SLS37CSAEU V2X HSM

Datasheet

Plug and play solution for secured V2X communication

Devices

SLS37CSAEU

Infineon V2X security solutions address different global markets and are therefore tailored to meet the requirements introduced by regional standards and regulation.

This document covers the V2X solution with Common Criteria certification for the European Region (indicated by 'EU'). For other regions please refer to the respective separate document (e.g. V2X solution with FIPS-certification for the North-America market: SLS37CSAUS).

Key features

SLS37CSAEU V2X security solution

- Full HSM functionalities for 802.11p and C-V2X based communication
- Cryptographic functions according to IEEE 1609.2 and ETSI TS 103 097
- Supporting all major vehicle credential management systems, such as SCMS, CCMS, ESPS incl. support for butterfly key expansion
- Secured storage of private keys, V2X PKI certificates, and customer specific sensitive data
- Compliant with Car-2-Car Protection Profile for V2X HSM
- High performance cryptographic engine for ECDSA calculations
- NIST P-256, NIST P-384, brainpoolP256r1 and brainpoolP384r1 elliptic curves
- Signature generation performance for V2X messages: 20 signatures per second
- Secured, end-to-end protected in-field update mechanism with rollback-prevention enabling e.g. security updates of the firmware
- Flexible user rights management allowing for customer-individual configuration
- Compatible and pre-integrated into Aerolink V2X security solution and major V2X software stacks

Security certification

- Composite certification Common Criteria EAL4+ moderate according to Car-2-Car Protection Profile for V2X HSM

Please read the Important Notice and Warnings at the end of this document

Key features

Hardware

- Tamper resistant microcontroller providing highest proven assets protection
- High Performance Cryptographic Engine (Crypto@2304T) for asymmetric cryptography
- Shielding and sensors against physical and logical attacks, internal memory and bus encryption
- Memory
  - based on reliable, certifiable SOLID FLASH™ NVM technology and protected by encryption and additional error detection
  - User memory: 2000 private key slots for V2X and 20 file slots for other data
  - 17 years of data retention
- High-speed SPI interface up to 10 MHz
- Single voltage supply from 1.62 V to 3.6 V
- 5x5 mm 32 pin VQFN Package
- Qualified according to AEC-Q100 (Grade 2), up to 105°C Ta

Target applications

SLS37CSAEU is a turnkey security solution for protecting V2X communication designed to be integrated into the corresponding ECU (typically the Telematics Control Unit TCU) in a vehicle. Other use cases of this solution may be the V2X-infrastructure outside the vehicle such as roadside units (RSU).

Figure 1 shows a simplified, generic system diagram of a V2X module and the role of SLS37CSAEU within.

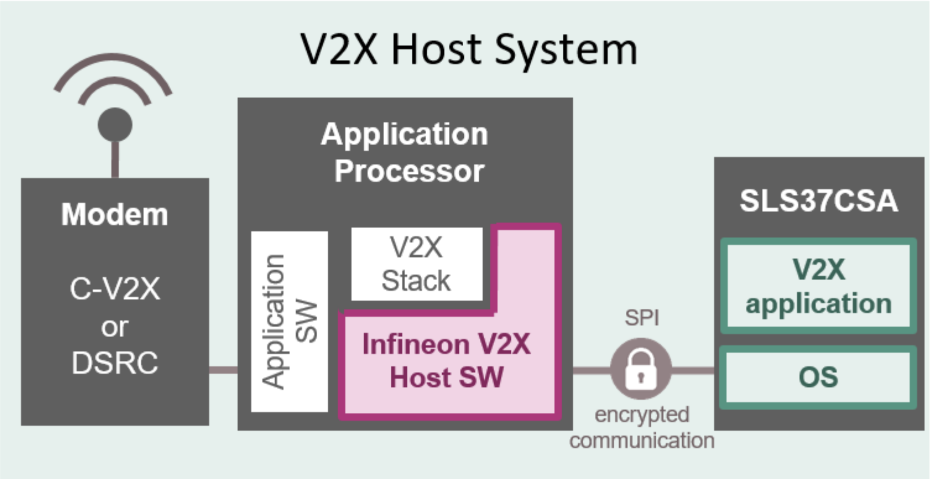


Figure 1 **Simplified automotive V2X setup**

About this document

Scope and purpose

This datasheet provides an overview of the hardware and software features and functionalities of the SLS37CSAEU, as well as information about the package characteristics.

Note: *Throughout this document the SLS37CSAEU may simply be referred to as the V2X HSM.*

Note: *The API of the V2X HSM contains references to FIPS, since the same API is used in the product for the US region (SLS37CSAUS).*

Intended audience

This datasheet is primarily intended for system developers. Target customers are automotive Original Equipment Manufacturers (OEMs), their Tier 1 suppliers as well as software partners.

Table of contents

Table of contents

List of tables

List of figures

1 General description

1.1 Overview

The Infineon SLS37CSAEU V2X HSM is a turnkey security solution safeguarding secured V2X communication based on a highly secured tamper resistant microcontroller providing highest proven assets protection.

The hardware architecture is based on 32-bit ARM® SecurCore® SC300 CPU with an additional high performance asymmetric cryptographic engine and the latest generation of hardware co-processor for symmetric cryptography. The V2X HSM is interfacing to a host processor via SPI. The SPI communication is thereby protected via encryption and MAC leveraging chip individual keys, which are unique for each link between a given V2X HSM and the respective host processor. With its AEC-Q100 (Grade 2) qualification, the hardware used in SLS37CSAEU is optimized for Automotive Security, meeting both the requirements of the harsh environment in the automotive industry as well as the highest security levels for the implementation of security and cryptography in cars.

SLS37CSAEU comes pre-programmed with Infineon V2X firmware and is ready-to-use. A secured and end-to-end protected in-field update mechanism with rollback-prevention enables security updates of the firmware in the field. Hardware and firmware are security certified by an independent third party and ready-to-use. Updated firmware is security certified as well before being rolled out in the field maintaining the security certification status of the overall product over its lifetime.

Major blocks of the V2X firmware in SLS37CSAEU are the embedded operating system and the V2X application. In combination, they are providing high performance functionality including cryptographic operations (e.g. ECDSA signature generation), certificate and key storage management. Both, the V2X application and the underlying operating system, are based on the latest V2X standards and market requirements. This software is developed according to secure coding standards and security certifications. Infineon aims to provide all needed features within this deployment.

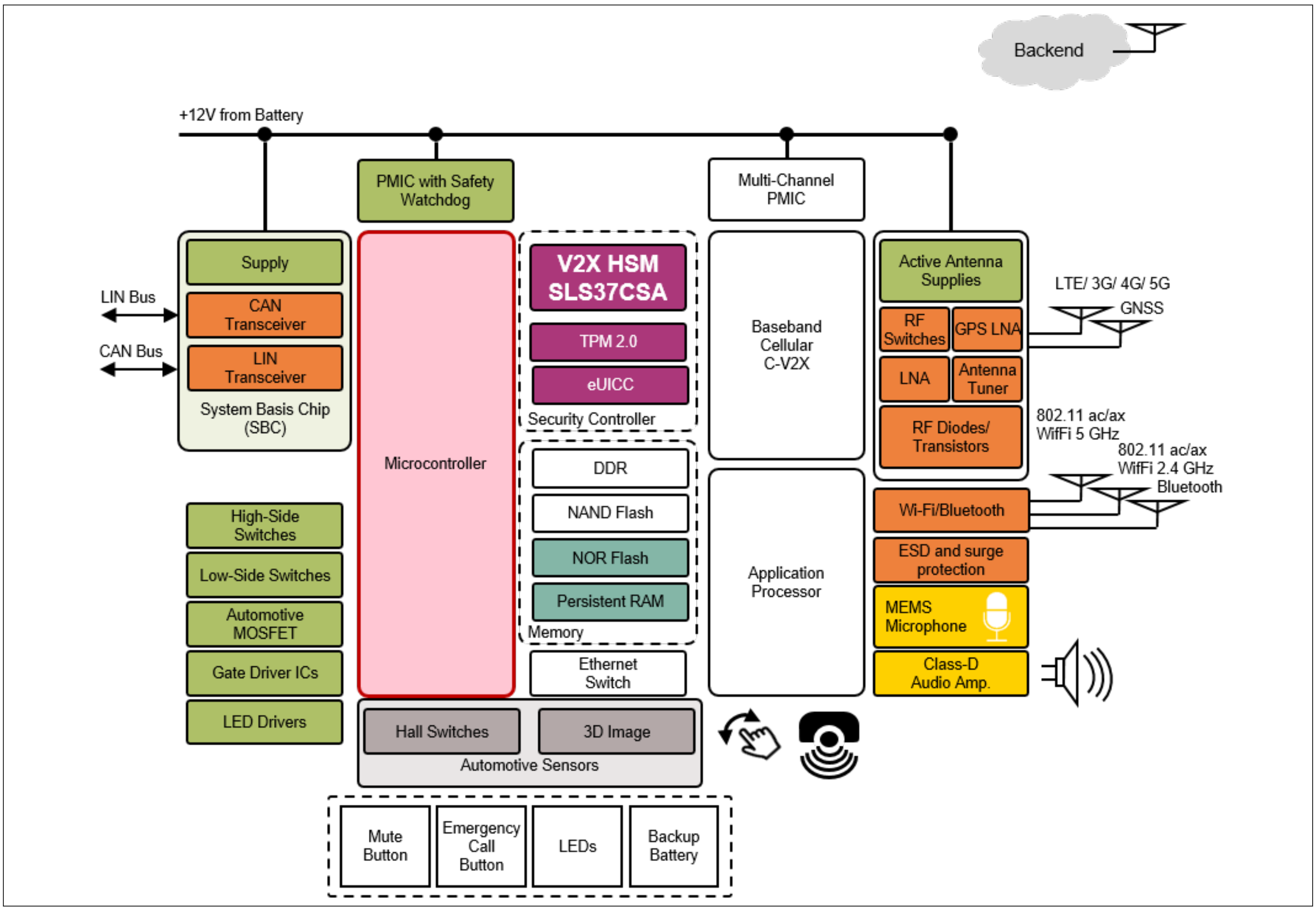


Figure 2 **Exemplary Telematics Control Unit Architecture**

For ease of use and faster time-to-market the SLS37CSAEU is complemented with a V2X Host Software Package. This software package encompasses demo code to be included into the software running on the host- or application processor the SLS37CSAEU is connected to intending to facilitate an easy integration.

Within this setup SLS37CSAEU serves as HSM, providing the host- or application processor with secured storage of private keys and performing the respective cryptographic operations attributed to the signing of V2X messages.

This includes but is not limited to:

- ECC private key management (generation, import and deletion)
- Butterfly key expansion
- ECDSA signature generation
- ECIES encryption and decryption
- Storage of generic data
- Infineon PKI provides customer-individual keys enabling a secured pairing between SLS37CSAEU and the respective host processor as well as secured in-field updates.

The verification of V2X messages is expected to be done on the host- or application processor. An exemplary TCU architecture is depicted in ***Figure 2***.

1.2 Main features and benefits

- Turnkey security solution (hardware + firmware + host software) for faster time-to-market
- Optimized for automotive security, i.e., harsh automotive environments as well as highest security levels
- Tamper resistant hardware platform enabling secured key storage and trusted execution of the respective cryptographic operations
- Security-certified solution, ready-to-use and tailored for the European region (Common Criteria)
- High performance solution meeting the market requirements to generate 20 signatures/sec
- Flexibility thanks to a wide range of security functions integrated (e.g. dedicated key management)
- Secured update in the field while maintaining the security certification status over the product lifetime
- Protected SPI communication leveraging chip individual keys
- The listed features support demanding customers to cope with increasing security requirements of today’s and future complex automotive systems. The Infineon V2X HSM as plug-and-play security solution helps tremendously to increase systems security level with very limited additional effort in software development and system integration and thus helps to reduce the total cost of ownership of the complete system.

1.2.1 Chip side hardware features

- 32-bit ARM® SecurCore® SC300 @100 MHz
- Secured storage inside the security controller leveraging SOLID FLASH™ which combines flexible flash memory technology with a sophisticated security mechanism and highest reliability
- Ultra Low Power design CMOS technology
- SPI Interface up to 10 MHz
- Symmetric co-processor (AES)
- Asymmetric co-processors: High Performance Cryptographic Engine (Crypto@2304T) for ECC calculations
- Hybrid Random Number Generation (True and Pseudo Random Number Generator) according to latest BSI AIS20/31 and NIST SP800- A and B statistical tests
- Supply voltage range: 1.62 V to 3.63 V
- Extended temperature range: -40°C to +105°C
- All memories are protected by hardware Error Correction Code and Error Detection Code
- Security Sensors (Frequency, Light, Temperature, Glitch, Voltage)
- Unique chip tracking number stored into each chip
- High Endurance
- Data retention of 17 years
- Qualification according to AEC-Q100 (Grade 2)
- PPAP documentation
- ESD protection 2 kV (HBM)
- Package: VQFN32-13 SMD package (5 mm x 5 mm), CAD files available on request

1.2.2 Chip side software features

The V2X application of SLS37CSAEU exposes its features to the host by providing an APDU Command Interface (API), which is compatible to the major V2X software stacks.

This API includes a rich set of features including reporting, management, storage and cryptographic functionalities attributed to signature generation for V2X messages including but not limited to the following:

- Cryptographic functionalities for signatures and certificate management according to IEEE 1609.2-2016 and ETSI TS 103 097
- ECC key pair generation on the chip
- ECDSA sign
- NIST P-256/P-384, brainpoolP256r1/P384r1 elliptic curves
- ECIES (Elliptic Curve Integrated Encryption Scheme) according to IEEE1609.2
- Support for butterfly key expansion *[7]*
- Secured storage for up to 2000 private keys (ECC 256/384bit)
- Secured storage for up to 20 general purpose files hosting customer specific data – each 2048 bytes with configurable access conditions per user (write/read/change)
- RNG according to NIST SP 800-90A
- Secure Channel Protocol 03 (SCP03) based on Global Platform Card Specification v2.3 – Amendment D Version 1.1.2
- Vendor-verification feature to verify genuineness of the chip
- Authentication scheme and user rights management including:
  - Different users with configurable access rights
  - Each user with key enabling dedicated encrypted and authenticated messaging channel (based on AES-256-CBC and AES-256-CMAC)
- Life cycle management: supporting different life cycle states with different access conditions for each state and transition
- Secured and protected in-field update mechanism with rollback-prevention
  - Minimal downtime of V2X HSM during firmware update:
    - Fast image signature verification
    - Fast verified image installation (replaces current image).
  - Data (private keys and files) stored in NVM is not impacted by the firmware update
- SPI Device Drivers and Protocols
  - SPI protocol implementing *GlobalPlatform APDU Transport over SPI/I2C Version 1.0* standard
  - APDU compatible with ISO/IEC 7816-4: 2013

1.2.3 Infineon V2X Host Software Package

An overview of the components of the host software package is depicted in *Figure 3*.

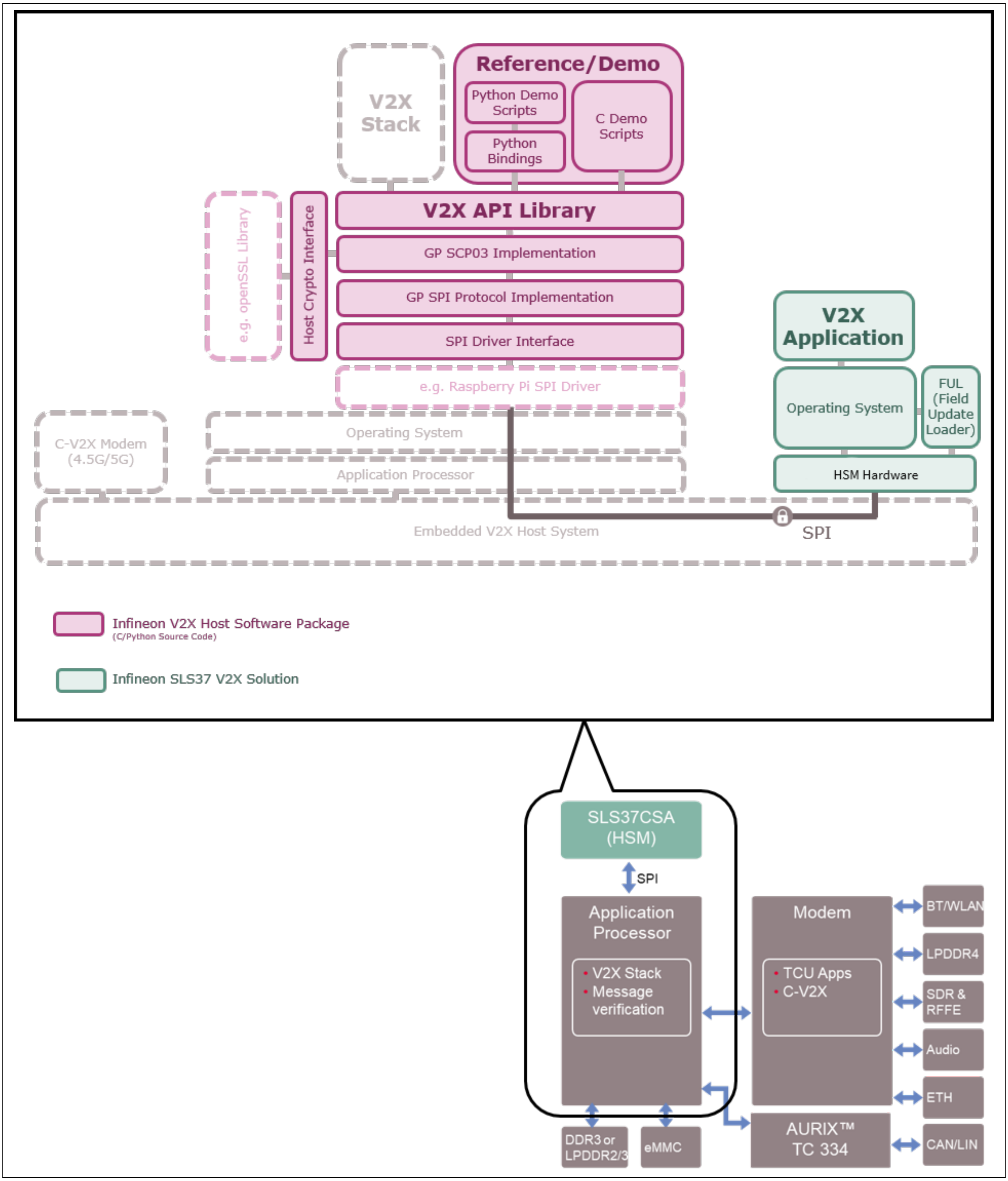


Figure 3 **V2X solution Software Stack**

The left block in *Figure 3* represents the code running on the host processor (V2X Host Software Package) and the right hand side reflects the software or firmware residing on the chip side (SLS37CSAEU).

The V2X Host Software Package consists of several demo modules, that show how to integrate and use the V2X HSM for V2X purposes on a host system. The V2X Host Software Package is delivered as demo source code for Raspberry Pi. Due to the modular approach, it is easy to use, to adapt or to integrate into other software.

Features

- Complete V2X API Library with access to all V2X HSM APDU commands delivered as C source code including SPI protocol implementation and GlobalPlatform Secure Channel Protocol 03 (SCP03)
- Library can be compiled as both static or dynamic library
- Python bindings for easy usage within the Python interpreter (via *import* function)
- Example scripts for Initialization, Message Signing, In-Field Update, etc. delivered as Python scripts and C source code
- Wrapper functions for Host-side cryptographic operations (OpenSSL) and Host SPI driver (Raspberry Pi SPI Driver) for easy porting onto other platforms

1.3 Applications and use cases

The Infineon V2X HSM is a security companion chip providing a turnkey security solution to safeguard V2X communication.

V2X Application

Based on V2X (*vehicle-to-everything*) technology various services are envisioned to be deployed, for example, traffic jam information can be transmitted on short notice between vehicles via V2X communication to other vehicles in order to avoid crashes and congestions. Incorporating environmental data can help to improve driving strategies and for example reduce fuel consumption. V2X communication encompasses thereby communication between cars and the surrounding infrastructure (i.e., V2V, V2I, V2N, V2P).

Thus, V2X technology is expected to help preventing a large amount of traffic fatalities thereby significantly contributing to enhance road safety. Depending on region and the sophistication of the corresponding services it is distinguished between different use cases where *day 1* use cases are the initial services to be deployed and encompass road safety use cases. That includes the exchange of so-called *base safety messages* (BSMs) between vehicles and the infrastructure.

V2X Communication Security

For the V2X ecosystem to provide its safety benefit, it is fundamental that exchanged messages be trusted so that vehicles can act upon the received information. Furthermore, for V2V messages, the privacy of the sender must be protected – the messages must not enable tracking of particular drivers, citizens or vehicles. These principles are embodied in all applicable V2X standards. Specifically, exchanged messages must be protected against undetected modification and a receiving party (i.e., any end entity, such as vehicle, road side unit, vulnerable road user) must be able to determine that the message came from an authorized origin.

Hence the integrity and authenticity of these messages are of utmost importance. For efficient authenticity and integrity enforcement corresponding standards mandate the use of ECC-based cryptography for V2X (i.e., ECDSA based message signing and verification) along with corresponding backend infrastructures - commonly referred to as *security credential management systems - SCMS* - maintaining security and privacy of the exchanged data and involved stakeholders of the V2X ecosystem.

SLS37CSAUS Use Cases

On an application level, the scope of SLS37CSAEU is *day 1* use cases.

SLS37CSAEU is designed for integration into the corresponding OBU within a vehicle but may also be deployed in other V2X end-entity devices, such as RSUs. Typically, it will be integrated into ECUs, which incorporate also other exposed interfaces for external communication (e.g., TCU) – depending where in a particular vehicle-platform and –architecture the V2X functions reside.

SLS37CSAEU is interfacing via SPI to a host- or application processor running the V2X communication stack and being in charge of the message verification.

The main functional use cases are secured key-generation and -storage as well as ECDSA signature generation.

Functional use cases on V2X security credential management system (SCMS) level:

SLS37CSAEU supports the V2X related use cases for signature generation, key management and the key provisioning process according to the SCMS architecture and IEEE 1609.2.

These use cases use the US SCMS and the respective terminology as example. The European CCMS and corresponding message types (e.g., CAM) are equally supported.

- Vehicle enrollment
  - SLS37CSAUS creates enrollment certificate key pair
  - SLS37CSAUS signs enrollment certificate CSR with registration key
  - Host gets back enrollment certificate
- Authenticate vehicle
  - SLS37CSAUS creates caterpillar keys (public key to host)
  - SLS37CSAUS signs certificate signing request (CSR) with enrollment certificate key (send to Certificate Authority (CA))
  - CA sends back pseudo/butterfly certs to host
  - SLS37CSAEU uses corresponding authorization certificate private key for required pseudo cert
- Send BSM messages
  - SLS37CSAUS generate signature using the authorization certificate private key
  - Host generates and sends message utilizing the signature

Functional V2X use cases on chip level:

- ECC key generation
- ECC key import
- Secured cryptographic key storage (for private keys to be stored within the V2X HSM only)
- Butterfly key expansion
- Message encryption and decryption: asymmetrically encrypt and decrypt symmetric session key using ECIES with public receiver key and private butterfly decryption key
- ECDSA signature creation

2 Block diagram

The following figure shows the hardware block diagram of the V2X HSM

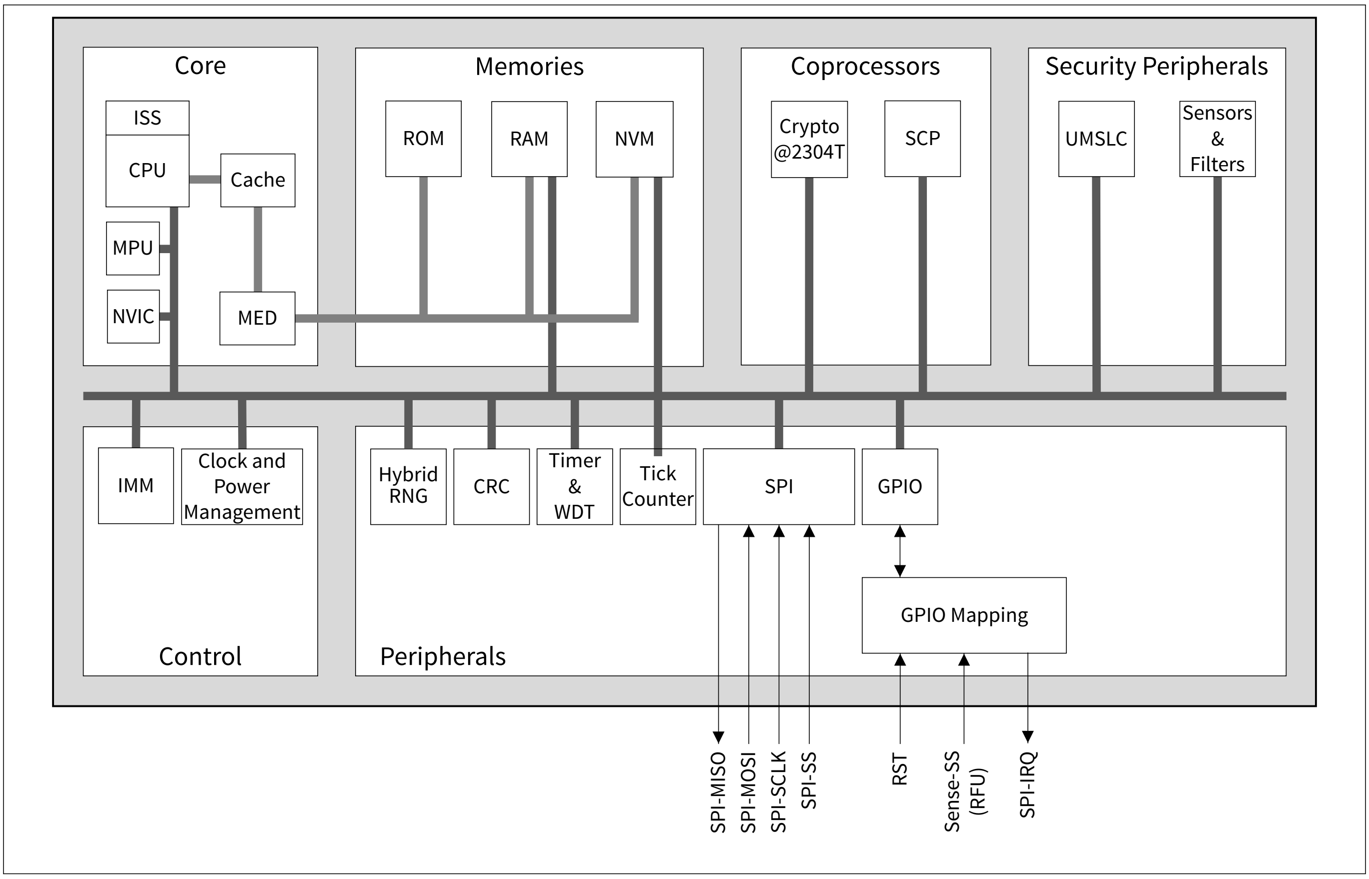


Figure 4 Block diagram of the V2X HSM

3 Pin description

The pad usage of the V2X HSM in a 32 pin VQFN package is illustrated by the next figure and table. A detailed description of the package can be found in ***Chapter 6***.

3.1 Abbreviations in pin description

The abbreviations listed here are used in the package description to classify each pin.

Table 1 Abbreviations for pin type

Abbreviation	Description
DNC	Do Not Connect. Must be left floating. Please do not connect externally.
I	Input. Digital levels
O	Output. Digital levels
I/O	Input/Output bi-directional. Digital levels
PWR	Power
GND	Ground
NCI	Not Connected Internally. May be connected externally

Table 2 Abbreviations for buffer type

Abbreviation	Description
GPIO_I	GPIO input pad
GPIO_O	GPIO output pad
SPI_I	SPI input pad
SPI_O	SPI output pad

3.2 Pad-to-signal reference

For the integration of the V2X solution onto a dedicated PCB board, the power supply, ground, the SPI interface pins and the additional pins have to be connected as shown in the following layout and tables:

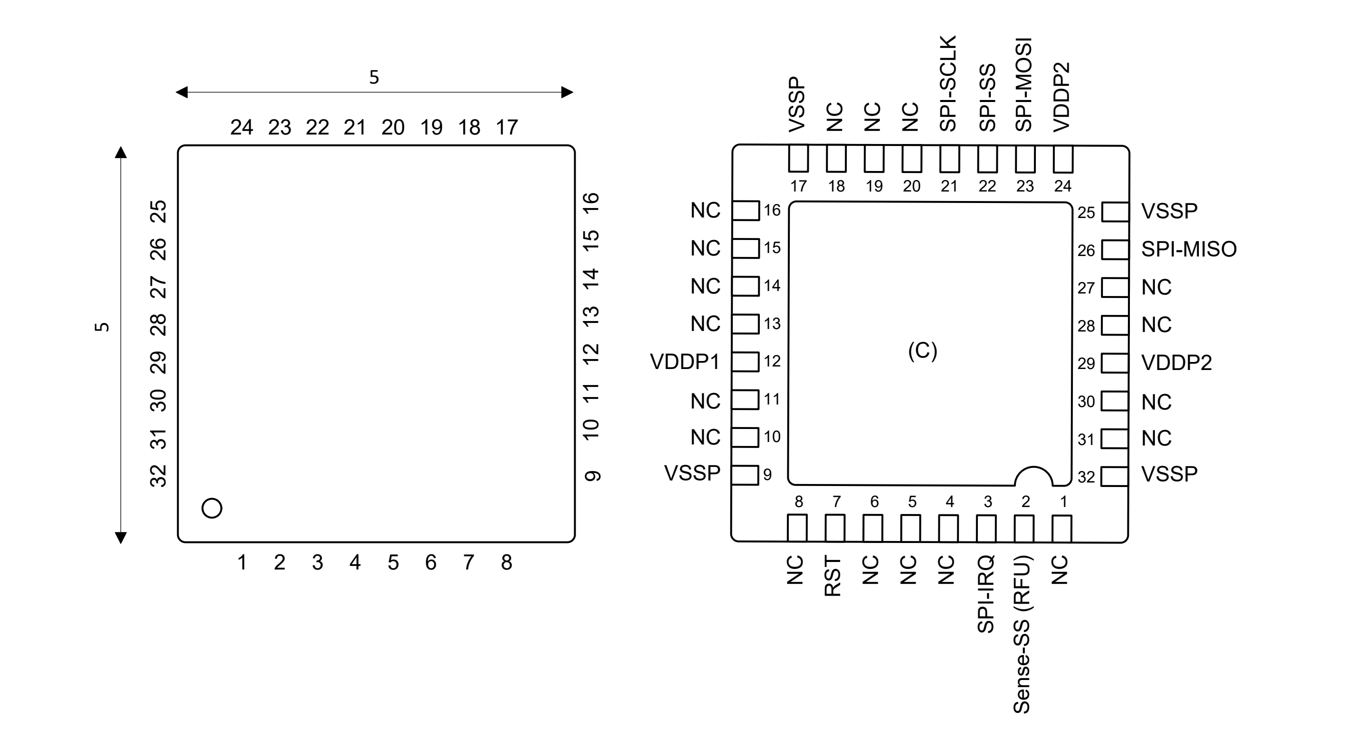


Figure 5 **PG: VQFN-32-13 package layout**

Table 3 **I/O signals**

Pad	Name	Pin type	Buffer type	Signal function/remark
2	Sense-SS	I	*GPIO_I*	**Shortcut to Pin 22 (SPI-SS sensing). Reserved for future use**
3	SPI-IRQ	O	*GPIO_O*	**Interrupt Request**, active high, host interrupt triggered on rising edge (SPI response ready)
7	RST	I	*GPIO_I*	**Reset**, active low, evaluated by software after start-up, internal pull-up
21	SPI-SCLK	I	*SPI_I*	**SPI Clock** The SPI clock signal. Only SPI mode 0 is supported by the device
22	SPI-SS	I	*SPI_I*	**Slave Select**, active low The SPI chip slave select signal. No internal pull-up
23	SPI-MOSI	I	*SPI_I*	**SPI Master Out Slave In (SPI Data)** SPI data which is received from the master.

Table 3 I/O signals (continued)

Pad	Name	Pin type	Buffer type	Signal function/remark
26	SPI-MISO	O	*SPI_O*	**SPI Master In Slave Out (SPI Data)** SPI data which is sent to the SPI bus master.

Table 4 Power supply

Pad	Name	Pin type	Buffer type	Signal function/remark
9, 17, 25, 32	VSSP	GND	-	**Power supply:** Common ground reference (VSS)
12	VDDP1	PWR	-	**Power supply:** Chip power
24, 29	VDDP2	PWR	-	**Power supply:** Chip power

Table 5 Not connected

Pad	Name	Pin type	Buffer type	Signal function/remark
6, 19, 20, 27, 28	NC	DNC	-	**Do Not Connect** All pins must not be connected externally (must be left floating).
1, 4, 5, 8, 10, 11, 13, 14, 15, 16, 18, 30, 31	NC	NCI	-	**Not Connected Internally** All pins are not connected internally (can be connected externally).

*Note: The exposed die pad referenced as (C) in **Figure 5** must be connected to the common ground reference (GND) for heat distribution.*

3.3 Typical schematic

Figure 6 shows the typical schematic for the V2X HSM. The power supply pins should be bypassed to GND with a capacitor located close to the device.

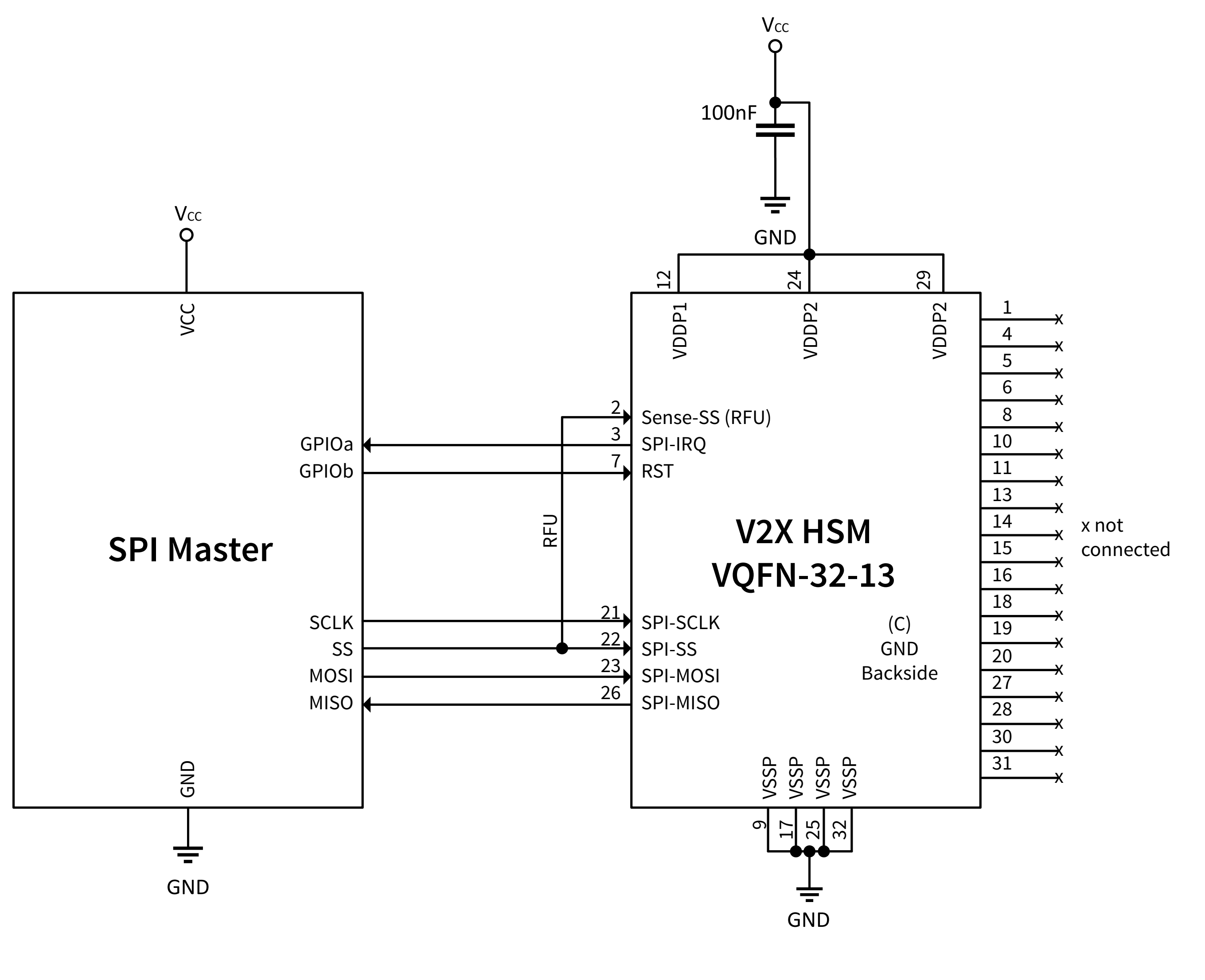


Figure 6 **Typical schematic**

3.4 CAD files

CAD files for design-in of the V2X HSM are available on request.

4 V2X HSM firmware

The V2X HSM firmware is described in detail in the corresponding chapter of the V2X databook.

5 Electrical characteristics

This section summarizes certain electrical characteristics of the controller. It provides operational characteristics as well as electrical DC and AC characteristics and particular interface characteristics.

Note: *T_A as given for the operating temperature range of the controller unless otherwise stated.*

Note: *All currents flowing into the controller are considered positive.*

Note: *V_{CC} is connected to VDDP1 and VDDP2. Throughout this document VDDP1 and VDDP2 will simply be referred to as V_{CC}.*

5.1 Absolute maximum ratings

Table 6 Absolute maximum ratings

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Operating temperature, ambient	T_A	−40	–	+105	°C	T_J must be kept
Junction temperature	T_J	–	–	+110	°C	–
Supply voltage	V_{CC}	−0.3	–	7.0	V	–
Input voltage, signal group *GPIO*	V_{IN_GPIO}	−0.3	–	7.0	V	
Input voltage, signal group *SPI*	V_{IN_SPI}	−0.5	–	7.0	V	–
ESD robustness HBM	$V_{ESD,HBM}$	–	–	2000	V	According to EIA/JESD22-A114-B
ESD robustness CDM	$V_{ESD,CDM}$	–	–	750	V	According to ESD Association Standard STM5.3.1 - 1999
Latchup immunity	I_{latch}	–	–	150	mA	According to EIA/JESD78 105°C, class II

Note: *Stresses exceeding the values listed under 'Absolute maximum ratings' may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or at any other conditions whose values exceed those indicated in the operational sections of this document is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability, including NVM data retention and write/erase endurance.*

5.2 Operational characteristics

This section specifies the AC and DC characteristics of the controller, along with details relating to the specific interfaces provided by the controller.

5.2.1 DC electrical characteristics

Table 7 **DC characteristics**

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Supply voltage	V_{CC}	2.97	3.3	3.63	V	Overall functional range
		1.62	1.8	1.98		
Supply current	I_{VCC_Active}	–	16.0	–	mA	During startup sporadic spikes up to 32 mA might occur
Supply current sleep	I_{VCCS_Sleep}	–	120	200	µA	RST inactive (= V_{CC}), SPI-IRQ inactive (= GND), SPI-SS inactive (= V_{CC}), SPI-MOSI, SPI-MISO and SPI-SCLK don't care

Note: *Current consumption does not include any currents flowing through resistive loads on output pins!*

5.2.2 AC electrical characteristics

Table 8 **AC characteristics**

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
V_{CC} rampup time	t_{VCCR}	1	–	–	µs	0 to 100% of V_{CC} target voltage ramp[1)]

1) Please refer to ***Power-up considerations***

5.2.2.1 Power-up considerations

The rampup times given in ***AC electrical characteristics*** apply under the assumption of a linear rise in voltage from 0% to 100% of the target voltage level. However, owing to possible current spike effects, it is recommended to follow the voltage characteristics shown in the figure below.

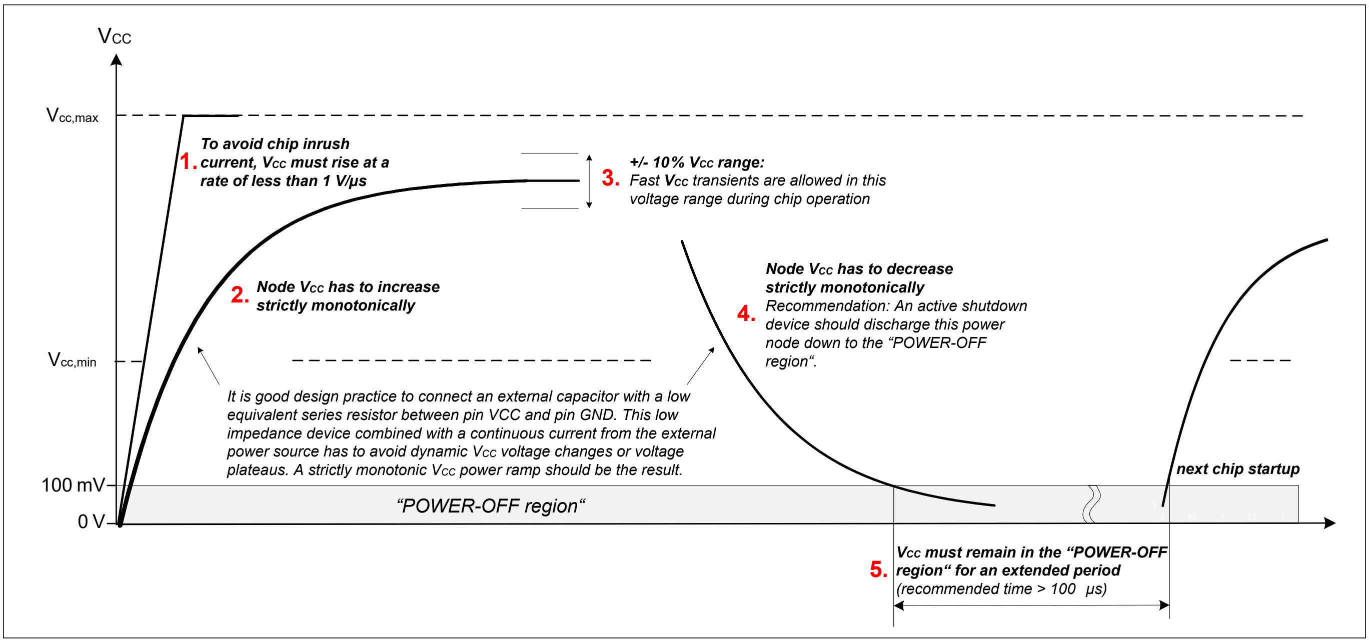

Vcc
Vcc,max
Vcc,min
100 mV
0 V
1. To avoid chip inrush current, Vcc must rise at a rate of less than 1 V/µs
2. Node Vcc has to increase strictly monotonically
3. +/- 10% Vcc range: Fast Vcc transients are allowed in this voltage range during chip operation
4. Node Vcc has to decrease strictly monotonically Recommendation: An active shutdown device should discharge this power node down to the "POWER-OFF region".
It is good design practice to connect an external capacitor with a low equivalent series resistor between pin VCC and pin GND. This low impedance device combined with a continuous current from the external power source has to avoid dynamic Vcc voltage changes or voltage plateaus. A strictly monotonic Vcc power ramp should be the result.
"POWER-OFF region"
next chip startup
5. Vcc must remain in the "POWER-OFF region" for an extended period (recommended time > 100 µs)

Figure 7 **Recommended power-up behavior**

5.3 Particular interface characteristics

This chapter provides electrical characteristics with respect to operation of particular interfaces of the controller.

Note: Unless otherwise stated, all values in this section are measured at the pins of the used package, i.e., the resistance, capacitance and inductance, for example, of the package and the bond wires are already included in these values!

5.3.1 GPIO interface characteristics

The electrical characteristics of the GPIOs including restrictions with respect to the maximum sink/source currents for all GPIOs of the controller are given below.

Table 9 GPIO operation supply and input voltages

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
GPIO pad input voltage	V_{IN_GPIO}	−0.3	–	V_{CC} + 0.3	V	V_{CC}[1] is in the operational supply range.

[1] *Table 7*

Table 10 GPIO DC electrical characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Input current, pull-up (weak) enabled	I_{PUW}	−3	–	−20	µA	$0 V \leq V_{IN\_GPIO} \leq V_{CC} - 0.5 V$
Input current, pull-down (weak) enabled	I_{PDW}	3	–	20	µA	$0.5 V \leq V_{IN\_GPIO} \leq V_{CC}$
Pull-up (strong) resistance	R_{PUS}	2.5	–	5.5	kΩ	$0 V \leq V_{IN\_GPIO} \leq V_{CC} - 0.5 V$
Input leakage current	I_{LI}	−2	–	2	µA	Pull-up/down off, output stage off; $0 V \leq V_{IN\_GPIO} \leq V_{CC}$
Input low voltage	V_{IL}	−0.3	–	0.3 * V_{CC}	V	
Input high voltage	V_{IH}	0.7 * V_{CC}	–	V_{CC} + 0.3	V	
Output low voltage	V_{OL}	–	–	0.3	V	I_{OL} = 1 mA
		–	–	0.4	V	I_{OL} = 4 mA, $V_{CC} \geq 2.7 V$
Output high voltage	V_{OH}	V_{CC} − 0.3	–	–	V	I_{OH} = −1 mA
		V_{CC} − 0.4	–	–	V	I_{OH} = −4 mA, $V_{CC} \geq 2.7 V$
Input capacitance	C_{IN}	–	–	10	pF	

Table 11 GPIO AC electrical characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Output signal rise time	t_r	–	3.5	15.0	ns	10% V_{CC} to 90% V_{CC}; C_{LOAD} = 15 pF, pull-up/down off, no DC load.
Output signal fall time	t_f	–	3.5	15.0	ns	90% V_{CC} to 10% V_{CC}; C_{LOAD} = 15 pF, pull-up/down off, no DC load; Slew Rate Control OFF (default operation mode).
Output signal fall time	t_f	30.0	50.0	–	ns	70% V_{CC} to 30% V_{CC}; C_{LOAD} = 50 pF, pull-up/down off, no DC load; slower slew rate.
Output signal fall time	t_f	15.0	25.0	–	ns	70% V_{CC} to 30% V_{CC}; C_{LOAD} = 50 pF, pull-up/down off, no DC load; faster slew rate.
GPIO input path low-pass filter	f_{CUTOFF}	20	–	40	MHz	50/50 duty cycle.
GPIO input path low-pass filter	t_{CUTOFF}[1]	12.5	–	25	ns	High or low pulse width.

[1] Spikes shorter than min. are filtered, spikes longer than max. are not filtered.

5.3.2 SPI interface characteristics

The V2X HSM operates as SPI Slave. The clock signal is received from an external master and synchronizes the data transfer. Transmission and reception speeds are not depending on the internal system clock.

The V2X HSM is configured for SPI mode 0 where polarity and phase is set to 0.

The assertion of the slave select signal starts the transfer. The rising clock edge is used to latch the incoming data bit while the falling clock edge shifts the next data bit onto the serial bus.

The following section describes the electrical characteristics of the SPI slave mode.

Table 12 Serial transfer mode

Polarity	Phase	SPI Mode	Description
0	0	0	Signal transmission through MISO and MOSI pads is activated on assertion of slave select signal (green arrow in ***Figure 8***). Data is latched by the receiver on the rising clock edge and is shifted by the transmitter on the falling clock edge. The idle state of the clock is low.

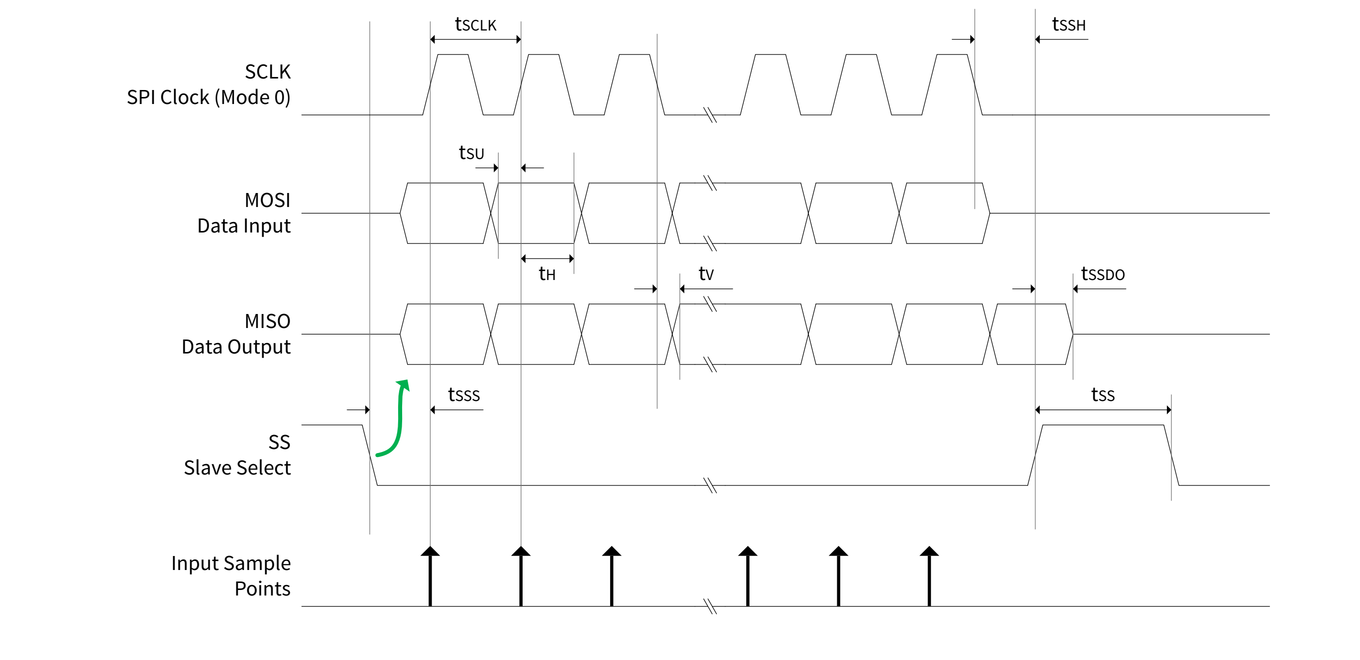


Figure 8 SPI Mode 0

*Note: A detailed timing diagram is shown in **Figure 9** and the respective values are given in **Table 15**.*

Table 13 DC characteristics for 3.3 V supply voltage range

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Pad supply voltage	V_{CC}	2.70	–	3.63	V	
Input high voltage	V_{IH}	0.7 * V_{CC}	–	V_{CC} + 0.5	V	
Input low voltage	V_{IL}	−0.5	–	0.3 * V_{CC}	V	
Output high voltage	V_{OH}	0.9 * V_{CC}	–	–	V	I_{OH} = −100 µA
Output low voltage	V_{OL}	–	–	0.1 * V_{CC}	V	I_{OL} = 1.5 mA

Table 13 **DC characteristics for 3.3 V supply voltage range (continued)**

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Pad leakage SPI input pads	I_{SIL}	−4	–	4	μA	0 V < V_{PAD} < V_{CC}
		−1.5	–	–	mA	−0.5 V < V_{PAD} < V_{CC} + 0.5 V
Pad leakage SPI output pads	I_{SOL}	−4	–	4	μA	0 V < V_{PAD} < V_{CC}
		−3	–	–	mA	−0.5 V < V_{PAD} < V_{CC} + 0.5 V

Table 14 **DC characteristics for 1.8 V supply voltage range**

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Pad supply voltage	V_{CC}	1.62	–	1.98	V	
Input high voltage	V_{IH}	0.7 * V_{CC}	–	V_{CC} + 0.3	V	
Input low voltage	V_{IL}	−0.3	–	0.3 * V_{CC}	V	
Output high voltage	V_{OH}	0.9 * V_{CC}	–	–	V	I_{OH} = −100 μA
Output low voltage	V_{OL}	–	–	0.1 * V_{CC}	V	I_{OL} = 1.5 mA
Pad leakage SPI input pads	I_{SIL}	−4	–	4	μA	0 V < V_{PAD} < V_{CC}
		−1	–	–	mA	−0.3 V < V_{PAD} < V_{CC} + 0.3 V
Pad leakage SPI output pads	I_{SOL}	−4	–	4	μA	0 V < V_{PAD} < V_{CC}
		−1	–	–	mA	−0.3 V < V_{PAD} < V_{CC} + 0.3 V

Table 15 **AC characteristics for 1.8 V and 3.3 V supply voltage range (Mode 0)**

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
SCLK frequency	f_{SCLK}	–	–	10	MHz	For 3.3 V supply voltage range
		–	–	10	MHz	For 1.8 V supply voltage range
SCLK clock period	t_{SCLK_range}	$1/f_{SCLK}$ − 5%	–	$1/f_{SCLK}$ + 5%	µs	Measured at input pad voltage of 0.5 * V_{CC}
SCLK nominal clock period	t_{SCLK}	–	$1/f_{SCLK}$	–	µs	Measured at input pad voltage of 0.5 * V_{CC}
SCLK low time	t_{SCLKL}	0.45 * t_{SCLK}	–	–	µs	Measured at input pad voltage of 0.5 * V_{CC}
SCLK high time	t_{SCLKH}	0.45 * t_{SCLK}	–	–	µs	Measured at input pad voltage of 0.5 * V_{CC}
SCLK input slew-rate	t_{Slew}	1	–	4	V/ns	SCLK input voltage slew-rate measured between 0.2 * V_{CC} and 0.6 * V_{CC}
SS inactive time	t_{SS}	30	–	–	ns	For 3.3 V supply voltage range

Table 15 AC characteristics for 1.8 V and 3.3 V supply voltage range (Mode 0) (continued)

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
		60	–	–	ns	For 1.8 V supply voltage range
SS setup time	t_{SSS}	30	–	–	ns	For 3.3 V supply voltage range: Setup time SS to SCLK rising edge.
		60	–	–	ns	For 1.8 V supply voltage range: Setup time SS to SCLK rising edge.
SS hold time	t_{SSH}	5	–	–	ns	Hold time SCLK falling edge to SS inactive
MOSI setup time	t_{SU}	2	–	–	ns	Data setup time to SCLK rising edge
MOSI hold time	t_H	3	–	–	ns	Data hold time from SCLK rising edge
MISO valid delay time from SS active	t_{SSV}	–	–	28	ns	For 3.3 V supply voltage range: Output valid delay time from SS active
		–	–	58	ns	For 1.8 V supply voltage range: Output valid delay time from SS active
MISO valid delay time from SCLK edge	t_V	–	–	21	ns	For 1.8 V supply voltage range Output valid delay time from SCLK falling edge SCLK input t_{slew} = 1 V/ns MISO C_{load} = 30 pF
		–	–	15	ns	For 3.3 V supply voltage range Output valid delay time from SCLK falling edge SCLK input t_{slew} = 1 V/ns MISO C_{load} = 30 pF
MISO output disable time	t_{SSDO}	0	–	30	ns	For 3.3 V supply voltage range: Output disable time from SS inactive
		0	–	60	ns	For 1.8 V supply voltage range: Output disable time from SS inactive
MISO hold time	t_{HO}	3.5	–	–	ns	For 1.8 V supply voltage range Output hold time to SCLK falling edge

Table 15 AC characteristics for 1.8 V and 3.3 V supply voltage range (Mode 0) (continued)

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
						SCLK input t_{slew} = 4 V/ns MISO C_{load} = 10 pF
		1.5	–	–	ns	For 3.3 V supply voltage range Output hold time to SCLK falling edge SCLK input t_{slew} = 4 V/ns MISO C_{load} = 10 pF
Input capacitance (package pin)	C_{IN}	–		10	pF	
Output load capacitance	C_{LOAD}	–		30	pF	A bigger load capacitance will decrease the performance.

*Note: All values and timings in **Table 15** are related to pin level.*

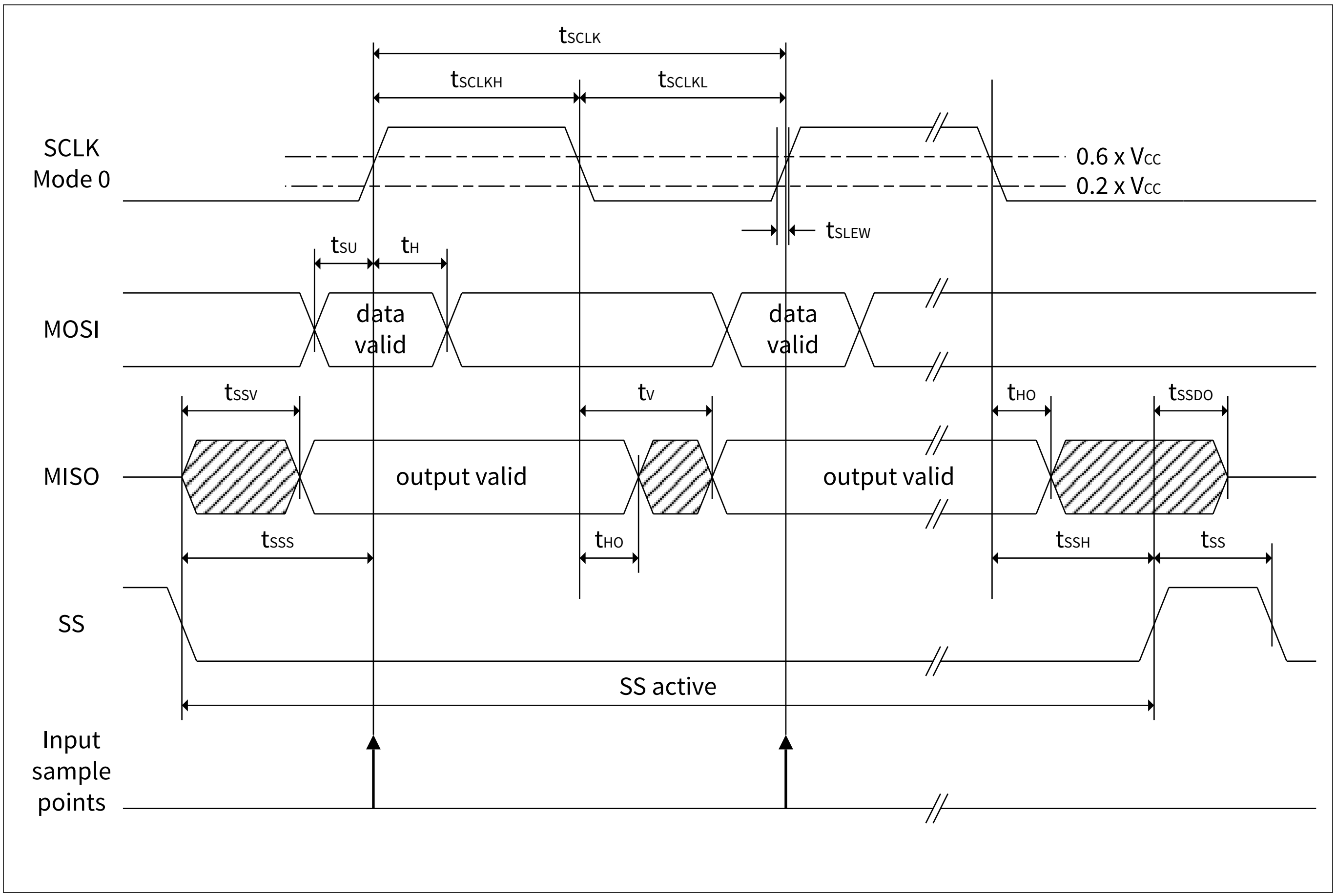


Figure 9 Timing diagram Mode 0

5.4 Thermal resistance

Table 16 Thermal resistance

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Junction to case	$R_{th(JC)}$	–	10.1	–	K/W	to exposed pad (bottom)[1]
	$R_{th(JC)}$	–	35.4	–	K/W	to top of package[2]
Junction to ambient	$R_{th(JA)}$	–	37.2	–	K/W	[1] [3]

[1] Not subject to production test, specified by design.

[2] https://www.infineon.com/cms/en/product/packages/PG-VQFN/PG-VQFN-32-13/

[3] According to JEDEC JESD 51-5, JESD 51-7 at free convection and radiation on FR4 2s2p board. Board size 76.2 mm x 114.3 mm x 1.5 mm, 2 inner copper layers (35 µm), thermal via array under the exposed pad connected to the first inner copper layer. Also refer to [2] .

As shown in **Table 6**, a maximum junction temperature T_J of 110°C must not be exceeded. Thermal simulations (done using the FEM software ANSYS®) show that this junction temperature T_J limit is not reached at an ambient temperature of 105°C when the device is mounted on a PCB according to JEDEC 2s2p (JESD 51-7, JESD 51-5).

If the device is mounted on a PCB compliant to JEDEC 1s0p (JESD 51-3), the simulation shows that due to selfheating of the device, the maximum junction temperature is exceeded at an ambient temperature of 105°C.

5.5 Storage and transport conditions

Table 17 Storage and transport conditions

Parameter	Symbol	Values			Unit
		Min.	Typ.	Max.	
Storage conditions					
Storage temperature	$T_{Storage}$	+5	–	+40	°C
Storage humidity	RH	10		75	%
Storage time				3[1]	Years
Transport conditions					
Transport temperature[2]	$T_{Transport}$	-25	–	+85	°C

[1] In reference to date code on BPL (Barecode Product Label).

BPL can be found on the Infineon packing.

Products shall be processed before the end of the maximum storage time defined above. Processing beyond expiring date may increase the risk of reduced processability, malfunction or non-function. Such recommendations are subject to storage time and storage conditions. Temperature, relative humidity, packing medium and environmental conditions.

[2] short term ≤ 15 days

5.6 IBIS Model

IBIS model is available on request.

6 Package description

A detailed description of the package can be found under the following link:
https://www.infineon.com/cms/en/product/packages/PG-VQFN/PG-VQFN-32-13/

6.1 PG-VQFN-32-13

Note: The drawings below are for information only and not drawn to scale. More detailed information about package characteristics and assembly instructions is available on request.

6.1.1 Package outline

The package dimensions (in mm) of the controller in PG-VQFN-32-13 packages are given below.

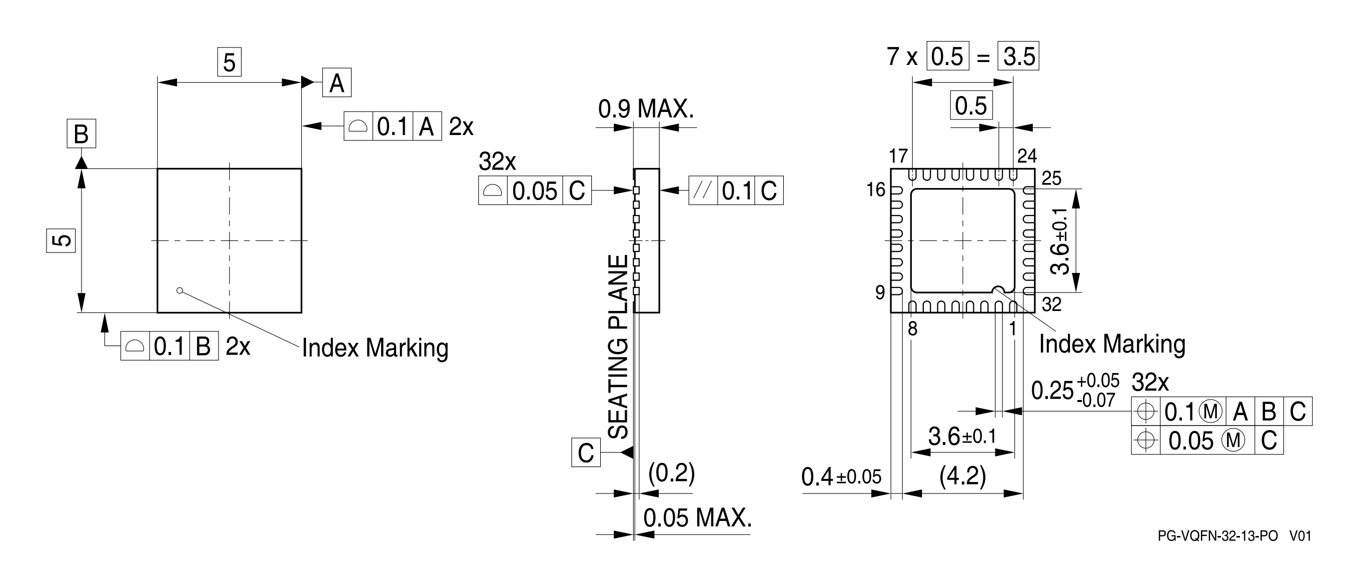


Figure 10 **PG-VQFN-32-13 package outline**

6.1.2 Package footprint

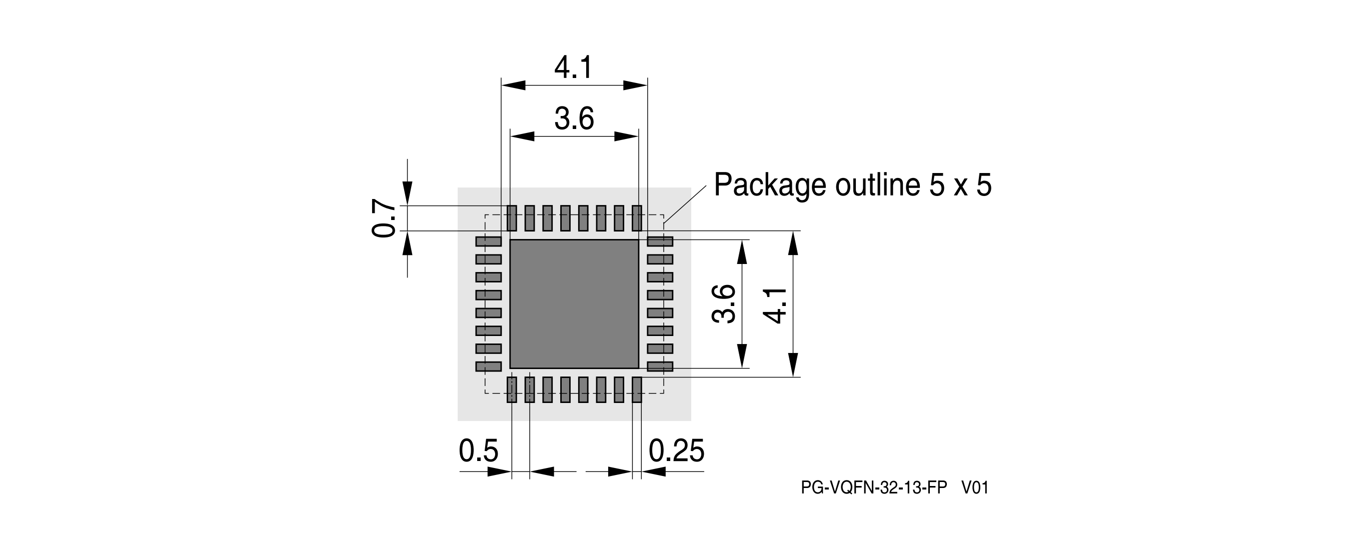
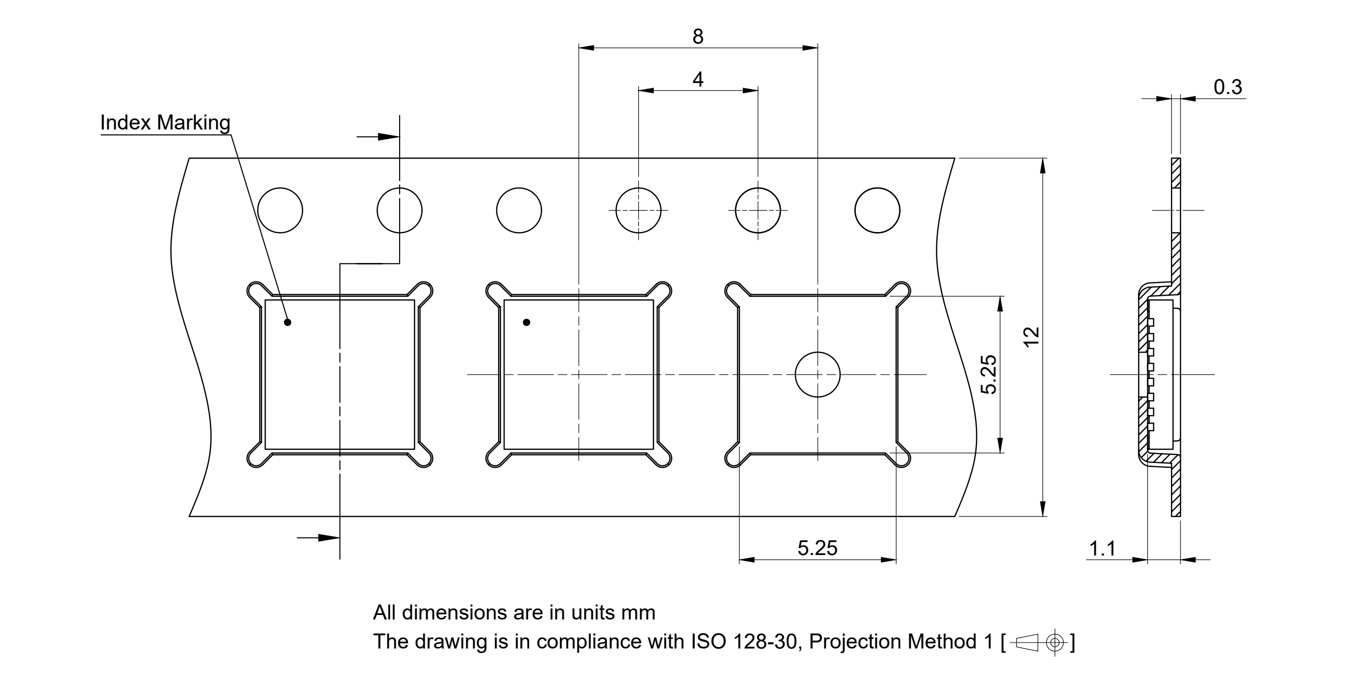


Figure 11 PG-VQFN-32-13 package footprint

6.1.3 Tape & reel packing



All dimensions are in units mm
The drawing is in compliance with ISO 128-30, Projection Method 1 [ ]

Figure 12 PG-VQFN-32-13 tape & reel packing

6.1.4 Production sample marking pattern

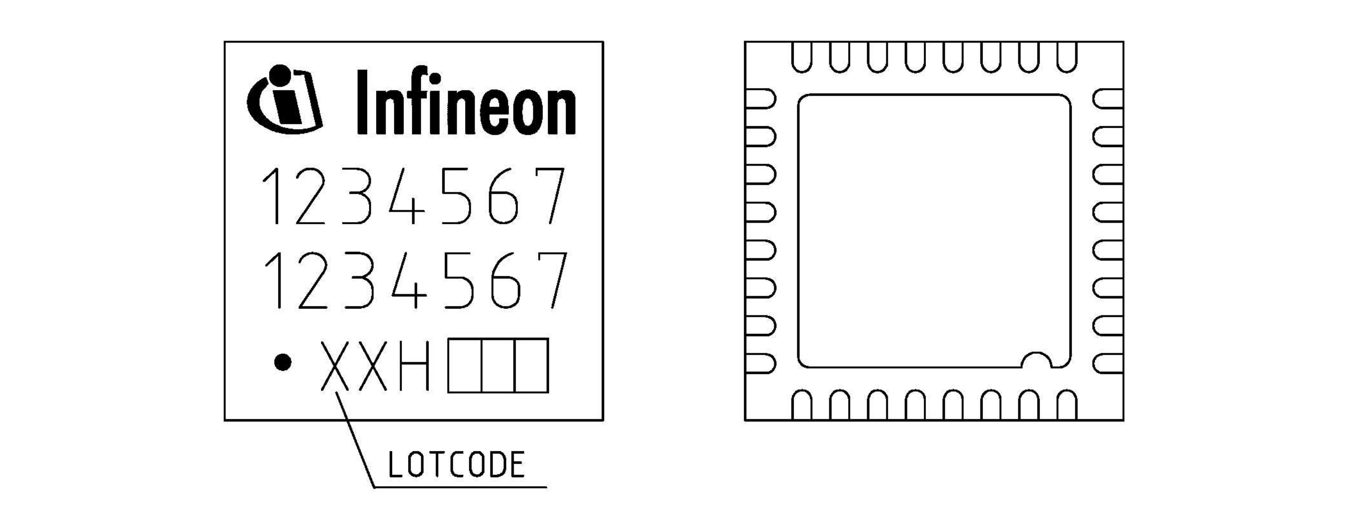


Figure 13 PG-VQFN-32-13 sample marking pattern

The black dot indicates pin 01 for the chip. The following table describes the sample marking pattern:

Table 18 Marking table for PG-VQFN-32-13 packages

Indicator	Description
Infineon (line 1)	Manufacturer
SLS37EU (line 2)	Abbreviation for sales code SLS37CSAEU.
BV2Xxxx (line 3)	Short ROM code with xxx as placeholder for different short ROM codes
XXH□□□ (line 4)	Lot code, defined and inserted during fabrication, issued by the packaging site

References

The following documents set out or describe specifications and/or standards referenced in the text of this document.

[1] GlobalPlatform Technology: *APDU Transport over SPI / I2C (Version 1.0)*, January 2020

[2] GlobalPlatform Technology: *Secure Channel Protocol '03' - Amendment D (Version 1.2)*, April 2020

[3] GlobalPlatform: *Card Specification (Version 2.3.1)*, March 2018

[4] ISO/IEC 7816-4: *Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange (Second edition)*, 2005-01-15

[5] IEEE1609.2-2016: IEEE Standard for Wireless Access in Vehicular Environments (WAVE) --Security Services for Applications and Management Messages, 2016-03-01

[6] IEEE1609.2a-2017: IEEE Standard for Wireless Access in Vehicular Environments (WAVE) --Security Services for Applications and Management Messages - Amendment 1, 2017-11-23

[7] IEEE 1609.2.1-2020: *IEEE Standard for Wireless Access in Vehicular Environments (WAVE) --Certificate Management Interfaces for End Entities*, December 2020

[8] ETSI TS 103 097: Intelligent Transport Systems (ITS); Security; Security header and certificate formats, V1.3.1 (2017-10)

[9] NIST FIPS 186-4: *Digital Signature Standard (DSS)*, July 2013

[10] RFC 2119: Bradner, Scott. "Key words for use in RFCs to Indicate Requirement Levels." RFC2119 (1997) ***https://tools.ietf.org/rfc/rfc2119.txt***.

Glossary

3D	Three-Dimensional
AC	Access condition
AC	Alternating Current
AEC	Automotive Electronics Council
AES	Advanced Encryption Standard
AES-CBC	Advanced Encryption Standard - Cipher Block Chaining
AES-CCM	Advanced Encryption Standard - Counter with CBC MAC mode
APDU	Application Protocol Data Unit
API	Application Programming Interface
Avg	Average
BPL	Barcode Product Label
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSM	Base Safety Message
BT	Bluetooth
BWT	Block Waiting Time
CA	Certificate Authority
CAD	Computer-Aided Design
CAN	Controller Area Network
CC	Common Criteria
CCMS	Cooperative ITS Credentials Management System
C-DECRYPTION	Command APDU Decryption
CDM	Charged-Device Model
CIP	Communication Interface Parameters
CLA	APDU Class Byte
CMAC	Cipher-based Message Authentication Code
C-MAC	Command APDU Message Authentication Code
CMOS	Complementary Metal–Oxide–Semiconductor
CPHA	Clock Phase
CPOL	Clock Polarity
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CS	Chip Select
CSR	Certificate Signing Request
CTR	Counter (Mode)
C-V2X	Cellular Vehicle to Everything

DC	Direct Current
DDR	Double Data Rate
DEK	Data Encryption Key
DER	Distinguished Encoding Rules
DH	Diffie-Hellman
DNC	Do Not Connect
DPWT	Default Power Wake-Up Time
DRBG	Deterministic Random Bit Generator
DRNG	Deterministic Random Number Generator
DST	Destination
DWUT	Default Wake-Up Time
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
ECSVDP-DHC	Elliptic Curve Secret Value Derivation Primitive–Diffie-Hellman version with cofactor multiplication
ECU	Electronic Control Unit
EE	End Entity
eMMC	embedded Multi-Media Card
ESD	Electrostatic Discharge
ESPS	Efficient Security Credental Provisioning Service
ETH	Ethernet
ETSI	European Telecommunications Standards Institute
EU	European Union
eUICC	embedded Universal Integrated Circuit Card
FIPS	Federal Information Processing Standard
FUL	Field Update Loader
FW	Firmware
GND	Ground
GNSS	Global Navigation Satellite System
GP	GlobalPlatform
GPIO	General Purpose Input Output
GPS	Global Positioning System
HBM	Human Body Model
HI	High

HMAC	Hash-based Message Authentication Code
HSM	Hardware Security Module
HW	Hardware
I/O	Input/Output
I2C	Inter-Integrated Circuit
IBIS	Input/Output Buffer Information Specification
IC	Integrated Circuit
ID	Identity
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IF	Interface
IFSC	Maximum Information Field Size
IMM	Interface Management Module
INS	APDU Instruction Byte
IRQ	Interrupt Request
ISO	International Organization for Standardization
ISS	Instruction Stream Signature
KCV	Key Check Value
KDdata	Key Diversification Data
KDF	Key Derivation Function
KID	Key Identifier
KVN	Key Version Number
KWP	Key Wrapping Protocol
LC	Lifecycle
Lc	APDU Length of Command Field
Le	APDU Length Expected
LED	Light Emitting Diode
LIN	Local Interconnect Network
LNA	Low Noise Amplifier
LO	Low
LPDDR	Low Power Double Data Rate
LSB	Least Significant Byte/Bit
LTE	Long Term Evolution
MAC	Message Authentication Code
MCF	Maximum Clock Frequency
MED	Memory Encryption Device

MEMS	Micro-Electro-Mechanical Systems
MISO	Master In Slave Out
MOSFET	Metal Oxide Semiconductor Field Effect Transistor
MOSI	Master Out Slave In
MPOT	Minimum Polling Time
MPU	Memory Protection Unit
MSB	Most Significant Byte/Bit
NAND	Not And
NCI	Not Connected Internally
NIST	National Institute of Standards and Technology
NOR	Not Or
NVIC	Nested Vector Interrupt Control
NVM	Non-Volatile Memory
OBU	On-Board Unit
OEM	Original Equipment Manufacturer
OpenSSL	Open Secure Sockets Layer
P1	APDU Parameter 1
P2	APDU Parameter 2
PCB	Printed Circuit Board
PCB	Protocol Control Byte
PGP	Pretty Good Privacy
PI	Platform Integrator
PKI	Public Key Infrastructure
PMIC	Power Management Integrated Circuit
POR	Power-On Reset
PP	Protection Profile
PPAP	Production Part Approval Process
PRNG	Pseudo Random Number Generator
PST	Power Saving Timeout
PWR	Power
PWT	Power Wake-Up Time
RAM	Random Access Memory
R-ENCRYPTION	Response APDU Encryption
RF	Radio Frequency
RFC	Request For Comments
RFFE	Radio Frequency Front End

RFU	Reserved for Future Use
R-MAC	Response APDU Message Authentication Code
RNG	Random Number Generator
ROM	Read-Only Memory
RST	Reset
RSU	Road-Side Unit
Rx	Receive
SBC	System Basis Chip
SCLK	Serial Peripheral Interface Clock
SCMS	Security Credential Management System
SCP	Symmetric Co-Processor
SCP03	Secure Channel Protocol 03
SDR	Software Defined Radio
SEAL	Secure Element Access Length
SEC1	Standard for Efficient Cryptography 1
SEGT	Secure Element Guard Time
S-ENC	Session Key for Encryption
SHA	Secure Hash Algorithm
S-MAC	Session Key for Command APDU Message Authentication Code
SMD	Surface-Mounted Device
SPI	Serial Peripheral Interface
SRC	Source
S-RMAC	Session Key for Response APDU Message Authentication Code
SS	Slave Select
SW	Software
SW1SW2	APDU Status Word 1, Status Word 2
SWR	Software Reset
TCU	Telematics Control Unit
TPM	Trusted Platform Module
TRNG	True Random Number Generator
Tx	Transmit
Typ	Typical
uint	Unsigned Integer
UMSLC	User Mode Security Life Control
US	United States
V2I	Vehicle to Infrastructure

V2N	Vehicle to Network
V2P	Vehicle to Physical
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
VCC	Supply Voltage
VFUL	V2X Field Update Loader
VQFN	Very Thin Quad Flat No Leads
VRU	Vulnerable Road User
VV	Vendor Verification
WDT	Watchdog Timer
WiFi	Wireless Fidelity
WUT	Wake-Up Time
XOR	Exclusive Or

Revision history

Reference	Description
Revision 1.2, 2021-10-25	
	Updated minor changes
Revision 1.1, 2021-09-29	
	Changed distribution status
Revision 1.0, 2021-09-21	
	Initial release

RoHS compliance

On January 27, 2003 the European Parliament and the council adopted the directives:

- 2002/95/EC on the Restriction of the use of certain Hazardous Substances in electrical and electronic equipment ("RoHS")
- 2002/96/EC on Waste Electrical and Electrical and Electronic Equipment ("WEEE")

Some of these restricted (lead) or recycling-relevant (brominated flame retardants) substances are currently found in the terminations (e.g. lead finish, bumps, balls) and substrate materials or mold compounds.

The European Union has finalized the Directives. It is the member states' task to convert these Directives into national laws. Most national laws are available, some member states have extended timelines for implementation. The laws arising from these Directives have come into force in 2006 or 2007.

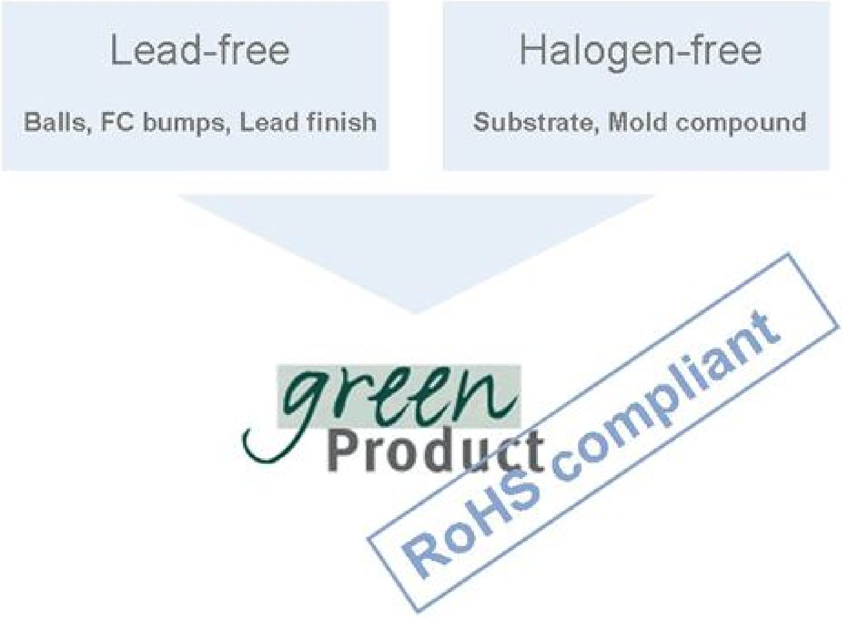
The electro and electronic industry has to eliminate lead and other hazardous materials from their products. In addition, discussions are on-going with regard to the separate recycling of certain materials, e.g. plastic containing brominated flame retardants.

Infineon is fully committed to giving its customers maximum support in their efforts to convert to lead-free and halogen-free[1] products. For this reason, Infineon's "Green Products" are ROHS-compliant.

Since all hazardous substances have been removed, Infineon calls its lead-free and halogen-free semiconductor packages "green." Details on Infineon's definition and upper limits for the restricted materials can be found here.

The assembly process of our high-technology semiconductor chips is an integral part of our quality strategy. Accordingly, we will accurately evaluate and test alternative materials in order to replace lead and halogen so that we end up with the same or higher quality standards for our products.

The use of lead-free solders for board assembly results in higher process temperatures and increased requirements for the heat resistivity of semiconductor packages. This issue is addressed by Infineon by a new classification of the Moisture Sensitivity Level (MSL). In a first step the existing products have been classified according to the new requirements.



[1] Any material used by Infineon is PBB and PBDE-free. Plastic containing brominated flame retardants, as mentioned in the WEEE directive, will be replaced if technically/economically beneficial.

Trademarks

All referenced product or service names and trademarks are the property of their respective owners.

Edition 2021-10-25

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about any aspect of this document?

Email:
CSSCustomerService@infineon.com

Document reference
IFX-xbq1612348608601

IMPORTANT NOTICE

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics (“Beschaffenheitsgarantie”).

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

In addition, any information given in this document is subject to customer’s compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer’s products and any use of the product of Infineon Technologies in customer’s applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer’s technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

WARNINGS

Due to technical requirements 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 Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies’ products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.