ST19NA18

Smartcard MCU with MAP, IART, High Speed CPU Clock & 18 KBytes High Density EEPROM

Data Brief

Features summary

ST19NA18 applications include:

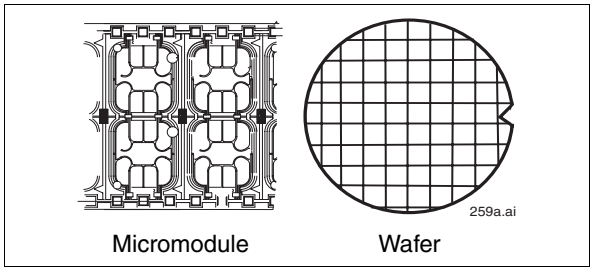
- Pay TV, Banking and Secure applications

Hardware and dedicated software

- Enhanced 8-bit CPU with extended addressing modes
- 128 Kbytes User ROM with partitioning
- 4 Kbytes User RAM with partitioning
- 18 Kbytes User EEPROM with partitioning, 64 Bytes User OTP and 64 Bytes ST OTP areas:
  - 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
  - Erase or Program 1 to 64 Bytes in 1.5 ms
- Three 8-bit timers with interrupt capability
- 3V and 5V supply voltage ranges
- Power-saving Standby mode
- Serial access I/Os, ISO 7816-3 compatible
- ISO Asynchronous Receiver Transmitter for high speed serial data support
- ESD protection greater than 5000 V

Security features

- Very high security features including:
  - EEPROM Flash programming
  - Clock management
  - User ROM protected area
  - Code signature capability
  - Built-in DFA countermeasures
  - Glitch detector
- Security firewalls for memories, MAP and Enhanced DES accelerator
- Hardware Security Enhanced DES accelerator with library support for symmetrical algorithms:
  - DES, 3 DES computations and CBC mode



- AES-128 software library
- 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 and AIS31 compliant True Random Number Generator (TRNG) with two TRNG registers
- Unique serial number on each die
- High performance provided using high speed internal clock frequency (up to 28 MHz)
- Cryptographic performances (1)
  - RSA 1024-bit signature with CRT(2): 39 ms
  - RSA 1024-bit signature without CRT(2): 130 ms
  - RSA 1024-bit verification (e='$10001'): 2.4 ms
  - RSA 1024-bit key generation: 1.2 s
  - RSA 2048-bit signature with CRT(2): 264 ms
  - RSA 2048-bit verification (e='$10001'): 42 ms
  - Triple DES (with enhanced security): 27 µs
  - Single DES (with enhanced security): 20 µs

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

1 Description

The product, member of the ST19N 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 a Modular Arithmetic Processor (MAP) based on a 1088-bit processor architecture. It processes modular multiplication, squaring and additional operand calculations up to 2176 bits.

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

As with the other ST19N products, two serial interfaces compatible with the ISO 7816 standard are available.

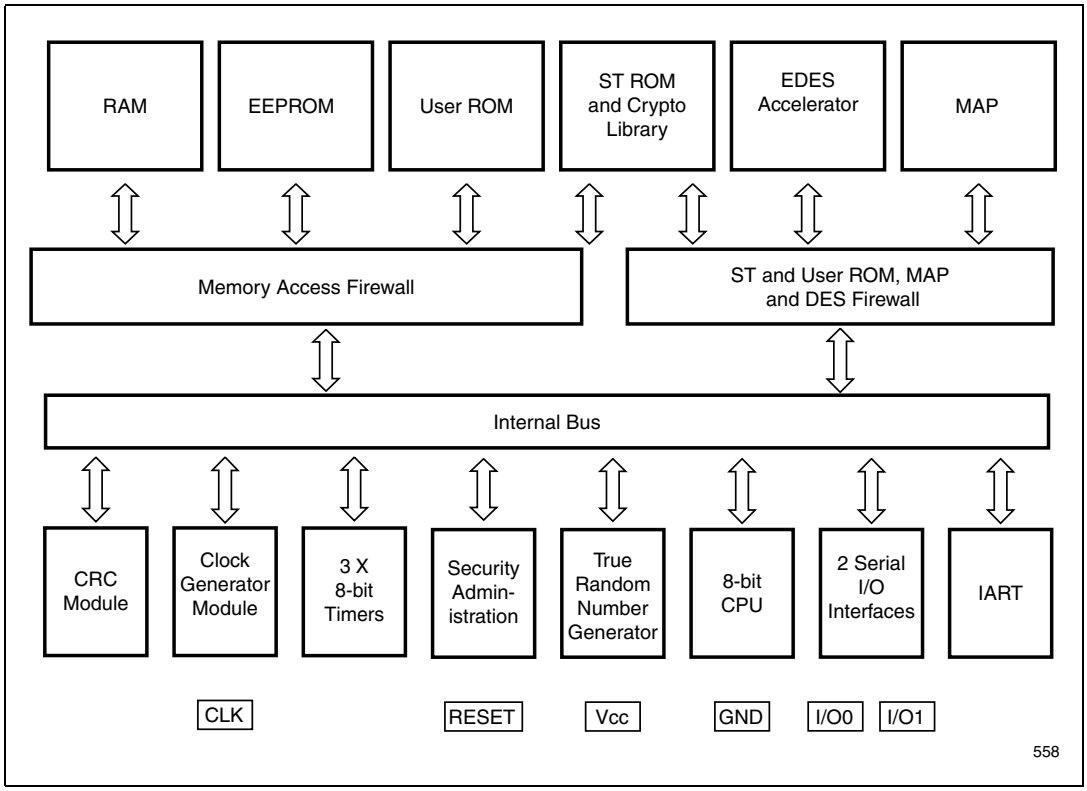
A CRC calculation block is also available and is directly accessible by the User.

1.1 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 software:

- Smartcard ICs Emulator
- ScDevTools environment for Windows™ NT, 2000, and XP based stations
- Powerful C/C++ compiler and debugger are also available (third-party tools)

Figure 1. Block diagram



2 Revision history

Table 1. Summary of modifications

Date	Reference	Description of modifications
14-Nov-2005	1	Initial release.
31-Jan-2006	2	Disclaimer updated.
23-Feb-2007	3	Reformatted document.

Please Read Carefully:

Information in this document is provided solely in connection with ST products. STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, modifications or improvements, to this document, and the products and services described herein at any time, without notice.

All ST products are sold pursuant to ST’s terms and conditions of sale.

Purchasers are solely responsible for the choice, selection and use of the ST products and services described herein, and ST assumes no liability whatsoever relating to the choice, selection or use of the ST products and services described herein.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted under this document. If any part of this document refers to any third party products or services it shall not be deemed a license grant by ST for the use of such third party products or services, or any intellectual property contained therein or considered as a warranty covering the use in any manner whatsoever of such third party products or services or any intellectual property contained therein.

UNLESS OTHERWISE SET FORTH IN ST’S TERMS AND CONDITIONS OF SALE ST DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE USE AND/OR SALE OF ST PRODUCTS INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE (AND THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION), OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS EXPRESSLY APPROVED IN WRITING BY AN AUTHORIZED ST REPRESENTATIVE, ST PRODUCTS ARE NOT RECOMMENDED, AUTHORIZED OR WARRANTED FOR USE IN MILITARY, AIR CRAFT, SPACE, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS, NOR IN PRODUCTS OR SYSTEMS WHERE FAILURE OR MALFUNCTION MAY RESULT IN PERSONAL INJURY, DEATH, OR SEVERE PROPERTY OR ENVIRONMENTAL DAMAGE. ST PRODUCTS WHICH ARE NOT SPECIFIED AS "AUTOMOTIVE GRADE" MAY ONLY BE USED IN AUTOMOTIVE APPLICATIONS AT USER’S OWN RISK.

Resale of ST products with provisions different from the statements and/or technical features set forth in this document shall immediately void any warranty granted by ST for the ST product or service described herein and shall not create or extend in any manner whatsoever, any liability of ST.

ST and the ST logo are trademarks or registered trademarks of ST in various countries.

Information in this document supersedes and replaces all information previously supplied.

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

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 of America

www.st.com