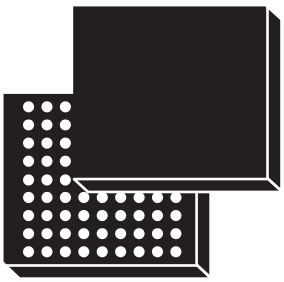
life.augmented

ST54K

Data brief

NFC controller, secure ultra-wideband subsystem host and secure element system on chip



81-ball WLCSP

Product status link
ST54K

Features

- Single die integrating an NFC controller, a secure element and a UWB secure, fine-ranging subsystem host
- Small, ECOPACK-compliant WLCSP81 package
- State of-the-art secure element and eSIM Java® operating system.

NFC controller

- Arm® Cortex®-M3 microcontroller
- 100% re-flashing capability for firmware update
- Enhanced active load modulation technology
- Enhanced TX drive up to 2 W with support of an external 5 V DC/DC converter for TX supply
- Optimized for extremely small or metal-frame antennas
- Optimized power consumption modes
- Ultralow-power Hibernate mode with field detection for low-power mode support
- Proprietary in-frame synchronization (IFS) in Card Emulation (CE) mode to ensure stability in battery Low and Switched OFF modes
- System clock:
  - Fractional-N PLL input range of 19.2 to 76.8 MHz
  - 27.12 MHz external crystal oscillator
- Automatic wakeup via communication interfaces, internal timers, GPIO, RF field or tag detection

RF communications

- NFC active and passive Peer-to-Peer mode
  - ISO/IEC 18092 - NFCIP-1 Initiator & Target
- NFC Reader/Writer mode
  - NFC Forum™ Type 1/2/3/4/5 tags
  - FeliCa™
  - ISO/IEC 15693
  - MIFARE®
- NFC Card Emulation mode
  - ISO/IEC 14443 Type A & Type B
  - FeliCa™
  - MIFARE®
- Ultra-wideband (UWB) subsystem host control:
  - Car Connectivity Consortium® (CCC) digital key (DK) phase 3
  - FiRa™ (fine ranging) secure UWB use cases

External communication interfaces

- Two master SWP interfaces operating at up to 1.695 Mbit/s
- Slave I²C interface supporting Standard-mode, Fast-mode, Fast-mode Plus and High-speed mode

- Master SPI running at up to 8 MHz dedicated to the UWB subsystem
- Slave SPI interface running at up to 26 MHz
- ISO/IEC 7816-3 interface
- General-purpose inputs/outputs (GPIOs)

Internal communication interfaces

- CLF/SE SWP digital interface
- 120 Mbits/s interprocessor communication (IPC) based on a shared internal memory

Secure microcontroller

- Arm® SecurCore® SC300™ 32-bit RISC core cadenced at 100 MHz
- Up to 2048 Kbytes of user Flash memory
- 2 Kbytes of memory cache
- 64 Kbytes of user RAM
- Power-saving Standby and Hibernate states

Secure operating system

- Supports state-of-the-art secure element operating systems:
  - Java® Card 3.0.5
  - GlobalPlatform® 2.3 with Amdts
  - EMVCo™ certification
  - FeliCa™ certification
- Security-certified according to CC EAL5+
- Hardware security-enhanced DES & AES accelerators
- MIFARE Classic cryptography hardware accelerator
- NESCRYPT coprocessor for public key cryptography algorithms

Electrical characteristics

- Battery voltage support from 2.4 V to 5.0 V
- I/O dedicated voltage level (V_{PS_IO}) from 1.62 V to 3.3 V
- Supports Class B and Class C operating conditions for external universal integrated-circuit cards (UICCs)
- Ambient operating temperature −25 to + 85 °C

Applications

- Mobile devices
- Wearable devices
- Smartwatches
- Secure connected devices
- eSE and eSIM convergence
- Secure NFC and UWB connectivity for secure ranging

1 Description

The ST54K is a single-die solution integrating a contactless front-end (CLF) and a secure element, called ST54K_CLF and ST54K_SE, respectively. It is designed for integration in mobile devices and NFC-compliant products.

The ST54K_CLF includes near-field communication (NFC) functions in the three operating modes: Card Emulation, Reader/Writer and Peer-to-Peer communication.

It is best in class in terms of RF output power (up to 2 W). With its outstanding output power and optimized efficiency, the ST54K driver can be connected to metal frame antennas. Thanks to improved low-power card detection sensitivity, in Reader/Writer mode, the ST54K_CLF operating in low-power mode is capable of detecting the presence of a card/tag from a distance greater than the Reader mode performance.

In Card Emulation mode, the ST54K_CLF is capable of operating without an external quartz or an external reference clock source, contributing to further reducing the current consumption of the system in low-power mode. Moreover, thanks to its improved field detection sensitivity, the ST54K_CLF is capable, in low-power mode, of detecting the presence of a reader's RF field from a distance greater than the CE mode performance.

The ST54K_SE is a serial access microcontroller designed for secure mobile applications. It incorporates the most recent generation of Arm® processors for embedded secure systems. The 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 ST54K device offers connectivity and security with its UWB subsystem, which supports emerging secure fine ranging as defined and standardized by the Car Connectivity Consortium® (CCC) and the FiRa™ Consortium.

The CCC specifies and ensures the interoperability of digital key (DK) phase 3 seamless car opening applications while the FiRa™ Consortium specifies and ensures the interoperability of multiple UWB use cases including access control and transit.

2 Product overview

The ST54K_CLF is based on an advanced Arm® Cortex®-M3 32-bit microcontroller running at 56 MHz. It features two external master SWP interfaces and controls the embedded SE (ST54K_SE) with an internal SWP interface. Thanks to an enhanced power switch system, the CLF manages its own power supply and that of the associated secure elements (ST54K_SE, UICC_1 and UICC_2). It supports NCI 2.0.

The ST54K_SE provides high performance thanks to a fast SC300™ processor, crypto-accelerators and improved Flash memory operations. Cadenced at 100 MHz, the SC300 core brings great performance and excellent code density thanks to the Thumb®-2 instruction set.

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

The ST54K offers strong, multiple-fault protection mechanisms that ensure high detection coverage, thus facilitating 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.

The ST54K platform offers a serial communication interface that is fully compatible with the ISO/IEC 7816-3 standard (T=0, T=1) and is intended for use in embedded SIM (eSIM) applications. It includes a single-wire protocol (SWP) interface that internally connects to the ST54K_CLF. ST54K_SE features hardware accelerators for advanced cryptographic functions. The EDES peripheral provides 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 (advanced encryption standard) algorithm implementation.

A comprehensive range of power-saving modes enables the design of efficient low-power applications.

In terms of application, ST offers optional software packages: NesLib public key cryptographic library and MIFARE4Mobile® v2.1.1 with MIFARE Classic® or MIFARE® DESFire® EV1.

The MIFARE® R/W mode feature availability depends on the license conditions. Please contact your local ST representative for further information.

Note: MIFARE, MIFARE4Mobile, MIFARE DESFire and MIFARE Classic are trademarks of NXP B.V. and are used under license.

The ST54K includes an I²C slave interface dedicated to the ST54K_CLF and an SPI slave interface dedicated to the ST54K_SE.

Data transfer between the ST54K_CLF and the ST54K_SE is optimized by the use of an internal shared memory.

The ST54K is manufactured in an ECOPACK-compliant, 3.5 × 3.5 × 0.41 mm, 81-ball wafer-level chip-scale package (WLCSP). The WLCSP offers a more compact footprint, while minimizing die-to-PCB inductance and improving thermal performance.

In order to meet environmental requirements, ST offers the ST54K 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

arm

LICENSED DPA COUNTERMEASURES™

Revision history

Table 1. **Document revision history**

Date	Version	Changes
20-Sep-2018	1	Initial release.
04-May-2021	2	New device with a secure UWB subsystem host: • Updated document title. • Updated Features, in particular: – Package – Fractional-N PLL input range – RF communications – External communication interfaces – Secure operating system • Updated Applications. • Updated Section 1 Description.