

Микроконтроллер ST23R160

с российской операционной системой СКЗИ ОС «ФОРΟΣ х.х.»
по стандарту ГОСТ Р ИСО/МЭК 7816

Технические характеристики:

- ▶ Микроконтроллер в модульной ленте СВ4;
- ▶ Защищенная энергонезависимая память (EEPROM) — 160 Кбайт;
- ▶ Время хранения данных - не менее 30 лет;
- ▶ Ресурс - не менее 500000 циклов запись/чтение;
- ▶ Интерфейс - ГОСТ Р ИСО/МЭК 14443 типа В;
- ▶ Питание по бесконтактному интерфейсу;
- ▶ Режим низкого энергопотребления;
- ▶ Защита от электростатического разряда (ESD) - до 5000 В;
- ▶ Скорость чтения данных - до 13300 байт/сек;
- ▶ Диапазон рабочих температур: от -25° до +85°;
- ▶ Диапазон предельных температур хранения: от -65° до +150°;
- ▶ Сертификат Common Criteria на микроконтроллер с уровнем доверия EAL 6+;
- ▶ Аппаратные средства защиты от статического исследования;
- ▶ Аппаратные средства защиты от динамического исследования методами SPA, DPA, DFA;
- ▶ Встроенные меры логической защиты от атак к хранимым и обрабатываемым данным, реализуемым как с применением методов инженерного проникновения, так и с помощью анализа побочных сигналов;
- ▶ Сертификат ФСТЭК России на операционную систему по 4 уровню доверия.



Оснащение:

- ▶ Операционная система СКЗИ ОС «ФОРΟΣ х.х.» отечественной разработки (запись в Реестре российского ПО №1542 от 31.10.2022г.), реализующей набор команд в соответствии с ГОСТ Р ИСО/МЭК 7816 включает:
 - создание файловой системы с разграничением доступа, в соответствии с ГОСТ Р ИСО/МЭК 7816-4;
 - криптографические команды в соответствии с ГОСТ Р ИСО/МЭК 7816-8 включая поддержку отечественной и зарубежной криптографии;
 - команды управления жизненным циклом файлов в соответствии с ГОСТ Р ИСО/МЭК 7816-9;
 - средства выработки случайных последовательностей, соответствующие стандартам FIPS 140-2 и AIS31.

Возможности:

- ▶ Защищенное хранение прикладных данных, аутентификация внешних субъектов доступа;
- ▶ Гибкая и полностью настраиваемая система разграничения доступа к внутренним данным и ресурсам приложений. Возможность создать до 64 различных ролей субъектов доступа включая их различные комбинации;
- ▶ Генерация и хранение ключей RSA 1024, 2048;
- ▶ Генерация и хранение ключей ГОСТ 34.10 – 2012;
- ▶ Функция электронной подписи в соответствии с алгоритмами RSA и ГОСТ 34.10-2012;
- ▶ Алгоритмы шифрования в соответствии с ГОСТ 28147-89, ГОСТ Р34.12-2018 (Магма), DES, 3DES;
- ▶ ХЭШ-алгоритмы в соответствии с ГОСТ Р34.11-94, ГОСТ Р34.11-2012, SHA-1;
- ▶ Генерация простого числа заданной длины.

Применяется в качестве:

- ▶ Средства аутентификации внешних субъектов доступа с использованием встроенных в микросхему парольных и криптографических механизмов;
- ▶ Защищенного от несанкционированного доступа средства хранения ключевых, аутентификационных, идентификационных данных;
- ▶ Защищенного, энергонезависимого средства хранения прикладных данных;
- ▶ Доверенного генератора случайных последовательностей типа ПДСЧ, обеспечивающего генерацию случайного числа заданной длины;
- ▶ Средства реализации специфических функций, таких, как ведение независимого счетчика, средства выработки контрольных сумм, ведение защищенного журнала событий и т.д.

Техническая поддержка:

- ▶ Руководство программиста, позволяющее использовать все возможности ОС микроконтроллера микросхемы для реализации задач потребителя;
- ▶ Утилита, которая по файлу конфигурации создаёт необходимую файловую структуру;
- ▶ Исходные коды примеров применения команд ОС.

