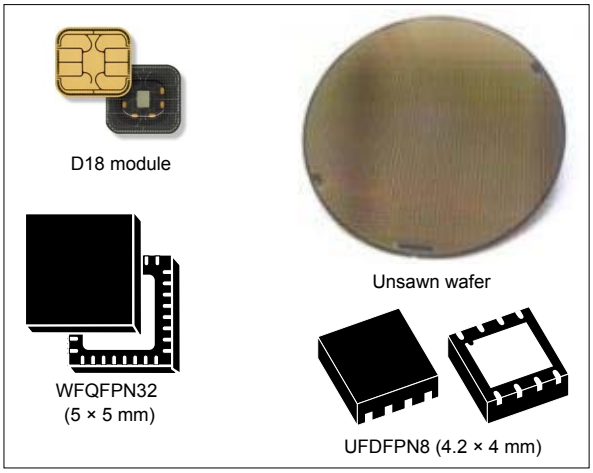
ST33H768, ST33H640, ST33H512, ST33H384

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 768 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 memory Loader
- Flash memory 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

Major applications include:

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

Table 1. Device summary

Part number	Flash (Kbytes)
ST33H768	768
ST33H640	640
ST33H512	512
ST33H384	384

1 Description

The ST33H768, ST33H640, ST33H512 and ST33H384 are serial access microcontrollers designed for secure mobile applications that incorporate the most recent generation of ARM® processors for embedded secure systems. Their 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 ST33H768, ST33H640, ST33H512 and ST33H384 also offer 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 ST33H768, ST33H640, ST33H512 and ST33H384 feature 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 ST33H family 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.

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.

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 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 memory loader with very high-speed software downloading capabilities.

3 Revision history

Table 2. Document revision history

Date	Revision	Changes
26-Feb-2015	1	Initial release.