ST19WK08

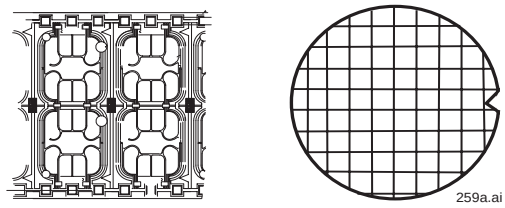
Smartcard MCU With Modular Arithmetic Processor & 8 Kbytes EEPROM

DATA BRIEF

PRODUCT FEATURES

- ENHANCED 8 BIT CPU WITH EXTENDED ADDRESSING MODES
- 112 KBYTES USER ROM WITH PARTITIONING
- 4 KBYTES USER RAM WITH PARTITIONING
- 8 KBYTES USER EEPROM WITH PARTITIONING plus 128 BYTES USER and ST OTP AREA:
  - Highly reliable CMOS EEPROM submicron technology
  - Error Correction Code for single bit fail correction within a byte
  - 10 year data retention
  - 500,000 Erase/Write cycles endurance
  - 1 to 32 bytes Erase or Program in 1 ms
- SECURITY FIREWALLS FOR MEMORIES, MODULAR ARITHMETIC PROCESSOR and ENHANCED DES ACCELERATOR.
- VERY HIGH SECURITY FEATURES INCLUDING EEPROM FLASH PROGRAMMING AND CLOCK MANAGEMENT.
- 2x8 BIT TIMERS WITH INTERRUPT CAPABILITY
- HARDWARE SECURITY ENHANCED DES ACCELERATOR WITH LIBRARY SUPPORT FOR SYMMETRICAL ALGORITHMS:
  - DES, triple DES computations and CBC chaining mode...
- 1088 Bit MODULAR ARITHMETIC PROCESSOR WITH LIBRARY SUPPORT FOR ASYMMETRICAL ALGORITHMS
  - Fast modular multiplication and squaring using Montgomery method
  - Software Crypto libraries in separate ST ROM area for efficient algorithm coding using a set of advanced functions
  - Software selectable operand length up to 2176 bits.
- ISO 3309 CRC CALCULATION BLOCK
- FIPS 140-2 COMPLIANT RANDOM NUMBER GENERATOR WITH TWO GUN REGISTERS (Generators of Unpredictable Number)
- 2.7 V TO 5.5 V SUPPLY VOLTAGE
- EXTERNAL CLOCK FREQUENCY UP TO 10 MHz
- HIGH PERFORMANCE PROVIDED USING INTERNAL CLOCK FREQUENCY
- UNIQUE SERIAL NUMBER ON EACH DIE
- POWER SAVING STANDBY MODE
- CONTACT ASSIGNMENT COMPATIBLE ISO 7816-2
- SERIAL ACCESS I/O, ISO 7816-3 COMPATIBLE
- ESD PROTECTION GREATER THAN 5000 V

Figure 1. Delivery Form



Micromodule Wafer

Function	Speed(1)
RSA 1024 bits signature with CRT(2)	85 ms
RSA 1024 bits signature without CRT(2)	282 ms
RSA 1024 bits verification (e='$10001')	5.5 ms
RSA 1024 bits key generation	2.5 s
RSA 2048 bits signature with CRT(2)	570 ms
RSA 2048 bits verification (e='$10001')	91 ms
Triple DES (with enhanced security)	58.0 µs
Single DES (with enhanced security)	43.0 µs

1. Typical values, independent from external clock frequency and supply voltage.
2. CRT: Chinese Remainder Theorem.

HARDWARE DESCRIPTION

The product, member of the ST19W platform, is a serial access microcontroller specially designed for cost effective secure portable applications.

It is manufactured using an advanced highly reliable ST CMOS EEPROM technology.

It is based on the STMicroelectronics 8 bit CPU already implemented on the ST19X product family and includes on-chip memories: User ROM, User RAM and EEPROM with state of the art security features. ROM, RAM and EEPROM memories can be configured into partitions with customized access rules.

An additional ST ROM contains all ST provided functions and libraries.

Access from any memory area to another are protected by hardware FIREWALLS. Access rules are User defined and can be selected by mask options.

The chip includes an Enhanced DES accelerator which is accessible via cryptographic software libraries located in ST ROM.

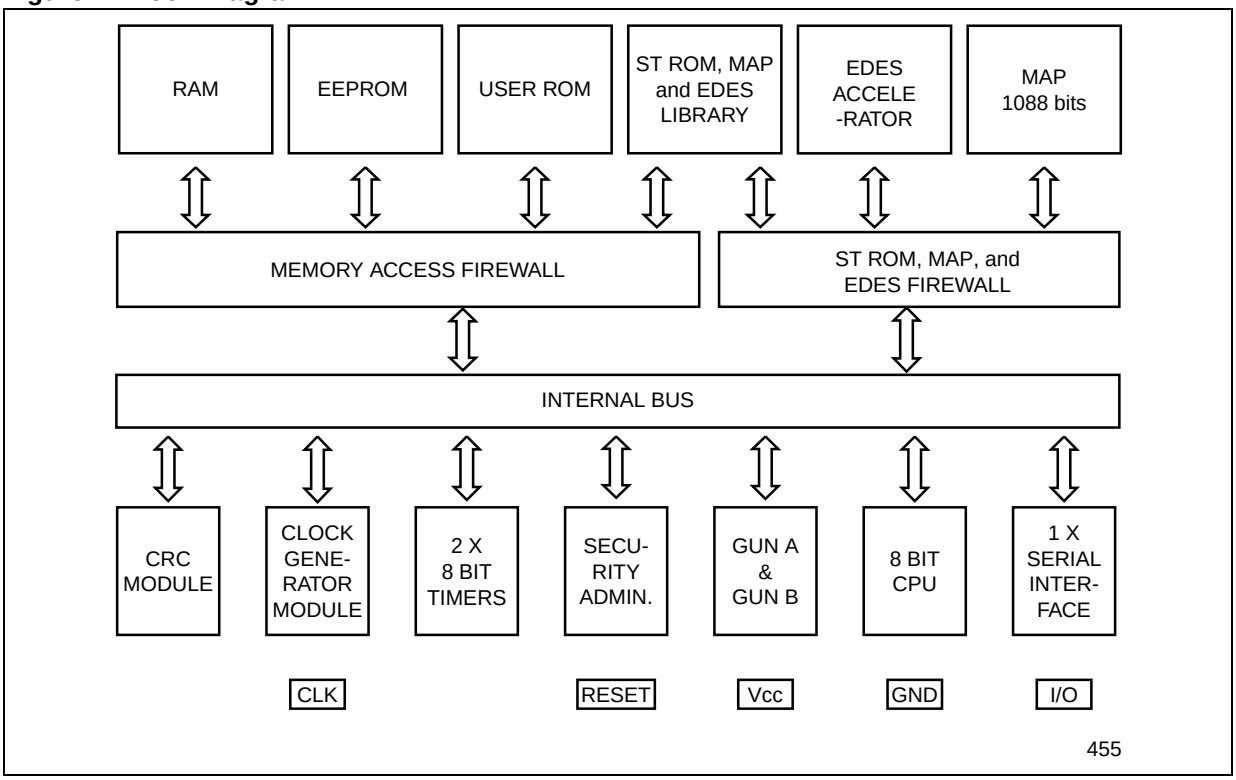
The chip includes also a MAP which is based on a 1088 bits processor architecture. It processes modular multiplication, squaring and additional calculations up to 2176 bit operands.

Internal Modular Arithmetic Processor (MAP) and enhanced DES accelerator are designed to speed up cryptographic calculations using Public Key Algorithms and Secret Key Algorithms.

As with all the other ST19W products, a serial interface fully compatible with the ISO7816 standard for Smartcard applications is available.

A CRC calculation block is also available and is directly accessible by the User.

Figure 2. Block Diagram



SOFTWARE DEVELOPMENT

Software development and firmware generation (ROM and options) are supported by a comprehensive set of development tools, dedicated at development and validation of softwares:

- ST19-HDSX Emulator,
- ST19X simulation package,
- ST19 tools pack environment for Windows™ NT, 2000, XP based stations,
- Powerful C/C++ compiler and debugger are also available (third party tools).