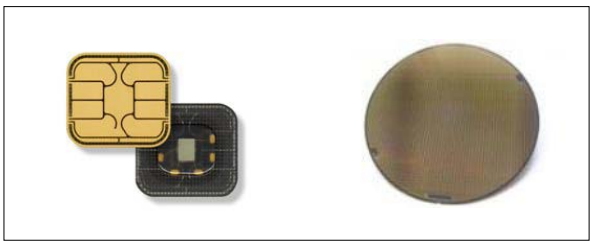
ST33G1M2, ST33G1M0, ST33G896, ST33G768, ST33G640, ST33G512

Secure MCU with 32-bit ARM® SecurCore® SC300™ CPU, SWP, ISO, SPI and GPIO interfaces and high-density Flash memory

Data brief



Features

Hardware features

- ARM® SecurCore® SC300™ 32-bit RISC core cadenced at 25 MHz
- 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 (ETSI 102-613 compliant)
- Serial peripheral interface (SPI) master/slave interface
- Three 16-bit timers with interrupt capability
- Seven general purpose I/Os enabling proprietary protocol implementation
- 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
- 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
- 16- and 32-bit CRC calculation block (ISO 13239, IEEE 802.3, etc.)
- True random number generator
- Unique serial number on each die
- Hardware security-enhanced DES accelerator
- Hardware security-enhanced AES accelerator
- NESCRYPT coprocessor for public key cryptography algorithm

Applications

ST33G1M2[(a)] major applications include:

- Mobile communications (GSM, 3G and CDMA)
- NFC mobile transactions
- Java Card applications
- Multimedia

Table 1. Device summary

Part number	Flash (Kbytes)
ST33G1M2	1280
ST33G1M0	1024
ST33G896	896
ST33G768	768
ST33G640	640
ST33G512	512

a. ST33G1M2* is the master product that refers to all commercial derivatives summarized in *Table 1*.

1 Description

The ST33G1M2 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.

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

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

The ST33G1M2 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 Master/Slave interface is also available for communication in non-SIM applications.

The ST33G1M2 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 AES peripheral ensures secure and fast AES algorithm implementation.

The ST33G 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.

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 STMicroelectronics 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
01-Oct-2013	1	Initial release.
20-Jun-2014	2	Added derivative devices.