# ST19XL34

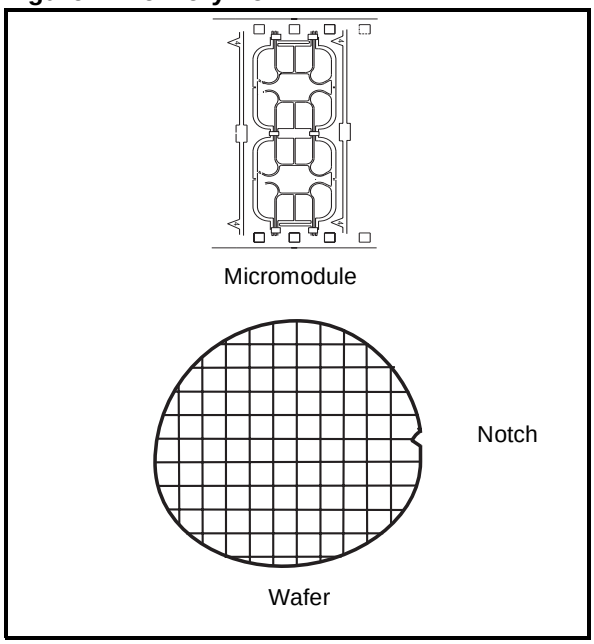
## Smartcard MCU With Modular Arithmetic Processor & 34 KBytes High Density EEPROM

**DATA BRIEFING**

### PRODUCT FEATURES

- ENHANCED 8 BIT CPU WITH EXTENDED ADDRESSING MODES
- 96 KBYTES USER ROM WITH PARTITIONING
- 4 KBYTES USER RAM WITH PARTITIONING
- 34 KBYTES USER EEPROM WITH PARTITIONING INCLUDING 64 BYTES USER AND ST OPT 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 64 bytes Erase or Program in 2 ms
- SECURITY FIREWALLS FOR MEMORIES and MAP.
- VERY HIGH SECURITY FEATURES INCLUDING CLOCK MANAGEMENT.
- 3x8 BIT TIMERS WITH INTERRUPT CAPABILITY
- HARDWARE DES ACCELERATOR
- 1088 Bit MODULAR ARITHMETIC PROCESSOR WITH LIBRARY SUPPORT FOR ASYMETRIC ALGORITHMS
- CRYPTOGRAPHIC LIBRARY: DES, TRIPLE DES, DESX COMPUTATIONS AND CBC CHAINING MODE
- ISO 3309 CRC CALCULATION BLOCK
- 2.7 V TO 5.5 V SUPPLY VOLTAGE WITH 10 MHz INTERNAL OPERATING FREQUENCY
- UNIQUE SERIAL NUMBER ON EACH DIE
- POWER SAVING STANDBY MODE
- CONTACT ASSIGNMENT COMPATIBLE ISO 7816-2
- 2 SERIAL ACCESS I/O'S, ISO 7816-3 COMPATIBLE
- ESD PROTECTION GREATER THAN 5000

**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) | 24 µs |
| Single DES (with keys loaded) | 15 µs |

Note: (1) Typical values, independent from external clock frequency and supply voltage.

Note: (2) CRT: Chinese Reminder Theorem.

## HARDWARE DESCRIPTION

The ST19XL34, a member of the ST19X platform, is a serial access microcontroller especially designed for very large volume and cost effective secure portable applications.

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: User ROM, User RAM and 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.

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

As with all the other ST19X products, serial interfaces fully compatible with the ISO7816 standard for Smartcard applications are available.

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

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

## SOFTWARE DEVELOPMENT

Software development and firmware (ROM code/ options) generation are done with the ST19-HDSX development system, on Windows NT, Windows 98 and Windows 2000.

Powerful C/C++ compiler, debugger and simulator are also available.

### SYMMETRICAL ALGORITHMS:

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

## 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

**Figure 2. Block Diagram**