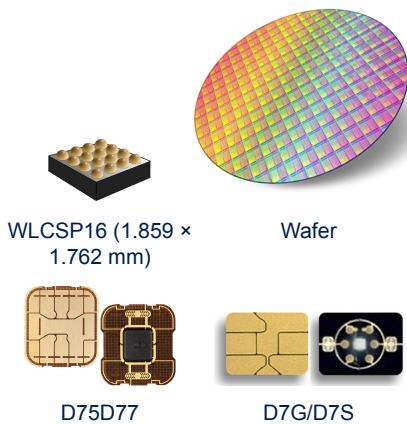


Secure dual interface microcontroller with enhanced security and up to 608 Kbytes of Flash memory



Features

Hardware features

- Lockstep Arm® SecurCore® SC000™ 32-bit core cadenced at up to 60 MHz
- 16 Kbytes of user RAM
- Up to 608 Kbytes of secure User high-density Flash memory including 512 bytes of user area:
 - 25-year data retention
 - 500 000 Erase/Write cycle endurance
 - Page Erase time down to 0.8 ms
 - Programming performance up to 3 μs/byte in chained mode
 - Flash Erase/Write protection programmable on 32-Kbyte sectors
- RF harvesting
- Operating temperature: –25 °C to +85 °C
- Three 16-bit timers with interrupt
- Watchdog timer
- 2.7 V to 5.5 V supply voltages
- 1.4 V to 2.5 V external power supply generator for biometric components
- External clock frequency up to 10 MHz
- Power-saving Standby state
- Contact assignment compatible with ISO/IEC 7816-3 standards
- Four general-purpose inputs/outputs (GPIOs) and hardware SPI for biometric applications
- ESD protection:
 - HBM: 6 kV for ISO pads, 2 kV for GPIO pads and 4 kV and AC0/AC1 contactless pads and GPIO pads
 - CDM: 500 V
- IART with RAM buffer for high-speed serial data support (ISO/IEC 78163 T=0/T=1 and EMV® compliant)
- SPI master/slave interface running at up to 6.2 MHz
- I²C software library available at up to 400 kbps

Contactless features

- Complies with ISO/IEC 14443 Type A and Type B, and ISO/IEC 18092 Type F, with programmable autodetection of Type A, B or F
- 35 pF and 68 pF tuning capacitor
- Automatic CPU frequency adaptation for optimum power consumption
- 13.56 MHz carrier frequency
- RFUART (RF universal asynchronous receiver transmitter) up to 848 kbps
- Very high bitrate (ASK VHBR) up to 6.8 Mbps in reception and transmission
- 1-Kbyte RF frame buffer in dedicated RFUART RAM
- MIFARE Plus® EV1, MIFARE Classic® and MIFARE® DESFire® EV2 hardware and software implementation
- Simultaneous mode (contact and contactless)

| Product status link | |
|------------------------|----------------------------|
| ST31N platform devices | Flash memory size (Kbytes) |
| ST31N600 | 608 |
| ST31N500 | 512 |
| ST31N400 | 416 |

Security features

- SC000 memory protection unit (MPU)
- Active shield
- Library protection unit (LPU)
- Monitoring of environmental parameters, including the temperature detector
- Three-key Triple DES accelerator
- AES accelerator
- AIS-31 Class PTG.2, NIST SP800-22 and NIST SP800-90B compliant true random number generator (TRNG)
- NESCRIPT lite low power (LLP) coprocessor for public key cryptography algorithm
- ISO/IEC 13239 calculation block
- Unique serial number on each die
- Highly efficient protection against fault injection
- Protection against multiple attacks

Targeted certifications

- EMVCo™, CC EAL6+, CUP, FIPS 140-2 compliance (NIST SP800-22 and SP800-90B)

1 Description

Designed for secure ID and banking applications, including biometry, the **ST31N600**, **ST31N500** and **ST31N400** devices are serial access microcontrollers that incorporate the most recent generation of Arm® processors for embedded secure systems. The SecurCore® SC000™ 32-bit RISC core is built on the Cortex®-M0 core with additional security features to help to protect against advanced forms of attack.

Cadenced at 60 MHz, the SC000™ core brings great performance and excellent code density thanks to the Thumb®-2 instruction set.

Some of the devices implement the MIFARE® DESFire® EV2 or MIFARE Plus® EV1 (including MIFARE Classic®) technology.

Note: **MIFARE**, **DESFire**, **MIFARE Plus** and **MIFARE Classic** are registered trademarks of NXP B.V. and are used under license.

An RF interface including an RF universal asynchronous receiver (RFUART) enables contactless communication compatible with ISO/IEC 14443 Type A and Type B at up to 848 kbps, and up to 6.8 Mbps with VHBR. It also supports the ISO/IEC 18092 Type F at up to 424 kbps.

The ST31N platform devices also offer a serial communication interface fully compatible with the ISO/IEC 7816-3 standard (T=0, T=1).

Three 16-bit general-purpose timers are available as well as a watchdog timer.

The ST31N platform devices feature hardware accelerators for advanced cryptographic functions. The **AES** accelerator provides a high-performance implementation of the AES-128, AES-192 and AES-256 algorithms. The 3-key Triple **DES** accelerator (EDES+) peripheral enables cipher block chaining (CBC) mode, fast DES and triple DES computation based on three key registers and one data register, while the NESCRIPT LLP cryptoprocessor efficiently supports the public key algorithm with native operations up to 4096 bits long.

With their dedicated interface, the ST31N platform devices also support biometry or multiple applications by managing the power supply to external components, and offering an **SPI** master/slave interface or **GPIOs** in both contact (via the VCC pad) and contactless (RF harvesting) mode.

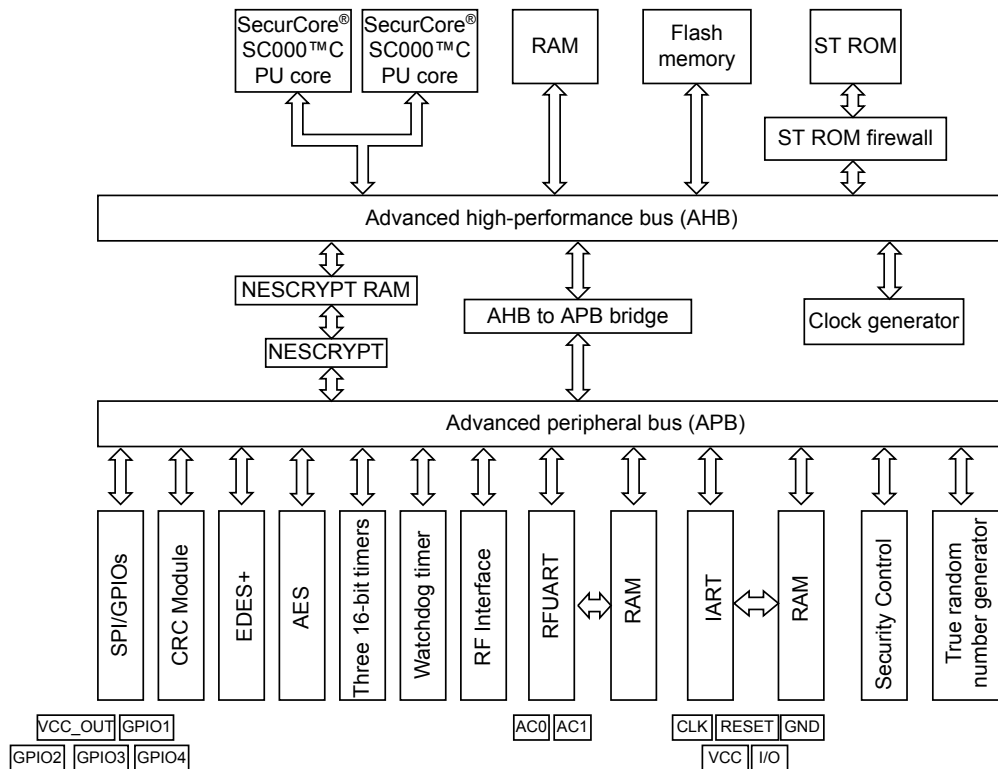
The ST31N platform devices operate in the -25 to +85 °C temperature range, in the 2.7 V and 5.5 V supply voltage ranges in contact mode, and complies with ISO/IEC 14443 specification limits. A comprehensive range of power-saving modes enables the design of efficient low-power and contactless applications.

Note: **Arm** is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

arm



Figure 1. ST31N platform block diagram



1.1 Software development tools description

Dedicated Arm® SecurCore® SC000™ software development tools are provided by Arm® and Keil®. This includes the instruction set simulator (ISS) and C compiler. The documentation is available on the Arm and Keil websites. Moreover, STMicroelectronics provides:

- A time-accurate hardware emulator controlled by the Keil debugger and the ST development environment.
- A complete product simulator based on Keil's ISS simulator for the Arm® SecurCore® SC000™ CPU.

Revision history

Table 1. Document revision history

| Date | Version | Changes |
|-------------|---------|---|
| 29-May-2019 | 1 | Initial release. |
| 16-Nov-2021 | 2 | Document confidentiality changed from ST Restricted to public. Added ST31N500 and ST31N400 part numbers. Updated package images on cover page. Updated Section Features and Section 1 Description . Added Section 1.1 Software development tools description . Added glossary. |

Glossary

AES Advanced encryption standard

ASK Amplitude-shift keying

CBC Cipher block chaining

CC Common Criteria

CDM Charged device model

CPU Central processing unit

CUP China UnionPay

DES Data encryption standard

EAL Evaluation assurance level

ESD Electrostatic discharge

FIPS Federal Information Processing Standards

GPIO General purpose input/output

HBM Human body model

IART ISO/IEC 7816-3 asynchronous receiver transmitter

ISO Relative to the ISO/IEC 7816 asynchronous receiver transmitter.

ISS Instruction set simulator

I²C Inter-integrated circuit

KB Kilobyte

LLP Lite low power

LPU Library protection unit

MCU Microcontroller unit

MPU Memory protection unit

NIST National Institute of Standards and Technology

NVM Nonvolatile memory

OS Operating system

RF Radio frequency

RFUART Radio-frequency universal asynchronous receiver/transmitter

SE Secure element

SPI Serial peripheral interface

TRNG True random number generator

VHBR Very high bit rate



IMPORTANT NOTICE – PLEASE READ CAREFULLY

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgement.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of Purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, please refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.

© 2021 STMicroelectronics – All rights reserved