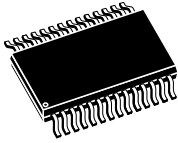# Automotive digital key application Java® Card system-on-chip based on a 32-bits M35P Arm® Cortex® with SPI interface

TSSOP20 6.5 × 4.4 × 1.2 mm

0.65 mm pitch

Product status link
STSAFE-VJ100-CCC

Features

- AEC-Q100 Grade 2 qualified
- Vehicle keys and certificates storage
- Friend keys and associated access profiles storage
- Validates and verifies device provided certificates signature
- Implements SPAKE2+ based cryptography
- End-to-End security by encrypting/decrypting data exchanged with the device
- Ephemeral keys generation
- Attestation's signature
- Owner pairing and Standard/Fast transactions
- BLE out of band session keys generation
- URSK and ranging keys derivation

Application

- In-Vehicle Secure Element for Secure Car Access based on CCC Digital Key Release 3 standard specification.

DB4611 - Rev 2 - May 2022
For further information contact your local STMicroelectronics sales office.

www.st.com

1 Description

The STSAFE-VJ100-CCC system-on-chip is a top-class embedded secure element (eSE) based on Java® Card platform.

This product is integrated with "Digital Key" and "UWB Services" applications in compliance with CCC Digital Key Release 3 specification and it can host STMicroelectronics applications for secure storage.

This In-Vehicle Secure Element provides state-of-the-art security for the CCC functionalities, based on the most advanced products from both STMicroelectronics and its partners to offer a competitive and flexible solution.

This product is based on an advanced Arm® Cortex®-M35P 32-bit microcontroller.

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

1.1 Embedded Java® Card applets

Java® Card-based applets have been developed to store credentials, sensitive information, and perform cryptographic operations required to implement CCC Digital Key Rel.3 uses cases like owner pairing, key sharing, key termination/deletion.

1.2 Java® Card

The STSAFE-VJ100-CCC system-on-chip supports Java® Card v3.0.5 classic edition with all the mandatory features. It is based on GlobalPlatform® (version 2.3.0), supporting SCP03 (Amendment D) and SCP11a/c protocols (Amendment F), and Executable Load File Upgrade (Amendment H)

The interface defined is SPI/GP "APDU over SPI/I2C" protocol and the system-on-chip solution includes Operating System and Applets upgrade mechanism.

1.3 Hardware and security features

The STSAFE-VJ100-CCC system on chip solution is based on hardware Secure Element ST33K-A, AEC-Q100 qualified (Grade 2).

Hardware features:

- Arm® Cortex®- M35P 32-bit RISC core cadenced at 63 MHz
- Operating temperature range: –40 °C to 105 °C
- Serial peripheral interface (SPI) - Master (up to 15 MHz) and Slave (up to 48 MHz)
- Class C (1.8 V), Class B (3 V) and 3.3 V supply voltage ranges
- ESD protection greater than 4 kV (HBM)
- TSSOP20 (6.5 × 4.4 × 1.2 mm) ECOPACK-compliant package

Hardware-based security features:

- Platform and Flash memory loader security certification target according to Common Criteria
- Hardware security-enhanced DES accelerator
- Hardware security-enhanced AES accelerator
- Optional hardware security enhanced SM4 accelerator
- NESCRYPT LLP coprocessor for public key cryptography algorithm
- 16- and 32-bit CRC calculation block (such as ISO 13239, IEEE 802.3)
- Active shield
- Highly efficient protection against faults
- True random number generator

Revision history

Table 1. Document revision history

Date	Version	Changes
24-Mar-2022	1	Initial release.
11-May-2022	2	Replaced MP35P by M35P in main document title. Replaced ST33-A by ST33K-A in Section 1.3 Hardware and security features.

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.