

Инструкция по построению СКУД со считывателями Gate-Reader-MF и картами MIFARE Plus в защищенном режиме.

Общие принципы

Возможность клонирования идентификаторов в СКУД может приводить к случаям несанкционированного доступа, саботажа системы, искажению сведений учета рабочего времени. Кроме того, такая возможность не соответствует требованиям ряда законодательных актов по построению СКУД и обеспечению безопасности целого ряда государственных объектов.

Данная инструкция описывает построение СКУД с защитой идентификаторов от клонирования с применением карт MIFARE Plus. Надежность защиты гарантируется использованием надежного алгоритма шифрования AES с ключом 128 бит. Для реализации защищенного режима необходимо следующее:

- настольный считыватель Gate-USB-MF;
- дверные считыватели Gate-Reader-MF с поддержкой режима безопасности SL-3;
- карты или брелки MIFARE Plus (размер ID, 4 или 7 байт, не имеет значения).

В защищенном режиме в составе СКУД могут использоваться только те карты, и только те считыватели, которые были запрограммированы для работы на данном объекте. Причем защищенные области данных карт не подвержены вскрытию и копированию, а также невозможно считывание ключа и иных служебных данных из рабочего считывателя. При успешном опознании (совпадении ключа защиты) поднесенной карты (идентификатора) считыватель выдает в контроллер СКУД wiegand-код заданной длины, содержащий идентификационный код соответствующего пользователя. Существует два основных варианта (два режима) работы системы:

- а) в контроллер СКУД выдается уникальный идентификационный код пользователя, записанный в защищенный сектор карты при эмиссии;
- б) в контроллер СКУД выдается UID данной карты.

Эти режимы имеют отличия и особенности, как при построении системы, так и при ее эксплуатации. Данная Инструкция отражает работу в первом режиме а) с выдачей уникального идентификационного кода пользователя из защищенного блока. Этот режим считается предпочтительным. Особенности настройки и построения системы во втором режиме б) описаны в дополнительной инструкции на сайте skd-gate.ru

Для хранения уникального ключа защиты и иных специальных параметров защищенной системы объекта, а также для эмиссии рабочих карт объекта (карт пользователей системы), используется специальная Мастер-карта объекта. Для программирования считывателей идентификаторов используется Мастер-карта объекта и специальные карты Инициализации двух типов:

- карта Инициализации для Нового считывателя — для активации и подготовки к записи технологических и объектовых параметров Нового считывателя. Под термином Новый понимается считыватель с заводскими настройками. После программирования Нового считывателя он становится Рабочим для данной системы. Под термином Рабочий понимается считыватель, запрограммированный для работы в СКУД данного объекта.

- карта Инициализации для Рабочего считывателя - для активации и подготовки к изменению технологических и объектовых параметров Рабочего считывателя данной системы.

Таким образом, минимальный комплект служебных карт системы содержит две карты Инициализации (для Новых и для Рабочих считывателей) и Мастер-карту объекта. При необходимости можно создать несколько подобных комплектов карт. Во избежание вскрытия и дискредитации защищенной системы доступа необходимо предпринимать особые организационно-технические меры по сохранению в тайне фактического значения ключа защиты, а также по защите от несанкционированного использования комплекта служебных карт объекта.

Процесс создания защищенной системы включает этапы:

1. Инициализация карт

Бесконтактные карты MIFARE Plus поддерживают три уровня безопасности (SL-1, SL-2, SL-3). Карты MIFARE Plus поступают с завода-изготовителя в незащищенном режиме (SL-0) и в таком виде не предназначены для использования. Заказчик должен проинициализировать все карты MIFARE Plus и перевести их на уровень безопасности SL-3 (это касается и рабочих, и служебных карт)

2. Генерация уникального ключа объекта и создание комплекта служебных карт Инициализации и Мастер-карты объекта.

3. Программирование и перевод используемых считывателей в защищенный режим.

4. Эмиссия защищенных рабочих карт объекта (карт пользователей).

В процессе эксплуатации объекта для работы с картами пользователей используется настольный считыватель Gate-USB-MF и Мастер-карта объекта.

Для работы с настольным считывателем Gate-USB-MF используется бесплатная утилита «Gate-USB-MF-Plus Configurator», которая есть на общем CD дистрибутива ПО Gate, а также на сайте

http://skd-gate.ru/materiali/tehnicheskaya_gate/po

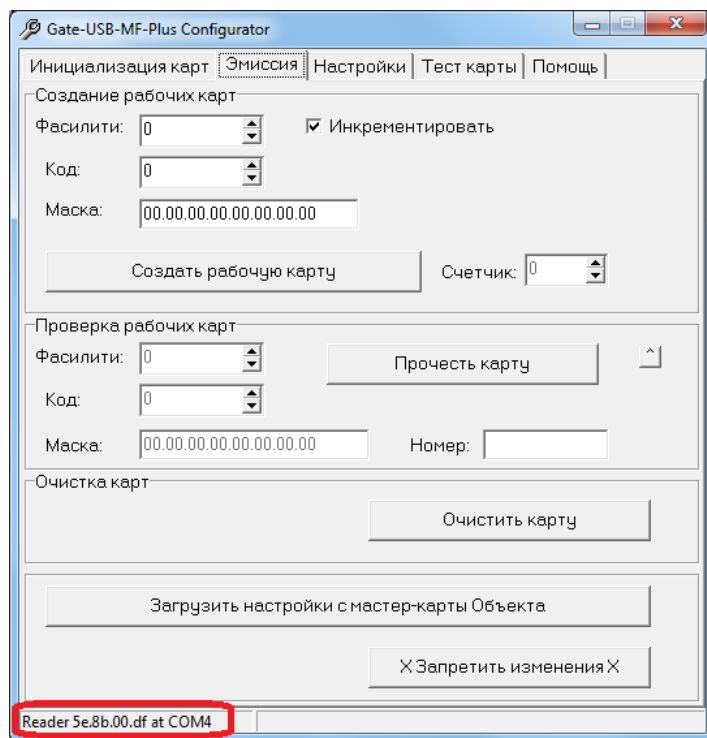
Порядок создания защищенной системы

1. Подготовка к работе настольного считывателя Gate-USB-MF:

- 1.1. Установите микропереключатели на задней стенке настольного считывателя следующим образом: 5 - ON, 6 - ON, остальные переключатели в нижнем положении (off).
- 1.2. Скачайте с сайта skd-gate.ru (или с общего CD ПО Gate) и установите драйвер настольного считывателя Gate-USB-MF.
- 1.3. Подключите считыватель к ПК USB кабелем.

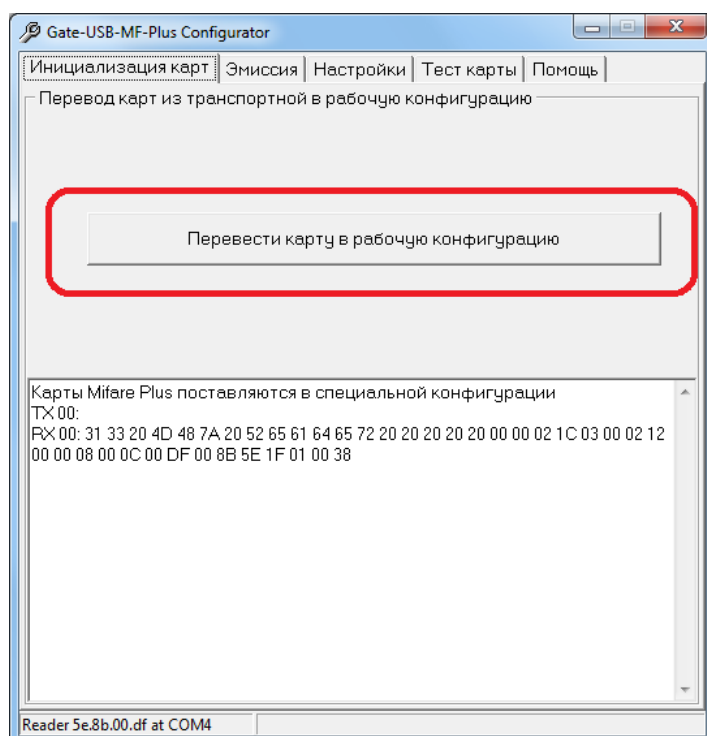
2. Настройка работы утилиты «Gate-USB-MF-Plus Configurator»

Скачайте с сайта skd-gate.ru (или с общего CD ПО Gate) и запустите утилиту «Gate-USB-MF-Plus Configurator». Убедитесь, что считыватель найден программой (см. информационное поле в левом нижнем углу интерфейса):

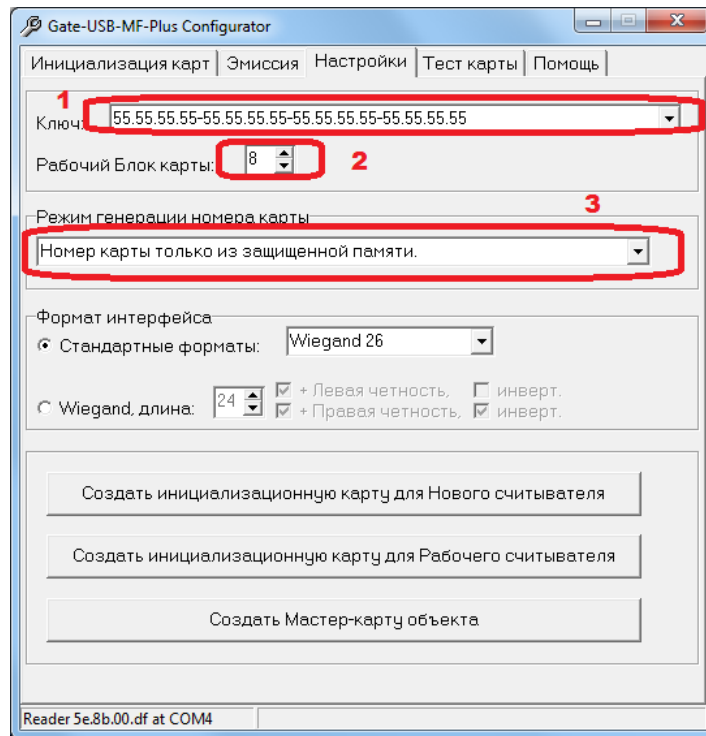


3. Инициализация карт (перевод новых карт на уровень безопасности SL-3)

Перед началом использования все неинициализированные карты MIFARE Plus (на уровне SL-0) должны быть переведены на уровень SL-3.



4. Задание необходимых параметров защищенной системы.



- 4.1. Введите значение крипто ключа (AES), длиной 16 байт. Для непредвиденных случаев утраты Мастер-карты объекта этот ключ надо запомнить и хранить в тайне от посторонних лиц.
- 4.2. Выберите номер блока памяти MIFARE Plus, в котором будет храниться идентификатор, и из которого считыватель Gate-Reader-MF будет его считывать (нумерация блоков памяти Mifare сквозная, начиная от 0).
- 4.3. Выберите режим генерации номера карты «Номер карты только из защищенной памяти»

5. Создание комплекта служебных карт объекта.

- 5.1. Создайте Мастер-карту объекта. Для этого поднесите новую карту к настольному считывателю и нажмите кнопку «Создать Мастер-карту объекта». Теперь все настройки вашей системы находятся на этой карте.
- 5.2. Создайте карту Инициализации для Нового считывателя. Для этого поднесите новую карту к считывателю и нажмите «Создать инициализационную карту для Нового считывателя». Эта карта понадобится при программировании Новых считывателей, находящихся в заводской конфигурации.
- 5.3. Создайте карту Инициализации для Рабочего считывателя. Для этого поднесите новую карту к считывателю и нажмите «Создать инициализационную карту для Рабочего считывателя». Эта карта понадобится, когда потребуется сменить Ключ или другие параметры системы в Рабочем считывателе, находящемся в эксплуатации на объекте.

Примечания:

- при необходимости можно создать несколько комплектов служебных карт объекта;
- сброс Рабочего считывателя в исходную заводскую конфигурацию возможен **только в лаборатории производителя** (сервисный отдел бренда Gate).

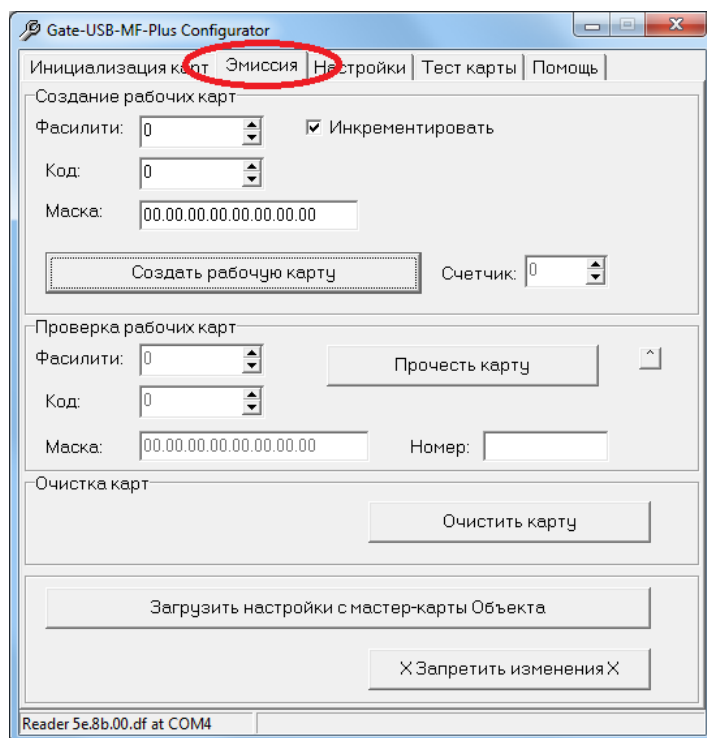
6. Программирование считывателей Gate-Reader-MF, предназначенных для установки на объекте:

- включите питание считывателя и в течение следующих 30 секунд поднести к нему **карту Инициализации для Нового считывателя**. Считыватель перейдет в режим программирования – начнет издавать частые звуковые сигналы.
- поднесите **Мастер-карту объекта**. Считыватель примет настройки из карты, прекратит звуковые сигналы, выйдет из режима программирования и перейдет в категорию Рабочего считывателя данного объекта.
- повторите эту операцию со всеми Новыми считывателями, предназначенными для данного объекта.

Примечание: В процессе эксплуатации системы может возникнуть необходимость изменения настроек Рабочих считывателей. Перепрограммирование Рабочих считывателей производится аналогичным способом, но при этом используется **карта Инициализации для Рабочего считывателя** и новая **Мастер-карта объекта** (с новыми параметрами системы).

7. Эмиссия рабочих карт:

7.1. Запустите приложения «Gate-USB-MF-Plus Configurator». Убедитесь, что считыватель найден программой (информационное поле в левом нижнем углу интерфейса). Перейдите на закладку «Эмиссия», поднесите к настольному считывателю Мастер-карту объекта и нажмите кнопку «Загрузить настройки с Мастер-карты»



7.2. Задайте значение кода идентификации пользователя (в разделе «Создание рабочих карт»). Для этого можно использовать два способа формирования значения кода идентификации пользователя: автоматический или ручной.

Автоматический: установить начальные фасилити и код карты; установить флаг «Инкрементировать», чтобы после каждого нажатия кнопки «Создать рабочую карту» значение поля «Код» увеличивалось на единицу (в противном случае все карты будут выпущены с одним и тем же кодом идентификации пользователя).

Ручной: вручную задать требуемый код рабочей карты (это бывает удобно при переходе от старой системы, в которой за пользователем уже был закреплен определенный идентификационный код).

Примечания:

- поле «Маска» при работе со считывателями с выходом Wiegand-26 рекомендуется оставить нулевым;
- после подготовки настроек Эмиссии можно нажать кнопку «X Запретить изменения X», что не позволит оператору, производящему работу по эмиссии карт, посмотреть настройки шифрования или случайными действиями сбить их;
- по окончании эмиссии карт есть возможность проконтролировать работу оператора по количеству выпущенных карт на основании значения поля Счетчик.

7.3. Поднесите новую карту к настольному считывателю и нажмите кнопку «Создать рабочую карту».

Примечание: для создания очередной рабочей карты в режиме автоматического формирования кода достаточно поднести очередную новую карту к считывателю и нажать кнопку «Создать рабочую карту». В режиме ручного формирования кода перед нажатием данной кнопки необходимо вручную задать новое значение кода.

8. Чтение запрограммированных рабочих карт.

В процессе эксплуатации системы, в частности, в процессе занесения карты в СКУД и выдачи ее пользователю, требуется чтение рабочей карты. Для этого:

- 8.1. Запустите приложение «Gate-USB-MF-Plus Configurator». Убедитесь, что считыватель найден программой (информационное поле в левом нижнем углу интерфейса). Перейдите на закладку «Эмиссия», поднесите к настольному считывателю Мастер-карту объекта и нажмите кнопку «Загрузить настройки с Мастер-карты»
- 8.2. Поднесите рабочую карту к настольному считывателю и нажмите кнопку «Прочитать карту». В поле «Номер» отобразится полный номер карты в формате, требуемом для программы Gate-Terminal. Его можно скопировать и использовать в учетной карточке пользователя в ПО СКУД.

Методика поэтапного перевода СКУД с незащищенных карт формата Em-Marine на защищенный режим с картами MIFARE Plus.

1. Приобрести необходимое для замены количество считывателей Gate-Reader-MF, настольных считывателей Gate-USB-MF и карт MIFARE Plus.
 2. Выполнить инициализацию карты в соответствии с п.3 данной инструкции.
 3. Изготовить комплект служебных карт защищенной системы данного объекта в соответствии с п.5 данной инструкции.
 4. Произвести программирование комплекта считывателей Gate-Reader-MF, предназначенных для установки на объекте в соответствии с п.6 данной инструкции.
 5. Произвести полную единовременную или постепенную эмиссию защищенных рабочих карт Mifare для каждого пользователя системы в соответствии с п.7 данной инструкции. При этом использовать режим ручного ввода кода карты, в качестве которого указывать wiegand код действующей в СКУД карты Em-Marine данного пользователя. Код действующей карты Em-Marine каждого пользователя можно скопировать из БД СКУД или считать с помощью настольного считывателя Z2-USB.
 6. Произвести полную единовременную или постепенную выдачу новых рабочих карт пользователям системы, с рекомендацией хранить и использовать обе карты вместе. После полного завершения процесса выдачи новых карт всем пользователям можно перейти к следующему этапу.
 7. Произвести полную единовременную или постепенную замену старых считывателей на новые рабочие считыватели Gate-Reader-MF. В случае постепенной замены считывателей доступ пользователей во всех точках прохода обеспечивается наличием у них двух карт разного стандарта (старых Em-Marine и новых защищенных MIFARE Plus).
 8. По окончании процесса замены считывателей можно организовать сбор старых карт или оповестить пользователей об окончании их функционирования.
- Важными удобствами данной методики перехода на защищенные идентификаторы с наследованием кодов старых карт являются отсутствие необходимости каких либо изменений в БД СКУД и возможность постепенного выполнения основных этапов.

Приложение 2.

Последствия утраты или компрометации ключа защиты системы.

1. Физическая утрата служебных карт при отсутствии знания фактического кода защиты автоматически приводит к невозможности наращивания системы (добавления точек доступа), изменения настроек системы, эмиссии карт и чтения карт настольным считывателем. В этом случае неизбежно встает вопрос о необходимости создания новой системы. С использованием настольного считывателя Gate-USB-MF и чистых новых карт MIFARE Plus можно создать новый комплект служебных карт для новой системы. Рабочие считыватели Gate-Reader-MF невозможно перепрограммировать на месте и их придется снимать и отправлять производителю для сброса к заводским установкам.
 2. Компрометация ключа защиты или Мастер-карты объекта не блокирует возможность работы системы или ее наращивания, но обеспечивает возможность и вызывает реальную угрозу создания действующих дубликатов карт или реализации диверсионного перепрограммирования рабочих считывателей объекта. Поэтому в подобной ситуации требуется обновление системы:
 - создать новый комплект служебных карт с новым ключом защиты в соответствии с п.4 данной инструкции;
 - перепрограммировать Рабочие считыватели в соответствии с п.5 данной инструкции, но с использованием старой карты Инициализации для Рабочего считывателя и новой Мастер-карты объекта (с новыми параметрами системы);
 - произвести эмиссию и выдачу новых карт в соответствии с п. 6 данной инструкции, или перевыпустить старые рабочие карты. При этом каждую карту предварительно нужно очистить (очистить рабочую карту) и создать заново с новыми параметрами.
- В период проведения данных работ СКУД находится в нерабочем состоянии и это надо учитывать при планировании и организации работ по обновлению системы.