SGS-THOMSON MICROELECTRONICS

ST16CF54

CMOS MCU BASED SAFEGUARDED SMART CARD IC WITH MODULAR ARITHMETIC PROCESSOR

BRIEF DATA

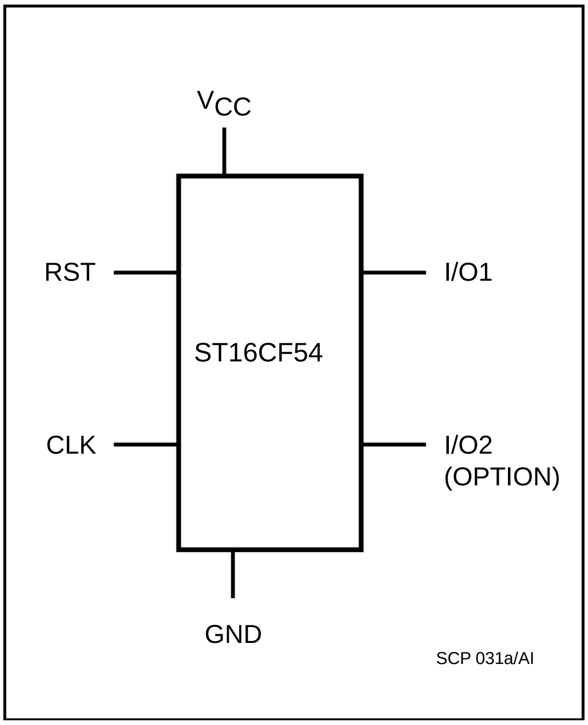
- 8 BIT ARCHITECTURE CPU
- 16 Kbytes OF USER ROM, SECTOR COMBINATIVE
- 4 Kbytes OF SYSTEM ROM
- 480 bytes OF RAM
- 4 Kbytes OF EEPROM, SECTOR COMBINATIVE
  - Highly reliable CMOS EEPROM technology
  - 10 years data retention
  - 100 000 Erase/Write cycles endurance
  - Protected One Time Programmable block (32 or 64 bytes)
  - Separate Write and Erase cycle for fast “1” programming
  - 1 to 32 bytes block Erase or Write in single cycle programming
- MODULAR ARITHMETIC PROCESSOR
  - Fast modular multiplication and squaring using Montgomery method
  - Software Crypto Libraries in separate ROM area for efficient algorithm coding using a set of advanced functions
  - Software selectable operand length (256/512/768 bits)
- 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
- ESD PROTECTION GREATER THAN 5000V
- 2 OPERATING CONFIGURATIONS
  - ISSUER
  - USER
- SOFTWARE SUPPORT
  - Cryptographic Library
  - Crypto Manager
- FAST CRYPTOGRAPHIC FUNCTIONS PROCESSING

	Level A	Level B *
512 bits signature without CRT **	385 ms	195 ms
768 bits signature with CRT	870 ms	185 ms
768 bits authentication (e=$10001)	445 ms	160 ms
1024 bits signature with CRT	N/A	395 ms
1024 bits authentication (e=$10001)	N/A	310 ms

Notes * Available soon

** CRT: Chinese Reminder Theorem

Pin Connection



This is Advance Data from SGS THOMSON. Details are subject to change without notice.

INTRODUCTION

The ST16CF54, a member of the ST16XYZ family devices, is a serial access microcontroller especially designed for very large volume and cost competitive smartcards 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 using Public Key Algorithms. It processes modular multiplication and squaring on 256/512/768 bit operands or a double operand of 1024 bits using software. The ST16CF54 is based on an SGS-THOMSON 8 bit CPU core including on-chip memories: 480 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 any other are setup by the User defined Memory Access Control Matrix.

It is manufactured using the high reliable SGS-THOMSON CMOS EEPROM technology.

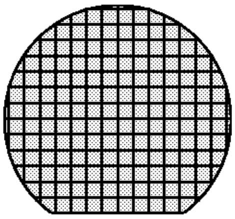
As all the other ST16xyz family members, it is fully compatible with the ISO standards for smartcards applications.

Software development and firmware (ROM code/ options) generation are done with the ST16S-CEXT crypto extension of the ST16S-EMU development system.

Contact name

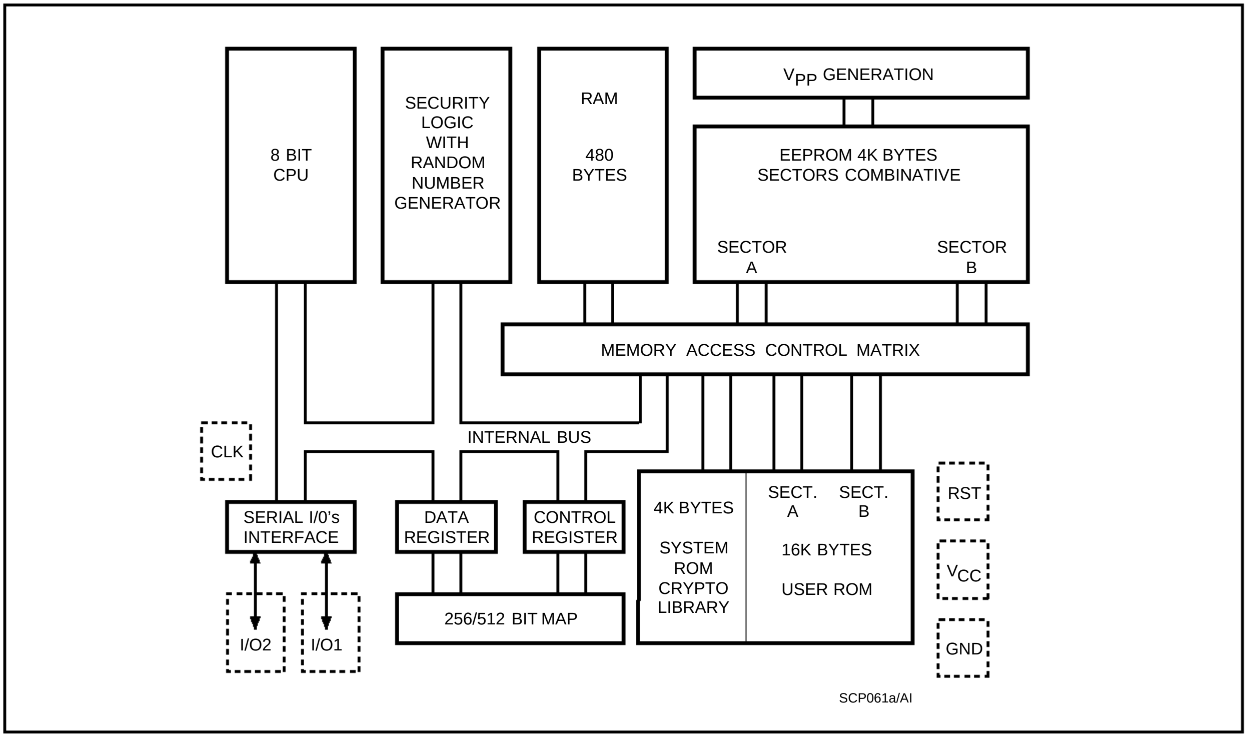
CLK	Clock
RST	Reset
I/O1	Data Input/Output
I/O2	Data Input / Output (option)
Vcc	Supply Voltage
GND	Ground

Delivery form



The ST16CF54 can be delivered either in unsawn or sawn wafers, 180 or 275 micron thickness.

ST16CF54 Block Diagram



This is Advance Data from SGS THOMSON. Details are subject to change without notice.

SOFTWARE SUPPORT

CRYPTO LIBRARIES

For an easy and efficient use of the Modular Arithmetic Processor (MAP), SGS THOMSON proposes a complete set of firmware subroutines. The first introduction, corresponding to Level A, is named “LIB1”. This library is located in a specific ROM area, leaving 16 Kbytes in the User ROM for the application software.

It saves the operating system designer from coding first layers functions and allows to concentrate on algorithms and Public Key Cryptographic (PKC) protocols 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, such as modular squaring and multiplication for various length
- modular exponentiation with or without using the Chinese Reminder Theorem (CRT),
- more elaborate functions such as RSA signatures and authentications for modulo length ranging from 256 to 768 bits long
- fully internal key generation for calculating the key set necessary for signatures/authentications. This guarantees that the secret key will never be known outside the Smartcard, and contributes to overall system security.
- long random numbers generation

This introduction will be followed by Level B library which will include more elaborate algorithms such as 1024 bits operations, DSA and SHA.

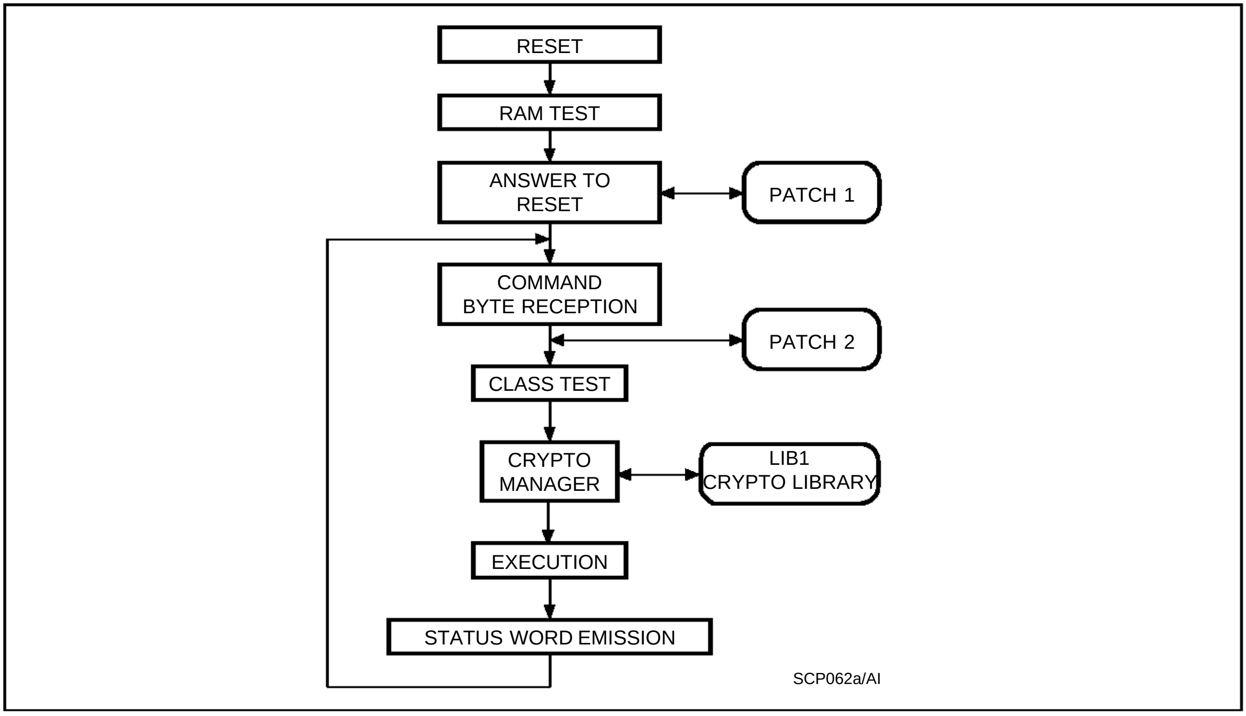
CRYPTO MANAGER

The ST16CF54 Crypto Manager is a firmware in accordance to the SGS THOMSON Chip Manager concept, implemented on the MCU based Smartcard IC. It includes ISO compatible commands allowing an easy access to the chip memories, and commands for activating functions of the LIB1 crypto library.

This Crypto Manager is designed to reduce the time required for the product evaluation and the development of smartcard cryptographic applications, by giving an easy access to the MAP calculations through the library.

Patches can be made in this Crypto Manager, allowing to add/remove functions and adapt it to specific applications for evaluations, tests or field trials.

ST16CF54 Manager flowchart



This is Advance Data from SGS THOMSON. Details are subject to change without notice.

Information furnished is believed to be accurate and reliable. However, SGS-THOMSON Microelectronics assumes no responsibility for the consequences of use of such information nor for any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SGS-THOMSON Microelectronics. Specifications mentioned in this publication are subject to change without notice. This publication supersedes and replaces all information previously supplied. SGS-THOMSON Microelectronics products are not authorized for use as critical components in life support devices or systems without the express written approval of SGS-THOMSON Microelectronics.

BULL CP8 Patents

SGS-THOMSON Microelectronics Group of Companies
Australia - Brazil - China - France - Germany - Hong Kong - Italy - Japan - Korea - Malaysia - Malta -
Morocco - The Netherlands - Singapore - Spain - Sweden - Switzerland -
Taiwan - Thailand - United Kingdom - U.S.A.