ОДНОКРИСТАЛЬНЫЙ МИКРОКОНТРОЛЛЕР С ПОДДЕРЖКОЙ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ, КОНТАКТНОГО И БЕСКОНТАКТНОГО ИНТЕРФЕЙСОВ

ОБЩАЯ ИНФОРМАЦИЯ

Микросхема представляет собой специализированный контроллер с двумя типами интерфейса, изготавливаемый по КМОП технологии, и предназначена для использования в защищенных системах в качестве идентификационных документов, банковской карты, системы защищенного доступа, системы цифровой подписи и передачи, которые предъявляют высокие требования к степени защиты информации от мошеннических действий.

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ:

Площадь микросхемы 14 мм^2

ИНТЕРФЕЙСЫ:

- Бесконтактный интерфейс в соответствии с ISO 14443-2,3,4 тип B:
  - Несущая частота: 13,56 MHz ±7KHz
  - Скорость обмена данными: до 424 Кбит/с
- Контактный интерфейс в соответствии с ISO 7816 с поддержкой протоколов T0 и T1

ПРОГРАММНАЯ ПАМЯТЬ:

- Масочное ПЗУ объемом 364 Кбайт
- Срок хранения информации: 10 лет

ЭНЕРГОНЕЗАВИСИМАЯ ПОЛЬЗОВАТЕЛЬСКАЯ ПАМЯТЬ:

- Объем: 72 кбайт
- Количество циклов перезаписи: >100000
- Срок хранения информации: 10 лет
- Побайтный доступ для считывания ЭППЗУ
- Постраничный режим записи/стирания: от 4 до 128 байт
- 128 байт области защиты:
  - 64 байта: аппаратно защищенная от модификации область памяти
  - 64 байта: аппаратно защищенная от стирания область памяти
- Типовое время стирания страницы: 2 мс
- Типовое время записи страницы: 2 мс
- 6 Кбайт: основное ОЗУ данных (XRAM) и 768 байт внутреннее ОЗУ
- 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 33 МГц
- Два 16-разрядных таймера

СИСТЕМЫ БЕЗОПАСНОСТИ И ЗАЩИТЫ:

- Микросхема обеспечивает хранение уникального номера микросхемы размером 8 байт
- Поверхностная металлизация, экранирующая области памяти данных (ЭСППЗУ)
- 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
- Аппаратная система защиты: от светового излучения, температуры
- Модуль управления памятью (Memory Management Unit) с контролем обращения за границей памяти

ЭЛЕМЕНТЫ КРИПТОГРАФИИ:

- Аппаратно-программный генератор случайных чисел (ГСЧ), обеспечивающий выработку 64 байт за время не более 20 мс, с блоком контроля статистических качеств выходной последовательности и функцией усложнения
- Микроконтроллер обеспечивает формирование ЭЦП по алгоритму ГОСТ Р 34.10-2001 за 200 мс, проверку ЭЦП за 400 мс на частоте 10МГц
- Алгоритм шифрования ГОСТ 28147-89 обеспечивает шифрование блока данных длиной 64 бита за 0.3 мс на частоте 20 МГц
- Алгоритм хеширования ГОСТ Р 34.11-94 обеспечивает вычисление хеша для блока длины 256 бит за 13мс на частоте 20 МГц
- 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 шифрования: 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
- Аппаратная поддержка Crypto-1

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, а также в ГОСТ 18725, в том числе:
    - линейное ускорение 5000 м/с2 (500g)
    - давление 220 бар
    - повышенная температура среды: рабочая +85°С
    - пониженная температура среды: рабочая - 40°С
    - изменение температуры среды в пределах от минус 60°С до плюс 100°С
- Энергосберегающий режим
- Внутренне напряжение питания: 1.8 В

ОПИСАНИЕ АРХИТЕКТУРЫ

На рисунке 1 приведена блок-схема микроконтроллера.

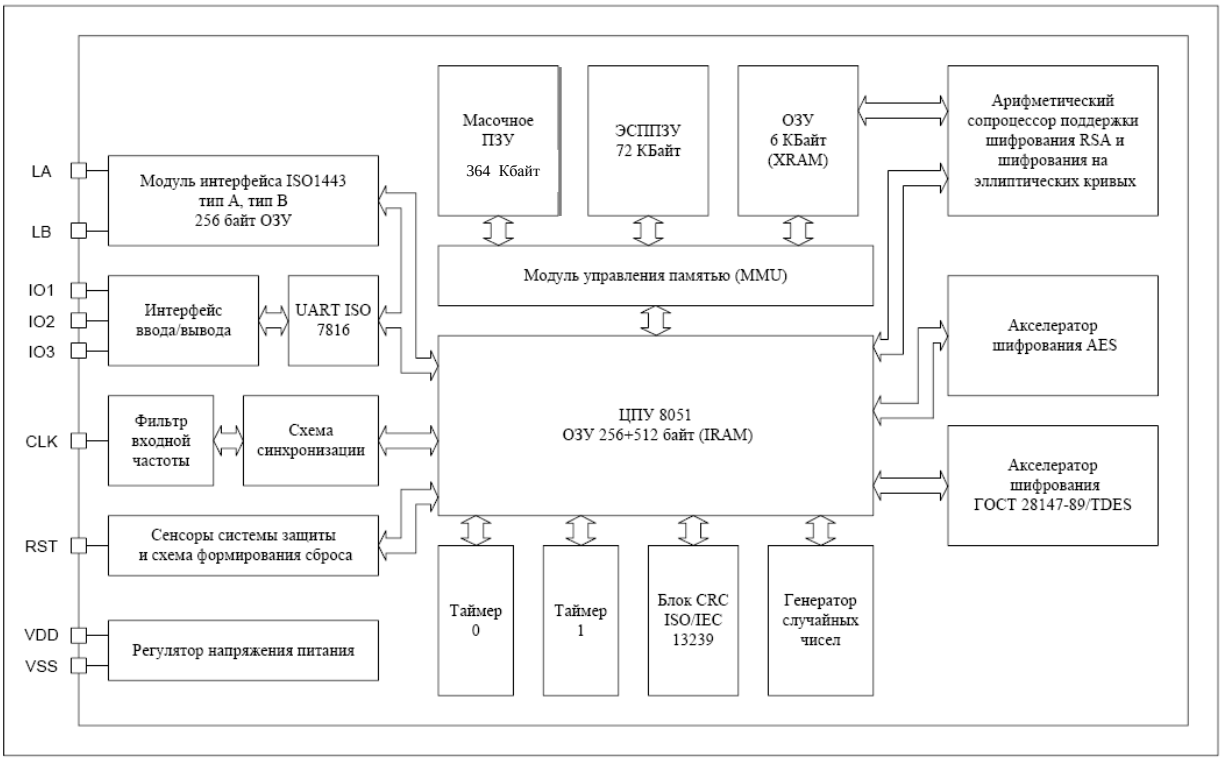

Рис. 1 Блок-схема микроконтроллера.

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 33 МГц, независимо от внешнего тактирующего сигнала. Микроконтроллер имеет оптимизированную архитектуру с переменным временем выполнения команд и выполняет инструкции до 4 раз быстрее стандартного 8051 при той же тактовой частоте. Процессор может адресоваться к 8 Мбайт памяти программ и 8 Мбайт памяти данных.

ПАМЯТЬ

Микросхема имеет 160 Кбайт пользовательского ПЗУ, 256+512 байт внутреннего процессорного ОЗУ, 6 Кбайта основного ОЗУ, 128 байт области регистров специальных функций (SFR) и 72 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.

МОДУЛЬ УПРАВЛЕНИЯ ПАМЯТЬЮ

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

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.

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.

БЕСКОНТАКТНЫЙ (РАДИОЧАСТОТНЫЙ) ИНТЕРФЕЙС

Бесконтактный интерфейс (питание от радиочастоты и радиочастотный интерфейс связи) 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. Бесконтактный интерфейс обеспечивает:

- Интерфейс в соответствии с ISO 14443 тип B
- Несущая частота: 13,56 МГц
- 256-байтный буфер обмена данными
- Скорость передачи: до 848 кбит/сек в режиме B
- Обеспечивается параллельная работа бесконтактного интерфейса и ЦПУ

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 33 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.

УНИВЕРСАЛЬНЫЙ АСИНХРОННЫЙ ПРИЕМОПЕРЕДАТЧИК (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.

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

ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ
Аппаратный генератор случайных чисел предназначен для формирования случайной последовательности байт.

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 33 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.

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.

АРИФМЕТИЧЕСКИЙ СОПРОЦЕССОР ПОДДЕРЖКИ ШИФРОВАНИЯ ПО AES
Арифметический сопроцессор предназначен для быстрого шифрования блока данных размером 128 бит. Длина ключа может составлять 128 или 256 бит.

МОДУЛЯРНЫЙ СОПРОЦЕССОР
Модулярный сопроцессор обеспечивает выполнение арифметических операций по модулю над операндами размером до 1024 бита. Предназначен для реализации следующих криптографических алгоритмов:

- Вычисление и проверка ЭЦП по алгоритмам ГОСТ Р34.10-2001, RSA, EC-DSA
- Шифрование / расшифрование данных по алгоритму RSA

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)
- При срабатывании системы безопасности активного экрана формируется сигнал очистки, который напрямую стирает ЭСППЗУ

ДАТЧИКИ БЕЗОПАСНОСТИ:
Датчик температуры производит контроль температуры микроконтроллера. Если температура выходит за заданный диапазон температур, то система безопасности формирует прерывание.
Датчик уровня освещенности находится под верхним слоем металлизации, и при его удалении активизирует прерывание.

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.

ПОСТАВКА

Микросхема поставляется в виде чип-модулей на ленте.

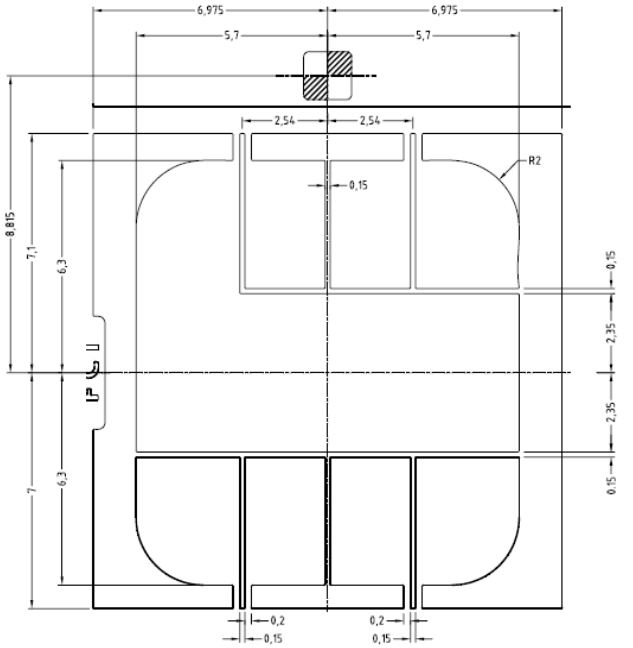

Рисунок 2. Лицевая сторона чип-модуля

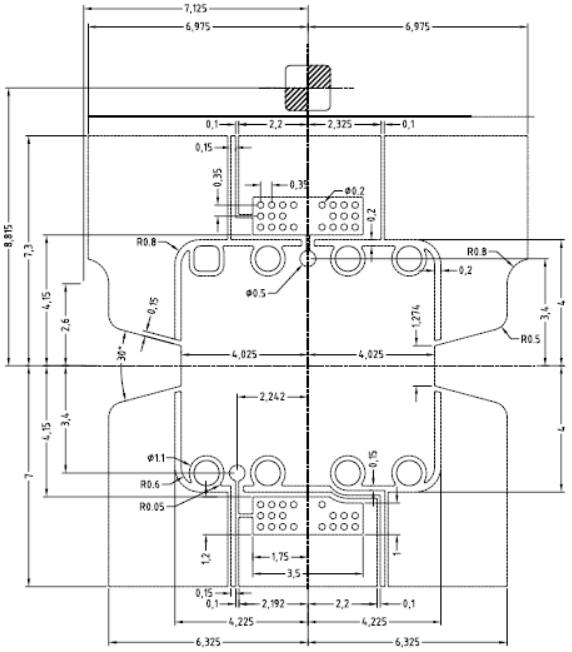

Рисунок 3. Обратная сторона чип-модуля

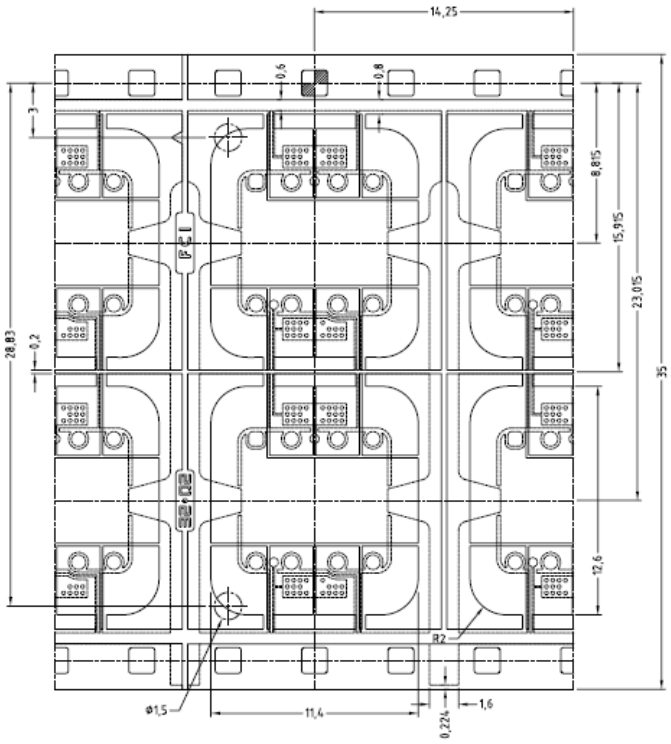

Рисунок 4. Расположение чип-модулей на ленте.

ПРАВИЛА ПРИЁМКИ

Таблица 1: состав испытаний, испытания по группам, последовательность проведения, методы проведения квалификационных и периодических испытаний для контактных и дуальных чип-модулей.

№	Наименование теста	Ссылка	Условия проведения	Длительность	Частота
1. Механические свойства модулей					
1.1	Физические размеры	MIL-STD 883 Meth.2016	В соответствии с утв. чертежом		1 раз в 1,5 года
1.2	Внешний визуальный контроль	MIL-STD 883 Meth.2009	10х увеличение		1 раз в 1,5 года
1.3	Внутренний контроль		Cond. B, 75-150х увеличение		1 раз в 1,5 года
1.3.1	Внутренний визуальный контроль	MIL-STD 883 Meth.2010			
1.3.2	Рентгеновское исследование (присоединение выводов, распределение клея)	MIL-STD 883 Meth.2012 (part 6)			
1.4	Испытания присоединения выводов				1 раз в 1,5 года
1.4.1	Тест на отрыв проволоки	MIL-STD 883 Meth.2011	> 3 cN		
1.4.2	Тест на сдвиг шарика	Внутренняя процедура	> 35 cN		
1.4.3	Измерение высоты петли	Внутренняя процедура	В зависимости от изделия		
1.5	Испытания монтажа кристаллов				1 раз в 1,5 года
1.5.1	Толщина кристалла с клеем	Внутренняя процедура	В зависимости от изделия		
1.6	Соответствие размеров и расположения контактов (лента)[1]	EMV 2000, ISO/IEC 7816-2			1 раз в 1,5 года
2. Термическая и климатическая устойчивость модулей					
2.1	Термоциклирование	MIL-STD 883 Meth.1010	40ºC - +85ºC	10 раз	1 раз в 1,5 года
2.2	Кривая температура / влажность	JESD22-A101	85 ºC, 85% hr	168 часов	1 раз в 1,5 года
3.Химические и электрические свойства модулей					
3.1	Химическая устойчивость поверхности обратной стороны				1 раз в 1,5 года
3.1.1	Химическая устойчивость контактов	ISO/IEC 103-73-1 (part 5.4)	Визуальный контроль и электрический тест	1 мин. (соотв. ISO-Std)	
3.1.2	Тест в соляной атмосфере	MIL-STD 883 Meth.1009 (визуальные критерии) ISO/IEC 103-73-1 (part 5.4)	5% NaCl, 35 ºC, Визуальный контроль и электрический тест	24 ч	
3.2	Электрическое сопротивление контактов	ISO 7816-1; ISO/IEC 103-73-3 (part 5.3)	< 500 мОм		1 раз в 1,5 года
3.3	Устойчивость к УФ излучению	ISO 7816-1	Электрический тест		1 раз в 1,5 года

[1] *Гарантируется поставщиком ленто-носителя, если он CQM-сертифицирован или согласен выполнять требования CQM, указанные в контрактах на поставку*

4. Механическая устойчивость модулей					
4.1	Механическая устойчивость контактов визуальный контроль	ISO 7816-1 (part 4.24)	D=1,0 мм, F max =1,5N Визуальный контроль		1 раз в 1,5 года
5. Механическая устойчивость модулей в картах					
5.1	Тесты на изгиб карт				1 раз в 1,5 года
5.1.2	Динамический стресс на изгиб	ISO/IEC 103-73-3 (part 5.8)	Визуальный контроль и электрический тест	4000 раз	
5.1.3	Динамический стресс на скручивание	ISO/IEC 103-73-3 (part 5.9)	Визуальный контроль и электрический тест	4000 раз	
5.1.4	Тест на свертывание	CQM (10.323)	R =25 мм обязательный, R =40 мм,50 мм дополнительно	3 по 10 раз	
5.1.5	3-колесный тест	CQM (10.323)	F=8N обязательно, F=15N дополнительно	2 по 100 раз	
6. Дополнительные тесты					
6.1	Тестирование профиля поверхности контактов	CQM (6.1.9)		7 модулей 5 точек на каждом	1 раз в 1,5 года
6.2	Токсичность[2]	ISO 7810			
6.3	Тест на изгиб кристалла	CQM (6.2.6) TM-106	$S=3/2xFx\frac{(L-2h)}{(W \times e^2)}$	20 чипов лицевой стороной вверх; 20 чипов лицевой стороной вниз	при разработке нового продукта или его модификации

[2] *Гарантируется поставщиками материалов*