# 1. ОБЩАЯ ИНФОРМАЦИЯ

Микросхема представляет собой специализированный контроллер, изготавливаемый по КМОП технологии, и предназначена для использования в качестве системы шифрования данных и организации защищенных каналов связи и доступа с использованием отечественных и зарубежных алгоритмов шифрования, которые предъявляют высокие требования к степени защиты информации от мошеннических действий.

## 1.1. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ:

### ИНТЕРВЕЙС

- Контактный интерфейс в соответствии с ISO 7816 с поддержкой протоколов T0 и T1.

### ПРОГРАММНАЯ ПАМЯТЬ

- Масочное ПЗУ объемом 256 Кбайт
- Срок хранения информации: 10 лет

### ЭНЕРГОНЕЗАВИСИМАЯ ПОЛЬЗОВАТЕЛЬСКАЯ ПАМЯТЬ

- Объем: 16 Кбайт
- Количество циклов перезаписи: >100 000
- 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 с 10 векторами прерываний и 3 уровнями приоритета для работы в режиме реального времени.

- Генератор на базе ФАПЧ для повышения внутреннего тактового сигнала ЦПУ до 30 МГц
- Два 16-разрядных таймера.

### СИСТЕМЫ БЕЗОПАСНОСТИ И ЗАЩИТЫ:

- Микросхема обеспечивает хранение уникального номера микросхемы размером 8 байт.

- Активный металлический щит;
- 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;
- Аппаратная система защиты: светового излучения, повышенного напряжения.
- Модуль управления памятью (Memory Management Unit) с контролем обращения за границей памяти.

## ОСНОВНЫЕ БЛОКИ МИКРОПРОЦЕССОРА:

- Аппаратно-программный генератор случайных чисел (ГСЧ);
- Аппаратный ускоритель для выполнения Dual Key Triple DES (3DES) и ГОСТ 28147-89;
- Модулярный сопроцессор для работы с операндами размером до 4096 битов;
- Модуль вычисления контрольной суммы (CRC) в соответствии с ISO 3309

## ОПЕРАЦИОННАЯ СИСТЕМА:

В состав ОС Trust 3.30I входят приложения:

- CRISP – обеспечивает поддержку основного функционала программно-аппаратного комплекса (ПАК) «Звезда»;
- Crypto – предоставляет криптографические сервисы конечному устройству для решения его собственных задач.

Приложение «Элемент безопасности для Интернета вещей» (CRISP) реализует следующий функционал:

- защищенный канал обмена с сервером;
- удаленное управление ключами;
- формирование электронной подписи (ЭП) передаваемых данных;

Поддерживаемые криптографические алгоритмы:

- ГОСТ 28147-89;
- ГОСТ Р34.12-15 Магма;
- ГОСТ Р34.10-12 (ЭП).

Приложение поддерживает протокол CRISP, предназначенный для защиты передачи данных в Интернете вещей.

Приложение Crypto обеспечивает возможность использования ЭБ в качестве универсального криптографического модуля безопасности (SAM).

## ПОДДЕРЖИВАЕМЫЕ КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ:

- вычисление и проверка ЭП: ГОСТ Р34.10-12 в 256-битном режиме;
- шифрование и вычисление имитовставки: ГОСТ 28147-89, ГОСТ Р34.12-15 Магма, ГОСТ Р34.12-15 Кузнечик;
- хэширование: ГОСТ Р34.11-12 в 256-битном и 512-битном режимах;

- согласование ключей (VKO)/
- шифрование и вычисление имитовставки: DES, 3DES, AES-128, AES-256;
- хэширование: SHA-1, SHA-256.

## 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 (в том числе в корпусном исполнении) обладает стойкостью к воздействию механических и климатических факторов, приведенных в ISO 14443-1 и 7816-1.

## 2. ОПИСАНИЕ АРХИТЕКТУРЫ

На рисунке 1 приведена блок-схема микроконтроллера.

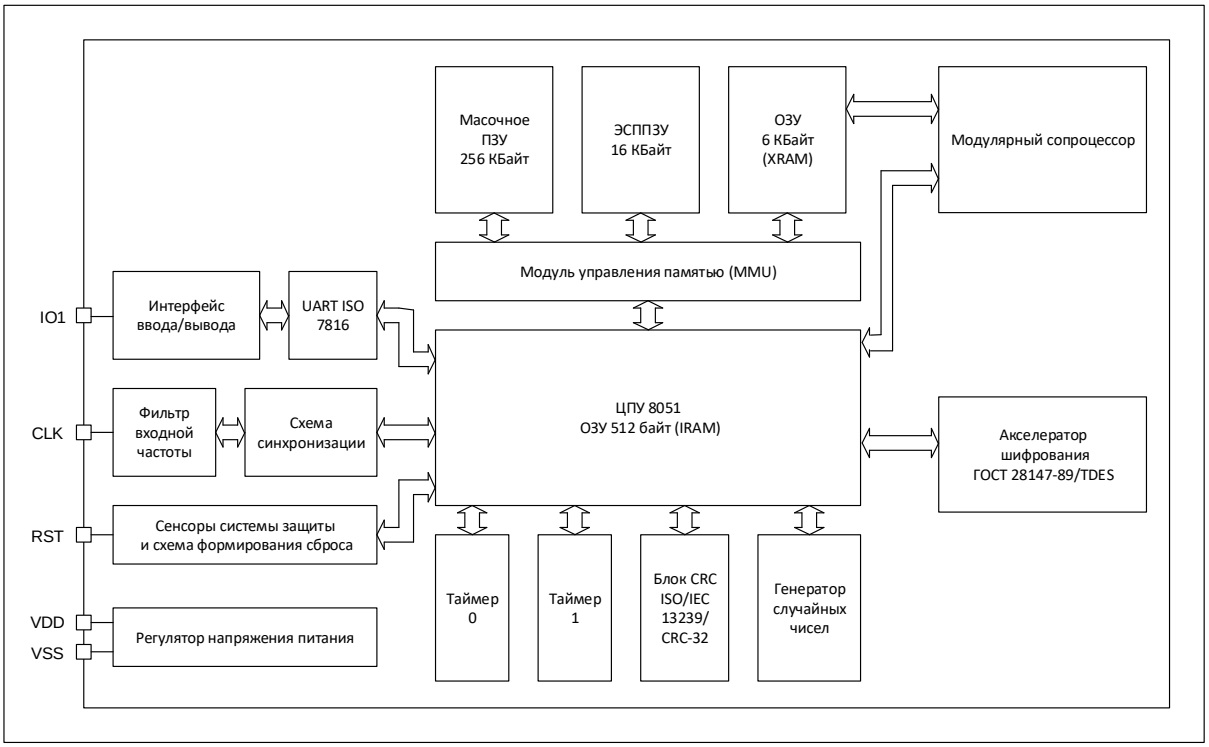



Рис. 1 Блок-схема микроконтроллера.

### 2.1. ЦПУ

Процессор совместим по системе команд с микроконтроллером 8051 и имеет набор дополнительных команд управления расширенной памятью.

Используя встроенный генератор с ФАПЧ, внутренний тактовый синхросигнал программируется до 30 МГц, независимо от внешнего тактирующего сигнала. Микроконтроллер имеет оптимизированную архитектуру с переменным временем выполнения команд и выполняет инструкции до 3 раз быстрее

стандартного 8051 при той же тактовой частоте. Процессор может адресоваться к 8 Мбайт памяти программ и 8 Мбайт памяти данных.

## 2.2. ПАМЯТЬ

Микросхема имеет 256 Кбайт пользовательского ПЗУ, 6 Кбайта основоного ОЗУ, 128 байт области регистров специальных функций (SFR) и 16 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. МОДУЛЬ УПРАВЛЕНИЯ ПАМЯТЬЮ

Модуль управления памятью обеспечивает контроль выхода адресов за границы памяти и отображение памяти программ на ЭСППЗУ и ОЗУ.

## 2.4. МОДУЛЬ ПРЕРЫВАНИЙ

Модуль прерываний поддерживает 10 источников прерываний, включая немаскируемое прерывание NMI, которое вызывается при срабатывании механизмов защиты.

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

## 2.5. ТАЙМЕРЫ

Два интегрированных 16-разрядных таймера имеют структуру и режимы работы в соответствии с архитектурой микроконтроллера 8051. Каждый таймер может быть запрограммирован на работу от встроенного генератора тактовой частоты или от внешнего тактового сигнала. Таймеры работают независимо от состояния микроконтроллера (активное состояние или спящий режим). Выход из спящего режима микроконтроллера возможен по прерыванию от таймера.

## 2.6. ИНТЕРФЕЙС ВВОДА-ВЫВОДА

Интерфейс ввода-вывода обеспечивает передачу данных между СБИС и интерфейсным устройством (устройством чтения карт). Контактный интерфейс обеспечивает:

- Конфигурация контактов и последовательный интерфейс в соответствии с ISO 7816
- Универсальный асинхронный приемопередатчик обеспечивает последовательный интерфейс ISO 7816 с поддержкой протоколов T=0 и T=1.
- Диапазон напряжений питания:
  - 5В±10% (Класс А)
  - 3В± 10% (Класс В)
- Внешний тактовый сигнал синхронизации: от 1 до 10 МГц.
- Внутренний тактовый сигнал ЦПУ до 30 МГц.
- Ток потребления < 15 мА при 5.5В и тактовой частоте ЦПУ не более 24 МГц.
- Защита от электростатического потенциала не менее 4кВ.

Интерфейс ввода-вывода определяет состояние сброса в соответствии с ISO. Логика приемника синхронизируется внешней частотой, а логика передатчика синхронизируется системной частотой.

Порты ввода вывода имеют встроенные pull-up резисторы. Принимаемый с внешних выводов сигнал фильтруется от импульсных помех и выбросов напряжения.

Чтение портов интерфейса определяется инструкциями микроконтроллера. Инструкции микроконтроллера позволяют производить чтение непосредственно с внешнего вывода или из регистров порта.

При каждом изменении состояния входа интерфейса с "1" на "0" устанавливается соответствующий флаг и формируется запрос на прерывание, если оно разрешено.

Интерфейс ввода-вывода позволяет аппаратно организовать выдачу информации на порт по сигналу переполнения таймера.

## 2.7. УНИВЕРСАЛЬНЫЙ АСИНХРОННЫЙ ПРИЁМОПЕРЕДАТЧИК (UART)

UART обеспечивает последовательную передачу данных между микроконтроллером и внешним устройством. Приемопередатчик поддерживает полудуплексный и дуплексный режим передачи. Полнодуплексная передача осуществляется с использованием двух линий ввода-вывода. Приемник позволяет осуществлять контроль паритета, наличие коллизий, целостность фрейма и переполнение FIFO.

Приемник имеет FIFO принятых данных на четыре байта. Размер буфера передатчика составляет один байт. Скорость передачи может меняться в широких пределах посредством программирования одиннадцати бит предварительного делителя с коэффициентом деления от 16 до 2047. Максимальная скорость передачи составляет 625 кбод при входной частоте синхронизации 10 МГц.

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

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

Передающий и принимающий регистры UART тактируются внешней тактовой частотой, управляющая логика UART тактируется системной тактовой частотой, генерируемой схемой синхронизации.

## 2.8. БЛОК ПОДСЧЁТА CRC

Для ускорения проверки целостности принимаемых и передаваемых данных микроконтроллер имеет блок подсчета контрольной суммы согласно стандарту ISO3309.

## 2.9. ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ

Аппаратный генератор случайных чисел предназначен для формирования случайной последовательности байт.

## 2.10. СХЕМА СИНХРОНИЗАЦИИ

Генератор схемы синхронизации выполнен на базе системы фазовой автоподстройки частоты (ФАПЧ) и обеспечивает работу ядра контроллера и периферийных устройств с запрограммированной тактовой частотой до 30 МГц. Генератор может работать как в синхронном режиме с синхронизацией по входной частоте, так и асинхронно.

Микроконтроллер имеет режим пониженного потребления, в котором отключается системная тактовая частота для процессора и части периферийных схем. В этом режиме таймеры могут синхронизироваться системной тактовой частотой или внешней тактовой частотой. Выход из спящего режима производится по следующим событиям – общесистемный сброс, прерывание от таймера или от интерфейса ввода/вывода.

## 2.11. АКСЕЛЕРАТОР ШИФРОВАНИЯ ПО ГОСТ 28147-89 и DES

Акселератор предназначен для шифрования 64-битного блока данных в соответствии с алгоритмами ГОСТ 28147-89, DES и 3DES.

При шифровании по алгоритму ГОСТ 28147-89 позволяет загружать таблицу перестановок. Ускоритель может работать в режиме 16 раундов (для вычисления имитовставки) или 32 раундов.

## 2.12. МОДУЛЯРНЫЙ СОПРОЦЕССОР

Модулярный сопроцессор обеспечивает выполнение арифметических операций по модулю над операндами размером до 4096 бит. Предназначен для реализации следующих криптографических алгоритмов:

- Вычисление и проверка ЭЦП.
- Шифрование / расшифрование данных по алгоритму RSA.

## 2.13. ЗАЩИТА ИНФОРМАЦИИ

Микроконтроллер обеспечивает следующие виды защиты информации от физических и логических атак:

- Мониторинг внешней тактовой частоты и питающего напряжения.
- Контроль доступа к памяти при помощи блока управления и защиты памяти.
- Металлизация областей данных кристалла и специальные сигнальные слои для определения попытки зондирования внутренних компонентов и сигнальных линий.
- Модуль маскирования тока потребления на основе генератора случайных чисел для противодействия анализу (SPA/DPA-атаки).
- Датчик света

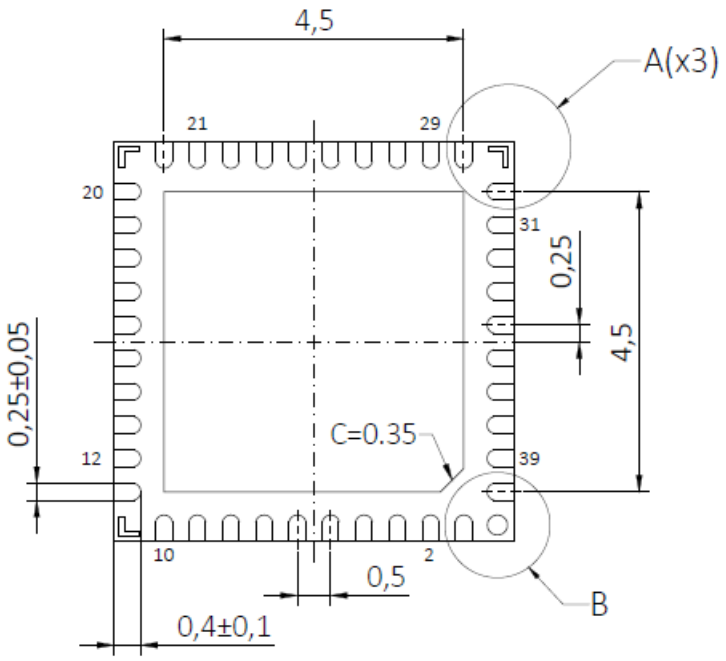
## 2.14. МОДУЛЬ МАСКИРОВАНИЯ ТОКА ПОТРЕБЛЕНИЯ

Модуль маскирует ток 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.

## 3. КОРПУС И НАЗНАЧЕНИЕ ВЫВОДОВ

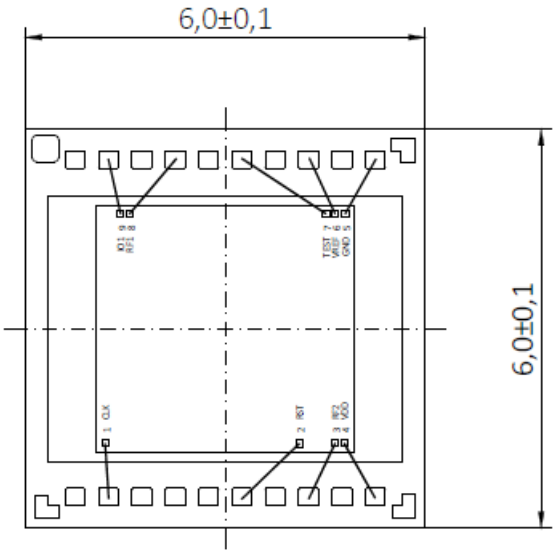
Тип корпуса: LGA40

### ВИД СНИЗУ




### ВИД СВЕРХУ

(Молд компаунд не показан)



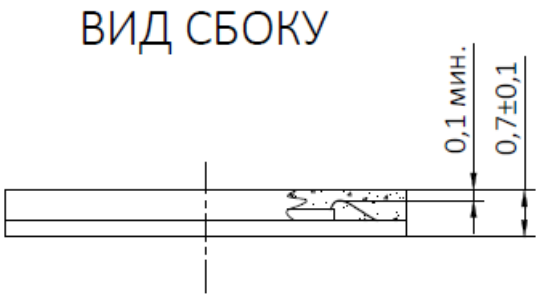



Схема разварки согласно таблице:

| № контакта корпуса | Назначение | Уровни электрических параметров при эксплуатации |
|---|---|---|
| 2 | CLK | В соответствии с ISO 7816-3 |
| 6 | RST | В соответствии с ISO 7816-3 |
| 8 | RF2 | Для подключения антенны в соответствии с ISO 14443 |
| 10 | VDD | В соответствии с ISO 7816-3 |
| 21 | GND | В соответствии с ISO 7816-3 |
| 23 | VREF | Не используется |
| 25 | TEST | Не используется |
| 27 | RF1 | Для подключения антенны в соответствии с ISO 14443 |
| 29 | IO1 | В соответствии с ISO 7816-3 |

Возможно разварка на ленту типа СИМ в соответствии с ISO 7816-2.