

ООО "СмартПарк"

СКЗИ ОС ФОРΟΣ х.х
Описание эксплуатации

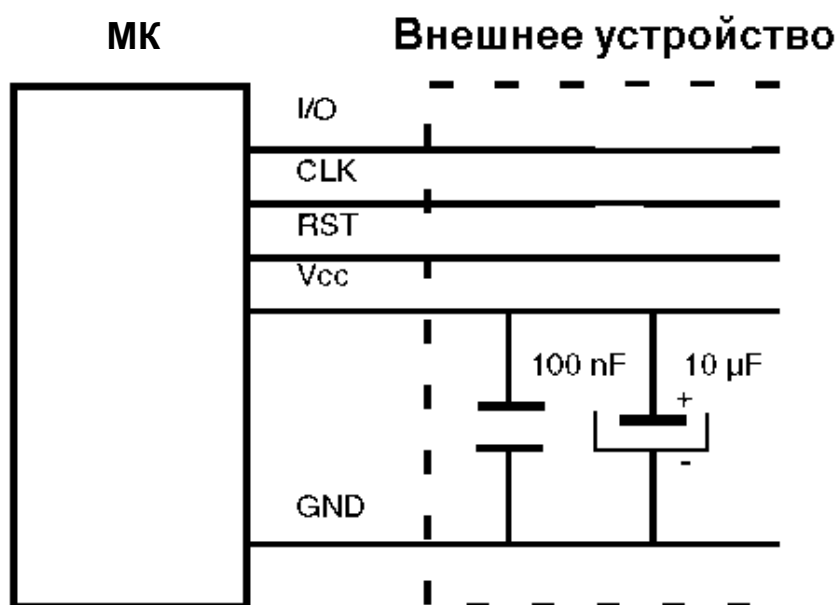
СОДЕРЖАНИЕ

1 ТРЕБОВАНИЯ К ПАРАМЕТРАМ ЭЛЕКТРОПИТАНИЯ ПРИ ЭКСПЛУАТАЦИИ.....	3
2 ТРЕБОВАНИЯ К ПАРАМЕТРАМ ОКРУЖАЮЩЕЙ СРЕДЫ ПРИ ЭКСПЛУАТАЦИИ МК С ОС	4
3 ТРЕБОВАНИЯ К ТРАНСПОРТИРОВАНИЮ И ХРАНЕНИЮ ...	5
4 ОГРАНИЧЕНИЯ ПО МЕХАНИЧЕСКИМ ВОЗДЕЙСТВИЯМ	6
5 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ	6
6 ТЕКУЩИЙ РЕМОНТ МК С ОС	6
7 ПРОТОКОЛЫ ВЗАИМОДЕЙСТВИЯ ТЕРМИНАЛЬНОГО ОБОРУДОВАНИЯ С МК	7
7.1 Протокол ISO7816-3.....	8
7.2 Протокол ISO14443-3.....	9
8 КОНТРОЛЬ И ДИАГНОСТИКА МК.....	9
9 СПРАВОЧНИК ПО СТАТУСАМ КОМАНД.....	12

1 Требования к параметрам электропитания при эксплуатации

Внешнее оборудование, применяемое совместно с микроконтроллерами с СКЗИ ОС ФОРΟΣ х.х (далее – МК) должно обеспечивать электропитание в диапазонах 1,8В \pm 10%, 3В \pm 10% и 5В \pm 10% (может уточняться в документации на модель изделия).

Рекомендуемая схема подключения электропитания к МК



Электрические параметры МК соответствуют следующим нормам (при напряжении питания $V_{CC}=5\text{ В} \pm 10\%$ и температуре окружающей среды от -25°C до $+85^{\circ}\text{C}$)¹:

Наименование параметра, единица измерения	Буквенное обозначение	Норма		Условия
		не менее	не более	
1. Выходное напряжение низкого уровня по выводу IO, В	U_{OL}	0	0,4	
2. Выходное напряжение высокого уровня по выводу IO, В	U_{OH}	3,8	V_{CC}	$I_{OHMAX}=20\text{ мкА}$
3. Ток потребления, мА	I_{CC}	2,2	18,3	В зависимости от режима работы
4. Ток утечки низкого уровня на входе по выводам CLC, RST, мкА	$I_{LIL}(\text{CLC})$ $I_{LIL}(\text{RST})$	-20	20	
5. Ток утечки высокого уровня на	$I_{LIH}(\text{CLC})$	-20	20	

¹ Приведены оценочные характеристики

входе по выводам CLC, RST, mA	$I_{LH(RST)}$			
6. Выходной ток низкого уровня в состоянии "Выключено" по выводу IO, mA	I_{OZL}	-20	20	
7. Выходной ток высокого уровня в состоянии "Выключено" по выводу IO, mA	I_{OZH}	-20	20	

Может уточняться в документации на модель изделия

Значения предельно-допустимых электрических режимов эксплуатации в диапазоне температур среды составляют:

Наименование параметра, единица измерения	Буквенное обозначение	Предельно-допустимый режим	
		не менее	не более
Напряжение питания, В	U_{CC}	-0,3	7,0
Напряжение на любом входе, В	U_I	-0,3	$U_{CC}+0,3$
Входное напряжение низкого уровня на выводах CLC, RST, IO, В	U_{IL}	-0,3	0,8
Входное напряжение высокого уровня на выводах CLC, RST, IO, В	U_{IH}	$(U_{CC}-0,7)$	$U_{CC}+0,3$
Выходной ток низкого и высокого уровня на выводе IO, mA	I_{OL}	-	1
	I_{OH}		0,02
Время нарастания и спада на выводе IO, mks	t_{LH}	-	1
	t_{HL}		
Время цикла записи (перезаписи), ms	t_{CYPR}	-	5
Количество циклов записи (перезаписи)	N_{PR}	-	500000

Может уточняться в документации на модель изделия

Предприятие - изготовитель гарантирует срок хранения МК с ОС при соблюдении условий хранения - 30 лет со дня их изготовления.

2 Требования к параметрам окружающей среды при эксплуатации МК с ОС

Параметры окружающей среды, в которой эксплуатируются смарт-карты на базе МК с ОС, не должны превышать рабочих значений, указанных в п. **Ошибка! Источник ссылки не найден.** настоящего документа. В частности:

- влажность должна находиться в пределах 5% до 95% при температуре мокрого градусника не более 25° С;

- температура окружающей среды должна находиться в пределах от 0° С до 50° С;

Смарт-карты на базе МК сохраняют работоспособность после воздействия предельно допустимой пониженной температуры окружающей среды до минус 35° С.

Указанные требования могут уточняться в документации на модель изделия

3 Требования к транспортированию и хранению

Смарт-карты должны храниться в складских помещениях, защищающих изделие от воздействия атмосферных осадков, в транспортной упаковке при отсутствии в воздухе паров кислот, щелочей и других агрессивных примесей.

В складских помещениях должна обеспечиваться температура от плюс 5 до плюс 30°С и относительная влажность воздуха не более 85%.

Распаковку изделия в зимнее время после воздействия отрицательных температур, производить в отапливаемом помещении, предварительно выдержав его в этом помещении не распакованным не менее двух часов.

Транспортирование смарт-карт может производиться авиационным, автомобильным, железнодорожным или иным транспортом в условиях, исключающих механические повреждения, прямое попадание на транспортную упаковку влаги, пыли и грязи, превышение предельных значений температуры окружающей среды.

Транспортная упаковка на транспортных средствах должна быть закреплена так, чтобы была исключена возможность смещения и соударений упаковок.

При транспортировке должны соблюдаться следующие условия:

- температура окружающего воздуха от -20°С до +50°С;
- относительная влажность воздуха до 95% (без конденсации);
- исключение прямого воздействия солнечных лучей, атмосферных осадков и агрессивных примесей (паров кислот, щелочей);
- отсутствие повреждений упаковки.

Приведенные требования могут уточняться в документации на модель изделия

4 Ограничения по механическим воздействиям

Параметры прочности и устойчивости к механическим воздействиям обеспечиваются предприятием - изготовителем смарт-карт.

Должны обеспечиваться такие условия эксплуатации смарт-карт, при которых:

- Воздействие вибрации не превышает значений по ГОСТ 20.57.406 (таблица 3, X степень жесткости).

- Нагрузка статического поперечного изгиба не превышает 0,5 Н.

- Динамические продольные изгибы не превышают по частоте 0,5 Гц, а максимальные значения стрелы прогиба не превышают 10 мм и 20 мм.

- Многократные кручения не превышают по частоте 0,5 Гц и по углу $\pm 15^{\circ}$.

- Усилия отрыва, прикладываемые к микромодулю смарт-карт не должны быть более чем 30 ньютонов.

Механический удар многократного действия (в транспортной таре):

- пиковое ударное ускорение 147 м/с² (15 g);

- длительность действия ударного ускорения (2 – 15) мс.

5 Техническое обслуживание

Техническое обслуживание смарт-карт на базе МК с ОС проводится пользователем и заключается в визуальном осмотре с целью выявления критических деформаций пластикового основания и протирке контактной группы (при необходимости).

6 Текущий ремонт МК

МК не подлежат ремонту. При выходе изделия из строя в период гарантийного срока, оно подлежит возврату поставщику с целью замены на исправный экземпляр.

В случаях блокирования в период гарантийного срока, а также выхода из строя в данный период вследствие:

- неправильных действий обслуживающего персонала,

- отказов и ошибок аппаратуры взаимодействующей с МК, гарантийная замена не производится.

7 Протоколы взаимодействия терминального оборудования с МК

В зависимости от модели МК, поддерживается контактный и/или бесконтактный (RF) интерфейсы. *Перечень поддерживаемых интерфейсов уточняется в документации на модель изделия.*

Для контактного интерфейса, могут применяться следующие протоколы обмена МК с терминалом:

- Протокол ISO 7816-3 T=0
- Протокол ISO 7816-3 T=1

Для RF интерфейса, могут применяться следующие протоколы обмена МК с терминалом:

- Протокол ISO 14443-3,4 B T=CL
- Эмуляция *TPDU ISO 7816-3 T=0* по *ISO 14443-3,4 B T=CL* (активизируется на фазе инициализации по запросу заказчика)

Сразу после подачи питания или RESET, МК выполняет набор служебных процедур (самотестирование, восстановление памяти и т.д. - состав процедур определяется моделью МК). После этого МК отвечает терминалу последовательностью данных ATR или ATQB по RF-интерфейсу.

Служебные процедуры могут быть достаточно длительными и, если терминал снял питание не дождавшись ответа МК, то в этом случае не завершенные процедуры будут продолжены при следующем рестарте.

В случае использования контактного интерфейса вся процедура выполняется до выдачи ATR.

В случае использования RF интерфейса, процедура в основном выполняется до выдачи ATQB - кроме действий, связанных с дефрагментацией файловой системы (может уточняться в документации на конкретную модель изделия).

На фазе блокирования МК не выдает ATR/ATQB.

В случае использования контактного интерфейса, по согласованию с заказчиком изделий с МК, поставщик может установить протокольные байты ATR, установив, таким образом, выбираемый протокол (ISO 7816-3 T=0 и/или T=1), скорость для взаимодействия с терминальным оборудованием, прямой или обратный порядок кодирования байтов, и, при необходимости, запретив PPS.

В случае использования RF интерфейса, по согласованию с заказчиком изделий, поставщик может установить компоненты поля Protocol Info, установив, таким образом, скорость, таймауты, и размер фрейма при взаимодействии с терминальным оборудованием.

Байты истории могут быть получены командой GET_DATA (при этом MF не обязательно должен быть текущим файлом) с параметрами:

- **5F51** – ATR полностью
- **5F52** – байты истории
- **5F53** – байты Application Data из ATQB

7.1 Протокол ISO7816-3

По-умолчанию, МК использует прямой порядок кодирования байтов (direct convention, см. ISO 7816-3, раздел 6.4) и протокол T=0. Поддерживается процедура PPS и выбор скорости обмена до 16 тактов/бит, что примерно равно 223200 бит/сек при стандартной частоте тактирования 3.57 МГц.

Размер передаваемых данных ограничен размером **255** байт в запросе и **256** байт в ответе.

Если в контексте MF существует запись с тэгом 5F52 и размером от 1 до 15 байт, то ее содержимое будет выдаваться в качестве байтов истории вместо стандартных (значение T0 изменится на 8X, где X – число байтов истории).

Протокольные байты ATR^(*)

Байт	значение	пояснение
TS	3В	direct convention
T0	93	9 – признаки присутствия TA1 и TD1 3 – число байтов истории
TA1	96	максимальная частота 5MHz минимальный период передачи бита ETU = F/D тактов где F=512, D=32 (т.е. ETU >= 15 тактов/бит)
TD1	00	предлагается протокол T0 нет дальнейших байтов TA2..TD2

(*) Байты ATR могут быть скорректированы при инициализации МК

Байты истории на фазе инициализации

Байт	значение	пояснение
HB1	80	category indicator byte в конце признак фазы жизни в формате CompactTLV
HB2..3	81 03	фаза жизни МК – инициализация

Стандартные байты истории на фазе эксплуатации^(*)

Байт	значение	пояснение
НВ1	80	category indicator byte в конце признак фазы жизни в формате CompactTLV
НВ2..3	31 C0	Card service data byte - разрешен выбор приложения по полному и частичному имени
НВ4..6	72 F7 41	Card capabilities - доступен выбор DF по полному и частичному имени, по пути и по идентификатору - поддерживаются короткие идентификаторы EF - поддерживаются номера записей - поддерживаются идентификаторы (тэги) записей - WRITE BINARY выполняет OR - единицей адресации в ВФ является 1 байт
НВ7..8	81 07	фаза жизни МК - эксплуатация

(*) Байты истории могут быть скорректированы при эксплуатации МК

7.2 Протокол ISO14443-3

По-умолчанию, МК с RF-интерфейсом использует скорость 106 Кбит/с, размер фрейма 256 байт.

Размер передаваемых данных ограничен размером **255** байт в запросе и **256** байт в ответе.

Байты Protocol Info ATQB^(*)

Байт	значение	пояснение
1	00	Скорость 106 Кбит/с
2	81	8 - размер фрейма 256 байт 1 - МК совместим с ISO14443-4
3	87	8 - FWT = ~77.3 мс 7 - Application Data совместим с ISO14443-3, МК поддерживает поля NAD и CID
4	00	0 - SFGT = ~302 мкс (если используется расширенный ATQB)

(*) Байты Protocol InfoATQB могут быть скорректированы при инициализации МК

Байты Application Data ATQB^(*)

Байт	значение	пояснение
1	00	Любые типы приложений
2-3	FF FF	Значение CRC (AID) не определено
4	01	Количество приложений

(*) Байты Application Data ATQB могут быть скорректированы при инициализации МК

8 Контроль и диагностика МК

В МК предусмотрены ряд автоматических (не отключаемых) и дополнительных (запускаемых вручную) средств контроля исправности МК и целостности данных.

К автоматическим средствам контроля относятся:

- Самотестирование МК при старте.
- Аппаратный механизм коррекции однократных ошибок в энергонезависимой памяти и детектирования многократных ошибок.
- Программно-вычисляемая контрольная сумма заголовков файлов, содержимого служебных файлов и пользовательских данных².
- Механизм буферизации и поддержки транзакций записи энергонезависимой памяти.

При невозможности восстановить целостность аппаратно-программной среды исполнения, МК переходит в состояние "MUTE" ("повисает"). В этом случае восстановление работы МК возможно только после подачи сигнала «Reset». Причинами «повисания» могут быть:

- Ошибка выполнения самотестирования³
- Выход параметров, контролируемых датчиками, из диапазона допустимых значений.
- Обнаружение невосстанавливаемой ошибки в энергонезависимой памяти.
- Невозможность произвести безошибочную запись в энергонезависимой памяти.

К дополнительным средствам контроля и диагностики относятся:

- Диагностические флаги.
- Команда диагностики VALIDATE CARD, которая позволяет:
 - проверить диагностические флаги;
 - проверить всю энергонезависимую память на предмет наличия неисправных блоков;
 - выполняет диагностику оборудования;
 - вычислить некриптографическую контрольную сумму двоичного кода ОС;
 - вычислить криптографическую контрольную сумму двоичного кода ОС.

В ОС определены следующие диагностические флаги:

- Флаг наличия неисправленной ошибки чтения в области файловой

² включается пользователем при создании файла

³ перед «зависанием» может быть выдан аварийный ATR/ATQB

системы энергонезависимой памяти.

- Флаг наличия неисправленной ошибки чтения в области буфера транзакций.
- Флаг наличия неисправленной ошибки чтения в служебных областях энергонезависимой памяти или в области кода расширения.
- Флаг выявления ошибки записи в области файловой системы энергонезависимой памяти.
- Флаг выявления ошибки записи в области буфера транзакций.
- Флаг выявления ошибки записи в служебных областях энергонезависимой памяти или в области кода расширения.

При наличии специальных требований заказчика, МК может выполнять расширенные процедуры самотестирования. Вследствие их значительной продолжительности, эти процедуры выполняются после выдачи ATR/ATQB, но до выполнения МК первой команды от терминального оборудования. В случае выявления этими процедурами ошибок, МК выдаст соответствующий код ошибки в ответ на первую команду, вместо ее выполнения. Из всего множества команд будет разрешено выполнение лишь только команды диагностики⁴.

К расширенным процедурам самотестирования относятся:

- проверка некриптографической контрольной суммы ОС
- статистическая проверка ДСЧ
- проверка криптографического сопроцессора

⁴ при необходимости можно запретить и обработку команды диагностики (режим "MUTE")

9 Справочник по статусам команд

Статусы выполнения команд (могут уточняться для конкретных моделей МК)

Статус	Расшифровка
65 81	Ошибка целостности энергонезависимой памяти
67 00	Неверная длина данных
67 01	Запрошено слишком много данных
67 02	Слишком много данных для проведения SM
67 10	Значение Le превышает размер коммуникационного буфера
67 11	Значение Lc превышает размер коммуникационного буфера
69 00	Выполнение команды запрещено
69 10	Директория не пуста (при попытке удалить)
69 11	Нельзя удалять MF
69 81	Команда не совместима со структурой файла
69 82	Доступ запрещен
69 83	Ключ заблокирован
69 85	Не выполнены предварительные условия
69 86	Команда не применима к данному типу файла
69 87	Отсутствуют данные необходимые для проведения SM
69 88	Некорректный объект SM
69 89	Команда недопустима на данной фазе жизни файла или МК
69 90	Ошибочная имитовставка при SM
69 91	Поврежден файл
69 92	Правило доступа с указанным номером уже определено
69 93	Требуется генерация производного ключа
69 94	Ключ не предназначен для выполнения указанной операции
69 95	Криптографическая операция не может быть продолжена
69 96	Неверная ЭЦП
69 97	Необходимо использовать SM
69 98	Запрещено менять настройки SM при активном SM
69 99	Ключ не найден
69 9A	Не найден указанный CRT
69 9B	Недопустимый криптографический алгоритм ключа
69 9C	Неверное выравнивание данных при SM
69 9D	Ключ не загружен
69 9E	Некорректное правило разграничения доступа
69 A1	Раздел уже занят
69 A2	Пересечение разделов
69 A3	Вектор расширения занят или заблокирован
69 A4	Список команд-расширений уже полон
69 A5	Адрес обработчика вне заполненной части текущего раздела
69 A6	МК еще не отформатирован
69 A7	Недостаточно памяти
69 A8	Вектор вне допустимого диапазона
69 A9	Команда вне допустимого диапазона
6A 00	Неверные параметры команды
6A 80	Неверные данные команды
6A 82	Файл не найден Ошибка создания файла
6A 83	Запись не найдена
6A 84	Не хватает места
6A 86	Неверные параметры P1-P2
6A 91	Неверные параметры криптографического алгоритма
6A 92	Неправильные параметры операции
6A 93	Недопустимая длина СЧ
6A 94	Недопустимый номер санкции
6A 95	Несовместимость алгоритма и назначения ключа или битов назначения ключа
6B 00	Указано смещение за границами файла

6C xx	Неверное значение Le; xx – правильное значение Le
6D 00	Не найдена команда с данным INS
6E 00	Не найдена команда с данным CLA
91 00	Аппаратная ошибка без уточнения
91 01	Таймаут ожидания данных
91 02	Обращение по несуществующему адресу в энергонезависимой памяти
91 03	Переполнение буфера транзакций
91 04	Недостаточно оперативной памяти
91 05	Ошибочное освобождение памяти
91 06	Commit без открытия транзакции
91 07	Ошибка в транзакционном буфере
91 08	Недостаточно место в файловой системе
91 09	Повреждены служебные области энергонезависимой памяти
91 0A	Повреждена энергонезависимая память
91 0B	Недопустимые условия среды выполнения
91 0C	Не найден идентификатор памяти
91 0D	Неправильные данные для записи
91 0E	Ошибка размера буфера
91 0F	Сброс из-за ошибки оборудования
91 10	Не пройден контроль конфигурации оборудования
91 11	Ошибка записи энергонезависимой памяти
91 12	Ошибка чтения энергонезависимой памяти
91 13	Неправильная фаза жизни
91 14	Полный отказ ДСЧ
91 15	Статистический отказ ДСЧ
91 16	СЧ не подходит для ГОСТ Р34.10-2001
91 17	HANG CARD
91 18	Ошибка счетчика операций криптопроцессора
91 19	Ошибка акселератора CRC
91 1A	Ошибка генератора
91 1B	Ошибка таймера
91 1C	Ошибка акселератора DES
91 1D	Ошибка криптопроцессора
91 1E	Ошибка контрольной суммы ROM
91 1F	Значение вне домена допустимых
91 20	Алгоритм не определен
91 21	Неверный параметр алгоритма
91 22	Операция неприменима к данному типу алгоритма
91 23	Режим не определен
91 24	Неверный размер входных данных
91 25	Недостаточный размер буфера для выходных данных
91 26	Ошибка при выполнении криптографического преобразования
91 27	Тэг не определен
91 28	Контекст не инициализирован или поврежден
91 29	Переполнение буфера контекстов
91 2A	Переполнение буфера данных
91 2B	Неверное направление криптооперации (зашифровать /расшифровать)
91 2C	Совпадение случайных чисел при выработке сессионного ключа
91 2D	Неверное значение индекса параметра по умолчанию
91 2E	Ошибка ДСЧ
91 2F	Ошибка выравнивания
91 30	Неправильные входные данные
91 31	Неправильный входной ключ
93 00	Ошибка в ОС без уточнения
95 00	Функция не реализована