Model
SBSK-03.0402 / x1.0100

ОПИСАНИЕ УСТРОЙСТВА

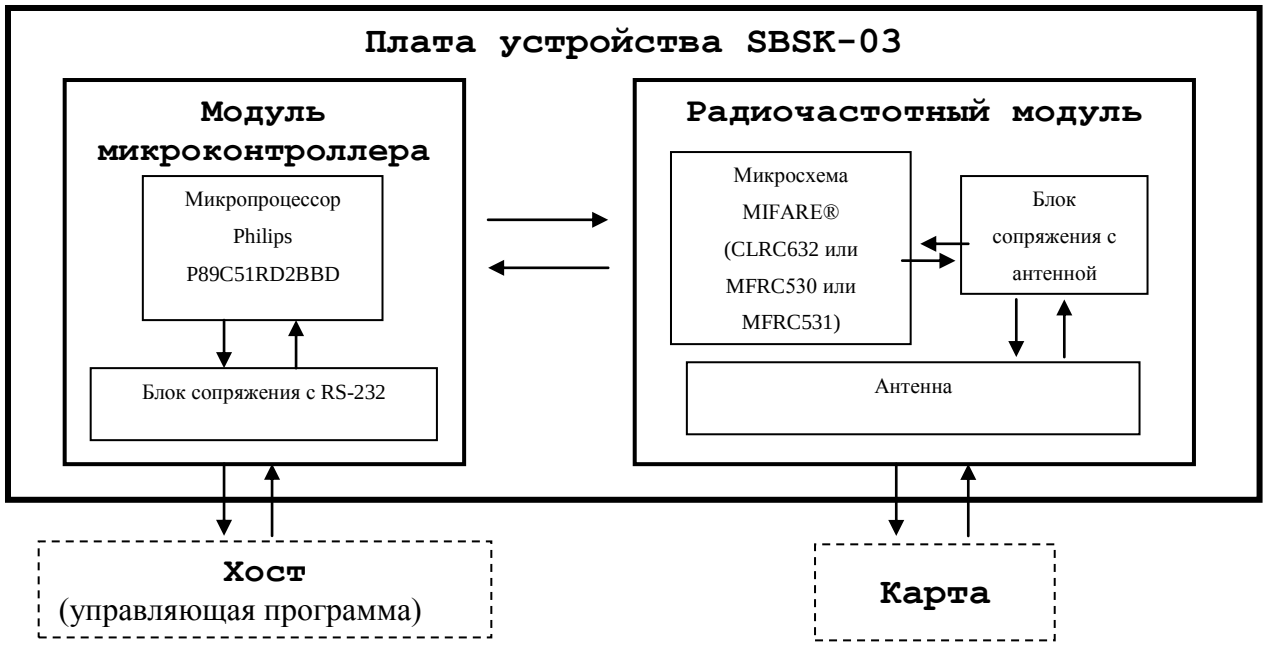
1 Назначение

Устройство SBSK-03 (далее Устройство) предназначено для обмена информацией между управляющим устройством (компьютером, терминалом – далее Хостом) и бесконтактными смарт-картами MIFARE® Standard 1K и 4K[1], MIFARE® Ultralight, а также с дуальными смарт-картами MIFARE® ProX Platform, работающих согласно ISO/IEC 14443A по протоколу T=CL (включая карту JCOP 30). Устройство разработано и производится компанией «РОЗАН» (www.rosan.ru).

2 Состав Устройства

Устройство состоит из следующих функциональных узлов:

- корпус 90*20*50 мм с установленной в нем печатной платой, которая содержит радиочастотный модуль (микросхемы CLRC632, или MFRC530, или MFRC531, блока сопряжения с антенной и собственно антенны) и модуль микроконтроллера (микропроцессор Philips P89C51RD2BBD и блок сопряжения с Хостом по интерфейсу RS-232);
- кабель связи с Хостом и разъемом DB9 к стандартному последовательному порту Хоста с интерфейсом RS-232 (трехпроводной Tx/Rx/Gnd);
- разъем питания включаемый в USB порт, присоединенный к разъему DB9 методом пайки;



Вес устройства – не более 100 г, потребляемая мощность – не более 1.5 Вт, расстояние гарантированного действия антенны – не менее 3 см. Конструкция Устройства предусматривает его круглосуточную эксплуатацию при температуре от -15Cº до +35Cº при относительной влажности воздуха 98% (при 25Cº).

[1] С картой MIFARE® Standard 4K Устройство может работать только с первыми 1K байтами памяти карты.

3 Принцип работы и команды Устройства

3.1 Принцип работы Устройства

Основной задачей Устройства является исполнение функции посредника по передаче информации между картой и управляющей программой Хоста. Устройство может читать и записывать данные на карту (в память MIFARE®) при обеспечении определенных условий безопасности транзакции - аутентификации отдельных областей памяти карты на основе секретных ключей, предварительно загруженных в защищенную память Устройства. Согласно стандарту MIFARE® Устройство поддерживает три набора пары секретных ключей на каждую область памяти MIFARE® Standard 1K (всего 16 областей) или на первые 16 областей памяти MIFARE® Standard 4K. Безопасность работы с картой MIFARE® ProX Platform определяется загруженным в карту приложением (апплетом), используемым для работы с данными памяти карты. Команды, используемые Устройством для работы с картой, перечислены ниже. Связь Устройства с картой осуществляется по радиоканалу со скоростью106 Кбод.

Радиочастотный модуль включает в себя антенну и радиочастотный блок. Антенна обеспечивает прием и передачу зашифрованных радиосигналов, секретность которых обеспечивается микросхемой MIFARE®, а радиочастотный блок производит их модуляцию и демодуляцию для получения Устройством доступа к карте.

Модуль микроконтроллера осуществляет взаимодействие между микросхемой MIFARE® и хостом через последовательный порт RS-232. Скорость обмена по последовательному порту устанавливается специальной командой Устройства. Возможные скорости обмена информации с хостом — 115.2 Кбод, 57.6 Кбод, 38.4 Кбод, 19.2 Кбод или 9.6 Кбод. Протокол обмена данными между Устройством и Хостом полностью совместим с MIFARE® Serial Reader Protocol.

При получении от радиочастотного блока сигнала о наличии карты в поле действия антенны, микросхема MIFARE® передает эту информацию микропроцессору, который, в свою очередь, пересылает ее управляющей программе.

От Хоста микропроцессор получает команду о дальнейших действиях с картой и передает их микросхеме MIFARE® (с картой по радиоканалу через радиочастотный блок и антенну работает только микросхема MIFARE®). После завершения какого-либо цикла операций, карта посылает подтверждение о том, что все операции выполнены и ожидает следующей команды. Ряд команд не предназначен для проведения операций с картой, а управляет только самим Устройством.

3.2 Типы команд

Команды Устройства делятся на следующие группы:

- команды идентификации карты;
- команды работы с памятью карты;
- служебные команды.

3.3 Команды идентификации карты (согласно стандарту ISO/IEC 14443A)

Для идентификации карты, с которой Устройство может проводить операции чтения и записи, используется следующие команды:

Anticoll - устранение коллизий при неоднозначном выборе карты с серийным номером чипа 4 байта (MIFARE® Standard 1K и 4K, MIFARE® ProX Platform) в случае наличия нескольких карт в поле действия антенны.

Anticoll Cascade level 2 - устранение коллизий при неоднозначном выборе карты в поле действия антенны в случае наличия нескольких карт, имеющих серийный номер чипа более 4-х байтов (карты MIFARE® Ultralight и MIFARE® DESFire).

Deselect - закрывает сессию с выбранной картой с дуальным интерфейсом.

Halt - завершение сеанса работы с картой.

Request - запрос по радиоканалу о наличии какой-либо карты в поле действия антенны.

Request Answer To Select (RATS) - открывает сессию работы с выбранной картой с дуальным интерфейсом для обмена данными по формату команды стандарта ISO/IEC 7816.

Select - выбор карты с определенным серийным номером чипа в 4-е байта и определение размера её памяти.

Select Cascade level 2 - выбор карты с определенным серийным номером чипа более 4-х байтов, и определение размера её памяти.

3.4 Команды работы с памятью карты

Для работы с памятью карты, т.е. для непосредственного проведения операций чтения информации с карты или записи информации на карту, либо увеличения или уменьшения параметров счетчика («электронного кошелька») применяется следующий набор команд:

Authenticate - процесс аутентификации выбранной области памяти карты.

Decrement - уменьшение (вычитание) значения какой-либо ячейки памяти, размеченной как счетчик («электронный кошелек»), и запись измененного (нового) значения во внутренний регистр карты.

Exchange Transparent Data (Exchange APDU) - обеспечение обмена командами в формате ISO 7816 для карт с дуальным интерфейсом (команда ISO/IEC 14443A T=CL).

Increment - увеличение (сложение) значения какой-либо ячейки памяти, размеченной как счетчик («электронный кошелек»), и запись измененного (нового) значения во внутренний регистр карты.

Read - чтение информации из определенной области памяти карты.

Restore - запись значения ячейки памяти, являющейся счетчиком («электронным кошельком») карты, во внутренний регистр карты.

Transfer - при получении этой команды происходит запись значения из внутреннего регистра памяти карты в ту ячейку, с которой производились операции **Increment**, **Decrement** или **Restore**.

Ultralight Page Write - команда записи информации в определенную страницу памяти карты MIFARE® Ultralight.

Write - команда записи информации в определенную область памяти карты MIFARE® Standard и Ultralight.

3.5 Служебные команды

Служебные команды необходимы для настройки Устройства для дальнейшей работы:

Change Rate – команда изменения скорости обмена данными между Устройством и Хостом.

Flash Defragmentation - команда дефрагментации флэш-памяти микропроцессора (периодически используется для оптимизации памяти в случае частой загрузки ключей в Устройство).

Get Info - команда чтения идентификационных данных Устройства.

Get Version - команда чтения версии внутреннего программного обеспечения Устройства, а также типов микросхемы MIFARE® и микропроцессора.

Load Key - команда загрузки значений ключей в память Устройства (или же замены записанных туда ранее ключей).

Reset - команда выключения обмена по радиоканалу (отключает антенну с возможностью установки времени отключения).

Set Command Timeout - команда установки временного интервала между исполнениями отдельных команд Устройства.

Set Port (или **Indicator Drive**) - команда установки определенных битов для управления дополнительным портом. В Устройстве команда **Set Port** используется для управления световым индикатором Устройства; возможны четыре состояния индикатора – зеленый индикатор, красный индикатор, желтый индикатор, индикатор выключен.

4 Смена внутреннего программного обеспечения Устройства

Устройство обладает возможностью загрузки внутреннего программного обеспечения, используя интерфейс RS-232. Для замены этого программного обеспечения необходимо запустить программу загрузки (поставляется отдельно) на персональном компьютере, к последовательному порту которого подключено Устройство. Данные будут переданы в Устройство в зашифрованном виде. Для шифрования используется алгоритм Triple D.E.S. Программы, которые производят смену внутреннего программного обеспечения Устройства, могут быть созданы только производителем Устройства.

5 Комплект поставки Устройства

В стандартный комплект поставки входит: Устройство (плата в корпусе, соединительные кабели с разъемами в едином конструктиве) и паспорт к Устройству. Дополнительно может быть поставлен блок питания 220В/5В. Для платежных терминалов возможна модификация Устройства с USBB-1J розеткой на корпусе Устройства или с соединительным кабелем с разъемом USB на конце в едином конструктиве с Устройством с подачей питания через эти же розетку или разъем. Для встраивания Устройства в другие электронные устройства возможна также поставка OEM-варианта Устройства – платы без корпуса и соединительных кабелей.

По желанию заказчика к партии Устройств может быть приложена тестирующая программа и набор тестовых карт. Дополнительно может быть поставлен комплект разработчика приложений для карт MIFARE® Standard, MIFARE® Ultralight, MIFARE® ProX Platform, включающий описание карт и библиотеки функций, реализующих описанные выше команды. При необходимости к комплекту на условиях конфиденциальности может быть приложено описание протокола передачи данных между Устройством и Хостом.

6 Сертификаты

Устройство сертифицировано в системе сертификации ГОСТ Р Госстандарта России, сертификат соответствия РОСС RU.ОС03.В01117 № 5995067. Соответствует требованиям нормативных документов ГОСТ 12997-84, ГОСТ Р 51241-98, ГОСТ Р 50009-2000, ГОСТ Р МЭК 60065-2002.