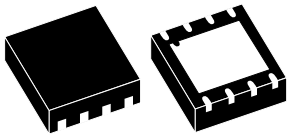
ST33GxxxA

Secure MCU with 32-bit ARM® SecurCore® SC300™ CPU, SWP interface and high-density Flash memory, automotive grade

Data brief



DFN8 6 × 5 mm

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)

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

Major ST33G1M2A applications include:

- Mobile communications (Automotive grade)
- Java Card™ applications
- AECQ100 compliant

Table 1. Device summary

Part number	Memory size in Kbytes
ST33G1M2A	1280
ST33G1M0A	1024
ST33G896A	896
ST33G768A	768
ST33G640A	640
ST33G512A	512
ST33G384A	384

1 Description

The ST33GxxxA (see *Table 1*) 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 ST33GxxxA 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.

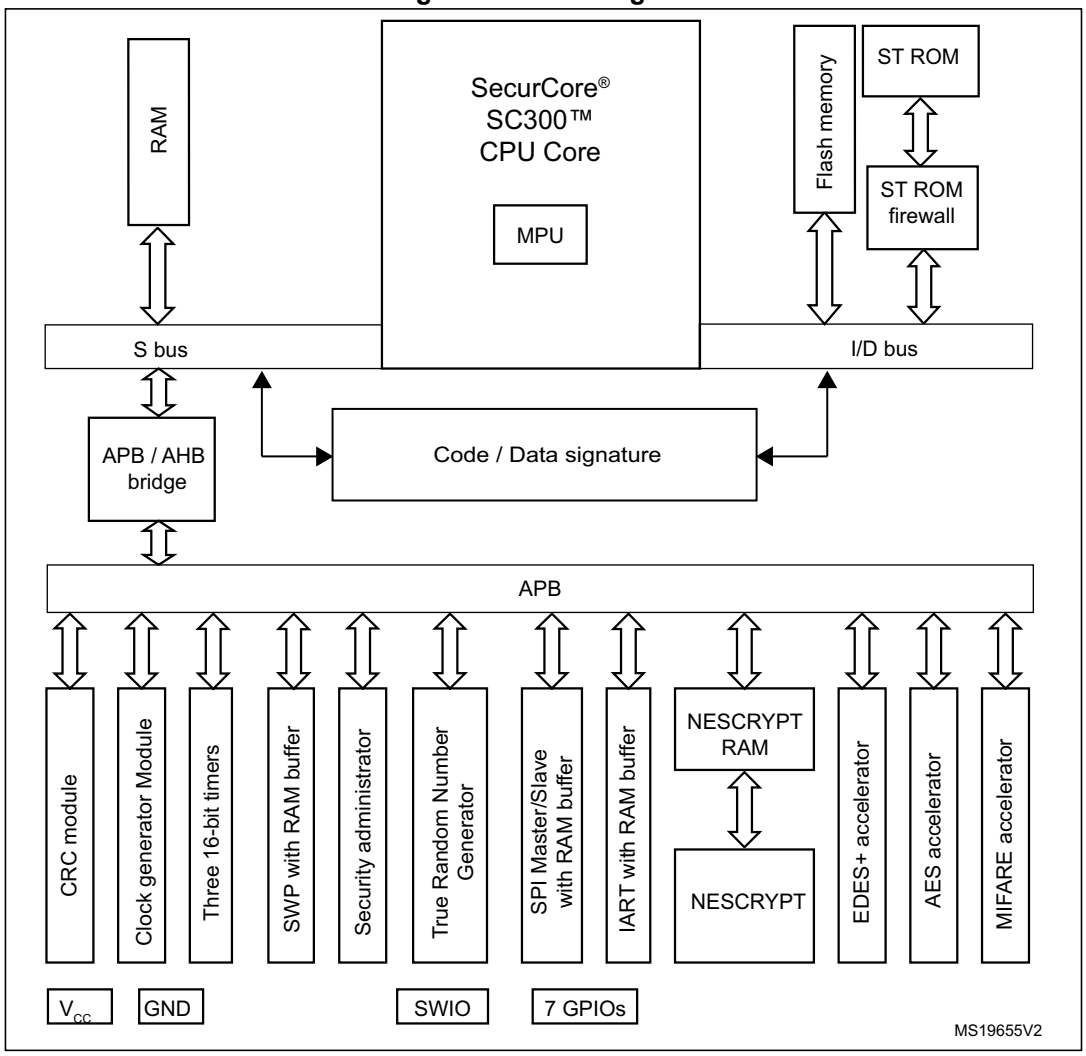
The ST33GxxxA features hardware accelerators for advanced cryptographic functions. The EDES peripheral provides a secure DES (Data Encryption Standard) algorithm implementation, while the NESCRYPT cryptoprocessor efficiently supports the public key algorithm. The AES peripheral ensures secure and fast AES algorithm implementation.

The device operates in the –40 to +105 °C temperature range and 1.8 V, 3 V and 5 V supply voltage ranges. A comprehensive range of power-saving modes enables the design of efficient low-power applications.

The ST33GxxxA's automotive grade is AEQ100 compliant and provides user Flash memory capability up to 500 kcycles with 15 years' data retention.

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. Block diagram



2 Software development tool 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 websites.

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 memory loader with very high-speed software downloading capabilities.

3 Revision history

Table 2. Document revision history

Date	Revision	Changes
19-Nov-2014	1	Initial release.
10-Mar-2016	2	Added *Figure 1: Block diagram*. Small text changes.