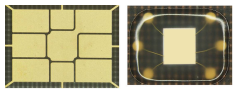
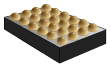
ST33K1M5C ST33K1M2C ST33K1M0C ST33K768C

Data brief

High-speed secure MCU with 32-bit Arm® Cortex®-M35P CPU with SWP, ISO, SPI and I²C interfaces, and high-density Flash memory

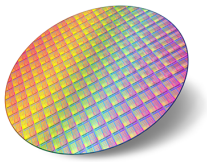


D18 micromodule



WLCSP24

VFDFPN8, wettable flank, 5 × 6 mm



Wafer

Product summary	
ST33KxxxC	**NVM size (in Kilobytes)**
ST33K1M5C	1534
ST33K1M2C	1280
ST33K1M0C	1024
ST33K768C	768

Features

Hardware features

- Arm® Cortex®-M35P 32-bit RISC core cadenced at 70 MHz
- Operating temperature range: −30°C to 85 °C
- 2 Kbytes of cache memory
- Up to 1.5 Mbytes of User Flash memory
- 64 Kbytes of User RAM
- External interfaces
  - Two ISO/IEC 7816-3 interfaces supporting the T=0 and T=1 protocols (Slave mode)
  - Single-wire protocol (SWP) slave interface (ETSI 102613 compliant)
  - Serial peripheral interface (SPI) - Master (up to 17 MHz) and Slave (up to 48 MHz)
  - Master/Slave I²C interface up to 1 Mb/s
- Three 16-bit timers with interrupt capability
- Permanent timer in low-power Standby mode
- Watchdog timer
- Ten multiplexed general-purpose I/Os
- Class C (1.8 V), Class B (3 V) and 3.3 V supply voltage ranges
- Current consumption compatible with GSM and ETSI TS 102 221 release 12 and beyond
- Contact assignment compatible with ISO/IEC 7816-2
- ESD protection greater than 4 kV (HBM)
- Delivery forms:
  - D18 micromodule
  - WLCSP24 and wettable flank VFDFPN8 (5 × 6 mm) ECOPACK-compliant packages
  - Sawn/unsawn 12” wafers

Security features

- Platform and Flash memory loader security certification target according to Common Criteria EMVCo™ / MTPS (Mobile Trustable Public Service Platform)
- Hardware security-enhanced DES accelerator
- Hardware security-enhanced AES accelerator
- Optional hardware security-enhanced SM4 accelerator
- MIFARE Classic® cryptography hardware accelerator
- NESCRYPT LLP coprocessor for public key cryptography algorithm
- 16- and 32-bit CRC calculation block (ISO 13239, IEEE 802.3, etc.)
- Active shield
- Highly efficient protection against faults
- True random number generator

Software features

- Secure Flash memory loader with high-speed downloading and post-delivery loading ability
- Optional security-certified cryptographic library "NesLib"

Applications

- Java® Card applications
- Single- and dual-interface embedded SIM (eSIM)
- Standard SIM
- 5G-compliant
- Generic embedded secure element (eSE)

1 Description

The ST33KxxxC is a serial access microcontroller designed for secure mobile applications. It incorporates the most recent generation of Arm® processors for embedded secure systems. Its Cortex®-M35P 32-bit RISC core includes additional security features to help protect against advanced forms of attack.

The ST33KxxxC provides high performance thanks to a fast Cortex®-M35P processor, cryptographic accelerators and improved Flash memory operations.

Cadenced at 70 MHz, the Cortex®-M35P core brings great performance and excellent code density thanks to the Thumb®-2 instruction set.

Strong and multiple fault protection mechanisms ensure a guaranteed high-detection coverage that facilitates the development of highly secure software. This is achieved by using two CPUs in Lockstep mode, error detection in sensitive memories and hardware logic.

The ST33KxxxC offers two serial communication slave interfaces fully compatible with the ISO/IEC 7816-3 standard (T=0, T=1) and a single-wire protocol (SWP) slave interface for communication with a near field communication (NFC) router in secure element (SE) applications. The device also includes a Master/Slave serial peripheral interface (SPI) as well as an inter-integrated circuit (I²C) Master/Slave interface for communication. The Slave SPI runs at up to 48 MHz and the Master SPI at up to 17 MHz while the Slave I²C Fast-mode Plus interface operates at up to 1 Mbit/s and the Master I²C Fast-mode plus at up to 1 Mbit/s.

Three general-purpose 16-bit timers as well as a watchdog timer are available.

One permanent timer (PMT) with a count capability in low-power mode is available.

The ST33KxxxC features hardware accelerators for advanced cryptographic functions. The EDES+ peripheral provides a secure DES (data encryption standard) algorithm implementation, while the NESCRYPT LLP cryptoprocessor efficiently supports the public key algorithm. The AES (advanced encryption standard) and SM4 peripherals ensure secure and fast AES and SM4 algorithm implementations.

The ST33KxxxC operates in the −30°C to 85 °C temperature range and 1.8 V, 3 V and 3.3 V supply voltage ranges. A comprehensive range of power-saving modes enables the design of efficient low-power applications:

- Hibernate mode at 1 µA (typical value)
- Standby mode at 30 µA (typical value)

In terms of application, STMicroelectronics offers the following optional software package:

- NesLib cryptographic library

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.

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

2 Software development tool description

Dedicated Cortex®-M35P software development tools are provided by Arm® and Keil®. 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.
- A secure Flash memory loader with high-speed software downloading capability and post-delivery loading ability in accordance with protection profile BSI-CC-PP-0084-2014 including Loader Package 2, and the ANSSI note ANSSI-CC-NOTE-06/2.0.

Revision history

Table 1. **Document revision history**

Date	Revision	Changes
14-Sep-2021	1	Initial release.