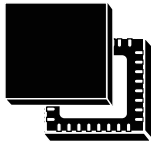
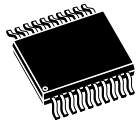


Automotive Open Java[®] Card system-on-chip based on 32-bit Arm[®]Cortex[®] - M35P CPU supporting StrongBox, in vehicle CCC digital key, Qi charging applications



UFQFPN32 WF (5 × 5 × 0.55 mm)




TSSOP20 (6.5 × 4.4 mm)

Optional

Features

Hardware features

- AEC-Q100 grade 2 
- Arm[®] Cortex[®]-M35P 32-bit RISC core cadenced at 63 MHz
- Operating temperature range: -40 °C to 105 °C
- High-stress memory:
 - Endurance of 500 000 erase/write cycles (without hardware wear leveling)
 - Configured to enhance specific objects endurance: up to 10 million write cycles with a total of 1 gigabyte of updated data
Software wear leveling capability for cycling extension and specific cases
 - 20 years data retention
- Available in a TSSOP20 and UFQFPN32 wettable flank package
- External interfaces:
 - ISO/IEC7816-3 (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)
- CC EAL 6+ certified

Software features

- Java[®] Card 3.0.5 classic operating system
- GlobalPlatform[®] 2.3 support
- Support for GlobalPlatform[®] SCP03 and SCP11
- Support for GlobalPlatform[®] ELF upgrade
- Android Ready SE Alliance secure element
- Dynamic memory management
- APDU communication over I²C/SPI based on the GlobalPlatform[®] APDU Transport over I²C/SPI specification
- Firmware upgrade mechanism
- Support of multiple logical secure element for hypervisor support
- In certification CC EAL5+ according to Java[®] Card open protection profile
- Proprietary Java[®] Card API for key derivation function (KDF)
- Proprietary Java[®] Card API for elliptic curves operations

Applications

- **JC:** Open Java® Card able to host any third party and any Java® Card Applet
- **SB:** StrongBox Android™ Weaver, Android™ Keymint, and Secure storage
- **DK:** In vehicle *Car Connectivity Consortium* v3.1 Car Digital Key
- **Qi:** v1.3 for in vehicle Phone power charging with secure authentication.

Note: Each application is identified as a dedicated product; application switch is not possible

1 General information

The STSAFE-V500 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.

arm



2 Description

The STSAFE-V500 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 STSAFE-V500 is providing a full range of solutions according to different use cases detailed in this document such as:

- StrongBox (SB)
- In vehicle CCC digital key (DK)
- Qi charging (Qi)
- Open Java® Card platform (JC)

Each solution is identified as a standalone *turn key* solution (no dynamic switch possible between the different solutions).

It also proposes an open Java® Card pen platform capable of loading any third-party Java® Card applet.

Both a *turn key* solution and an *Open Java® Card platform solution* offer a common backbone to ease final user integration; this document describes the common set of features (the common backbone) and highlights also specific features relevant for each *turn key* solution.

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 STSAFE-V500 is integrated with Android™ applications *Keymint* and *Weaver*. It can also host STMicroelectronics applications for secure storage.

It supports multiple logical secure elements that allow multiple Android™ Linux® virtual machines executing on a hypervisor environment accessing Java® Card applications.

It provides state-of-the-art security for the provided functionality, resistant to recent EMVCo/JIL hardware-related attacks subgroup (JHAS) identified vulnerabilities; it ensures a high level of security and isolation between applications, and Common Criteria EAL5+ certification is ongoing (specific for SB).

3 Ordering information

Example:	STSAFV50	SB	T2	B	XXX
Platform name					
STSAFV50					
Application					
SB = Strongbox					
DK = CCC 3.1					
Qi = Qi 1.3					
QC = Qi 1.3 + ccc 3.1					
JC = Open Java® Card					
Package					
3W = WQFN32					
T2 = TSSOP20					
Hardware version					
B = ST33K1M5A					
Customer code					
XXX					

Revision history

Table 1. Document revision history

Date	Revision	Changes
27-Jul-2023	1	Initial release.



Contents

1	General information	3
2	Description	4
3	Ordering information	5
	Revision history	6

IMPORTANT NOTICE – READ CAREFULLY

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgment.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.

© 2023 STMicroelectronics – All rights reserved