ST33F1M

Smartcard MCU with 32-bit ARM® SecurCore® SC300™ CPU and 1.25 Mbytes high-density Flash memory

Data brief

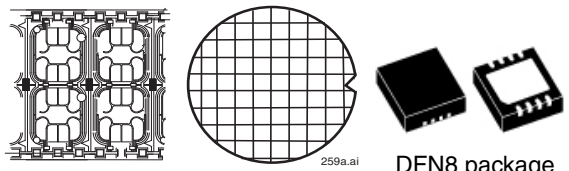
Features

ST33F1M major applications include:

- Mobile communications (GSM, 3G and CDMA)
- Java Card™ applications
- Multimedia
- Mobile TV, banking & transportation

Hardware features

- ARM® SecurCore® SC300™ 32-bit RISC core
- 30 Kbytes User RAM
- 1280 Kbytes User Flash memory with OTP area:
  - 10-year data retention
  - 100,000 Erase/Write cycles
  - Page granularity of 256 Bytes
  - Block granularity: 1 Kbyte
  - 256 Bytes of OTP for User
  - Page Erase time 5 ms
  - Block Erase 1 Kbyte in 15 ms
  - Programming performance up to 10µs/byte in Chained mode
  - Flash Erase / Write Protection software programmable on 128 Kbyte Sectors
- Asynchronous Receiver Transmitter supporting ISO/IEC 7816-3 T=0 and T=1 protocols
- Single Wire Protocol (SWP) Interface for communications with NFC router
- Optional Serial Peripheral Interface (SPI) Slave interface
- Two 16-bit timers with interrupt capability and one extra 16-bit timer with watchdog capability
- 1.8V, 3V and 5V supply voltage ranges
- External clock frequency from 1 up to 10 MHz
- High performance provided by:
  - CPU clock frequency up to 25 MHz
  - External clock multiplier (2x, 3x, and 4x)



Micromodule Wafer DFN8 package

- Current consumption compatible with GSM and ETSI specifications
- Power-saving Standby state
- Contact assignment compatible with ISO/IEC 7816-2
- ESD protection greater than 4 kV (HBM)
- 8-lead plastic small outline (208 mils body width) ECOPACK® package

Software features

- Secure Flash Loader
- Flash drivers

Security features

- Active shield
- Memory Protection Unit (MPU)
- Monitoring of environmental parameters
- Protection against faults
- ISO 3309 CRC calculation block
- True Random Number Generator
- Unique serial number on each die
- Hardware security-enhanced DES accelerator
- NESCRYPT coprocessor for public key cryptography algorithm

Development environment

Software development and firmware generation are supported by a comprehensive set of development tools dedicated to software design and validation:

- C Compiler
- Simulator
- Emulator

1 Description

1.1 Hardware description

The ST33F1M is a serial access microcontroller designed for secure mobile applications that incorporates the most recent generation of ARM processors for embedded secure systems. Its SecurCore® SC300™ 32-bit RISC core is built on the Cortex™ M3 core with additional security features to help to protect against advanced forms of attacks.

Cadenced at 25MHz, the SC300™ core brings great performance and excellent code density thanks to the Thumb®-2 instruction set.

The high-speed embedded Flash 1280 Kbyte memory introduces more flexibility to the system.

The ST33F1M also offers a serial communication interface fully compatible with the ISO/IEC 7816-3 standard (T=0, T=1) and a single-wire protocol (SWP) interface for communication with a near field communication (NFC) router in SIM/NFC applications.

An SPI Slave interface is also available for communication in non-SIM applications.

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

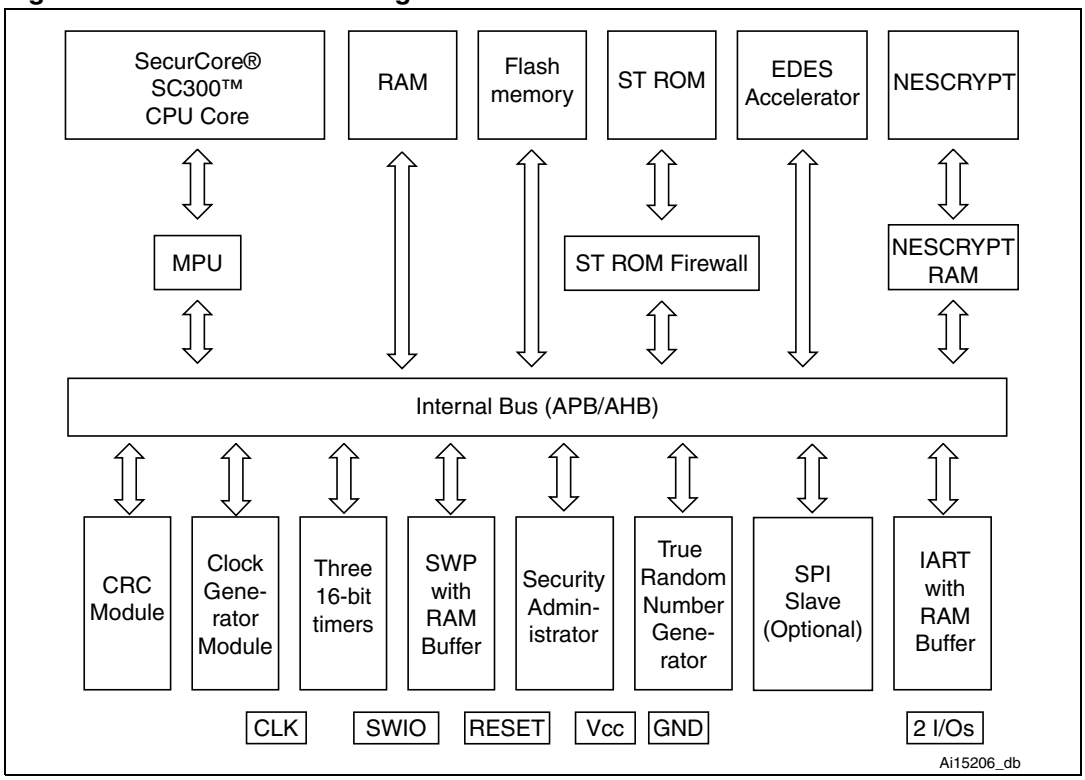
The ST33F1M features hardware accelerators for advanced cryptographic functions. The EDES peripheral provides a secure DES (Data Encryption Standard) algorithm implementation, while the NESCRYPT crypto-processor efficiently supports the public key algorithm.

The ST33F family operates in the –25 to +85°C temperature range and 1.8V, 3V and 5V supply voltage ranges. A comprehensive range of power-saving modes enables the design of efficient low-power applications.

In order to meet environmental requirements, ST (also) offers these devices in ECOPACK® packages. ECOPACK® packages are lead-free. The category of second Level Interconnect is marked on the package and on the inner box label, in compliance with JEDEC Standard JESD97. The maximum ratings related to soldering conditions are also marked on the inner box label.

ECOPACK is an ST trademark. ECOPACK specifications are available at: www.st.com.

Figure 1. ST33F1M block diagram



1.2 Software development tools description

Dedicated SecurCore® SC300™ 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® SC300™ CPU.
- A secured ROMed Flash Loader with very high-speed software downloading capabilities.

2 Revision history

Table 1. Document revision history

Date	Revision	Changes
24-Jan-2011	1	Initial release.
28-Nov-2011	2	Updated *Features* and *Description*.

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