ST19XG34

## Smartcard MCU with 34KBYTES HIGH DENSITY EEPROM

ST19XG34FEATURES

- ENHANCED 8 BIT CPU WITH EXTENDED ADDRESSING MODES
- 70K BYTES USER ROM WITH PARTITIONING
- 2K BYTES USER RAM WITH PARTITIONING
- 34K BYTES USER EEPROM WITH PARTITIONING
  - Highly reliable CMOS EEPROM submicron technology
  - Error Correction Code for single bit fail correction within a byte
  - 10 year data retention
  - 100,000 Erase/Write cycles endurance
  - 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
- CRYPTOGRAPHIC LIBRARY:
  - DES, triple DES, DESX computations and CBC chaining mode
- ISO 3309 CRC CALCULATION BLOCK
- UP TO 10MHz INTERNAL OPERATING FREQUENCY AT 5 AND 3 VOLTS
- 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 5000V
- 3 TO 5V SUPPLY VOLTAGE RANGE

Figure 1 Delivery Form

Micromodule

Notch

Wafer
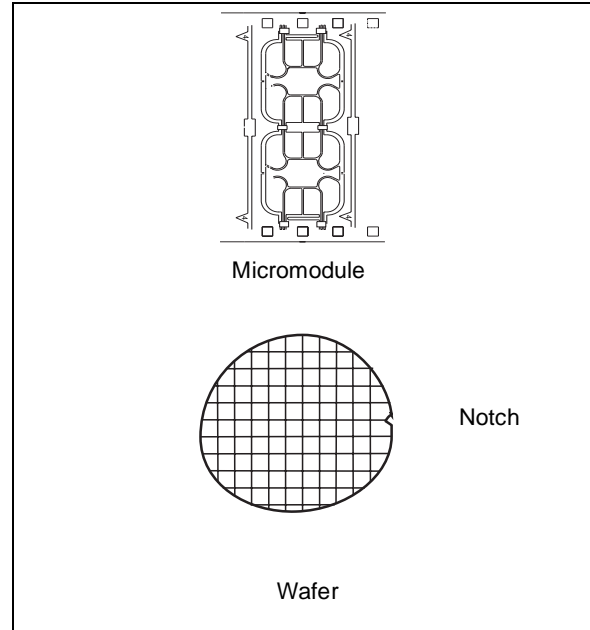
Function	Speed (1)
Triple DES (with keys loaded)	31µS
Single DES (with keys loaded)	19µS

(1) Typical values, independant from external clock frequency and supply voltage.

HARDWARE DESCRIPTION

The ST19XG34, a member of the ST19 platform, is a serial access microcontroller especially designed for very large volume and cost effective secure portable applications.

The ST19XG34 is based on a STMicrolectronics 8 bit CPU and includes on chip memories: 70 K User ROM, 2016-byte 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.

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

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.

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

Figure 2 Block diagram

SCP 155a/DS
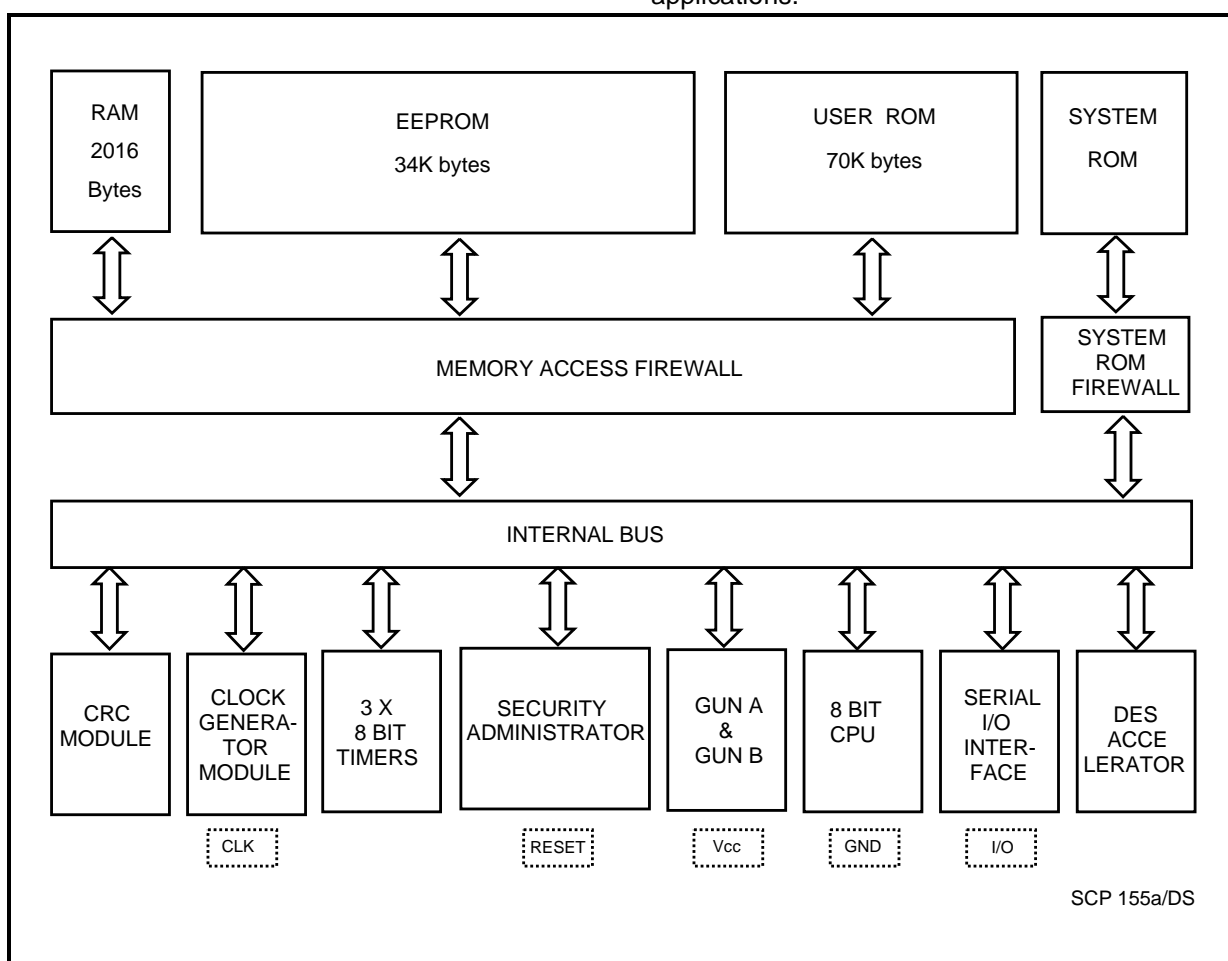
SOFTWARE DEVELOPMENT

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