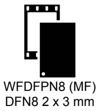
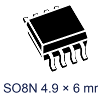
ST31R480 ST31R320

Data brief

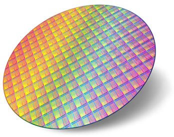
Secure dual interface microcontroller with enhanced security and up to 480 Kbytes of flash memory



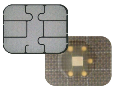
DFN8



SO8N

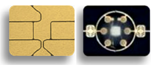


Wafer

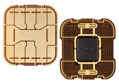


D12

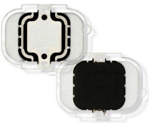
D17



D7G/D7S



D75/D77



CB6

Features

Hardware features

- Arm® SecurCore® SC000™ 32-bit RISC core cadenced at up to 55 MHz with MPU
- 12 Kbytes of user RAM
- Up to 480 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 down to 0.8 ms
  - Programming performance up to 3 µs/byte in chained mode
  - Flash erase/write protection programmable on 32-Kbyte sectors
- eSTM 34nm technology
- Operating temperature: –25°C to +85°C
- Three 16-bit timers with interrupt
- Watchdog timer
- 1.62 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:
  - Human body model (HBM): 6 kV HBM for ISO pads and AC0/AC1 contactless pads
  - Charged device model (CDM): 1KV based on the ST Module
- CQM 2.22; ISO/IEC 10373-1 compliancy
- Asynchronous receiver transmitter (IART) with RAM buffer for high speed serial data support (ISO/IEC 7816-3 T=0/T=1 and EMV compliant)
- I²C hardware interface up to 400 kHz

Contactless features

- Complies with ISO/IEC 14443 type A and EMVCo®
- 68pF tuning capacitor, adaptation possible for optimized performance on broad range of antennas
- 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® 1.5, MIFARE Plus® EV2, and MIFARE® DESFire® EV3 hardware and software implementation

Security features

- Lockstep SC000™
- SC000™ memory protection unit (MPU) and 1-cycle multiplier
- Library protection unit (LPU)
- Active shield
- Monitoring of environmental parameters including temperature detector
- Three-key triple DES accelerator
- AES accelerator
- AIS-31 class PTG.2 and NIST SP800-22 and SP800-90B compliant true random number generator (TRNG), Random library support (RngLib)
- NESCRYPT coprocessor for public key cryptography algorithm
- ISO/IEC 13239 CRC calculation block
- Unique serial number on each die
- Highly efficient protection against fault injection
- Protection against multiple attacks

1 Description

Designed for secure ID and banking applications, the ST31R480, and derivatives (ST31R) 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, including MPU and 1-cycle multiplier.

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® 1.5, MIFARE Plus® EV2, and MIFARE® DESFire® EV3.

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

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 ST31R devices also offer a serial communication interface fully compatible with the ISO/IEC 7816-3 standard (T=0, T=1), and an I2C target hardware interface.

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

An I^{2}C hardware interface running up to 400 kHz is available. The ISO 7816 pins are used as I^{2}C SCL and SDA.

The ST31R480 devices feature hardware accelerators for advanced cryptographic functions. The AES accelerator provides a high-performance implementation of the AES-128, AES-192 and AES-256 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. The NESCRYPT cryptographic processor efficiently supports the public key algorithm with native operations up to 4096 bits long.

The ST31R480 devices operate in the -25 to +85°C temperature range. In contact mode, the devices operate in the supply voltage range of 1.62 V to 5.5 V. They comply with the ISO/IEC 14443 specification limits. A comprehensive range of power-saving modes enables the design of efficient low-power and contactless applications.

Note: The NVM acronym means Non Volatile Memory which is based on flash technology. NVM and flash are equivalent in this datasheet.

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

arm

LICENSED DPA COUNTERMEASURES™

1.1 Software development tools description

Dedicated Arm® SecurCore® SC000™ software development tools are provided by Arm® and Keil®. This includes the instruction set simulator (ISS) and a 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 ST development environment.
- A complete product simulator based on Keil®'s ISS simulator for the Arm® SecurCore® SC000™ CPU.

Revision history

Table 1. **Document revision history**

Date	Revision	Changes
15-Sep-2023	1	Initial release.
27-Jun-2024	2	Updated the following sections: • Section Features • Section 1: Description
24-Sep-2024	3	Minor update.