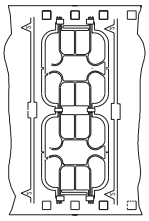
ST16CF54 Level B

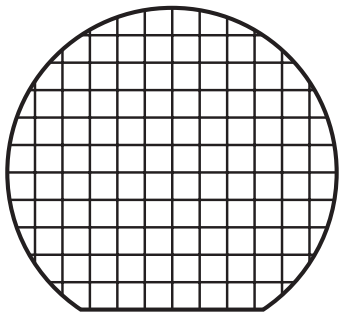
Smartcard MCU
With 4 KBytes EEPROM & 512 Bits Modular Arithmetic Processor

DATA BRIEFING

- 8 BIT ARCHITECTURE CPU
- 16 KBytes of USER ROM SECTOR COMBINATIVE
- 8 KBytes of SYSTEM ROM
- 512 Bytes of RAM
- 4 KBytes of EEPROM, SECTOR COMBINATIVE
- 512 BITS MODULAR ARITHMETIC PROCESSOR
  - Fast modular multiplication and squaring using Montgomery method
  - Driven by STMicroelectronics cryptographic library
- EFFICIENT CRYPTOGRAPHIC LIBRARY
  - Embedded software for driving the MAP through a set of advanced functions
  - Supports modular and non modular arithmetic
  - Operand length can be any size up to 1024 bits
  - Highly reliable CMOS EEPROM technology
  - 10 year data retention
  - 100,000 Erase/Write cycle endurance
  - Protected One Time Programmable block (32 or 64 Bytes)
  - Separate Write and Erase cycle for fast “1” programming
  - 1 to 32 Bytes block either Erase or Write in single cycle programming
- SERIAL ACCESS, ISO 7816-3 COMPATIBLE
- SINGLE 5V ±10% SUPPLY VOLTAGE
- STANDBY MODE FOR POWER SAVING
- UP TO 5 MHz INTERNAL OPERATING FREQUENCY
- VERY HIGH SECURITY FEATURES INCLUDING EEPROM FLASH ERASE
- CONTACT ASSIGNMENT COMPATIBLE ISO 7816-2



Micromodule (D4)



Wafer

- ESD PROTECTION GREATER THAN 5000V
- 2 OPERATING CONFIGURATIONS
  - ISSUER
  - USER
- SOFTWARE SUPPORT
  - Cryptographic Library
  - Manager
- FAST CRYPTOGRAPHIC FUNCTIONS PROCESSING

Function	Speed *
512 bits signature with CRT **	125 ms
512 bits signature without CRT	375 ms
768 bits signature with CRT	350 ms
768 bits authentication (e=$10001)	190 ms
1024 bits signature with CRT	770 ms
1024 bits authentication (e=$10001)	265 ms

Note * 5MHz clock CPU
** CRT: Chinese Remainder Theorem

This is Brief Data from STMicroelectronics. Details are subject to change without notice. For complete data, please contact your nearest Sales Office or SmartCard Products Divison, Rousset, France. Fax: (+33) 4 42 25 87 29

DESCRIPTION

The ST16CF54 Level B, a member of the ST16 device family, is a serial access microcontroller especially designed for high volume and cost competitive Smartcard applications, where high performance Public Key Algorithms will be implemented, to cut down initialization and communication costs and to increase security.

Its internal Modular Arithmetic Processor is designed to speed up cryptographic calculations required in Public Key Algorithms. It processes hardware modular multiplication and squaring on various size 32/256/288/384/416/512 bits operand. By using of software (cryptographic firmware library) this calculation can be extended for any size of operand from 3 to 1024 bits. The ST16CF54 Level B is based on an ST 8 bit CPU core including on-chip memories: 512 Bytes of RAM, 16 KBytes of USER ROM and 4 KBytes of EEPROM.

Both ROM and EEPROM memories can be configured into two sectors. Access rules from any memory section (sector) to another are setup by the User defined Memory Access Control Matrix.

In addition, to reinforce the security of this product, an hardware mechanism called SRAC (SYSTEM ROM Access Control) has been implemented. It protects against unauthorized access to both SYSTEM ROM and MAP.

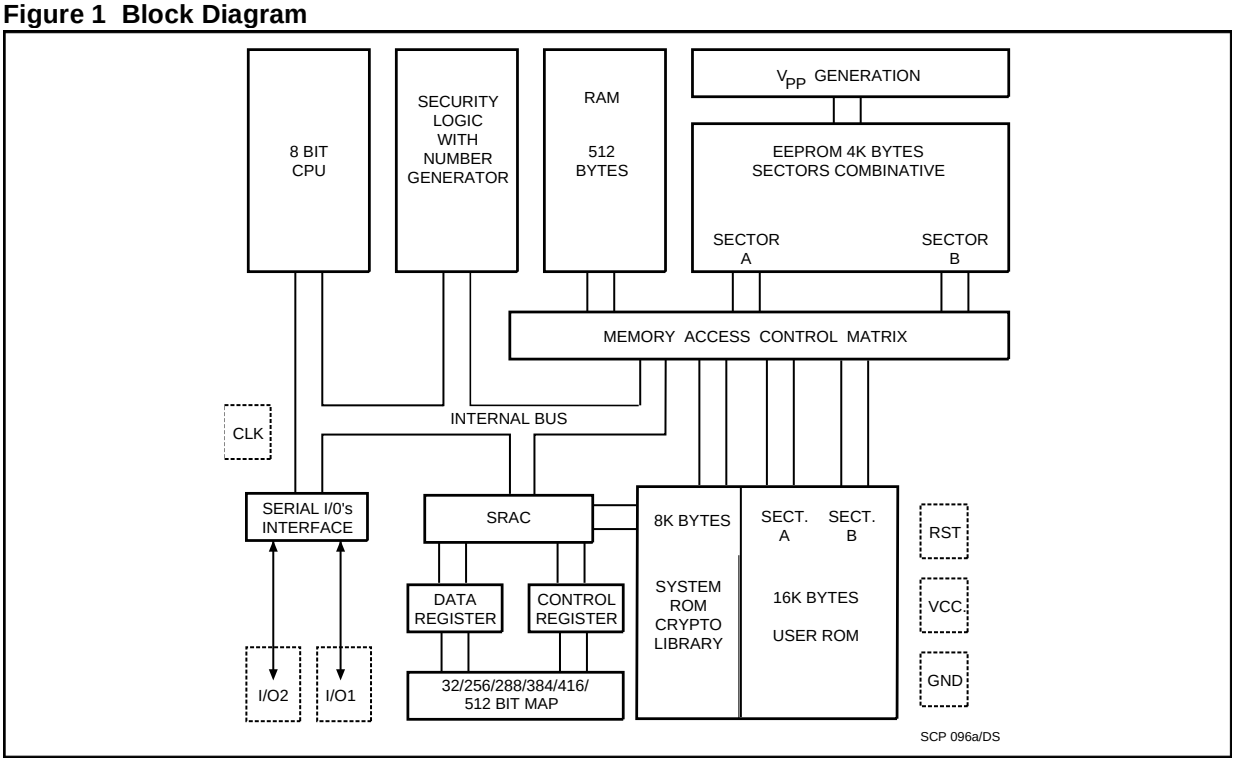
Reliability data related to the ST16CF54 Level B product, manufactured using ST's advanced CMOS EEPROM technology, confirm data retention of up to 10 years and endurance up to 100,000 Erase/Write cycles.

As all other ST16 family members, it is fully compatible with the ISO standards for Smartcard applications.

Software development and firmware (ROM code, options) generation are completed by the ST16-19HDS development system.

The ST16CF54 Level B can be delivered either as unsawn or sawn wafers, 180 or 275 micron thickness as well as in micromodule package.

Figure 1 Block Diagram



SOFTWARE SUPPORT

CRYPTO LIBRARY

For an easy and efficient use of the Modular Arithmetic Processor (MAP), ST proposes a complete set of firmware subroutines. This library is located in the System ROM area, leaving 16 KBytes in 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 for appropriate mathematical implementation of modular calculations
– basic mathematics for modular and non modular operations on any length operand up to 1024 bits
– modular experimentation on operands of any length up to 1024 bits
– more elaborate functions such as RSA based operations, digital signatures and hashing algorithms
– long random number generation