SC31ZD38

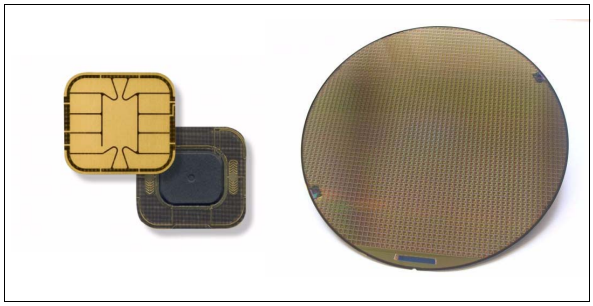
Secure MCU with enhanced security and 38 Kbytes of EEPROM

Data brief

Features

Hardware features

- ARM® SecurCore® SC000™ 32-bit RISC core
- 320 Kbytes of User ROM
- 8 Kbytes of User RAM
- 38 Kbytes of User EEPROM
- CPU clock frequency up to 28 MHz
- Power-saving Standby state
- Contact assignment compatible with ISO/IEC 7816-3 standards
- Asynchronous receiver transmitter (IART) for high speed serial data support (ISO/IEC 7816-3 T=0/T=1 and EMV compliant)
- ESD protection greater than 5 kV (HBM)



Security features

- Three-key Triple DES accelerator
- AES accelerator
- NESCRYPT coprocessor for public key cryptography algorithm
- Protection against multiple attacks

1 Description

Designed for secure ID and banking applications, the SC31ZD38 is a serial access microcontroller that incorporates the most recent generation of ARM processors for embedded secure systems. Its 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.

The SC31ZD38 also offers a serial communication interface fully compatible with the ISO/IEC 7816-3 standard (T=0, T=1).

Two 16-bit general-purpose timers are available; one is configurable as a watchdog.

The SC31ZD38 features hardware accelerators for advanced cryptographic functions. The AES accelerator provides a high-performance implementation of AES-128, AES-192, 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 crypto-processor efficiently supports the public key algorithm with native operations up to 4096 bits long.

The SC31Z family operates in the –25 to +85°C temperature range, at 1.8V, 3V and 5V supply voltage ranges in Contact mode. A comprehensive range of power-saving modes enables the design of efficient low-power applications.

Software development tools 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.

2 Revision history

Table 1. Document revision history

Date	Revision	Changes
24-Jul-2012	1	Initial release.

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 TWO AUTHORIZED ST REPRESENTATIVES, 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