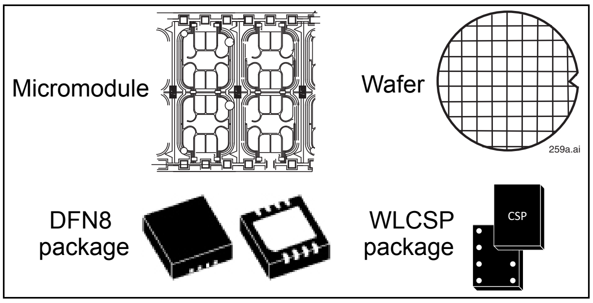
ST33F1M, ST33F1M0, ST33F896, ST33F768, ST33F640, ST33F512

Secure MCU with 32-bit ARM SC300 CPU, SWP interface, NESCRYPT cryptoprocessor and high-density Flash memory

Data brief



Features

ST33F1M[a] major applications include:

- Mobile communications (GSM, 3G and CDMA)
- Java Card™ applications
- NFC applications (Banking, Transportation, etc.)
- Optional MIFARE Classic & DESFire® EV1
- Secure Element (UICC or embedded)

Hardware features

- ARM® SecurCore® SC300™ 32-bit RISC core
- Up to 30 Kbytes of User RAM
- Up to 1280 Kbytes of User Flash memory with OTP area
- Asynchronous receiver transmitter supporting ISO/IEC 7816-3 T=0 and T=1 protocols (Slave mode supported)
- Single Wire Protocol (SWP) Interface for communications with NFC router
- Serial peripheral interface (SPI) slave interface
- Three 16-bit timers with interrupt capability including one 16-bit timer with watchdog capability
- 1.8 V, 3 V and 5 V supply voltage ranges
- External clock frequency from 1 up to 10 MHz
- Current consumption compatible with GSM and ETSI specifications
- High performance provided by:
  - CPU clock frequency up to 22.5 MHz
  - External clock multiplier (2x, 3x, and 4x)
- Power-saving standby state
- Contact assignment compatible with ISO/IEC 7816-2
- ESD protection greater than 4 kV (HBM)

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 algorithms (RSA, ECC, etc.)
- Code/data signature

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 and emulator.

Table 1. Device summary

Part numbers	Flash (Kbytes)
ST33F1M	1280
ST33F1M0	1024
ST33F896	896
ST33F768	768
ST33F640	640
ST33F512	512

[a] ST33F1M* is a generic term that refers to all devices summarized in *Table 1*.

1 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 22.5 MHz, the SC300™ core brings great performance and excellent code density thanks to the Thumb®-2 instruction set.

The high-speed embedded Flash with up to 1280 Kbytes of 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. Note that this interface is not available when ISO/IEC 7816 communications are required.

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

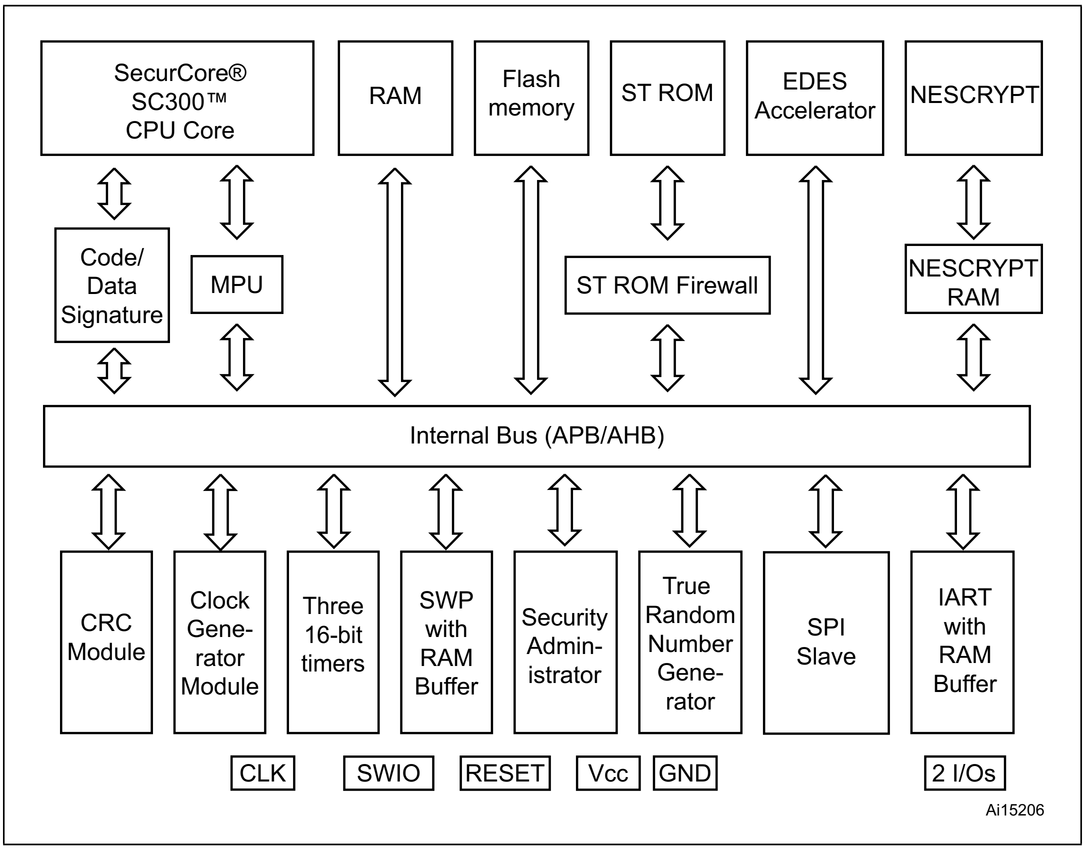
The ST33F1M features hardware accelerators for advanced cryptographic functions. The EDES peripheral provides a secure DES (Data Encryption Standard) algorithm implementation, while the NESCRYPT crypto-processor efficiently supports the public key algorithm.

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 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.

Figure 1. ST33F1M block diagram



1.1 Software development tools

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 2. Document revision history

Date	Revision	Changes
24-Jan-2011	1	Initial release.
28-Nov-2012	2	Updated *Features* and *Description*.
18-Sep-2012	3	Modified title, *Features* and added *Table 1: Device summary*.
26-Mar-2013	4	Updated document header to cover all part numbers. Added part numbers in *Table 1: Device summary*. Removed “optional” before SWP interface in *Features* and *Section 1: Description*. Added MIFARE in *Features*. Added WLCSP package.
07-Nov-2013	5	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