Product brief

SLS37 V2X HSM

Plug & play solution for secured V2X communication

Infineon's SLS37 V2X HSM safeguards V2X (Vehicle to Everything) communication based on a tamper-resistant security controller tailored to the security needs in V2X applications within telematics control units, protecting critical assets such as the integrity and moreover authenticity of messages, as well as the privacy of the sender. This plug & play security solution offers a host of benefits to automotive OEMs, tier-1 suppliers, and software providers for the development of connected vehicles.

Ease of use and faster time-to-market

- Robust automotive-qualified hardware with preprogrammed firmware, both security-certified, complemented by Infineon's V2X host library software package for seamless integration in various host application processors
- Trust along the full product lifecycle, starting with chip manufacturing thanks to a sophisticated personalization concept optimized for maximum security and ease of use – all designed to minimize customer logistics

Optimized security

- Security partitioning – focus on high security tasks such as key storage and generating signatures for outgoing messages while leaving less security relevant but performance hungry verification of incoming messages to the Host Processor
- Personalization concept leveraging a set of chip-unique and customer-individual certificates and keys optimized for maximum security and enabling vendor verification, pairing, and transport protection
- Future proof due to support for secured in-field updates with end-to-end protection

Scalability

- Support for security standards applicable in major automotive regions:
  - Common Criteria EAL4+ certified for deployment in Europe and other regions
  - Module in progress at US National Institute of Standards and Technology (NIST) targeting FIPS 140-2 level 3 certification for deployment in North America and other regions
- In regions with security requirements beyond the scope of embedded HSMs, the SLS37 can be added to existing platform designs
- As a discrete HSM, the SLS37 is agnostic to existing or upcoming modem standards

In a V2X application, the SLS37 serves as an HSM (hardware security module) for storing private keys and handling V2X security operations attributed to the most critical assets. This includes ECC private key management (generation, derivation, deletion), ECDSA signature generation, ECIES encryption and decryption, and storage of generic data.

The hardware architecture is based on a 32-bit Arm® SecurCore® SC300 CPU with an additional high-performance cryptographic engine and a latest-generation hardware coprocessor for asymmetric cryptography. For communication to the host processor, the SLS37 uses an SPI interface with data protection.

www.infineon.com/SLS37-V2X

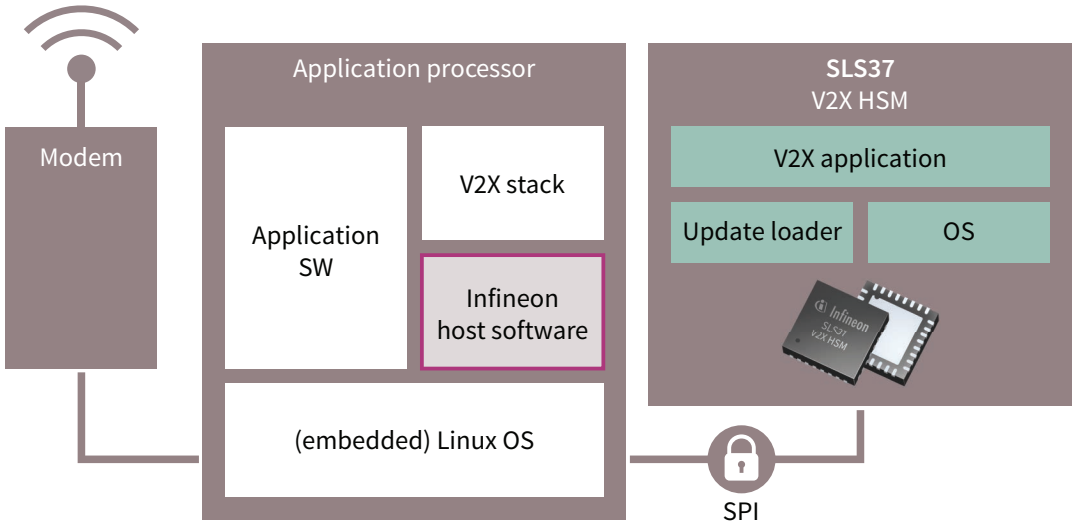
Key features

- Cryptographic functions according to IEEE 1609.2 and ETSI TS 103 097
- Support for 802.11p and cellular V2X-based communication
- Common Criteria-certified hardware platform at EAL6+ (high)
- Common Criteria-certified at EAL4+; compliance with CAR 2 CAR Communication Consortium Protection Profile V2X Hardware Security Module, version 1.4.1
- FIPS 140-2 level 3 certification (under review)
- Support for major vehicle credential management systems (SCMS, CCMS, ESPS)
- Supported by major V2X security stack providers
- Signature generation performance of 20 signatures/sec
- Secured storage of private keys, V2X PKI certificates, and customer-specific sensitive data
- User memory: 2000 key slots, 20 file slots; data retention for 17 years
- High-speed SPI interface (10 MHz)
- Single supply from 1.6 to 3.6 V
- 5x5 mm 32-pin VQFN package
- Qualified according to AEC-Q100, up to 105°C Ta
- Regional compliance supporting North America and EU standards for global deployment

Target applications

- Automotive V2X communication
- Roadside units or other infrastructure elements for V2X communication

V2X host system



How to get started

Reference design

› Qualcomm® Connected Car Application Reference Design (CCARD)

Evaluation hardware

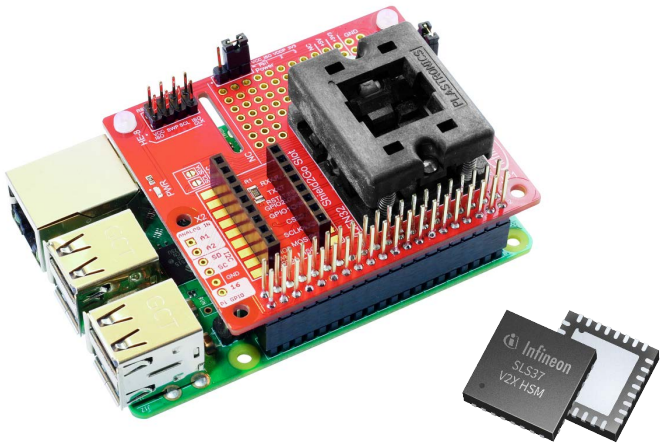
› VQFN32 SPI/I2C socket adapter for Raspberry Pi board with socket for SLx37-based samples

SLS37 V2X HSM

› Preprogrammed security controller in PG-VQFN-32 package

Development software

› The SLS37 V2X HSM is supported by Infineon host software (for Linux host environments)



Product and tool overview

Type	Scope	Sales Name	SP number	Where to find
HW tools	VQFN32 SPI/I2C socket adapter for Raspberry Pi	VQFN32 SOCKET A	SP005678818	Infineon Sample Request (ISaR)[1]
SLS37 V2X HSM (pre-programmed security controller)	Engineering samples (ES); Generic personalization; AEC-Q100-qualified; With certification intent	SLS37CSAUS (FIPS-certification in progress)	SP005593456	
		SLS37CSAEU (CC-certified)	SP005593617	
Host software	For Linux host environments	–	–	Infineon Toolbox[1]

1) Contact your Infineon sales representative for references and documentation

Published by
Infineon Technologies AG
81726 Munich, Germany

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office (www.infineon.com).

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question, please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.

Date: 2021-10