High-speed secure MCU with 32-bit Arm® SecurCore® SC300™ CPU with SWP, ISO, SPI, I2C and high-density Flash memory

Features

Hardware features
- Arm® SecurCore® SC300™ 32-bit RISC core cadenced at 60 MHz
- Up to 2048 Kbytes of User Flash memory
- 50 Kbytes of User RAM
- External interfaces
  - ISO/IEC 7816-3 T=0 and T=1 protocols (Slave and Master modes)
  - Single Wire Protocol (SWP) slave interface (ETSI 102-613 compliant)
  - Master/slave serial peripheral interface (SPI)
  - Two Master/Slave I2C interfaces
- Three 16-bit timers with interrupt capability
- Watchdog timer
- Eight multiplexed general-purpose I/Os
- 1.8 V, 3 V and 5 V supply voltage ranges
- External clock frequency from 1 up to 15 MHz
- Current consumption compatible with GSM and ETSI specifications
- Power-saving standby and hibernate states
- Contact assignment compatible with ISO/IEC 7816-2
- ESD protection greater than 4 kV (HBM) and up to 1 kV (CDM)
- Delivery forms:
  - D18 micromodule
  - ECOPACK®-compliant WLCSP12 and QFN20 packages
  - Sawn/unsawn 12" wafers

Security features
- Platform and Flash loader security certification target according to CC EAL5+ / EMVCo
- Hardware security-enhanced DES accelerator
- Hardware security-enhanced AES accelerator
- MIFARE Classic® cryptography hardware accelerator
- NESCORYPT coprocessor for public key cryptography algorithm
- 16- and 32-bit CRC calculation block (ISO 13239, IEEE 802.3, etc.)
- Active shield
- Memory management unit
- Highly efficient protection against faults
- True random number generator
- Permanent timer

Software features
- Secure Flash loader with high-speed downloading and post-delivery loading ability
- Optional NesLib public cryptographic library
- Optional MIFARE4Mobile®

Applications
- Java Card™ applications
- NFC - Secure Element (SWP SIM, eSE)
- Embedded SIM
- Embedded security (secure dongles, secure hubs, fingerprint eSE and secure access module)

The ST33Jxxx microcontrollers include the devices below:

<table>
<thead>
<tr>
<th>Devices</th>
<th>NVM size</th>
<th>Devices</th>
<th>NVM size</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST33J2M0</td>
<td>2048 KB</td>
<td>ST33J1M1</td>
<td>1152 KB</td>
</tr>
<tr>
<td>ST33J1M8</td>
<td>1792 KB</td>
<td>ST33J1M0</td>
<td>1024 KB</td>
</tr>
<tr>
<td>ST33J1M5</td>
<td>1536 KB</td>
<td>ST33J896</td>
<td>896 KB</td>
</tr>
<tr>
<td>ST33J1M3</td>
<td>1280 KB</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Table 1. Device summary

For further information contact your local STMicroelectronics sales office.

www.st.com
1 Description

The ST33Jxxx is a serial access microcontroller designed for secure mobile applications. It 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 ST33Jxxx provides high performance thanks to a fast SC300 processor, crypto-accelerators (DES, AES and MIFARE Classic®) and improved Flash memory operations. Cadenced at 60 MHz, the SC300™ 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 locked-step mode, error codes in sensitive memories and hardware logic.

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

b. MIFARE Classic is a registered trademark of NXP B.V. and is used under license.
2 General information

The ST33Jxxx 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 Secure Element (SE) applications. The device also includes an SPI Master/Slave interface as well as two I2C Master/Slave interfaces for communication in non-SIM applications: SPI Slave up to 26 MHz, SPI Master up to 13 MHz, I2C Slave High-speed mode up to 2.4 Mbit/s, I2C Master Fast-mode plus up to 1 Mbit/s. Up to four of these interfaces can run independently.

Three general-purpose 16-bit timers as well as a watchdog timer are available. One permanent timer (PMT) with a count capability up to 8 days in low-power mode is available. The ST33Jxxx 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 ST33Jxxx operates in the –25 to +85 °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:
- Hibernate mode down to 1 μA for embedded solutions
- Standby mode for SIM or embedded applications.

In terms of application, ST offers optional software packages:
- NesLib public key cryptographic library
- MIFARE4Mobile® (a)

In order to meet environmental requirements, ST offers this device 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.

---

(a) MIFARE4Mobile is a registered trademark of NXP B.V. and is used under license.
3 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 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 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 2. Document revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>02-Jan-2015</td>
<td>0.1</td>
<td>Initial release.</td>
</tr>
<tr>
<td>13-Nov-2015</td>
<td>1</td>
<td>Updated package information. Updated CC EAL level and added post-delivery loading capability of Flash loader. Updated Applications. Updated Section 1: Description and Section 2: Software development tool description.</td>
</tr>
<tr>
<td>07-Jan-2016</td>
<td>2</td>
<td>Added part numbers (see Table 1: Device summary).</td>
</tr>
<tr>
<td>03-Apr-2020</td>
<td>4</td>
<td>Modified CC EAL level. Reorganized Section 1: Description, with Arm logo update. Added Section 2: General information. Updated MIFARE data.</td>
</tr>
</tbody>
</table>