ST19XL34

SMARTCARD IC WITH 34KBYTES HIGH DENSITY EEPROM AND MODULAR ARITHMETIC PROCESSOR

PRELIMINARY DATA

ST19XL34 FEATURES

- ENHANCED 8 BIT CPU WITH EXTENDED ADDRESSING MODES
- 96K BYTES USER ROM WITH PARTITIONING
- 4K BYTES USER RAM WITH PARTITIONING
- 34K BYTES USER EEPROM WITH PARTITIONING
  - Highly reliable CMOS EEPROM 0.35µm submicron technology
  - Error Correction Code for single bit fail correction
  - 10 year data retention
  - 100,000 Erase/Write cycles endurance
  - Correction of single bit fail within a byte(ECC)
  - 1 to 64 bytes Erase or Program in 2 mS
- SECURITY FIREWALLS FOR MEMORIES
- VERY HIGH SECURITY FEATURES INCLUDING EEPROM FLASH PROGRAM, AND CLOCK MANAGEMENT.
- 3x8 BIT TIMERS WITH INTERRUPT CAPABILITY
- HARDWARE DES ACCELERATOR
- 1088 Bit MAP: MODULAR ARITHMETIC PROCESSOR WITH LIBRARY SUPPORT FOR ASYMETRIC ALGORITHMS
- CRYPTOGRAPHIC LIBRARY:
  - **ASYMMETRICAL ALGORITHMS**:

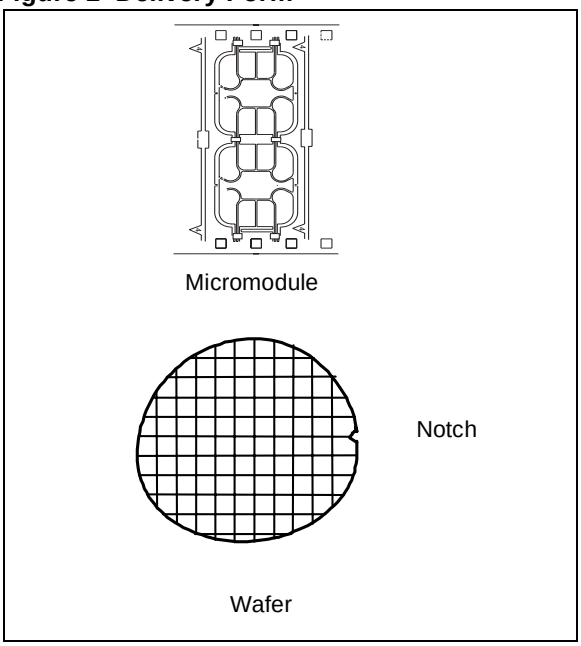
    Fast modular multiplication and squaring using Montgomery method

    Software Crypto libraries in separate ROM area for efficient algorithm coding using a set of advanced functions

    Software selectable operand length up to 2176 bits
  - **SYMMETRICAL ALGORITHMS**:

    DES, triple DES, DESX computations and CBC chaining mode
- CRC CALCULATION BLOCK
- UP TO 10MHz INTERNAL OPERATING FREQUENCY
- UNIQUE SERIAL NUMBER ON EACH DIE
- POWER SAVING STANDBY MODE
- CONTACT ASSIGNMENT COMPATIBLE ISO 7816-2
- 2 SERIAL ACCESS, ISO 7816-3 COMPATIBLE
- ESD PROTECTION GREATER THAN 5000V
- 3V ± 10% or 5V ± 10% SUPPLY VOLTAGE

Figure 1 Delivery Form



Function	Speed (1)
RSA 1024 bits signature with CRT (2)	110 ms
RSA 1024 bits signature without CRT (2)	367 ms
RSA 1024 bits verification (e=$10001)	7 ms
RSA 1024 bits key generation	3.2 s
RSA 2048 bits signature with CRT (2)	740 ms
RSA 2048 bits verification (e=$10001)	118 ms
Triple DES (with keys loaded)	31µs
Single DES (with keys loaded)	19µs

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

HARDWARE DESCRIPTION

The ST19XL34, a member of the ST19 platform, is a serial access microcontroller especially designed for very large volume and cost effective secure portable objects, for which high performance Public Key and secret key algorithms will be implemented to cut down initialization and communication costs and to increase security.

The chip includes a DES accelerator which is accessible via a cryptographic system ROM software library.

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 DES accelerator are designed to speed up cryptographic calculations using Public Key Algorithms and Secret Key Algorithms.

The ST19XL34 is based on a STMicrolectronics 8 bit CPU and includes on chip memories: 96K User ROM, 4K User RAM and 34K User EEPROM with state of the art security features.

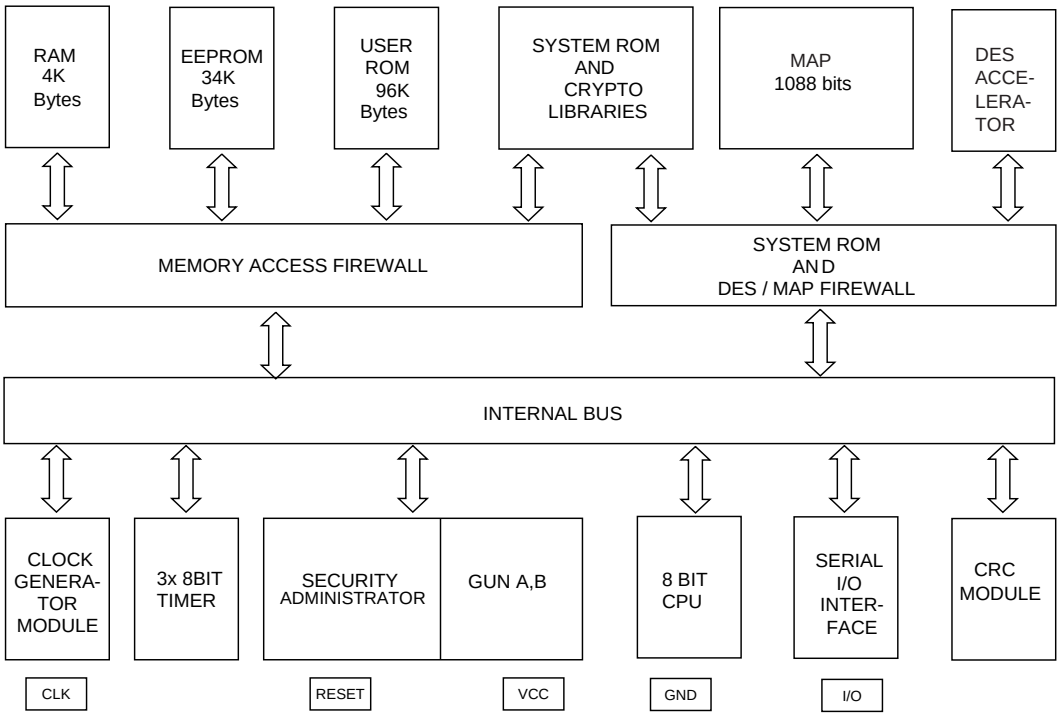
ROM, RAM and EEPROM memories can be configured into partitions with customized access rules. Access from any memory area to another. are protected by hardware FIREWALLS. Access rules are User defined and can be selected by mask options or during the life of the product.

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

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

As with all the other ST19 products, it is fully compatible with the ISO7816 standard for Smartcard applications.

Figure 2 Block diagram



SOFTWARE DEVELOPMENT

Software development and firmware (ROM code/ options) generation are done with the ST19-HDSX development system, on Windows NT or Windows 98. Powerfull C/C++ compiler, debugger and simulator are also available.

CRYPTOGRAPHIC LIBRARIES

For an easy and sufficient use of the Modular Arithmetic Processor (MAP), ST proposes a complete set of firmware subroutines. This library is located in a specific ROM area. This library saves the operating system designer from coding first layer functions and allows the designer to concentrate on algorithms, Public Key Cryptography and Secret Key Cryptography protocols implementation.

This library contains firmware functions for:

ASYMMETRICAL ALGORITHMS:

- 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 using or not the Chinese Remainder Theorem (CRT)
- more elaborate functions such as RSA signatures and verifications for modulo length up to 2176 bits long, DSA signature and authentication.
- full internal key generation for signatures/verifications. This guarantees that the secret key will never be known outside the chip and contributes to overall system security.
- long random number generation
- RSA up to 2176 bits
- DSA up to 1088 bits
- SHA-1
- RSA key generation

SYMMETRICAL ALGORITHMS:

- DES, triple DES, DESX computations
- CBC chaining mode
- Loading / Unloadings from / to registers are secured against SPA