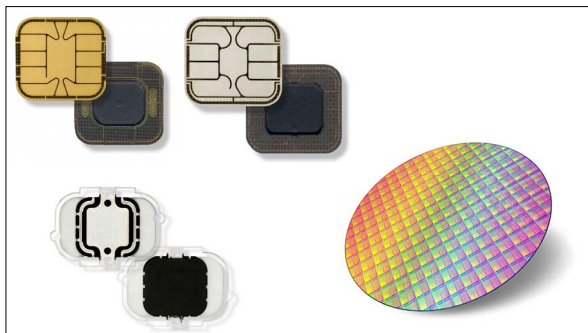


Secure dual interface microcontroller with enhanced security and up to 480 Kbytes of Flash memory

Data brief



Features

Hardware features

- ARM® SecurCore® SC000™ 32-bit RISC core
- 12 Kbytes of User RAM
- Up to 480 Kbytes of secure User high-density Flash memory including 128 bytes of User OTP area:
 - 30-year data retention
 - 500 000 Erase/Write cycle endurance
- Operating temperature: –25 °C to +85 °C
- Three 16-bit timers with interrupt
- Watchdog timer
- 21. V to 5.5 V supply voltages
- External clock frequency up to 10 MHz
- CPU clock frequency up to 28 MHz
- Power-saving Standby state
- Contact assignment compatible with ISO/IEC 7816-3 standards
- Asynchronous receiver transmitter (IART) with RAM buffer for high speed serial data support (ISO/IEC 7816-3 T=0/T=1 and EMV® compliant)
- ESD protection greater than 6 kV (HBM)
- CCEAL6+ and EMVCo certification target

Contactless features

- Complies with ISO/IEC 14443 Type A, B and B', PayPass™ and ISO/IEC 18092 passive mode standards
- Two tuning capacitor values: 20 pF and 68 pF
- Automatic CPU frequency adaptation for optimum power consumption
- Automatic RF communication type detection
- 13.56 MHz carrier frequency
- RFUART (RF universal asynchronous receiver transmitter) up to 848 Kbps
- Very high bitrate (ASK VHBR) up to 3.4 Mbps in reception and 6.8 Mbps in transmission
- Simultaneous mode (contact and contactless)
- 4-Kbyte RF frame buffer in dedicated RFUART RAM
- MIFARE Plus® and MIFARE® DESFire® EV1 hardware and software implementation
- MIFARE® Classic available as part of MIFARE Plus®

Security features

- Active shield
- Monitoring of environmental parameters
- Three-key Triple DES accelerator
- AES accelerator
- AIS-31 Class PTG2 compliant true random number generator (TRNG)
- NESCRYPT coprocessor for public key cryptography algorithm
- ISO/IEC 13239 CRC calculation block
- Unique serial number on each die
- Protection against multiple attacks

1 Description

Designed for secure ID and banking applications, the ST31G480, ST31G384, ST31G320 and ST31G256 are serial access microcontrollers that incorporate the most recent generation of ARM processors for embedded secure systems. Their 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 attacks.

Cadenced at 28 MHz, the SC000™ core brings great performance and excellent code density thanks to the Thumb®-2 instruction set.

Some devices implement the MIFARE® DESFire® EV1 or MIFARE Plus® (including MIFARE® Classic) technology. MIFARE, 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 up to 848 Kbps compatible with ISO/IEC 14443 Types A, B and B' as well as ISO/IEC 18092 standards.

Very-high bitrates (ASK VHBR) up to 3.4 Mbps in reception and 6.8 Mbps in transmission are possible.

A Simultaneous mode where contactless communication can be enabled while the device is in Contact mode is also available.

The 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 with interrupt capability are available as well as a watchdog timer.

The 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 NESCRYPT cryptoprocessor efficiently supports the public key algorithm with native operations up to 4096 bits long.

The devices operate in the –25 to +85 °C temperature range, at 2.1 V, 3 V and 5 V supply voltage ranges in Contact mode, and complies with the ISO/IEC 14443 and ISO/IEC 18092 specification limits. A comprehensive range of power-saving modes enables the design of efficient low-power and contactless applications.

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.



2 Software development tool description

Dedicated 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 web sites.

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 SecurCore® SC000™ CPU.

3 Ordering code

Example:

	ST31	G	480	M	R	XX	A	xxx
Platform type								
ST31 = ARM® SecurCore™ SC000 platform								
Product family								
Dual interface device in 80 nm technology								
Memory size (Flash memory)								
480 = 480 Kbytes								
320 = 320 Kbytes								
384 = 384 Kbytes								
256 = 256 Kbytes								
Specific software features								
S = No additional software								
M = MIFARE Plus™ or MIFARE DESFire™ EV1								
Specific hardware features								
B = Contact only, no NESCRIPT								
C = Contact only								
F = Contactless only, no NESCRIPT								
G = Contactless only								
Q = Dual, no NESCRIPT								
R = Dual								
Delivery form								
XX								
Product external revision								
A = Revision 1								
B = Revision 2								
Chameleon code								
xxx								

Not all combinations are necessarily available. For a list of available options (speed, package, etc.) or for further information on any aspect of these devices, please contact your nearest STMicroelectronics Sales Office.

4 Revision history

Table 1. Document revision history

Date	Revision	Changes
17-Jun-2014	1	Initial release.
13-Apr-2016	2	Added the ST31G384, ST31G320 and ST31G256 part numbers. Updated cover page features. Added ECOPACK text. Replaced <i>Device and feature summary of derivative devices</i> by Section 3: Ordering code .

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.

© 2016 STMicroelectronics - All rights reserved

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