SGS-THOMSON MICROELECTRONICS

ST16CF54 Level A

CMOS MCU BASED SAFEGUARDED SMART CARD IC WITH MODULAR ARITHMETIC PROCESSOR

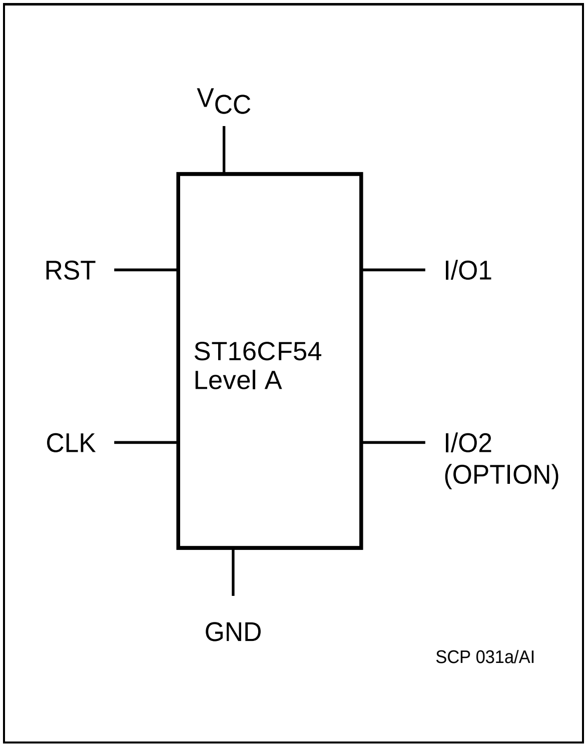
BRIEF DATA

- 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 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
- 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
- POWER SAVING STANDBY MODE
- 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

Function	Speed
512 bits signature without CRT *	385 ms
768 bits signature with CRT	870 ms
768 bits authentication (e=$10001)	445 ms
1024 bits signature with CRT	N/A
1024 bits authentication (e=$10001)	N/A

Note * CRT: Chinese Remainder Theorem

Figure 1 Pin Connection



This is Brief Data from SGS THOMSON Microelectronics. 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 A, a member of the ST16XYZ 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 using Public Key Algorithms. It processes modular multiplication and squaring on 256/512/768 bit operands. The ST16CF54 Level A is based on an SGS THOMSON Microelectronics 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's defined Memory Access Control Matrix.

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

Reliability data related to the ST16CF54 Level A 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.

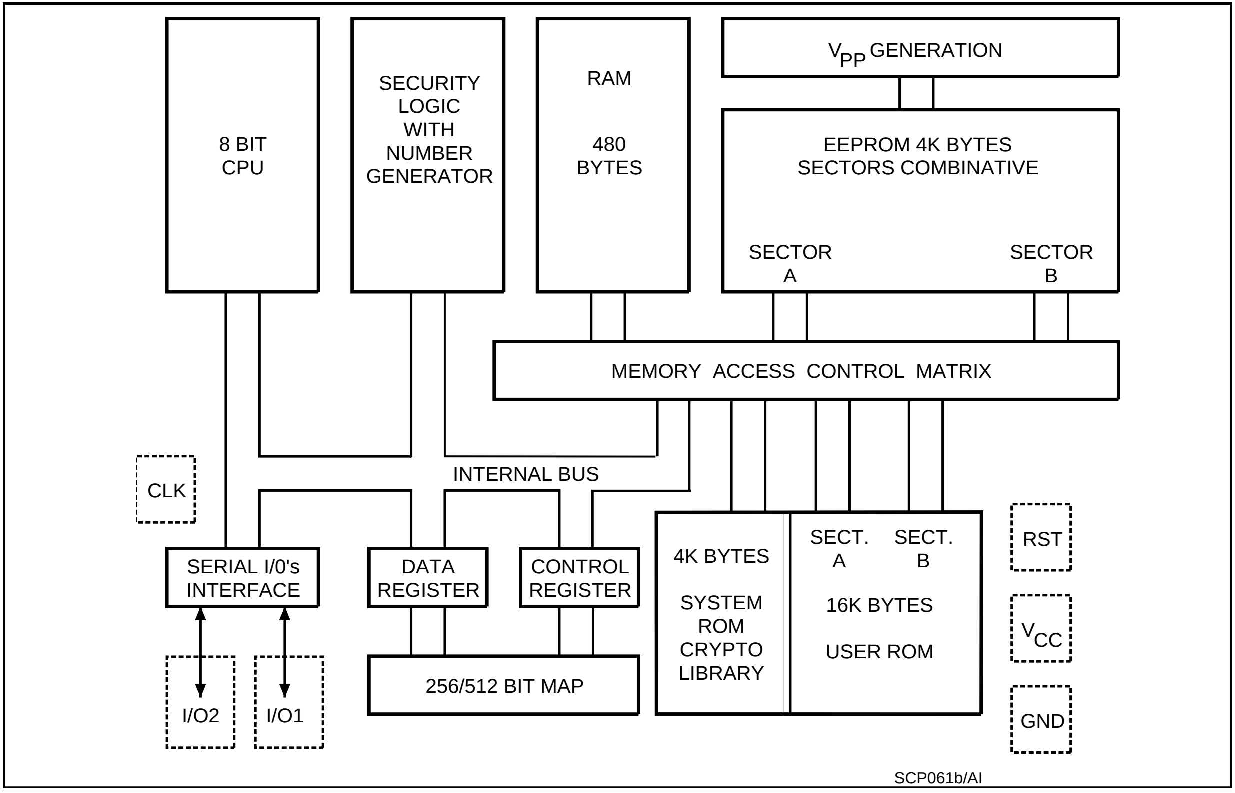
As all other ST16xyz family members, it is fully compatible with the ISO standards for Smartcard applications.

Software development and firmware (ROM code/ options) generation are completed by the ST16S-EMU + ST16S-CEXT development system.

Table 1 Contact name

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

Figure 2 ST16CF54 Level A 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 named “LIB1”, is located in a specific 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, such as modular squaring and multiplication for various length
- modular exponentiation with or without using the Chinese Remainder 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 number generation

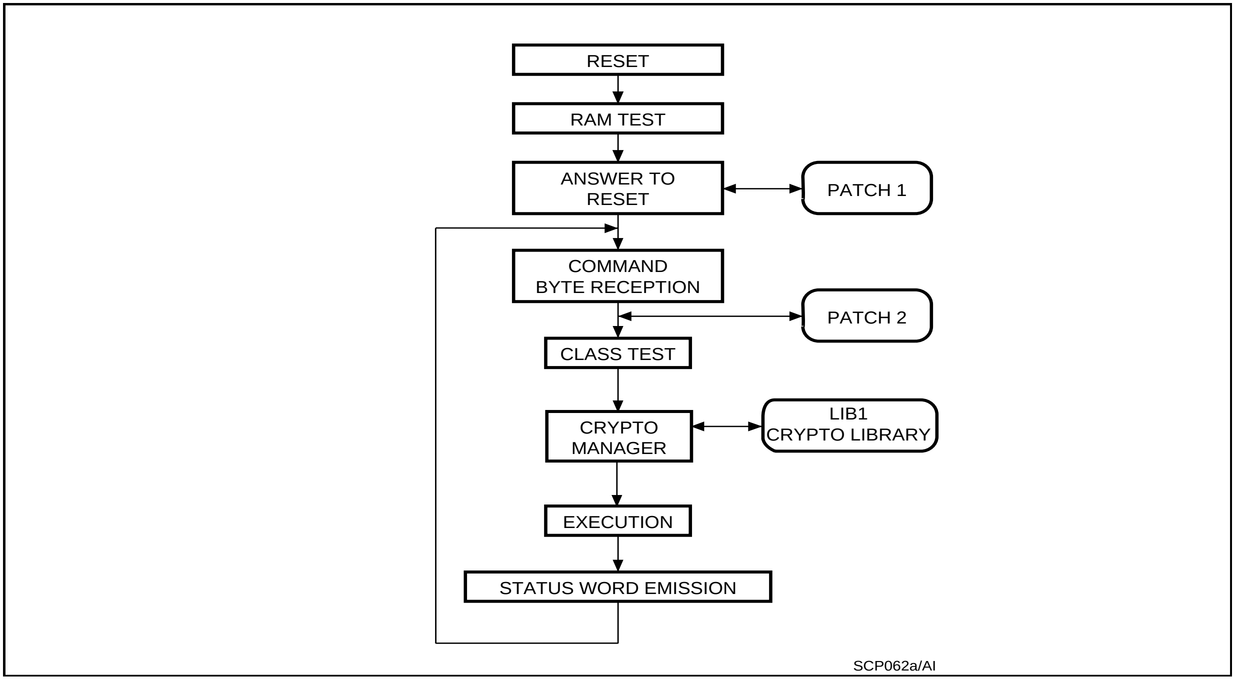
CRYPTO MANAGER

The ST16CF54 Level A Crypto Manager is firmware in accordance to the ST 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 the addition/removal of functions and the possibility to adapt to specific applications for evaluation, tests or field trials.

Figure 3 ST16CF54 Level A Manager flowchart


RESET
RAM TEST
ANSWER TO RESET
PATCH 1
COMMAND BYTE RECEPTION
PATCH 2
CLASS TEST
CRYPTO MANAGER
LIB1 CRYPTO LIBRARY
EXECUTION
STATUS WORD EMISSION
SCP062a/AI