



ST19XR34

Dual Contactless Smartcard MCU With Modular Arithmetic Processor & 34 Kbytes High Density EEPROM

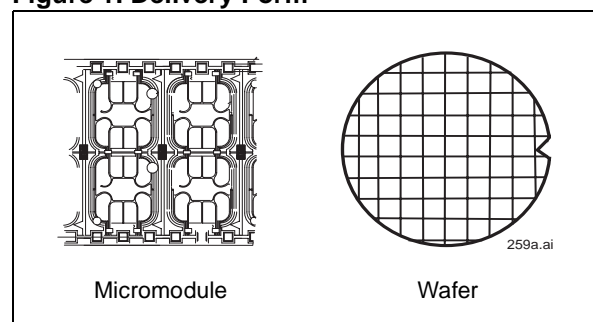
DATA BRIEF

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 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 64 bytes Erase or Program in 2 ms
- SECURITY FIREWALLS FOR MEMORIES, MODULAR ARITHMETIC PROCESSOR and DES ACCELERATOR.
- VERY HIGH SECURITY FEATURES INCLUDING EEPROM FLASH PROGRAMMING AND CLOCK MANAGEMENT.
- 3x8 BIT TIMERS WITH INTERRUPT CAPABILITY
- HARDWARE DES ACCELERATOR WITH LIBRARY SUPPORT FOR SYMMETRICAL ALGORITHMS:
 - DES, triple DES, DESX 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 WITH 10MHz INTERNAL OPERATING 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



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

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

(2) CRT: Chinese Remainder Theorem.

CONTACTLESS SPECIFIC FEATURES

- BASED UPON ISO 14443 TYPE B
- 13.56 MHz CARRIER FREQUENCY
- HIGH SPEED DATA TRANSFER CAPABILITY UP TO 424 KBAUDS
- RF FRAME UP TO 256 BYTES
- 10% AMPLITUDE MODULATION RECEPTION (READER TO CARD)
- BPSK - NRZ LOAD MODULATION (CARD TO READER)
- INTERFACE WITH RF READERS SUPPORTED THROUGH A LIBRARY OF EMBEDDED SOFTWARE FUNCTIONS COMPATIBLE WITH ISO 14443 STANDARD

HARDWARE DESCRIPTION

The product, member of the ST19X 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 a STMicroelectronics 8 bit CPU 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 or during the life of the product.

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

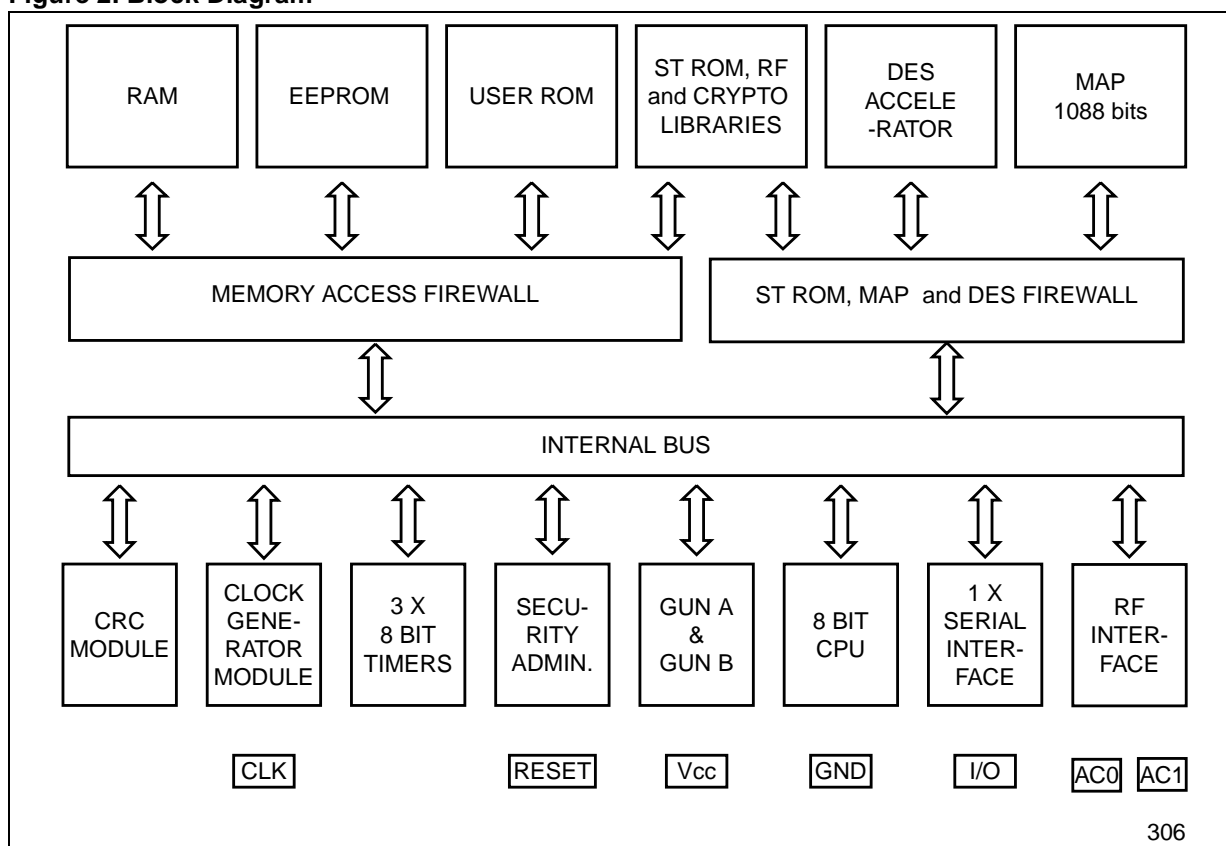
The chip includes also a MAP which is based on a 1088 bits processor architecture. It processes modular multiplication, squaring and additional calculations up to 2176 bit operands

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

As with all the other ST19X 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

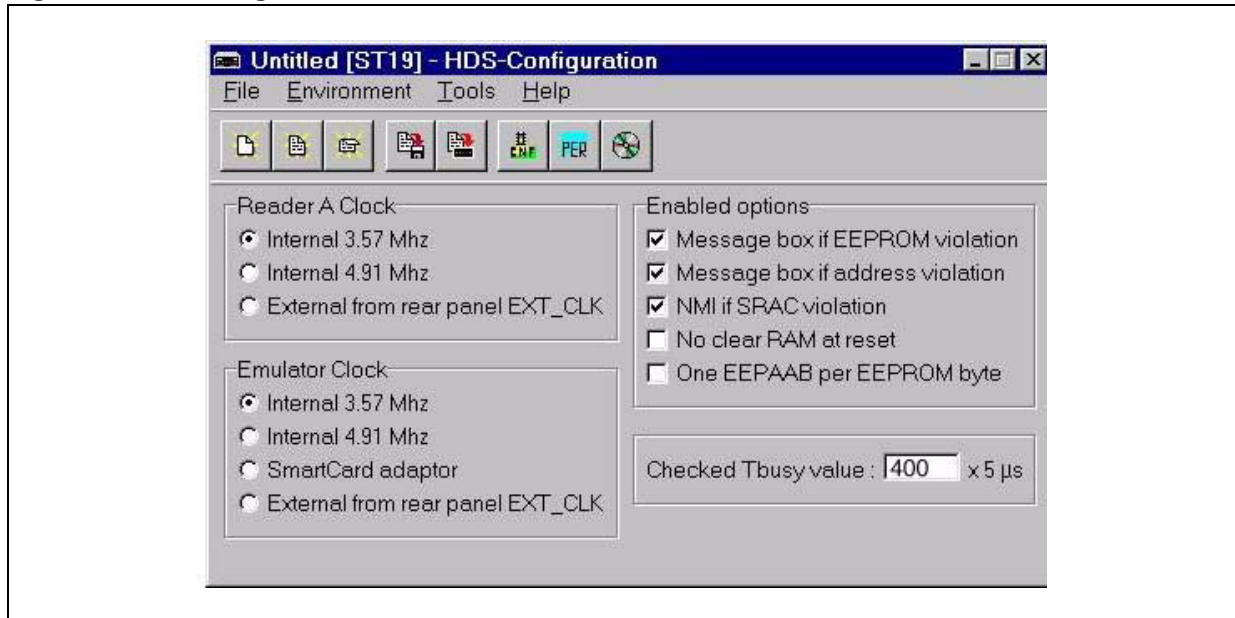


SOFTWARE DEVELOPMENT

Software development and firmware (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.

Figure 3. HDS configuration interface



Information furnished is believed to be accurate and reliable. However, STMicroelectronics assumes no responsibility for the consequences of use of such information nor for any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of STMicroelectronics. Specifications mentioned in this publication are subject to change without notice. This publication supersedes and replaces all information previously supplied. STMicroelectronics products are not authorized for use as critical components in life support devices or systems without express written approval of STMicroelectronics.

The ST logo is a registered trademark of STMicroelectronics.
All other names are the property of their respective owners

© 2002 STMicroelectronics - All rights reserved
BULL CP8 Patents

STMicroelectronics GROUP OF COMPANIES
Australia - Belgium - Brazil - Canada - China - Czech Republic - Finland - France - Germany -
Hong Kong - India - Israel - Italy - Japan - Malaysia - Malta - Morocco - Singapore -
Spain - Sweden - Switzerland - United Kingdom - United States
www.st.com