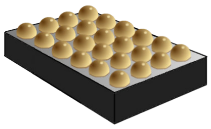
STSAFE-S320

Data brief

Multi-application Java® Card platform based on a 32-bit Arm® Cortex®-M35P CPU with I²C and SPI interfaces



WLCSP24

Product status
Custom data

Features

Hardware features

- Arm® Cortex®-M35P 32-bit *RISC* core cadenced at 70 MHz
- Operating temperature range: –30 °C to 85 °C
- High-stress memory (*HSM*):
  - Endurance of 200 000 erase/write cycles
  - Configured to enhance specific object endurance: 10 million write cycles for specific data
  - Provides a total of 1 gigabyte of updated data
  - 15 years' data retention
- Available in a 24-ball wafer-level chip-scale package (*WLCSP*24)
- External interfaces:
  - *ISO*/*IEC* 7816-3 (ST Reserved test feature)
  - Slave serial peripheral interface (*SPI*) up to 10 MHz
  - Slave *I²C* interface up to 1 Mb/s
- Class C (1.8 V), Class B (3 V) and 3.3 V supply voltage ranges
- *ESD* protection greater than 4 kV (*HBM*)

Software features

- Java® Card 3.0.5 Classic operating system
- GlobalPlatform® 2.3 support
- Support for GlobalPlatform® SCP03 and SCP11
- Support for GlobalPlatform® executable load file (ELF) upgrade
- Dynamic memory management
- *APDU* communication over *I²C*/*SPI* based on the GlobalPlatform® "*APDU Transport over I2C/SPI*" specification
- Firmware upgrade mechanism

Application

- Android™ Weaver
- Secure storage
- Android™ Keymint

1 Description

The STSAFS320WSBCS01 system on chip is a top-class embedded secure element (eSE) able to manage Java® Card applets from different stakeholders (such as the user, original equipment manufacturer (OEM), hardware integrator, or service provider).

The device is compliant with Java® Card 3.0.5 with enhanced mechanisms of memory management, security, and data management.

It also supports the GlobalPlatform® Card Specifications v.2.3 and related amendments:

- GlobalPlatform® Amendment C – Contactless Services v1.3 (support of the "Cumulative Delete" and "Get Status" sections)
- GlobalPlatform® Amendment D – Secure Channel Protocol SCP03 v1.1.1
- GlobalPlatform® Amendment F – Secure Channel Protocol '11' v1.2.1
- GlobalPlatform® Amendment H – Executable Load file Upgrade v1.1
- GlobalPlatform® Access Control v1.1
- GlobalPlatform® APDU communication over I²C/SPI based on the GlobalPlatform® "APDU Transport over I2C/SPI" specification v1.0
- GlobalPlatform® SE Configuration v2.0

The devices are based on Arm® cores.

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

Note: Java is a registered trademark of Oracle and/or its affiliates.

The STSAFS320WSBCS01 is integrated with Android™ applications "Keymint" and "Weaver". It can also host STMicroelectronics applications for secure storage.

It provides state-of-the-art security of the provided functionality, resistant to recent EMVCo/JIL Hardware-related Attacks Subgroup (JHAS)-identified vulnerabilities.

Moreover, the STSAFS320WSBCS01 ensures a high level of security and isolation between applications, and Common Criteria EAL5+ certification is ongoing.

1.1 Main features

The STSAFS320WSBCS01 system on chip (SoC) is a top-class multi-application Java® Card platform, developed on top of a performing hardware architecture based on a powerful Arm® Cortex®-M35 CPU.

The Java Card-based operating system complies with the Java Card 3.0.5 classic application programming interface (API).

The STSAFS320WSBCS01 SoC boasts SE remote applet management (RAM) fully integrated with GlobalPlatform card specification v.2.3, including the SCP03 protocol according to Amendment D, the elliptic curve-based secure channel protocol (SCP11a/SCP11b/SCP11c) according to Amendment F, and ELF upgrade according to Amendment H.

The STSAFS320WSBCS01 SoC also supports dynamic memory management integrated with the Java Card garbage collection mechanism.

It could be used to provide secure storage, cryptographic services, and other security functionality via Java Card applets.

Revision history

Table 1. **Document revision history**

Date	Revision	Changes
24-Nov-2022	1	Initial release.