Secure System with Advanced Cryptographic Accelerators

NCJ38A Automotive-Qualified Secure Element

The NCJ38A secure element (SE) is a dedicated hardware and software security architecture implemented with high resistance against physical attacks. It is typically used to protect valuable assets making it ideal to securely store the Digital Keys needed to unlock and start a car with a smart device.

OVERVIEW

The NCJ38A secure element family is an automotive-qualified secure microcontroller with advanced cryptographic accelerators and physical and electrical attack resistance. The NCJ38A SE stores security applications and their confidential data.

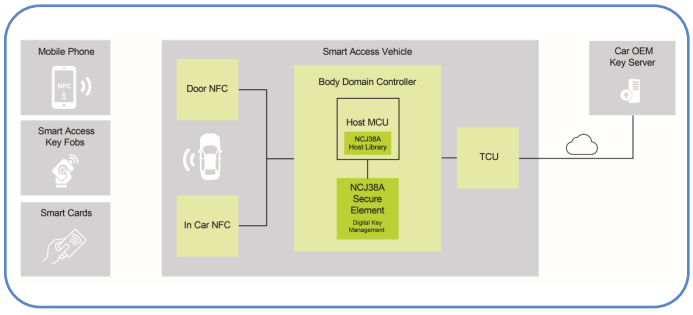
The software platform is offered to customers as open Java Card platform together with the NXP Automotive JCOP 4.4 operating system. Optionally customers can also order the generic authentication applet NCJ38xA supporting a broad spectrum of M2M authentication means, cryptographic key and data storage.

The device is based on a high-frequency clocked Arm® SC300 core, along with the newest generation of NXP's cryptographic hardware co-processors, and a flash module, bringing secured applications to a new level in performance and security.

TARGET APPLICATIONS

- CCC digital key management for smart car access
- Qi 1.3 Authentication
- Securing external and internal connections of a connected car

NCJ38A SECURE ELEMENT APPLICATION BLOCK DIAGRAM



KEY FEATURES

Core:

- NXP processor with Arm® SecurCore® SC300 technology

Memory:

- Up to 750 kB user memory

Interfaces:

- SPI slave interface
- I²C Bus slave interface

Cryptographic hardware coprocessors

- High-speed public-key co-processor (PKC) supporting major public key cryptography systems such as RSA, ECC and corresponding schemes
- High-speed triple-DES and AES coprocessors
- Random number generator in hardware AIS-31 compliant
- Two high-speed cyclical redundancy check engines

Quality

- AEC-Q100 Grade 2 qualified
- Hardware certification: Common Criteria EAL 5+

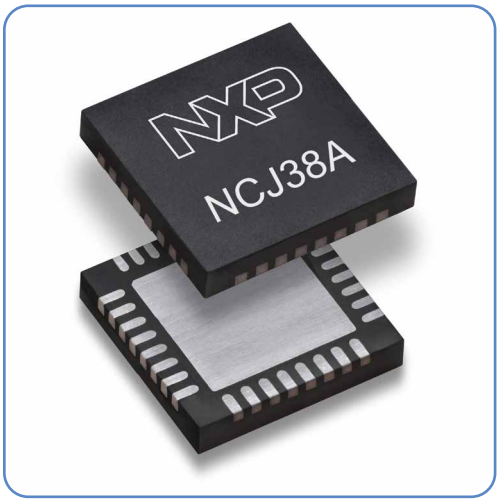
Package

- HVQFN32

ENABLEMENT

- Offered to customers as open Java® Card platform together with the NXP Automotive JCOP® 4.4 operating system
- Customers can also order the generic authentication applet NCJ38xA supporting a broad spectrum of M2M authentication means, cryptographic key and data storage
- Software stack: NXP JCOP4.4 secure Java Card operating platform
- Optional: generic authentication applet
- NCJ38A Host Library software package
- JCOP toolchain supporting customer applet development

NCJ38A SECURE ELEMENT CHIP



DIGITAL KEY SOLUTION

NXP offers a Digital Key Solution following the Car Connectivity Consortium's Standardization Release 2. This solution uses the NCJ38A SE and NXP's NCF3320 and NCF3340 NFC chipsets and enables the unlocking and starting a car with an NFC-enabled smartphone, key fob or an NFC smart card holding a digital key. This NFC-based solution makes it possible to trigger car access and driver authorization even if a phone's battery is drained, thus eliminating the need for a traditional physical key.

In the solution, NXP's secure elements are used inside the phones, key fobs and smart cards as well as on the car side using the NCJ38A automotive qualified secure element.

For more information, visit www.NXP.com/NCJ38A

Document Number: NCJ38ASECELFS REV 0