1.Общая информация

Микросхема представляет собой специализированный контроллер с двумя типами интерфейса, изготавливаемый по КМОП технологии, и предназначена для использования в защищенных смарт-картах, которые предъявляют высокие требования к степени защиты информации от мошеннических действий.

1.1. Основные характеристики:

- **Интерфейсы:**
  - Бесконтактный интерфейс в соответствии с ISO 14443-2,3,4 тип B:
    - Несущая частота 13,56 MHz ±7KHz,

- **Программная память:**
  - Масочное ПЗУ объемом 256 Кбайт

- **Энергонезависимая пользовательская память:**
  - Объем: 144 кбайт
  - Количество циклов перезаписи: => 500 000 циклов
  - Срок хранения информации: 10 лет
  - Побайтный доступ для считывания ЭППЗУ
  - Постраничный режим записи/стирания от 4 до 128 байт
  - 128 байт области защиты:
    - 64 байт – аппаратно защищенная от модификации область памяти
    - 64 байт – аппаратно защищенная от стирания область памяти

- 6 КБайт – основное ОЗУ данных.

- Выполняемый набор инструкций совместим со стандартным процессором 8051 с дополнительным набором команд, оптимизированным для применений в смарт-картах.

- Оптимизированная архитектура с ускоренным выполнением инструкций – в среднем, в 3 раза меньше тактов на инструкцию, чем в стандартном микроконтроллере 8051

- Контроллер прерываний.

- Генератор на базе ФАПЧ для повышения внутреннего тактового сигнала ЦПУ до 33 МГц

- Два 16-разрядных таймера.

- **Системы безопасности и защиты:**
  - Микросхема обеспечивает хранение уникального номера микросхемы размером 8 байт.
  - В микросхеме реализован механизм контроля целостности программного обеспечения, аппаратных компонентов и хранимых данных;
  - Предусмотрена возможность блокировки кристалла на различных стадиях производства транспортным кодом (ключом), исключающим несанкционированное внесение в чип изменений или считывание содержащейся в нем информации;
  - Исключено чтение программной памяти внешними командами;
  - В микросхеме реализован механизм (процедура) контроля несанкционированного случайного и/или преднамеренного искажения (изменения, модификации) и/или разрушения информации, программных и аппаратных компонентов;
  - Модуль управления памятью (Memory Management Unit) с контролем обращения за границей памяти.
  - Активный щит

- **Элементы криптографии:**
  - Аппаратно-программный генератор случайных чисел (ГСЧ);
  - Микроконтроллер обеспечивает формирование ЭЦП по алгоритму ГОСТ Р 34.10-2012;
  - Алгоритм шифрования ГОСТ 28147-89;
  - Алгоритм хеширования ГОСТ Р 34.11-94;
  - Алгоритмы хеширования и ЭЦП, приведенные в рекомендациях ICAO;
  - Аппаратный ускоритель для выполнения Dual Key Triple DES (3DES) и ГОСТ 28147-89;
  - Аппаратный ускоритель для выполнения шифрации AES 128, 192 или 256 бит;
  - Модулярный сопроцессор для работы с операндами размером до 1024 битов;
  - Модуль вычисления контрольной суммы (CRC) в соответствии с ISO 3309

- **Стойкость к климатическим и электрическим воздействиям:**
  - Микросхема по стойкости к ультрафиолетовому и рентгеновскому излучению соответствует стандартам ISO 14443-1 и 7816-1.
  - Микросхема по стойкости к электромагнитным полям, статическому электричеству соответствует стандартам ISO 14443-1 и 7816-1.
  - Микросхема обладает стойкостью к воздействию механических и климатических факторов, приведенных в ISO 14443-1 и 7816-1, а также в ГОСТ 18725, в том числе:
    - диапазон рабочей температуры среды: от 0 до 50°C;
    - повышенная температура среды: рабочая +105°C;
    - пониженная температура среды: рабочая - 25°C;
    - предельная температура среды: от -45°C до +125°C
    - относительная влажность от 5 до 95%.

- Внутренне напряжение питания 1.8 В.

2. Описание архитектуры

На рисунке 1 приведена блок-схема микроконтроллера.

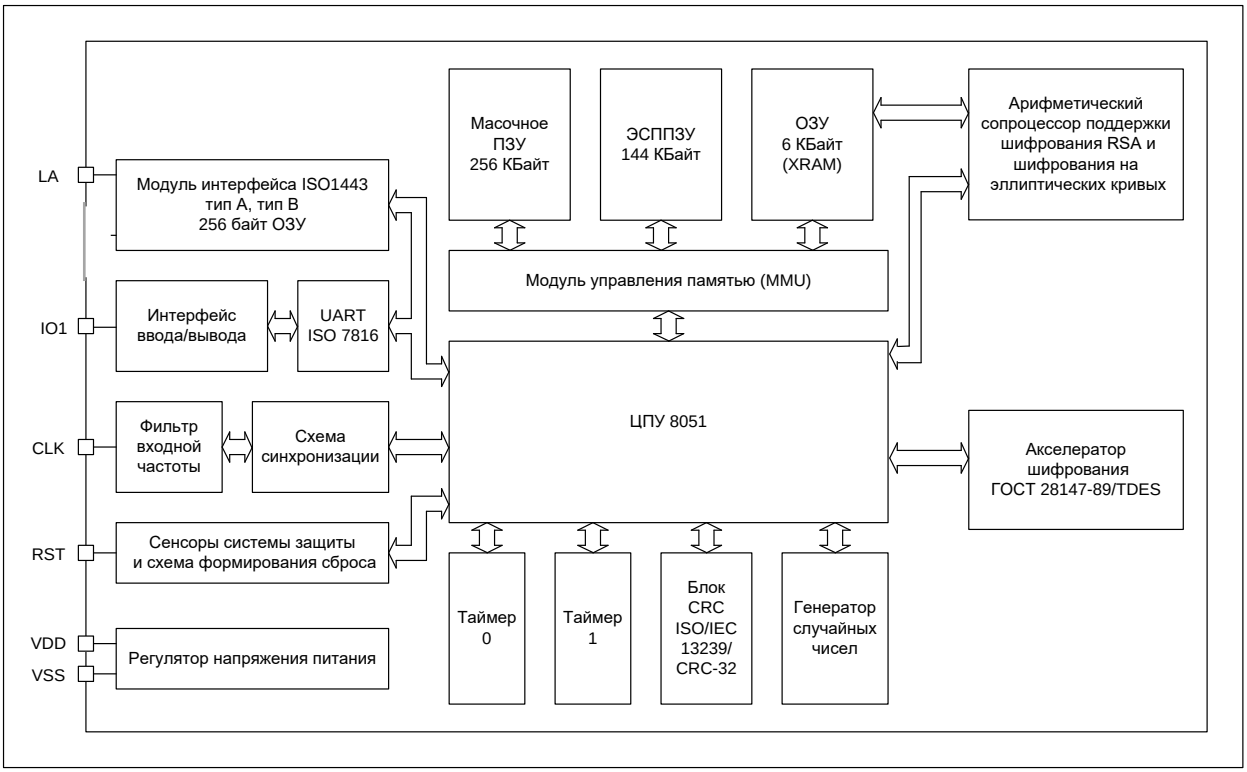

Рис. 1 Блок-схема микроконтроллера.

2.1. ЦПУ

Процессор совместим по системе команд с микроконтроллером 8051, имеет набор дополнительных команд управления расширенной памятью, реализованных через зарезервированный код A5 системы команд микроконтроллера 8051 и оптимизирован для эффективной поддержки компилятора языка Си. Размер встроенной оперативной памяти IRAM рассчитан на поддержку стека памяти компилятора с языка Си. Введены дополнительные указатели данных и команды для ускорения процедур обмена блоками данных между модулями памяти и сопроцессорами.

С использованием встроенного генератора с ФАПЧ внутренний тактовый синхросигнал программируется до 30 МГц независимо от несущей частоты радиочастотного интерфейса или входной частоты проводного интерфейса. Микроконтроллер имеет оптимизированную архитектуру и выполняет инструкции в 3-4 раз быстрее стандартного 8051 при той же тактовой частоте. Процессор может адресовать до 8 Мбайт памяти программ и до 8 Мбайт памяти данных.

2.2. Память.

Микросхема имеет 256 Кбайт пользовательского ПЗУ, 6 Кбайт основного ОЗУ, 128 байт области регистров специальных функций (SFR) и 144 Кбайта ЭСППЗУ.

Микросхема имеет память области защиты размером 128 байт, которая включает в себя:

- 64 байт – аппаратно защищенная от модификации область памяти
- 64 байт – аппаратно защищенная от стирания область памяти для аппаратной блокировки возможности перепрограммирования областей памяти EEPROM, организации счетчиков доступа и механизма защиты на стадиях производства и транспортировки.

2.3. Блок управления и защиты памяти (MMU)

Блок позволяет организовать защищенное выполнение операционной системы. Блок управления и защиты памяти позволяет организовать:

- адресацию памяти до 16 Мбайт;
- программирование до 8 логических сегментов;
- формирование прерывания NMI при обращении по некоректному адресу как при использовании MMU, так и при выключеном MMU.

2.4. Модуль прерываний

Модуль прерываний поддерживает десять источников прерываний. Девять из них выделены для периферийных блоков (ГСЧ, Таймер 0, Таймер 1, UART, интерфейс ввода-вывода и радиочастотный интерфейс, блок EEPROM, сопроцессор RSA/ECC). Одно прерывание (NMI) зарезервировано за аппаратной сигнализацией активного состояния защиты и устройства управления памятью (MMU).

Все источники прерываний, кроме прерывания NMI, могут быть программно отключены. Прерывания обслуживаются процессором в соответствии с запрограммированным приоритетом.

2.5. Таймеры

Микроконтроллер имеет два таймера/счетчика TC0 и TC1. Каждый таймер может быть запрограммирован на работу от встроенного генератора тактовой частоты или от внешнего тактового сигнала. При работе от встроенного генератора тактовой частоты входная частота таймера формируется программируемым предварительным делителем с коэффициентом деления от 2 до 510.

При работе от внешнего тактового сигнала содержимое регистров таймера инкрементируются при каждом переходе сигнала из 1 в 0 на входе CLK микроконтроллера. Максимальная частота подсчета внешних входных импульсов в два раза меньше системной частоты микроконтроллера.

Таймеры могут работать в четырех режимах: 13-разрядный таймер/счетчик, 16-разрядный таймер/счетчик, 8-разрядный таймер/счетчик с автоперезагрузкой и совмещенный режим.

2.6 Бесконтактный (радиочастотный) интерфейс

Радиочастотный интерфейс позволяет осуществить бесконтактный обмен информации между микроконтроллером и считывателем информации. Питающее напряжение и информация принимается антенной, которая состоит из катушки индуктивности, непосредственно подключенной к контроллеру.

Радиочастотный интерфейс обеспечивает передачу данных между микроконтроллером и внешним устройством согласно стандарту ISO14443 тип B.

Интерфейс поддерживает скорости обмена 106 Кбит/с, 212 Кбит/с и 424 Кбит/с при работе в режиме ISO14443-B.

2.7 Последовательный асинхронный интерфейс

Асинхронный приемопередатчик (АПП) обеспечивает последовательную передачу данных между микроконтроллером и внешним устройством. Приемопередатчик поддерживает полудуплексный режим передачи. Приемник позволяет осуществлять контроль паритета, наличие коллизий, целостность фрейма и переполнение FIFO. Функциональная схема блока последовательного интерфейса приведена на рисунке 2.

Приемник имеет FIFO принятых данных на четыре байта. Размер буфера передатчика составляет один байт. Скорость передачи может меняться в широких пределах посредством программирования предварительного делителя. Максимальная скорость передачи составляет 625 кбод при входной частоте синхронизации 10 МГц.

АПП обеспечивает запрос на повторение последнего переданного символа при обнаружении ошибки приема в соответствии с протоколом передачи ISO7816-3 (T=0).

АПП позволяет программировать скорость обмена, проверку паритета, количество стоповых бит, порядок передачи бит данных, полярность данных и условия формирования прерывания.

Передающий и принимающий регистры АПП тактируются внешней тактовой частотой, управляющая логика АПП тактируется системной тактовой частотой.

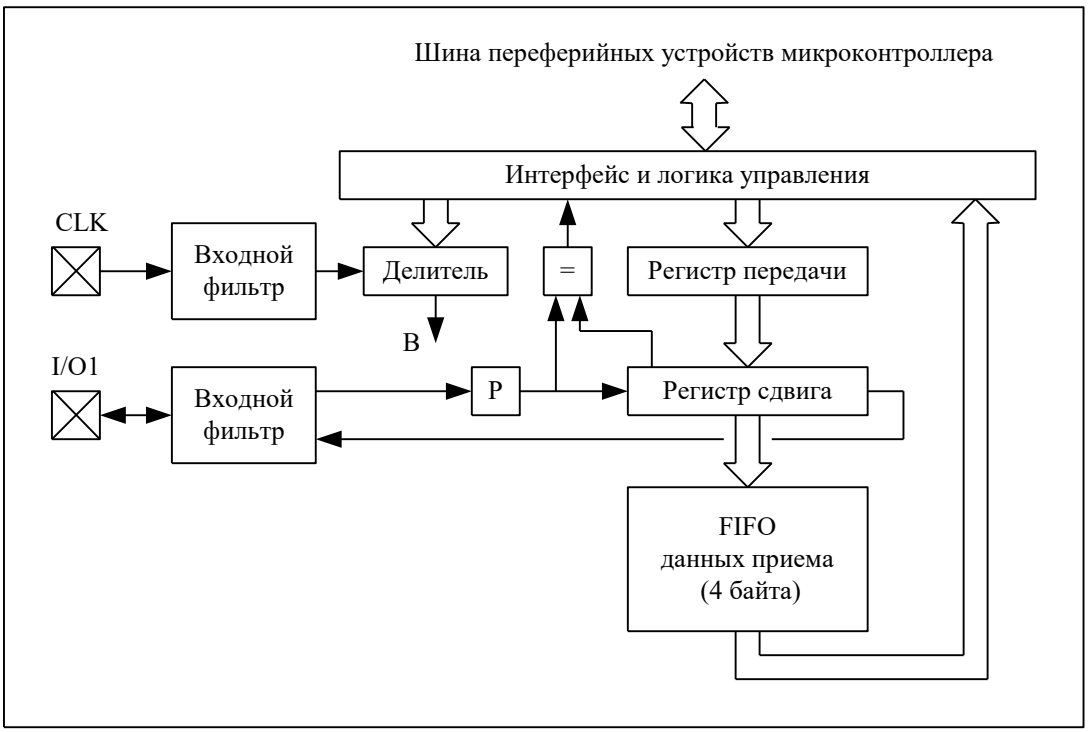

Рисунок 2. Функциональная схема блока последовательного интерфейса

2.8. Блок подсчета контрольной суммы ISO/IEC13239 и CRC-32

Для ускорения проверки целостности принимаемых и передаваемых данных микроконтроллер имеет блок подсчета контрольной суммы в соответствии со стандартами ISO/IEC13239 (ISO/IEC3309) и CRC-32, который генерирует 16-разрядную контрольную сумму в соответствии с полиномом x16+x12+x5+1 и 32-разрядную контрольную сумму в соответствии с полиномом x32+x26+x23+x22+x16+x12+x11+x10+x8 +x7+x5+x4+x2+x1+1.

2.9. Генератор случайных чисел.

Аппаратно-программный генератор случайных чисел предназначен для формирования случайной последовательности бит. Генератор работает от фазы шума сигнала сравнения фазы двух нестабильных RC-генераторов.

Аппаратная часть генератора формирует 8-битные случайные числа за время приблизительно равное 80 мкс. Полученные случайные числа после статистической проверки могут использоваться непосредственно или как начальное значение для программного криптографически стойкого генератора случайных чисел.

2.10. Сопроцессор блочного шифрования

Сопроцессор шифрования по ГОСТ 28147-89 и DES/TDES (шифрование TripleDES с двойным/тройным ключом) – специализированное вычислительное устройство, предназначенное для поддержки быстрого потокового шифрования/расшифровки блоков данных.

Сопроцессор предназначен для шифрования 64-битного блока данных в соответствии с ГОСТ 28147-89. Позволяет программировать значения таблицы замен. Алгоритм шифрования/расшифровки может работать в режиме 16 или 32 шагов.

Сопроцессор поддерживает стандарт шифрования DES. Модуль предназначен для аппаратной поддержки для алгоритмов шифрования DES с одинарным ключом и тройной DES с тройным ключом.

2.11. Арифметический сопроцессор поддержки шифрования RSA и шифрования на эллиптических кривых

Арифметический сопроцессор предназначен для поддержки шифрования RSA и шифрования на эллиптических кривых (ECC), а также для ускорения вычисления хэш-функций SHA-1, SHA-256, ГОСТ Р34.11-2012.

Сопроцессор представляет собой специализированное арифметическое устройство для модулярного и немодулярного перемножения длинных целых чисел. Сопроцессор поддерживает операнды длиной до 4096 бит.

2.12. Модуль шифрования тока потребления

Модуль предназначен для шифрования тока потребления работой ложного токового ключа, управляемого от генератора псевдослучайных чисел. Генератор псевдослучайных чисел основан на сдвиговом регистре с линейной обратной связью с большим периодом повторения. Инициализация генератора псевдослучайных чисел возможна от генератора случайного числа.