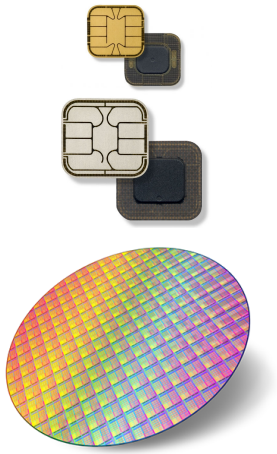
ST31P320 ST31P450

Data brief

Secure dual interface microcontroller with enhanced security and up to 450 Kbytes of Flash memory



Product status link

ST31P320 ST31P450

Features

Hardware features

- Arm® SecurCore® SC000™ 32-bit RISC core cadenced at up to 55 MHz
- 10 Kbytes of User RAM
- Up to 450 Kbytes of secure User high-density Flash memory including 512 bytes of User OTP area:
  - 25-year data retention
  - 500 000 Erase/Write cycle endurance
  - Page Erase time: 0.8 ms
  - Programming performance up to 2 µs/byte in chained mode
  - Flash Erase/Write protection programmable on 32-Kbyte sectors
- Operating temperature: –25 °C to +85 °C
- Three 16-bit timers with interrupt
- Watchdog timer
- 2.7 V to 5.5 V supply voltages
- External clock frequency up to 10 MHz
- Power-saving Standby state
- Contact assignment compatible with ISO/IEC 7816-3 standards
- ESD protection (HBM): 6 kV HBM for ISO pads and 4 kV for AC0/AC1 contactless pads
- Asynchronous receiver transmitter (IART) with RAM buffer for high speed serial data support (ISO/IEC 78163 T=0/T=1 and EMV compliant)

Contactless features

- Complies with ISO/IEC 14443 Type A and EMVCo™
- 68 pF tuning capacitor
- Automatic CPU frequency adaptation for optimum power consumption
- 13.56 MHz carrier frequency
- RFUART (RF universal asynchronous receiver transmitter) up to 848 kbps
- 1-Kbyte RF frame buffer in dedicated RFUART RAM
- MIFARE Classic®, MIFARE Plus® and MIFARE® DESFire® EV2 hardware and software implementation

Security features

- Active shield
- Monitoring of environmental parameters
- Three-key Triple DES accelerator
- AES accelerator
- AIS-31 Class PTG.2 compliant true random number generator (TRNG)
- NESCRYPT coprocessor for public key cryptography algorithm
- ISO/IEC 13239 CRC calculation block
- Unique serial number on each die
- Highly efficient protection against fault attacks

1 Description

Designed for secure ID and banking applications, the ST31P320 and ST31P450 devices are serial access microcontrollers that incorporate the most recent generation of Arm® processors for embedded secure systems. Their SecurCore® SC000™ 32-bit RISC core is built on the Cortex® M0 core with additional security features to help to protect against advanced forms of attacks.

Cadenced at 55 MHz, the SC000™ core brings great performance and excellent code density thanks to the Thumb®-2 instruction set.

Certain devices implement the MIFARE Classic® , MIFARE® DESFire® EV2 or MIFARE Plus® technology.

An RF interface including an RF universal asynchronous receiver (RFUART) enables contactless communication up to 848 kbps compatible with the ISO/IEC 14443 Type A standard.

The devices also offer a serial communication interface fully compatible with the ISO/IEC 7816-3 standard (T=0, T=1).

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

The devices feature hardware accelerators for advanced cryptographic functions. The AES accelerator provides a high-performance implementation of the AES-128, AES-192 and AES256 algorithms. The 3-key Triple DES accelerator (EDES+) peripheral enables Cipher block chaining (CBC) mode, fast DES and triple DES computation based on three key registers and one data register, while the NESCRYPT cryptoprocessor efficiently supports the public key algorithm with native operations up to 4096 bits long.

The devices operate in the –25 to +85 °C temperature range, in the 2.7 V and 5.5 V supply voltage ranges in Contact mode, and comply with ISO/IEC 14443 specification limits. A comprehensive range of power-saving modes enables the design of efficient low-power and contactless applications.

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

MIFARE, MIFARE Classic, MIFARE DESFire and MIFARE Plus are trademarks of NXP B.V. and are used under license.

Revision history

Table 1. Document revision history

Date	Revision	Changes
29-Jun-2018	1	Initial release.
29-Mar-2019	2	Corrected user RAM size in Features. Removed STS39 compatibility feature.
09-Aug-2019	3	Modified ESP protection (HBM) value in Features. Updated MIFARE Classic® data in Features and in Section 1 Description. Removed Figure 1.
29-Jan-2020	4	Added ST31P320 device.