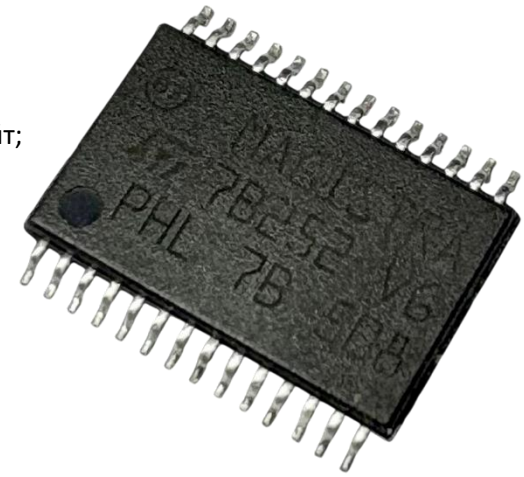
Микроконтроллеры ST19NR66

с российской операционной системой «Магистра» по стандарту ГОСТ Р ИСО/МЭК 7816

Технические характеристики:



► Корпус микросхемы — TSSOP28;

► Защищенная энергонезависимая память (EEPROM) — 66 Кбайт;

► Время хранения данных - не менее 20 лет;

► Ресурс - не менее 500000 циклов запись/чтение;

► Интерфейс - ГОСТ Р ИСО/МЭК 7816-3,4; протокол T=0; поддержка протокола PPS;

► Аппаратные средства защиты от статического исследования;

► Напряжение питания: 1.8В, 3.0В, 5.0В;

► 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 с уровнем доверия EAL 5+.

Оснащение:

► Операционная система Магистра отечественной разработки (запись в Реестре российского ПО №1911 от 23.09.2016 г.), 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.

► Аппаратные средства защиты от динамического исследования методами SPA, DPA, DFA.

ООО «СмартПарк» Москва, Петровско-Разумовский проезд, д.28, офис №616
Тел. +7(495)927-00-33 (многоканальный)
www.smart- park.ru

СмартПарк

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 – 2001;

► Функция электронной подписи в соответствии с алгоритмами RSA и ГОСТ 34.10-2001;

► Алгоритмы шифрования в соответствии с ГОСТ 28147-89, DES, 3DES;

► ХЭШ-алгоритмы в соответствии с ГОСТ Р34.11-94, 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;

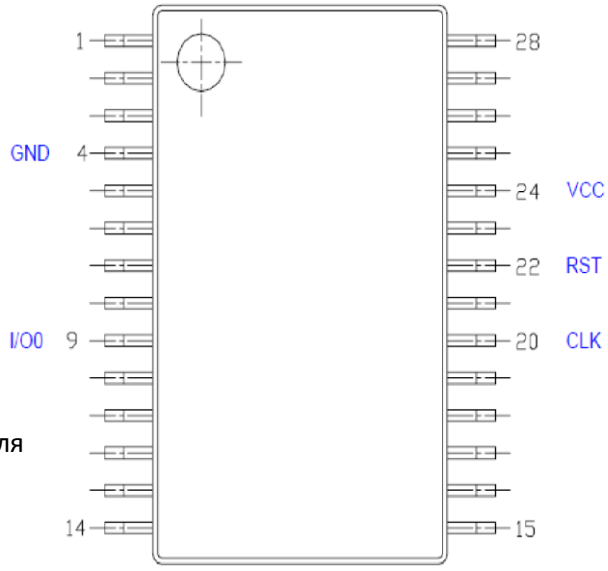
► Доверенного генератора случайных последовательностей типа ПДСЧ, обеспечивающего генерацию случайного числа заданной длины;

► средства реализации специфических функций, таких, как ведение независимого счетчика, средства выработки контрольных сумм, ведение защищенного журнала событий и т.д.;

► Носителя ключевой и идентификационной информации для криптопровайдеров КриптоПро CSP и VipNET CSP.

Техническая поддержка:

1. Размещение выводов микроконтроллера на микросхеме приведено на рисунке справа;
2. Руководство программиста, позволяющее использовать все возможности ОС микроконтроллера микросхемы для реализации задач потребителя;
3. Библиотека в исходных кодах на языке С, реализующую протоколы интерфейса ISO 7816-3. Библиотека ориентирована на платформу микроконтроллеров STM32F411, STM32F407. Возможна адаптация библиотеки для других платформ;
4. Исходные коды примеров применения.



ООО «СмартПарк» Москва, Петровско-Разумовский проезд, д.28, офис №616
Тел. +7(495)927-00-33 (многоканальный)
www.smart- park.ru