ST19CF68

CMOS MCU Based Safeguarded Smartcard With Modular Arithmetic Processor & 8 KBytes EEPROM

DATA BRIEF

PRODUCT FEATURES

- ENHANCED 8 BIT CPU WITH EXTENDED ADDRESSING MODES
- 23 KBYTES OF USER ROM WITH PARTITIONING
- SYSTEM ROM FOR LIBRARIES
- 960 BYTES OF USER RAM WITH PARTITIONING
- 8 KBYTES OF 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 1 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
- 512 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 1024 bits

- FAST CRYPTOGRAPHIC FUNCTIONS PROCESSING AT 5V, 10 MHZ:

Function	Time
RSA 512 bits signature with CRT (*)	70 ms
RSA 512 bits signature without CRT	195 ms
RSA 512 bits verification(e=$10001)	5 ms
RSA 768 bits signature with CRT	190 ms
RSA 768 bits signature without CRT	N/A
RSA 768 bits verification (e=$10001)	100 ms
RSA 1024 bits signature with CRT	400 ms
RSA 1024 bits signature without CRT	N/A
RSA 1024 bits verification(e=$10001)	145 ms

(*)CRT: Chinese Remainder Theorem

Figure 1 Delivery form

Micromodule (D4)

Wafer
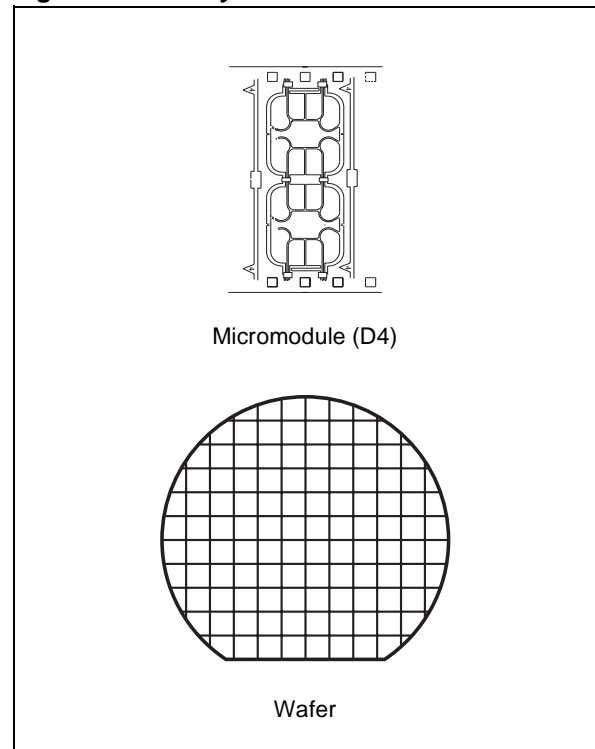
HARDWARE DESCRIPTION

The ST19CF68, a member of the ST19 device family, is a serial access microcontroller especially designed for very large volume and cost competitive secure portable objects.

Its internal Modular Arithmetic Processor (MAP) is designed to speed up cryptographic calculations using Public Key Algorithms. Based on a 512 bits processor architecture, it processes modular multiplication and squaring up to 512 bits modulo.

The ST19CF68 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 ISO 7816 standards for Smartcard applications.

SOFTWARE DEVELOPMENT

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

Figure 2 Block Diagram
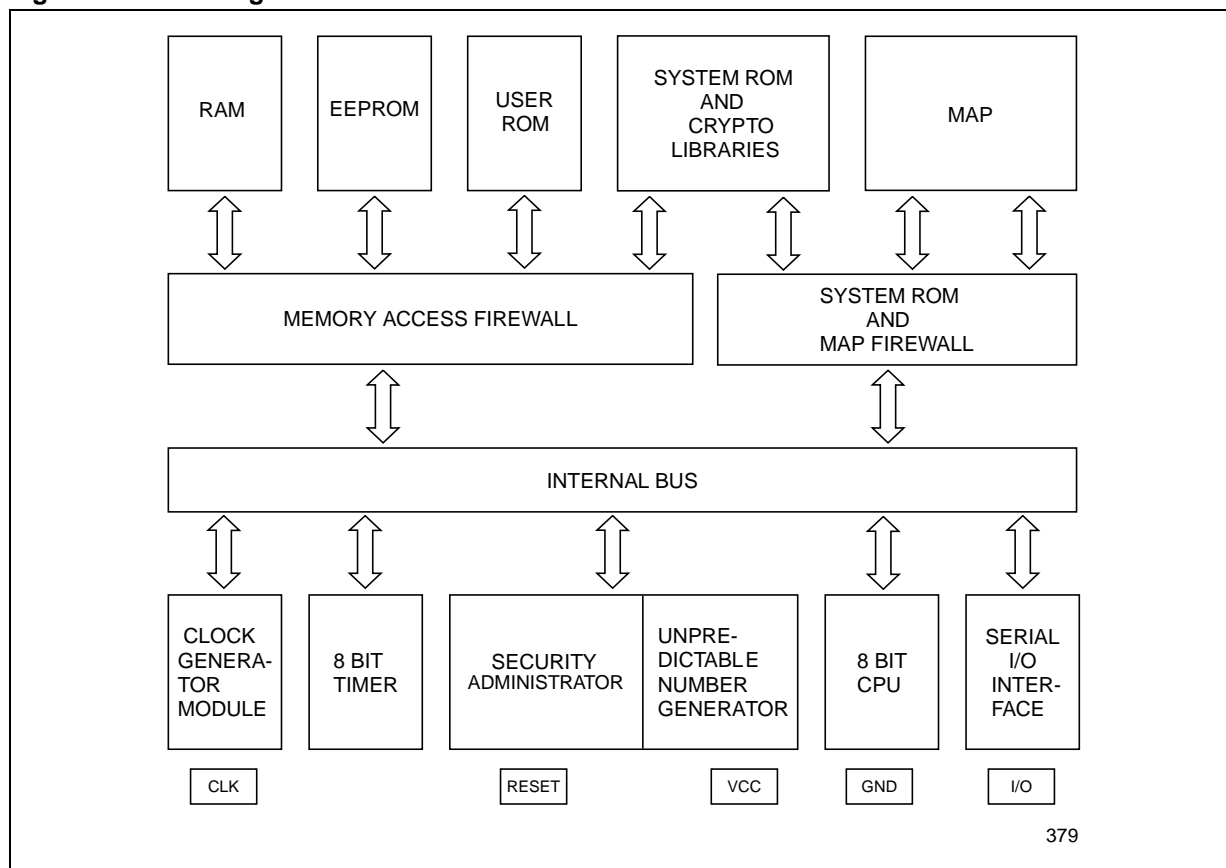
CRYPTOGRAPHIC LIBRARIES

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 1024 bits long, DSA signature and verification up to 512 bits.

– long random number generation.

– full key generation for RSA and DSA (including prime numbers generation)

– hashing algorithm SHA-1.

STMicroelectronics GROUP OF COMPANIES

Australia - Belgium - Brazil - Canada - China - Czech Republic - Finland - France - Germany -
Hong Kong - India - Israel - Italy - Japan - Malaysia - Malta - Morocco - Singapore -
Spain - Sweden - Switzerland - United Kingdom - United States
www.st.com