения работы с приложением WiegandTool процедура чтения виртуальной карты-пропуска на смартфоне и изменения ее идентификатора, в случае применения технологии NFC, аналогична процедуре чтения и изменения бесконтактной карты-пропуска.

Для чтения от крыт ого или защищенного идентификатора виртуальной карт ы-пропуска:

- выберите уже существующую виртуальную карту в настройках приложения MicroEM Virtual Card на смартфоне;
- если считывается открытый идентификатор со смартфона на базе Андроид, установите в приложении смартфона на главной странице галочку "Однократно передать открытый идентификатор";
- поместите на считыватель смартфон;
- выберите пункт "Прочитать/Изменить";
- убедитесь, что галочка "Работа со смартфонами при помощи QR-кодов" НЕ установлена;
- нажмите на кнопку "Прочитать".

WiegandTool - Карта-пропуск

Профиль В

☐ Изготовить новый пропуск

☒ Прочитать/Изменить

☐ Работа со смартфонами при помощи QR-кодов

Прочитать

Карты и смартфоны с NFC
Уберите со считывателя все карты и поместите карту-пропуск или смартфон

Задайте идентификатор, вручную или с помощью генератора

Integrated code (LSB)

Facility code

Card number (MSB)

Hex 00

Dec 0

0

000000000000

0

0

☐ Авто-Инкремент

Записать

Стереть

ОК

< Назад

Далее >

Отмена

В ячейках должны появиться прочитанные данные. Пример ниже.

Для изменения защищенного идентификатора виртуальной карты-пропуска:

- выполните последовательность действий при чтении защищенного идентификатора виртуальной карты-пропуска, описанную выше;
- измените уникальный идентификатор карты (можно разово увеличить значение на 1 при помощи кнопки "Инкремент", либо увеличивать автоматически при помощи галочки "Авто");
- нажмите на кнопку "Записать".

3.2.4.3 Пропуска в виде виртуальных карт на смартфонах с интерфейсом Bluetooth

Для работы в качестве бесконтактного пропуска в системе, на Android-смартфоне посредством Bluetooth:

- 1) должно быть установлено специализированное приложение по ссылке (в разделе программного обеспечения):
<https://www.uemdesign.ru/>
- 2) в настройках должен быть активирован модуль Bluetooth.

3.2.4.3.1 Изготовление виртуальной карты-пропуска

С точки зрения работы с приложением WiegandTool процедура изготовления виртуальной карты-пропуска на смартфоне, в случае применения технологии Bluetooth, аналогична процедуре изготовления бесконтактной карты-пропуска, однако передача информации от WiegandTool в приложение на смартфоне осуществляется при помощи графических QR-кодов.

Для изготовления виртуальной карты-пропуска с защищенным идентификатором:

- создайте новую виртуальную карту или выберите уже существующую виртуальную карту в списке карт в настройках приложения MicroEM Virtual Card на смартфоне;
- откройте настройки виртуальной карты на смартфоне, перейдите по ссылке "Добавить/изменить защищенный идентификатор";
- при необходимости разрешите приложению на смартфоне пользоваться камерой; в WiegandTool выберите пункт "Изготовить новый пропуск";
- убедитесь, что галочка "Работа со смартфонами при помощи QR-кодов" установлена;
- в поле "Integrated code" слева от слова "Hex" укажите уникальный идентификатор карты в формате HEX:

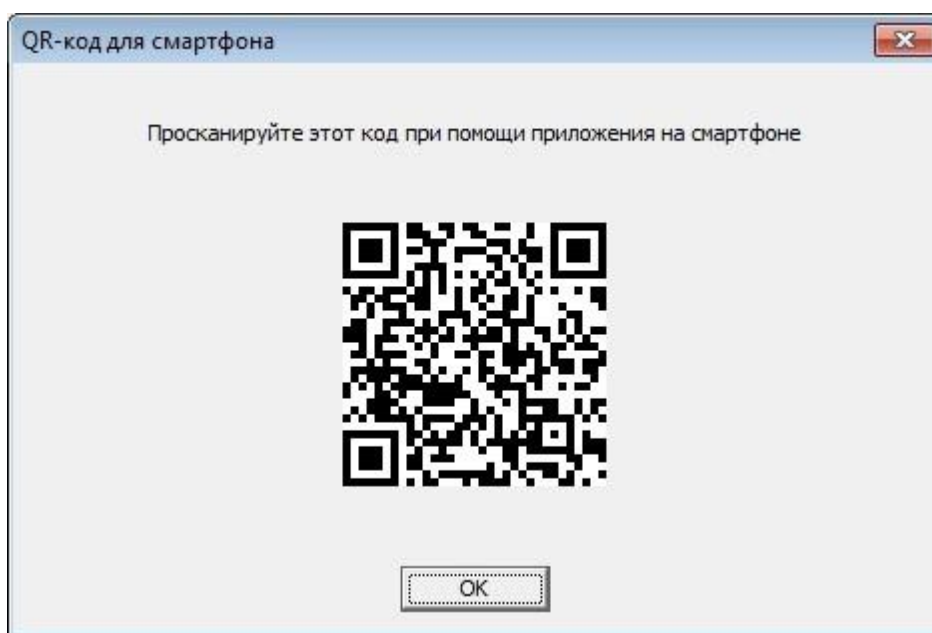
- для Wiegand-26: 3 байта;
- для Wiegand-33: 4 байта;
- для Wiegand-34: 4 байта;
- для Wiegand-37: 5 байт;
- для Wiegand-40: 5 байт;
- для Wiegand-42: 5 байт;
- для Wiegand-58: 7 байт;
- для 1-Wire: 6 байт.

Вы также можете задать идентификатор путем вписывания по отдельности значений Facility Code (код подразделения) и Card number (номер карты).

Как альтернатива, вы можете задать значения полей в десятичном формате, воспользовавшись дублирующими полями ввода, расположенными под полями ввода значения в шестнадцатеричном формате Hex.

Можно разово увеличить значение на 1 при помощи кнопки "Инкремент", либо увеличивать автоматически при помощи галочки "Авто".

- нажмите на кнопку "Записать";



- в открывшемся окне нажмите на кнопку "Нажмите и прочитайте QR-код справа", подождите, пока на диалоговом окне появится код; поднесите смартфон к экрану ПК и просканируйте QR-код;
- при успешном прохождении процедуры приложение на смартфоне уведомит вас об этом, и вы можете закрыть диалоговое окно с кодом в WiegandTool;

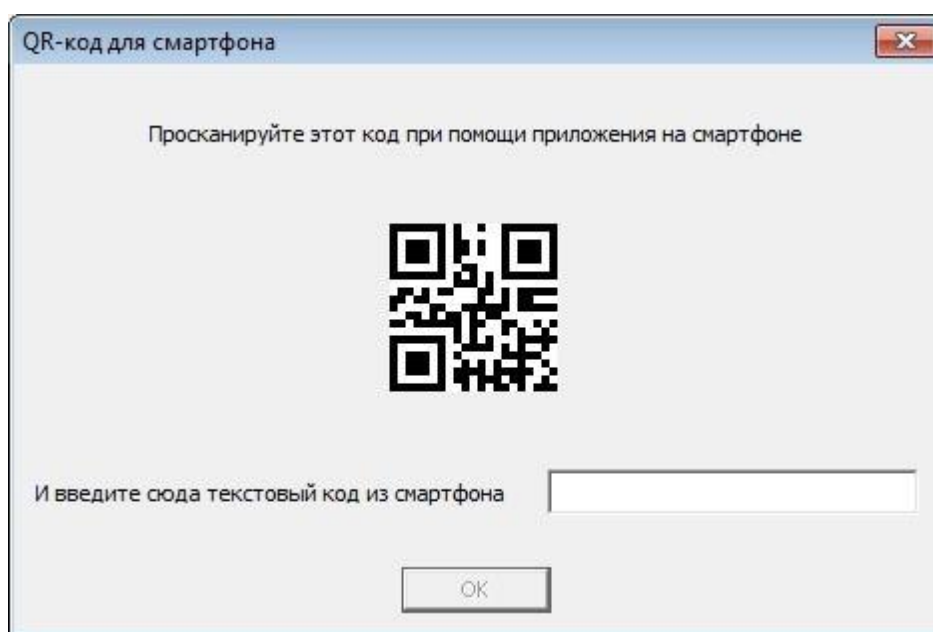
- при ошибке вы можете повторить попытку считывания кода или прекратить процедуру на смартфоне, вернувшись в настройки виртуальной карты.

3.2.4.3.2 Чтение и изменение настроек виртуальной карты-пропуска

С точки зрения работы с приложением WiegandTool процедура чтения защищенного идентификатора виртуальной карты-пропуска на смартфоне и его изменения, в случае применения технологии Bluetooth, аналогична процедуре чтения и изменения бесконтактной карты-пропуска, однако передача информации от WiegandTool в приложение на смартфоне осуществляется при помощи графических QR-кодов, а в обратную сторону - путем копирования специальной символьной строки.

Для чтения защищенного идентификатора виртуальной карты-пропуска:

- выберите уже существующую виртуальную карту в списке карт в настройках приложения MicroEM Virtual Card на смартфоне;
- откройте настройки виртуальной карты на смартфоне, перейдите по ссылке "Добавить/изменить защищенный идентификатор"; при необходимости разрешите приложению на смартфоне пользоваться камерой; в WiegandTool выберите пункт "Прочитать/Изменить";
- убедитесь, что галочка "Работа со смартфонами при помощи QR-кодов" установлена;
- нажмите на кнопку "Прочитать".



- поднесите смартфон к экрану ПК и просканируйте QR-код;
-

при ошибке вы можете повторить попытку считывания кода или прекратить процедуру на смартфоне и в программе, вернувшись в настройки виртуальной карты.

- при успешном прохождении процедуры приложение на смартфоне уведомит вас об этом и отобразит символьную строку;
- скопируйте эту строку в поле ввода WiegandTool; вы можете копировать визуально, либо воспользоваться средствами электронной связи между устройствами; при успешной проверке кода программой WiegandTool, активируется кнопка "OK";
- после этого вы можете нажать на "OK" и закрыть диалоговое окно с кодом в WiegandTool;
- прочитанный из приложения на смартфоне защищенный идентификатор виртуальной карты отобразится в WiegandTool.

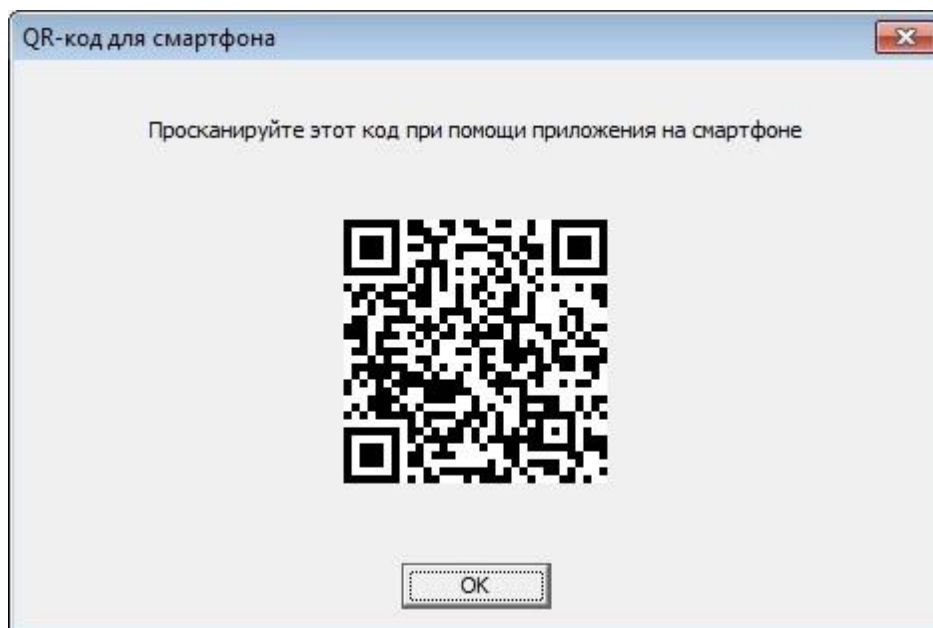
Для изменения защищенного идентификатора виртуальной карты-пропуска:

- выполните последовательность действий при чтении защищенного идентификатора виртуальной карты-пропуска, описанную выше;
- в поле "Integrated code" слева от слова "Hex" измените уникальный идентификатор карты в формате HEX:
 - для Wiegand-26: 3 байта;
 - для Wiegand-33: 4 байта;
 - для Wiegand-34: 4 байта;
 - для Wiegand-37: 5 байт;
 - для Wiegand-40: 5 байт;
 - для Wiegand-42: 5 байт;
 - для Wiegand-58: 7 байт;
 - для 1-Wire: 6 байт.

Вы также можете задать идентификатор путем вписывания по отдельности значений Facility Code (код подразделения) и Card number (номер карты).

Как альтернатива, вы можете задать значения полей в десятичном формате, воспользовавшись дублирующими полями ввода, расположенными под полями ввода значения в шестнадцатеричном формате Hex.

- нажмите на кнопку "Записать";

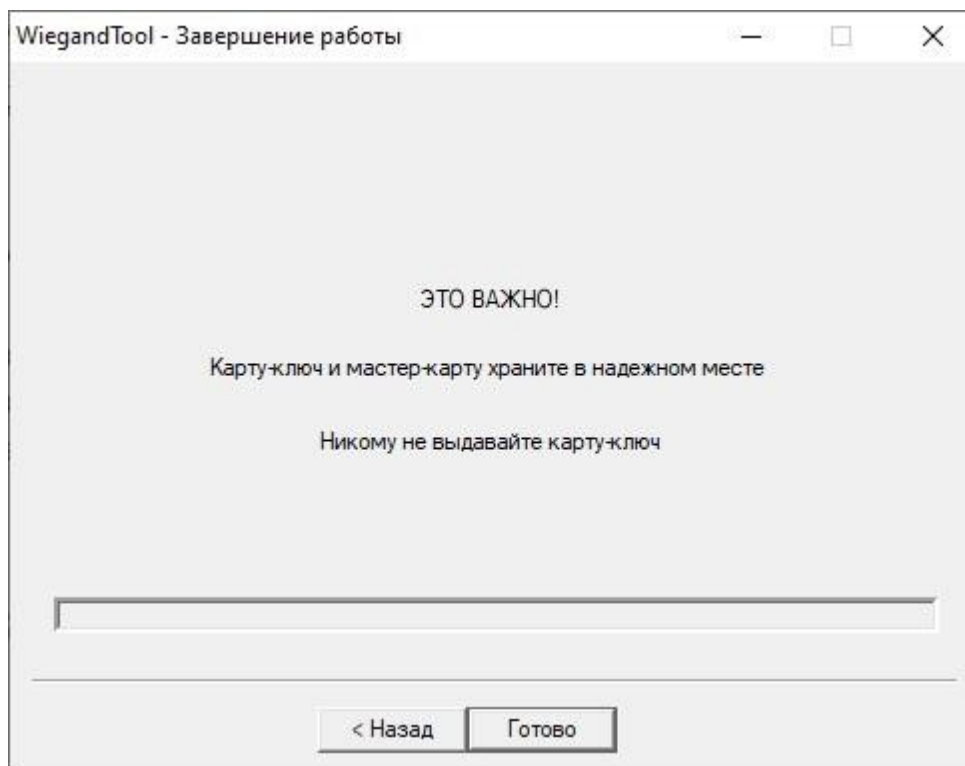


- поднесите смартфон к экрану ПК и просканируйте QR-код; при успешном
- прохождении процедуры приложение на смартфоне уведомит вас об этом, и вы можете закрыть диалоговое окно с кодом в WiegandTool;
- при ошибке вы можете повторить попытку считывания кода или прекратить процедуру на смартфоне, вернувшись в настройки виртуальной карты.

3.2.5 Завершение работы с программой

Вы можете выполнять операции по работе с картами-пропусками столько раз, сколько понадобится: пока приложение запущено, оно "помнит" необходимые настройки, вычитанные из ключ- и мастер-карт.

При необходимости приложение можно закрыть, нажав на "крестик" в правом верхнем углу. Также вы можете при помощи кнопок "Далее" дойти до конца программы и завершить ее там, нажав "Готово":



4 Доступ по картам-пропускам и смартфонам

Для доступа по карте-пропуску, поднесите карту к считывателю, дождитесь звукового сигнала.

В зависимости от выбранного интерфейса (1-Wire или Wiegand), при успешном считывании карты-пропуска или смартфона, идентификатор будет отсылаться по соответствующему интерфейсу.

Для доступа по смарт фону Android:

- 1) активируйте на смартфоне в настройках модуль NFC, либо Bluetooth (в зависимости от предпочитаемого вами интерфейса активации считывателей);
- 2) запустите приложение Virtual Card MicroEM, убедитесь, что в настройках приложения включен нужный вам интерфейс, и приложению дано разрешение на использование этого интерфейса;
- 3) при использовании интерфейса NFC, поднесите смартфон к считывателю, дождитесь звукового сигнала считывателя;
- 4) при использовании интерфейса Bluetooth, поднесите смартфон к считывателю, убедитесь, что считыватель появился в списке на главной странице приложения, нажмите на кнопку "Активировать", дождитесь звукового сигнала считывателя;

- 5) в целях экономии энергии, при желании деактивируйте модуль NFC или Bluetooth в смартфоне;
- 6) более подробную инструкцию по работе с приложением на смартфоне читайте в документе Wiegand - Mobile.pdf

Для получения максимального расстояния считывания бесконтактных карт или при использовании интерфейса NFC на смартфоне, подносите карту следующим образом: держите карту параллельно к поверхности считывателя, придвигайте карту медленно по направлению к считывателю до тех пор, пока не появится световая и/или звуковая индикация. Чтобы прочесть карту еще раз необходимо убрать ее из поля считывателя и поднести снова.

Для доступа по смартфону iPhone:

- 1) запустите приложение Virtual Card MicroEM;
- 2) поднесите смартфон к считывателю, убедитесь, что считыватель появился в списке на главной странице приложения, нажмите на кнопку "Активировать", дождитесь звукового сигнала считывателя;
- 3) в целях экономии энергии, при желании деактивируйте модуль Bluetooth в смартфоне;
- 4) более подробную инструкцию по работе с приложением на смартфоне читайте в документе Wiegand - Mobile.pdf

4.1 Вычитывание идентификатора по интерфейсу RS-485

Вычитать идентификатор можно тремя способами:

- протокол UEM;
- протокол Modbus;
- протокол OSDP.

4.1.1 Использование протокола UEM

Дополнительно прочесть последний считанный идентификатор можно по интерфейсу RS-485 в течение 3 секунд, по истечении которых он будет удален из памяти считывателя. Для этого нужно отправить команду 58 98 01 по нашему протоколу, описанному в документации на настольные считыватели на сайте производителя. Ответ на команду придет также в соответствии с протоколом, описанным в документации. Краткое описание команды:

// Запрос 0x58 0x98 0x01

```
// Ответ: ACK[1], TotalSize[1], Standard[1], ID[TotalSize-2] //
TotalSize[1] – Общая длина элемента (включая TotalSize)
//   Standard[1] :
//           0x01 - ISO14443A
//           0x02 - ISO14443B
//           0x04 - ISO15693
//           0x10 - EMV
//           0x20 - Bluetooth
//           0x40 - Защищенный режим
//           0x80 - Смартфон
```

Примеры:

Mifare 4 byte UID

58 98 01

00 06 01 94 C8 A6 03

Mifare 7 byte UID

58 98 01

00 09 01 04 82 6F F2 04 3E 80

ISO14443B

58 98 01

00 06 02 6F 33 24 02

4.1.2 Использование протокола MODBUS

Считыватель поддерживает стандартную команду протокола MODBUS RTU (интерфейс RS-485).

0x03 Read Holding Registers

Чтобы начать работать по протоколу Modbus, достаточно начать отправлять команды в соответствии с протоколом, где первый байт команды – адрес (из структуры команд протокола Modbus).

Конфигурация

При изготовлении считыватель получает адрес на шине RS485, равный 0, и производит обмен данными на скорости 9600 бод.

Есть возможность переключить скорость на 19200, 38400, 57600 или 115200 бод.

Для работы по протоколу MODBUS RTU адрес считывателя должен быть в пределах от 1 до 247.

Требуемые адрес и скорость устанавливаются с помощью микропереключателей (документ Wiegand-Installation-Guide.pdf).

4.1.3 Использование протокола OSDP

Считыватель поддерживает открытый и защищенный режимы протокола OSDP. Чтобы начать работать по протоколу OSDP, достаточно начать отправлять команды в соответствии с протоколом, где первый байт команды – 0x53 (из структуры команд протокола OSDP).

0x60 Poll Request (для получения идентификатора карты).

Конфигурация

При изготовлении считыватель получает адрес на шине RS485, равный 0, и производит обмен данными на скорости 9600 бод.

Есть возможность переключить скорость на 9600, 19200, 38400, 57600 или 115200 бод.

Для работы по протоколу OSDP адрес считывателя должен быть в пределах от 1 до 126.

Требуемые адрес и скорость устанавливаются с помощью микропереключателей (документ Wiegand-Installation-Guide.pdf).