ST19NR66

Dual contactless smartcard MCU with 66 Kbytes high density EEPROM, enhanced RF performances and dedicated packages

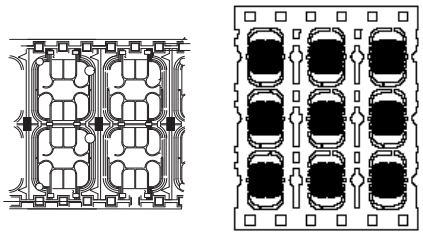
Features

Hardware features

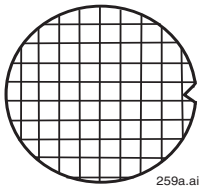
- Enhanced 8-bit CPU core with extended addressing modes
- 224 Kbytes User ROM
- 6 Kbytes User RAM
- 66 Kbytes User EEPROM including 128 Bytes User OTP area:
  - 1 to 64 Bytes Erase or Program in 1.5 ms
- Three 8-bit timers with interrupt capability
- 1.8 V, 3.0V and 5.0V supply voltage ranges
- Power-saving Standby mode
- ESD protection greater than 5000V
- Serial access I/O, ISO/IEC 7816-3 compatible
- ISO Asynchronous Receiver Transmitter for high speed serial data support

Contactless specific features

- Complies with ISO 14443 type B standards
- 13.56 MHz carrier frequency
- RF UART (RF Universal Asynchronous Receiver Transmitter) for easy-to-manage high speed data transfers up to 848 Kbits/s
- RF frame up to 256 Bytes
- 10% amplitude modulation reception (reader-to-card)
- BPSK - NRZ load modulation (card-to-reader)
- Enhanced RF performance provided by CPU clock frequency up to 20 MHz coupled with clock frequency divider
- Interface with RF readers supported through a library of embedded software functions compatible with ISO 14443 standard
- New dedicated contactless micromodule for thinnest packaging solutions
- ESD protection on antenna pads greater than 5000 V



Micromodules



Wafer

Security features

- EEPROM Flash programming and clock management
- Monitoring of environmental parameters
- Unique serial number on each die
- Hardware Security Enhanced DES accelerator with library support for symmetrical algorithms:
  - DES, triple DES, DESx computations and CBC chaining mode
- 1088-bit Modular Arithmetic Processor (MAP) with library support for asymmetrical algorithms:
  - RSA, DSA, SHA-1
  - AES-128 software library
- FIPS 140-2 and AIS31-compliant true random number generator (TRNG)
- See for additional security features.

Applications

ST19NR66 major applications include:

- ePassport, ID cards, eGovernment cards and contactless banking

1 Description

The device, 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 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 device.

The device includes an Enhanced DES accelerator which is accessible via cryptographic software libraries located in ST ROM.

The device 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.

An RF Interface including an RF Universal Asynchronous Receiver Transmitter (RF UART) enables contactless communication up to 848 Kbits/s compatible with the ISO 14443-B standard.

As with the other ST19N devices, a serial interface electrically compatible with the ISO 7816 standard is available as well as an ISO-compatible high-speed ISO Asynchronous Receiver Transmitter (IART) enabling communications up to 1.25 Mbit/s.

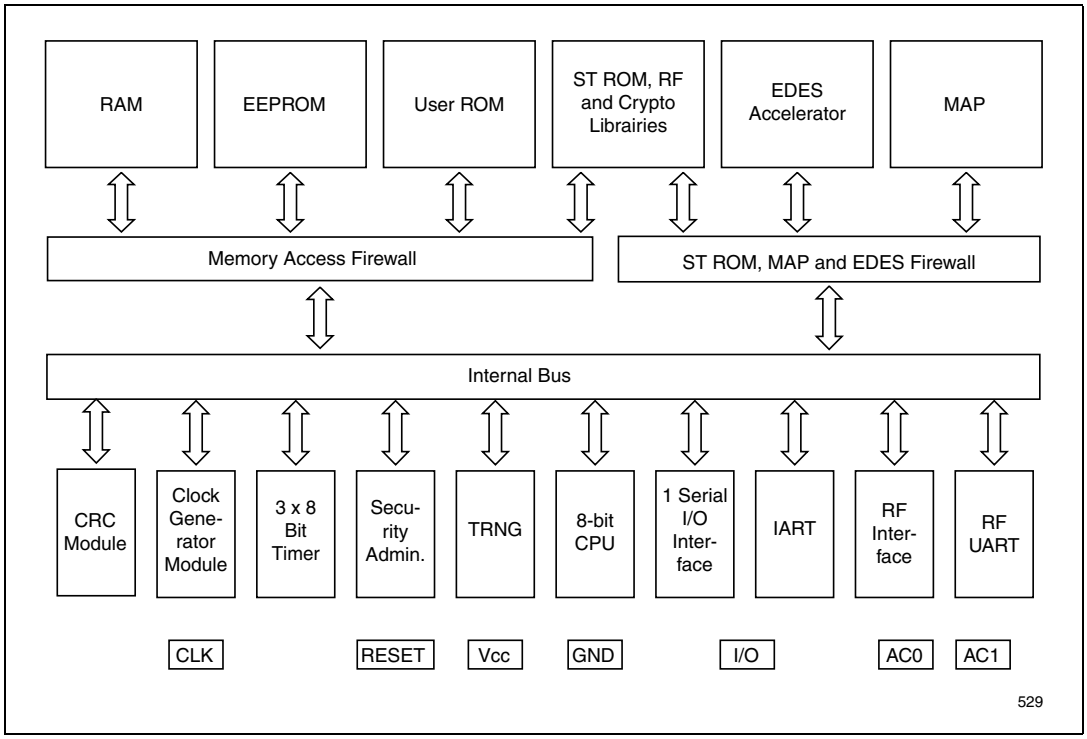
A CRC calculation block is also available and is directly accessible by the User.

Development environment

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
- ST19X simulation package
- ScDevTools environment for Windows® 2000 and XP -based stations
- Powerful C/C++ compiler and debugger are also available (third-party tools)
- RF contactless demokit based on ISO 14443 type B standard

Figure 1. ST19NR66 block diagram



1.1 Additional security features

- Security firewalls for protecting the memory arrays and the cryptographic coprocessors (MAP and EDES)
- ISO 3309 CRC calculation block
- Cryptographic performances(1):
  - RSA 1024-bit signature with CRT(2): 55 ms
  - RSA 1024-bit signature without CRT(2): 183 ms
  - RSA 1024-bit verification (e='$10001'): 3.6 ms
  - RSA 1024-bit key generation: 1.6 s
  - RSA 2048-bit signature with CRT(2): 371 ms
  - RSA 2048-bit verification (e='$10001'): 59 ms
  - Triple DES (with enhanced security): 38 µs
  - Single DES (with enhanced security): 28 µs

1. Best performance achieved using a 15-MHz clock frequency.
2. CRT: Chinese Remainder Theorem.

2 Revision history

Table 1. Document revision history

Date	Revision	Changes
03-Nov-2005	1	Initial release.
14-Nov-2005	2	Speed values updated. See *Speed* on page 2 in table.
17-Jan-2006	3	Disclaimer updated.
22-Jun-2009	4	Disclaimer updated.

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 - Philippines - Singapore - Spain - Sweden - Switzerland - United Kingdom - United States of America

www.st.com