ST19KF16

CMOS MCU Based Safeguarded Smartcard with MODULAR ARITHMETIC PROCESSOR

DATA BRIEFING

ST19KF16 FEATURES:

- Enhanced 8 BIT CPU with extended addressing modes
- USER ROM WITH PARTITIONING
- SYSTEM ROM FOR LIBRARIES
- USER RAM WITH PARTITIONING
- USER EEPROM WITH PARTITIONING
  - Highly reliable CMOS EEPROM submicron technology
  - 10 years data retention
  - 100,000 Erase/Write cycles endurance
  - Separate Write and Erase cycles for fast '1' programming
  - 1 to 64 bytes Erase or Program in 2 mS
- SECURITY FIREWALLS FOR MEMORIES AND MAP
- VERY HIGH SECURITY FEATURES INCLUDING EEPROM FLASH PROGRAM, AND CLOCK MANAGEMENT
- 8 BIT TIMER WITH INTERRUPT CAPABILITY
- 2 SERIAL ACCESS, ISO 7816-3 COMPATIBLE
- 3V ± 10% or 5V ± 10% SUPPLY VOLTAGE
- POWER SAVING STANDBY MODE
- CONTACT ASSIGNMENT COMPATIBLE ISO 7816-2
- UNIQUE SERIAL NUMBER ON EACH DIE
- ESD PROTECTION GREATER THAN 5000V

	Device type
	ST19KF16
ROM (Bytes)	32K
RAM (Bytes)	1984
EEPROM (Bytes)	16K

- 1088 Bit MODULAR ARITHMETIC PROCESSOR
  - Fast modular multiplication and squaring using Montgomery method
  - Software Crypto Libraries for efficient algorithm coding using a set of advanced functions
  - Software selectable operand length up to 2176 bits
- FAST CRYPTOGRAPHIC FUNCTIONS PROCESSING:

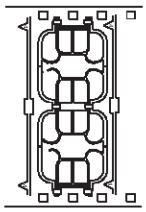
Function	Time Typ
RSA 1024 bits signature with CRT(*)	80 ms
RSA 1024 bits signature without CRT	260 mS
RSA 1024 bits verification(e=$10001)	5 ms
RSA 2048 bits signature with CRT	525 ms
RSA 2048 bits signature without CRT	N/A
RSA 2048 bits verification (e=$10001)	85 ms
EC 160 bits signature	175 ms
EC 160 bits verification	350 ms
Prime Number 512 bits generation	1.1 s

(*)CRT: Chinese Remainder Theorem

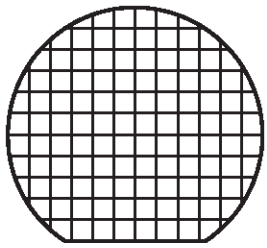
Notes:

– Typical values for 5v operation (Internal Clock)

Figure 1 Delivery form



Micromodule (D4)



Wafer

HARDWARE DESCRIPTION

The ST19KF16, a member of the ST19 device family, is a serial access microcontroller especially designed for very large volume and cost effective secure portable object applications, where high performance Public Key Algorithms are required.

Its internal Modular Arithmetic Processor (MAP) is designed to speed up cryptographic calculations using Public Key Algorithms. Based on a 1088 bits processor architecture, it processes modular multiplication and squaring up to 1088bits modulo.

The ST19KF16 is based on a STMicrolectronics 8 bit CPU and includes on chip memories: User ROM, User RAM and User EEPROM with state of the art security features.

ROM, RAM and EEPROM memories can be configured into partitions with customized access rules. Access from any memory area to another are protected by hardware FIREWALLS. Access rules are User defined and can be selected by mask options or during the life of the product..

It is manufactured using the highly reliable ST CMOS EEPROM submicron technology.

As with all the other ST19 family members, it is fully compatible with the ISO7816 standards for Smartcard applications.

SOFTWARE DEVELOPMENT

Software development and firmware (ROM code/ options) generation are done with the ST16-19 HDSE development system.

CRYPTOGRAPHIC LIBRARIES

For an easy and efficient use of the MAP, ST proposes a complete set of firmware subroutines. This library is located in a specific ROM area, leaving the User ROM for the application software. This library saves the operating system designer from coding first layer functions and allows the designer to concentrate on algorithms and Public Key Cryptographic (PKC) protocol implementation.

This library contains firmware functions for:

– loading and unloading parameters and results to or from the MAP
– calculating Montgomery constants
– basic mathematics including modular squaring and multiplication for various lengths
– modular exponentiation with or without using the Chinese Remainder Theorem (CRT),
– RSA signatures and authentications for any modulo length up to 2176 bits long, DSA signature and verification up to 1088 bits.
– long random number generation.
– full key generation for RSA and DSA (including prime numbers generation)
– hashing algorithm SHA-1.

Figure 2 ST19KF16 Block Diagram