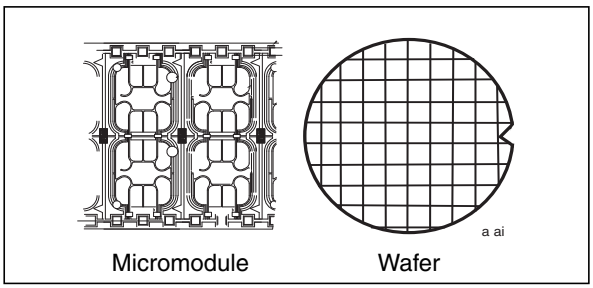
ST19WR66

Dual contactless secure MCU with MAP, RF UART, IART & 66 Kbytes high density EEPROM

Data brief



Micromodule Wafer

Features

- Enhanced 8-bit CPU with extended addressing modes
- 224 Kbytes user ROM with partitioning
- 6 Kbytes user RAM with partitioning
- 66 Kbytes user EEPROM with partitioning plus 128 Bytes user OTP and 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
  - 1 to 64Bytes Erase or Program in 1.5 ms
- Security firewalls for memories, modular arithmetic processor and Enhanced DES accelerator
- Very high security features including EEPROM Flash programming and clock management.
- 3x8-bit timers with interrupt capability
- Hardware Security Enhanced DES accelerator with library support for symmetrical algorithms:
  - DES, triple DES computations and CBC chaining 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 compliant True Random Number Generator (TRNG)with two Gun registers (Generators of Unpredictable Number)
- 1.62 V to 5.5 V supply voltage
- External clock frequency up to 10 MHz
- High performance provided using internal clock 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
- ISO asynchronous receiver transmitter for high speed serial data support
- ESD protection greater than 5000 V

Contactless specific features

- Based on ISO 14443 type B
- 13.56 MHz carrier frequency
- RF UART (RF Universal Asynchronous Receiver Transmitter) for easy-to-manage high speed data transfer 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)
- Interface with RF readers supported through a library of embedded software functions compatible with ISO 14443 standard
- ESD protection on antenna pads greater than 3000 V

1 Description

The product, member of the ST19W 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 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 ST19W products, a serial interface compatible with the ISO 7816 standard is available.

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

In order to meet environmental requirements, ST offers these devices in different grades of ECOPACK® packages, depending on their level of environmental compliance. ECOPACK® specifications, grade definitions and product status are available at: *www.st.com*. ECOPACK® is an ST trademark.

Table 1. Cryptographic performance

Function	Speed(1)
RSA 1024-bit signature with CRT(2)	85 ms
RSA 1024-bit signature without CRT(2)	282 ms
RSA 1024-bit verification (e='$10001')	5.5 ms

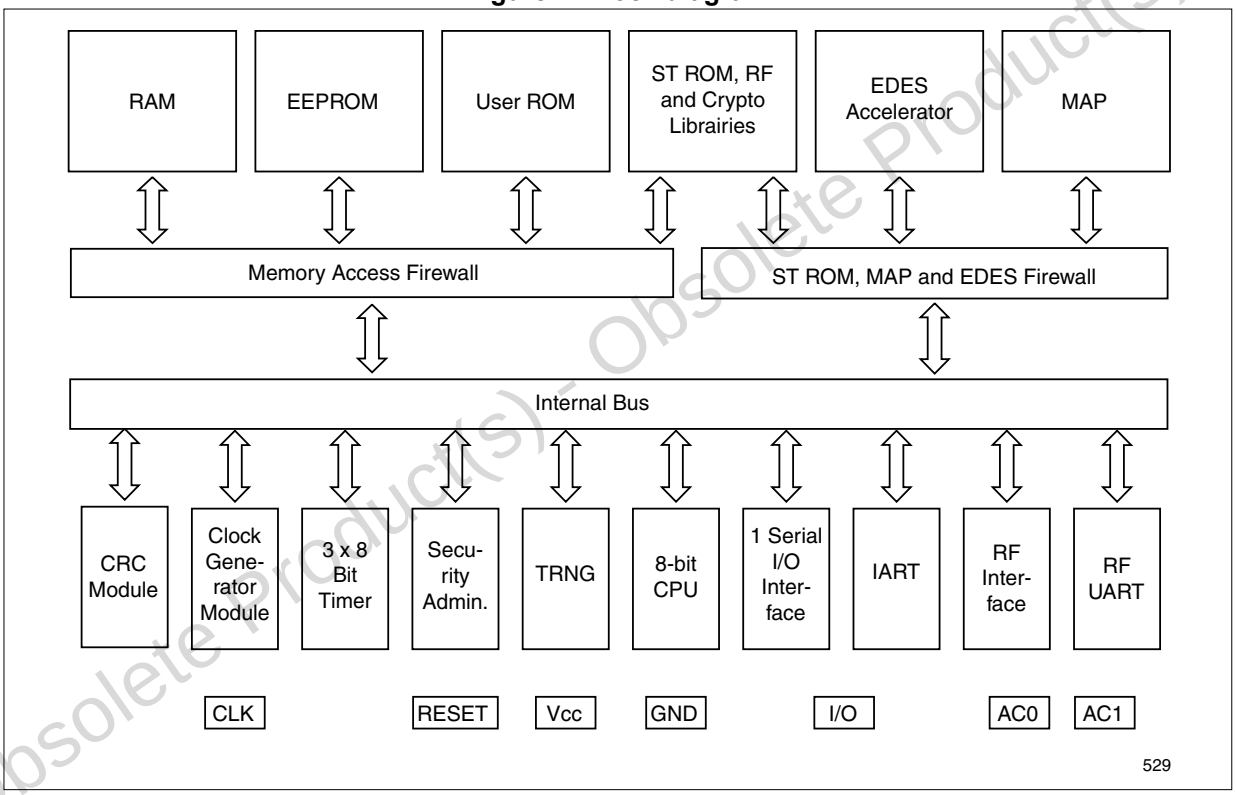
LICENSED DPA™ COUNTERMEASURES

Table 1. Cryptographic performance

Function	Speed(1)
RSA 1024-bit key generation	2.5 s
RSA 2048-bit signature with CRT(2)	570 ms
RSA 2048-bit verification (e='$10001')	91 ms
Triple DES (with enhanced security)	58.0 µs
Single DES (with enhanced security)	43.0 µs

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

Figure 1. Block diagram



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
- ST19X simulation package
- ScDevTools environment for Windows™ NT, 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 standards

2 Revision history

Table 2. Document revision history

Date	Revision	Changes
01-Aug-2004	1	Initial release.
07-Nov-2013	2	Updated logo information on page 2.

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.

ST PRODUCTS ARE NOT DESIGNED OR AUTHORIZED FOR USE IN: (A) SAFETY CRITICAL APPLICATIONS SUCH AS LIFE SUPPORTING, ACTIVE IMPLANTED DEVICES OR SYSTEMS WITH PRODUCT FUNCTIONAL SAFETY REQUIREMENTS; (B) AERONAUTIC APPLICATIONS; (C) AUTOMOTIVE APPLICATIONS OR ENVIRONMENTS, AND/OR (D) AEROSPACE APPLICATIONS OR ENVIRONMENTS. WHERE ST PRODUCTS ARE NOT DESIGNED FOR SUCH USE, THE PURCHASER SHALL USE PRODUCTS AT PURCHASER’S SOLE RISK, EVEN IF ST HAS BEEN INFORMED IN WRITING OF SUCH USAGE, UNLESS A PRODUCT IS EXPRESSLY DESIGNATED BY ST AS BEING INTENDED FOR “AUTOMOTIVE, AUTOMOTIVE SAFETY OR MEDICAL” INDUSTRY DOMAINS ACCORDING TO ST PRODUCT DESIGN SPECIFICATIONS. PRODUCTS FORMALLY ESCC, QML OR JAN QUALIFIED ARE DEEMED SUITABLE FOR USE IN AEROSPACE BY THE CORRESPONDING GOVERNMENTAL AGENCY.

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