# OPTIGA™ Trust Charge Automotive

## Datasheet

**Trusted authentication for Qi charging**

**Easy-to-integrate solution for Qi authentication in automotive wireless charging applications**

## Devices

**SLS37CSAE20TC**

This document describes a solution for Qi authentication. The Qi standard is issued by the WPC (http://www.wirelesspowerconsortium.com). Please refer to WPC website for protocol details. Requirements for this **Provisioned Secure Storage Subsystems** are also defined in the **Manufacturer CA Agreement** between WPC and the provider of the HSM. This agreement may be confidential.


## Key features

**SLS37CSAE20TC Qi authentication solution**

**Easy integration**

- Full turnkey solution for authentication for wireless charging (Qi 1.3 and higher)
- Full system integration support
- Customer specific certificate provided (provisioning)
- Host code and application notes for common host controller available
- Evaluation kit available

**Certificates and cryptographic algorithms**

- X.509/WPC certificate format supported
- Authentication based on ECDSA NIST-P256
- Cryptography support: ECC256, RNG (GET_RANDOM), SCP03

**Other key features**

- SPI GP protocol
- Secure Channel over SPI using GlobalPlatform SCP03 (optional)
- In-field Update Mechanism (optional)
- 32 pin VQFN Package (5 mm x 5 mm)
- AEC-Q100 REV.G (Grade 2)

**Deliverables**

- Secure Storage Subsystem in line with Qi Specification
- Provisioned with device-unique key material and certificate(s) (in certified manufacturing site, Drivers and host software for integration with host controller)

**WPC Qi compliant certificate chain**

- **Infineon offers the service to act as a "WPC Manufacturer CA". Infineon will create Manufacturer CA certificates for Secure Storage Subsystems in Qi certified devices; Creation and loading of unit specific keys and certificates will take place in certified and audited production sites**

**Security certification**

- Hardware platform certified according to Common Criteria Protection Profile (PP0084)

### Hardware

- Tamper resistant security controller providing highest proven assets protection
- High performance crypto accelerator
- 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
  - 17 years of data retention
- High-speed SPI interface up to 10 MHz
- Single voltage supply from 1.62 V to 3.6 V

## Target applications

SLS37CSAE20TC is a provisioned secure storage subsystem as defined by the Qi version 1.3 (and higher) standard. It offers core functionality for the authentication procedure to establish and verify the authenticity of a certified Power Transmitter to a Power Receiver. Being AEC-Q100 REV.G (Grade 2) qualified, SLS37CSAE20TC is optimized for use in automotive applications.

Figure 1 shows simplified the components of a power transmitter and power receiver according to the Qi authentication protocol.

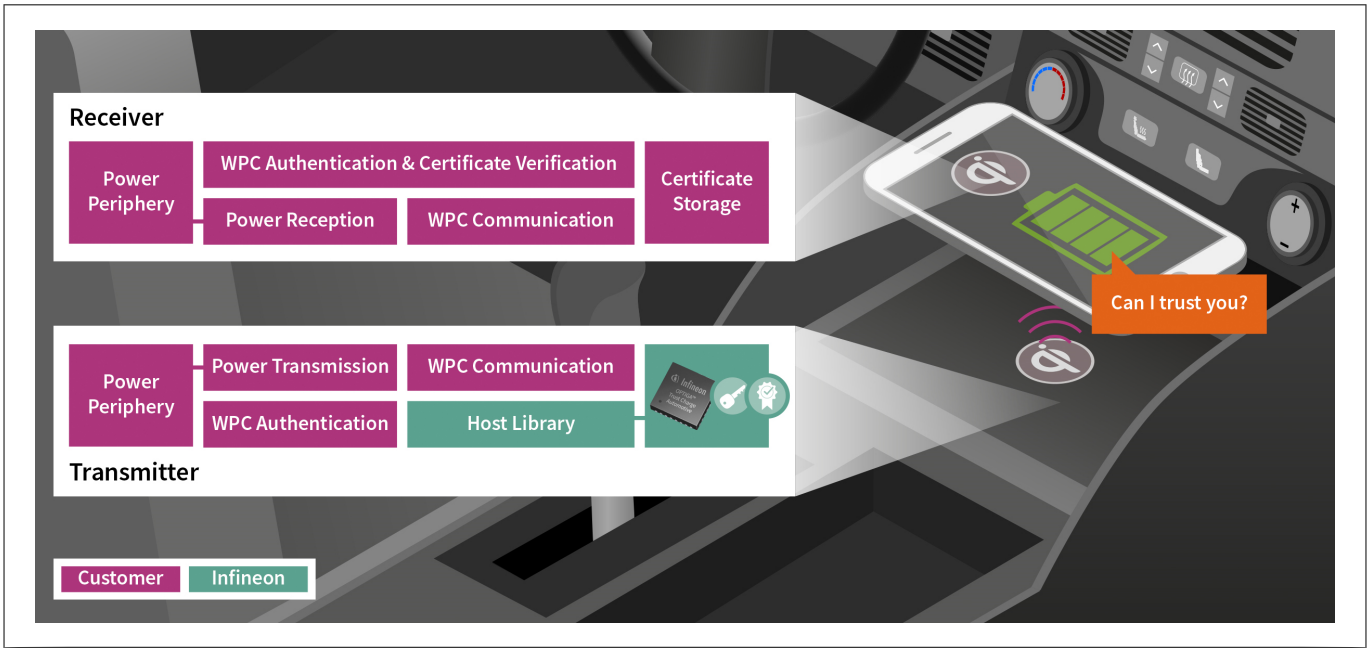


**Figure 1 Exemplary Wireless Charging System Architecture**

# About this document

## Scope and purpose

This datasheet provides an overview of the hardware, the software features and functionalities and information about the package characteristics of the OPTIGA™ Trust Charge Automotive.

*Note: OPTIGA™ Trust Charge Automotive secure storage subsystem is also referred to as HSM or SLS37CSAE20TC.*

## 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

**Devices** . . . 1
**Key features** . . . 1
**Target applications** . . . 2
**About this document** . . . 3
**Table of contents** . . . 4
**List of tables** . . . 6
**List of figures** . . . 7
**1 General description** . . . 8
1.1 Overview . . . 8
1.2 Main features and benefits . . . 9
1.2.1 Chip side hardware features . . . 10
1.2.2 Chip side software features . . . 11
1.2.3 Infineon OPTIGA™ Trust Charge Automotive host software package . . . 11
1.3 Applications and use cases . . . 12
**2 Block diagram** . . . 13
**3 Pin description** . . . 14
3.1 Abbreviations in pin description . . . 14
3.2 Pad-to-signal reference . . . 15
3.3 Typical schematic . . . 17
3.4 CAD files . . . 17
**4 HSM firmware** . . . 18
**5 Electrical characteristics** . . . 19
5.1 Absolute maximum ratings . . . 19
5.2 Operational characteristics . . . 20
5.2.1 DC electrical characteristics . . . 20
5.2.2 AC electrical characteristics . . . 20
5.2.2.1 Power-up considerations . . . 21
5.3 Particular interface characteristics . . . 22
5.3.1 GPIO interface characteristics . . . 22
5.3.2 SPI interface characteristics . . . 24
5.4 Thermal resistance . . . 28
5.5 Storage and transport conditions . . . 28
5.6 IBIS Model . . . 28
**6 Package description** . . . 29
6.1 PG-VQFN-32-13 . . . 29
6.1.1 Package outline . . . 29

## Table of contents

6.1.2 Package footprint . . . . . 30
6.1.3 Tape and reel packing . . . . . 30
6.1.4 Production sample marking pattern . . . . . 31
**References** . . . . . 32
**Glossary** . . . . . 33
**Revision history** . . . . . 36
**RoHS compliance** . . . . . 37
**Disclaimer** . . . . . 38

# List of tables

Table 1 Abbreviations for pin type . . . . . 14
Table 2 Abbreviations for buffer type . . . . . 14
Table 3 I/O signals . . . . . 15
Table 4 Power supply . . . . . 16
Table 5 Not connected . . . . . 16
Table 6 Absolute maximum ratings . . . . . 19
Table 7 DC characteristics . . . . . 20
Table 8 AC characteristics . . . . . 20
Table 9 GPIO operation supply and input voltages . . . . . 22
Table 10 GPIO DC electrical characteristics . . . . . 22
Table 11 GPIO AC electrical characteristics . . . . . 23
Table 12 Serial transfer mode . . . . . 24
Table 13 DC characteristics for 3.3 V supply voltage range . . . . . 24
Table 14 DC characteristics for 1.8 V supply voltage range . . . . . 25
Table 15 AC characteristics for 1.8 V and 3.3 V supply voltage range (Mode 0) . . . . . 25
Table 16 Thermal resistance . . . . . 28
Table 17 Storage and transport conditions . . . . . 28
Table 18 Marking table for PG-VQFN-32-13 packages . . . . . 31

# List of figures

Figure 1 Exemplary Wireless Charging System Architecture . . . . . 2
Figure 2 OPTIGA™ Trust Charge Automotive Software Stack . . . . . 12
Figure 3 Block diagram of the HSM . . . . . 13
Figure 4 PG-VQFN-32-13 package layout . . . . . 15
Figure 5 Typical schematic . . . . . 17
Figure 6 Recommended power-up behavior . . . . . 21
Figure 7 SPI Mode 0 . . . . . 24
Figure 8 Timing diagram Mode 0 . . . . . 27
Figure 9 PG-VQFN-32-13 package outline . . . . . 29
Figure 10 PG-VQFN-32-13 package footprint . . . . . 30
Figure 11 PG-VQFN-32-13 tape and reel packing . . . . . 30
Figure 12 PG-VQFN-32-13 sample marking pattern . . . . . 31

# 1 General description

## 1.1 Overview

The Infineon SLS37CSAE20TC OPTIGA™ Trust Charge Automotive is a provisioned secure storage subsystem in line with the WPC Qi 1.3 (and higher) standard. OPTIGA™ Trust Charge Automotive offers core functions for the authentication of a Qi Power Transmitter to a Qi Power Receiver. Being based on a highly-secured, tamper resistant security controller with highest proven asset protection, this secure storage subsystem protects the private key that is associated with the public key in the Product Unit Certificate of Qi certified products and offers functions to prove the authenticity via ECDSA signing operations.

The hardware architecture is based on 32-bit ARM® SecureCore® SC300 CPU with an additional high performance asymmetric cryptographic engine and the latest generation of an hardware co-processor for symmetric cryptography.

The OPTIGA™ Trust Charge Automotive herein called Provisioned Secure Storage Subsystem, is interfacing to a host processor via SPI. With the OPTIGA™ Trust Charge Automotive hardware certification according to Common Criteria (CC) EAL6+ high and AEC-Q100 (Grade 2) qualification, it 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. In addition, it fully meets the requirements for a Provisioned Secure Storage Subsystem in line with the WPC Qi Specification version 1.3 and higher.

The CC certificate can be found at https://www.tuv-nederland.nl/common-criteria/certificates.html by searching for the Hardware Identifier IFX_CCI_00005Ah and referring to the latest CC certificate.

The Qi standard is issued by the WPC (www.wirelesspowerconsortium.com). Please refer to WPC website for protocol details. Requirements for this **Provisioned Secure Storage Subsystems** are also defined in the **Manufacturer CA Agreement** between WPC and the provider of the Qi authenticator. This agreement may be confidential.

SLS37CSAE20TC comes pre-programmed with Infineon OPTIGA™ Trust Charge Automotive firmware and is ready-to-use.

Major blocks of the OPTIGA™ Trust Charge Automotive firmware in SLS37CSAE20TC are the embedded operating system and the Qi authentication protocol. In combination, they are providing high performance functionality including cryptographic operations (e.g. ECDSA signature generation), certificate and key storage/ management. Both, the Qi authentication and the underlying operating system, are based on the latest WPC standards and market requirements. This software is developed according to secure coding standards and security certifications.

For ease of use and faster time-to-market the SLS37CSAE20TC is complemented with a Host Software Package. This software package encompasses demo code to be included into the software running on the host- or application processor the SLS37CSAE20TC is connected to intending to facilitate an easy integration.

Within this setup SLS37CSAE20TC, provides the host-processor with secured storage of private keys and performs the respective cryptographic operations.

This includes but is not limited to:

- ECC private key management (generation, import, and deletion)
- ECDSA signature generation
- Storage of private keys and certificate data
- Infineon PKI provides customer-individual keys enabling a secured pairing between SLS37CSAE20TC and the respective host processor as well as secured in-field updates

Figure 1 shows a typical wireless charging system. The SLS37CSAE20TC in combination with the Host Software Package provide prepared communication messages according to the WPC Qi 1.3 Authentication Protocol.

## 1.2 Main features and benefits

**Easy integration**

- Full turnkey solution for Qi authentication for wireless charging
- Full system integration support
- Customer and chip unique certificates provided (provisioning)
- Host code and application notes for common host controllers available
- Evaluation kit available

**Security features**

- Tamper resistant hardware platform enabling secured key storage and trusted execution of the respective cryptographic operations
- X.509 certificate format according to the WPC Qi 1.3 supported
- Authentication based on ECDSA NIST-P256
- Cryptography support: ECC256, RNG (GET_RANDOM), SCP03

**Key features**

- Optimized for use in automotive Qi certified systems, i.e. harsh automotive environments as well as highest security levels
- SPI GP protocol
- Secure Channel over SPI using GlobalPlatform SCP03
- In-field Update Mechanism
- VQFN32 package
- AEC-Q100 REV.G Grade 2

SLS37CSAE20TC is a Provisioned Secure Storage Subsystem in line with the WPC Qi version 1.3 standard. It is a plug-and-play security solution that allows manufacturers of Qi certified devices to implement the standard compliant (WPC Qi version 1.3 and higher) authentication procedure 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
- True and Pseudo Random Number Generator
- Hybrid Random Number Generation (TRNG and PRNG) 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 OPTIGA™ Trust Charge Automotive application of SLS37CSAE20TC exposes its features to the host by providing an APDU Command Interface (API).

This API includes a set of features including reporting, management, storage and crypto functionalities required for the WPC Qi 1.3 Authentication protocol including but not limited to the following:

- ECC key pair generation on the chip
- ECDSA sign
- NIST P-256/P-384
- Secured storage for up to 4 private keys
- Secured storage for up to 4 certificate chains – each 2048 Bytes with configurable access conditions per user (write/read/change)
- RNG (GET_RANDOM)
- Secure Channel Protocol 03 (SCP03) based on GlobalPlatform Card Specification v2.3 – Amendment D Version 1.1.2
- Authentication scheme and user rights management including:
  - Different users with configurable access rights
  - Each user with key/password 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 during firmware update:
    - Fast image signature verification
    - Fast verified image installation (replaces current image)
  - Data (private keys and certificate chains) 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 OPTIGA™ Trust Charge Automotive host software package

For ease of integration OPTIGA™ Trust Charge Automotive offers a host software package abstracting its functionality and offering the corresponding functions to a host controller. The host software is developed with high re-usability in mind. Therefore the integration is split into two parts:

- The platform-independent core (OPTIGA™ Trust Charge Automotive – Host Software.zip) contains the main logic for the OPTIGA™ Trust Charge Automotive host integration as well as examples on how to use the provided API

  It uses a custom platform abstraction layer (PAL) to be as generic as possible. When porting the integration to a new hardware platform the core can be reused as is.
- Platform-specific integrations (for example: OPTIGA™ Trust Charge Automotive – Host Software – AURIX™ TC3xx.zip) build on top of the core and add platform-specific implementations of the PAL

To be able to use the OPTIGA™ Trust Charge Automotive host integration you will at least need the core package as well as a platform integration matching your desired host platform and toolchain.

For more information on the core package please refer to its provided documentation. For an overview of the available platform integrations refer to your Infineon downloads or contact Infineon sales representative.

An overview of the components of the host software package is shown in Figure 2.

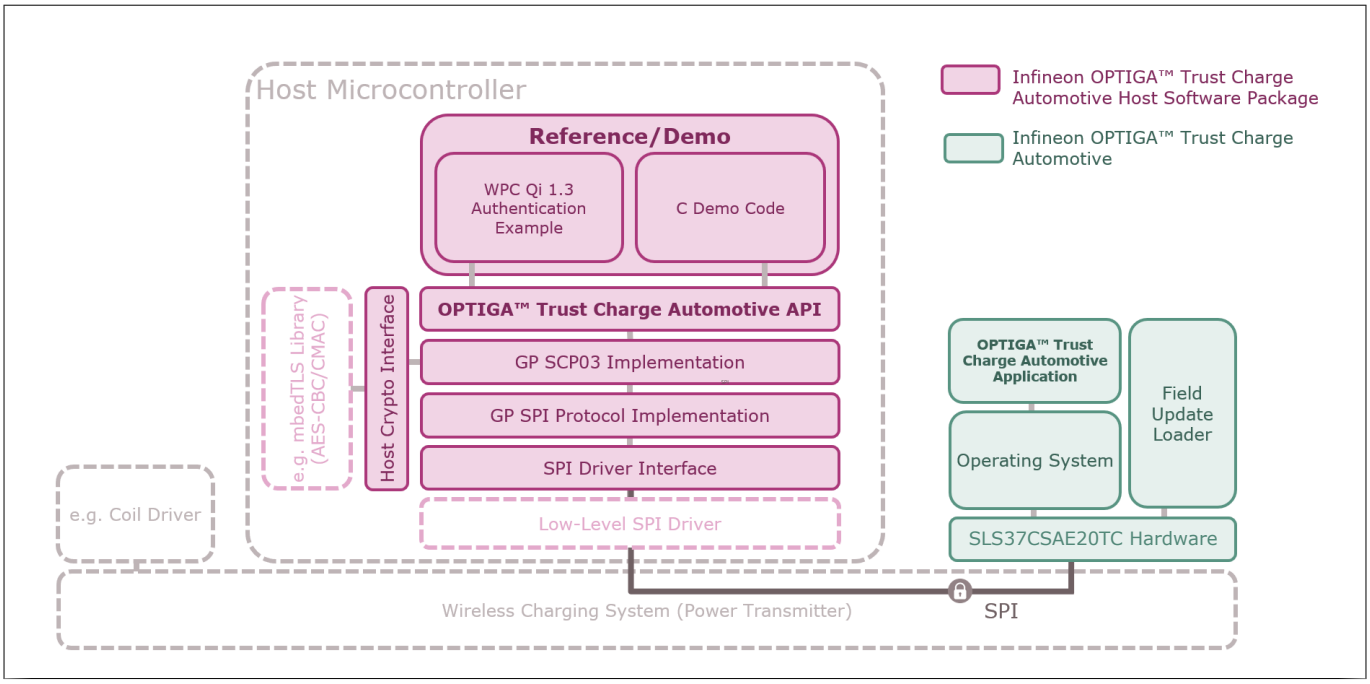


**Figure 2 OPTIGA™ Trust Charge Automotive Software Stack**

Figure 2 shows a generic wireless charging system, the middle section represents the code running on the host processor (OPTIGA™ Trust Charge Automotive host software package), the section on the right side reflects the software or firmware residing on the chip (SLS37CSAE20TC).

The OPTIGA™ Trust Charge Automotive Host Software Package consists of a demo module, which shows how to integrate and use the security controller or the target wireless charging system on a host platform. The Host Software Package is delivered as demo source code for the Evaluation Kit. Due to the modular approach, it is easy to use, to adapt or to integrate in other embedded systems.

**Features**

- Complete OPTIGA™ Trust Charge Automotive API Library with access to all APDU commands delivered as C source code including SPI protocol implementation and GlobalPlatform Secure Channel Protocol 03 (SCP03)
- Example scripts for Initialization, WPC Qi Authentication messages preparation Application Note, In-Field Update, etc. delivered as C source code
- Wrapper functions for Host-side crypto (mbedTLS) and Host SPI driver for easy porting onto other platforms

## 1.3 Applications and use cases

The Infineon security controller is a Provisioned Secure Storage Subsystem in line with WPC Qi version 1.3 (and higher) and as such is a turnkey authentication solution offering core functions for the authentication of a Qi certified Power Transmitter to a Power Receiver for the wireless charging use case.

**Power Transmitter authentication according to the WPC Qi Authentication**

The secure storage subsystem offers core functions for the authentication procedure of a Qi certified power transmitter according to the latest WPC Qi 1.3 Specification. Functions include, but are not limited to, secured storage of ECC private keys, Product Unit Certificate(s) and related certificate chain(s) and ECDSA signature generation as core function in order to prove the authenticity of a Qi certified device. Each chip has up to 4 private key and 4 file slots to store WPC Qi compliant certificate chains.

# 2 Block diagram

Figure 3 shows the hardware block diagram of the HSM.

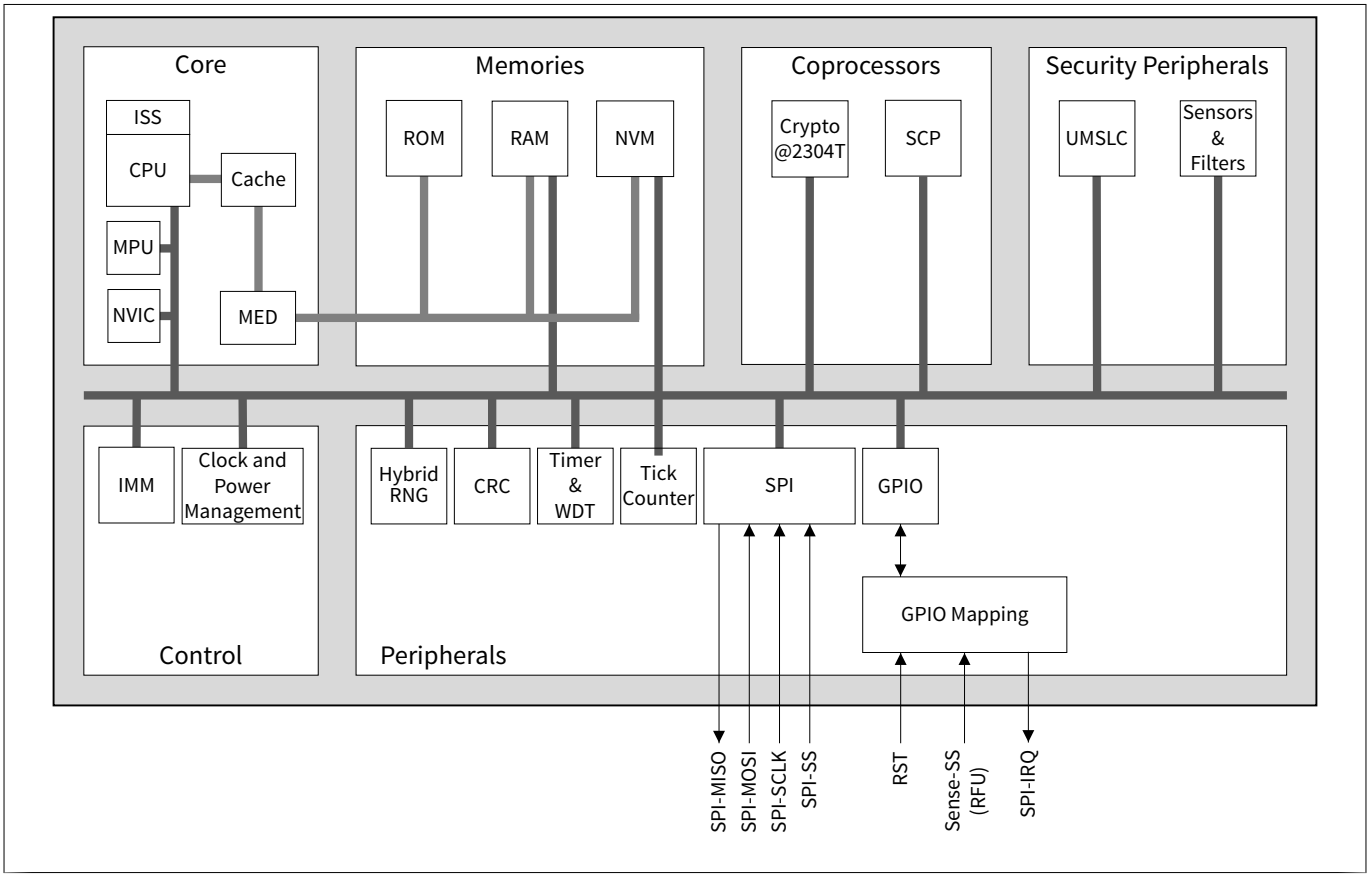


**Figure 3 Block diagram of the HSM**

# 3 Pin description

The pad usage of the 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 Package description.

## 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 OPTIGA™ Trust Charge Automotive 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:

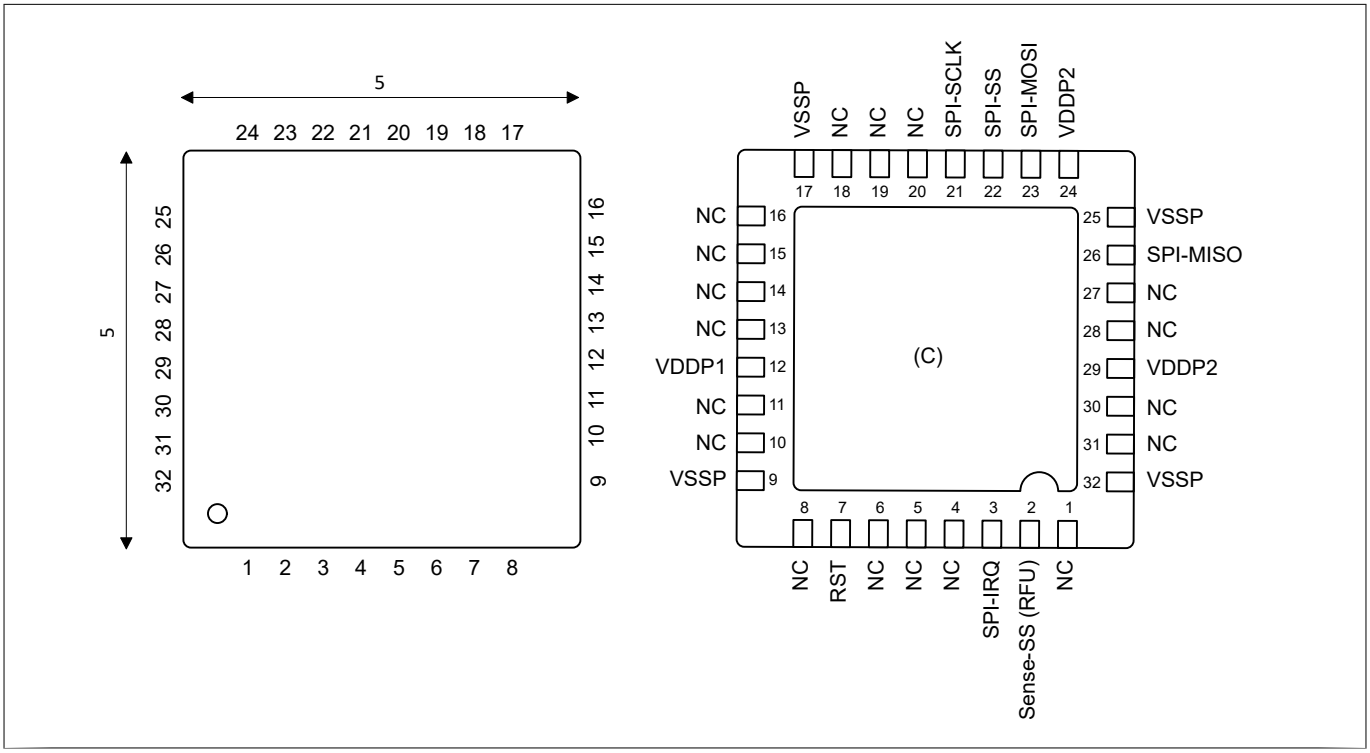


**Figure 4 PG-VQFN-32-13 package layout**

**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)<br>This pin is optional and does not have to be used. In this case, do not connect the pin and leave the pin floating |
| 7 | RST | I | GPIO_I | **Reset**, active low,<br>Evaluated by software after start-up,<br>Internal pull-up<br>This pin is optional and does not have to be used. In this case, do not connect the pin and leave the pin floating |
| 21 | SPI-SCLK | I | SPI_I | **SPI Clock**<br>The SPI clock signal. Only SPI mode 0 (CPOL = 0, CPHA = 0) is supported by the device. |

**(table continues...)**

**Table 3 (continued) I/O signals**

| Pad | Name | Pin type | Buffer type | Signal function/remark |
|---|---|---|---|---|
| 22 | SPI-SS | I | SPI_I | **Slave Select**, active low<br>The SPI chip slave select signal<br>No internal pull-up |
| 23 | SPI-MOSI | I | SPI_I | **SPI Master Out Slave In (SPI Data)**<br>SPI data which is received from the master |
| 26 | SPI-MISO | O | SPI_O | **SPI Master In Slave Out (SPI Data)**<br>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**<br>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**<br>All pins are not connected internally (can be connected externally). |

*Note: The exposed die pad referenced as (C) in Figure 4 must be connected to the common ground reference (GND) for heat distribution.*

## 3.3 Typical schematic

Figure 5 shows the typical schematic for the HSM. The power supply pins should be bypassed to GND with capacitors located close to the device.

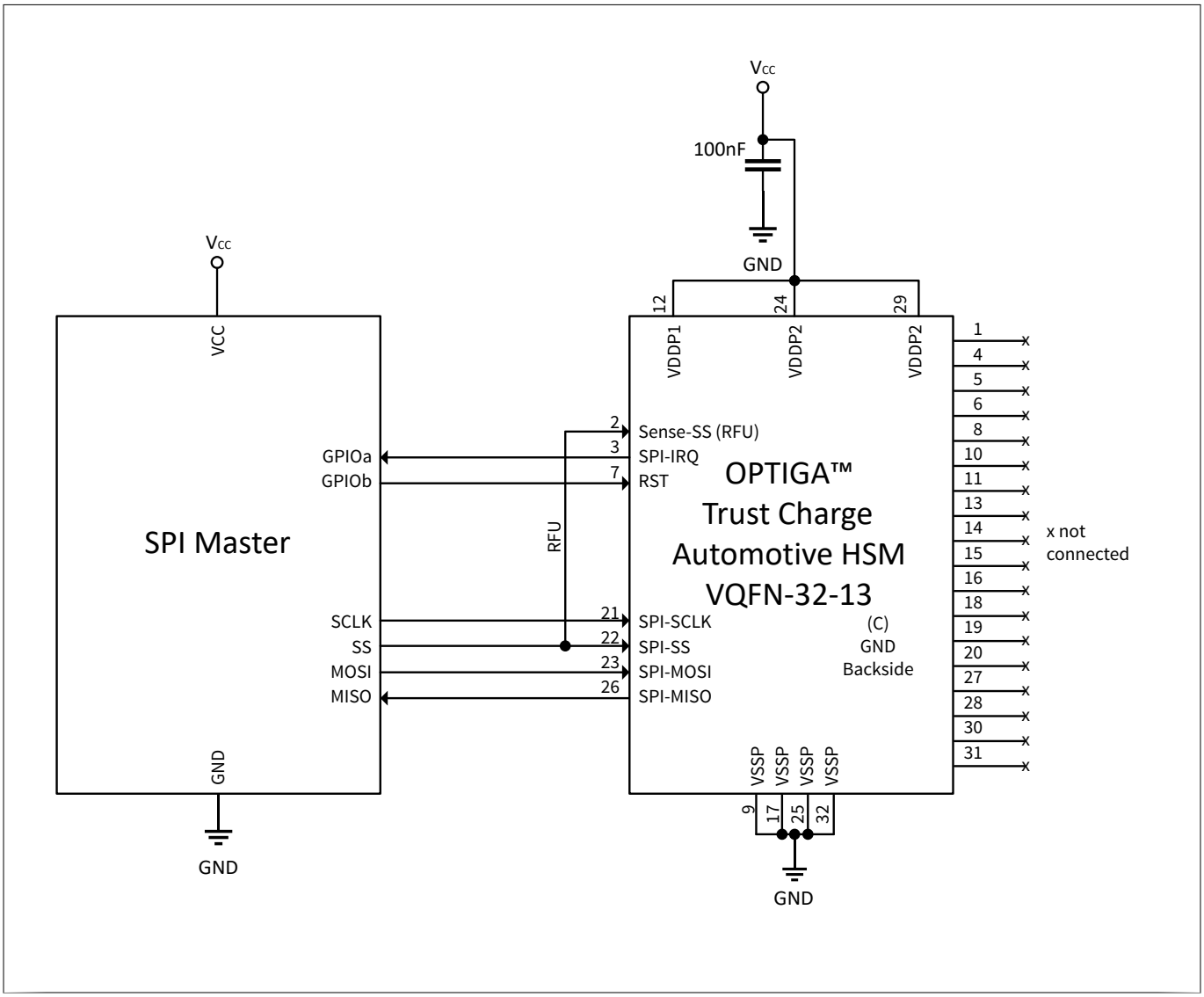


**Figure 5 Typical schematic**

## 3.4 CAD files

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

# 4 HSM firmware

The HSM firmware is described in detail in the corresponding chapter of the OPTIGA™ Trust Charge Automotive 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 (= $V_{CC}$),<br>SPI-IRQ inactive (= GND),<br>SPI-SS inactive (= $V_{CC}$),<br>SPI-MOSI, SPI-MISO and SPI-SCLK do not 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.

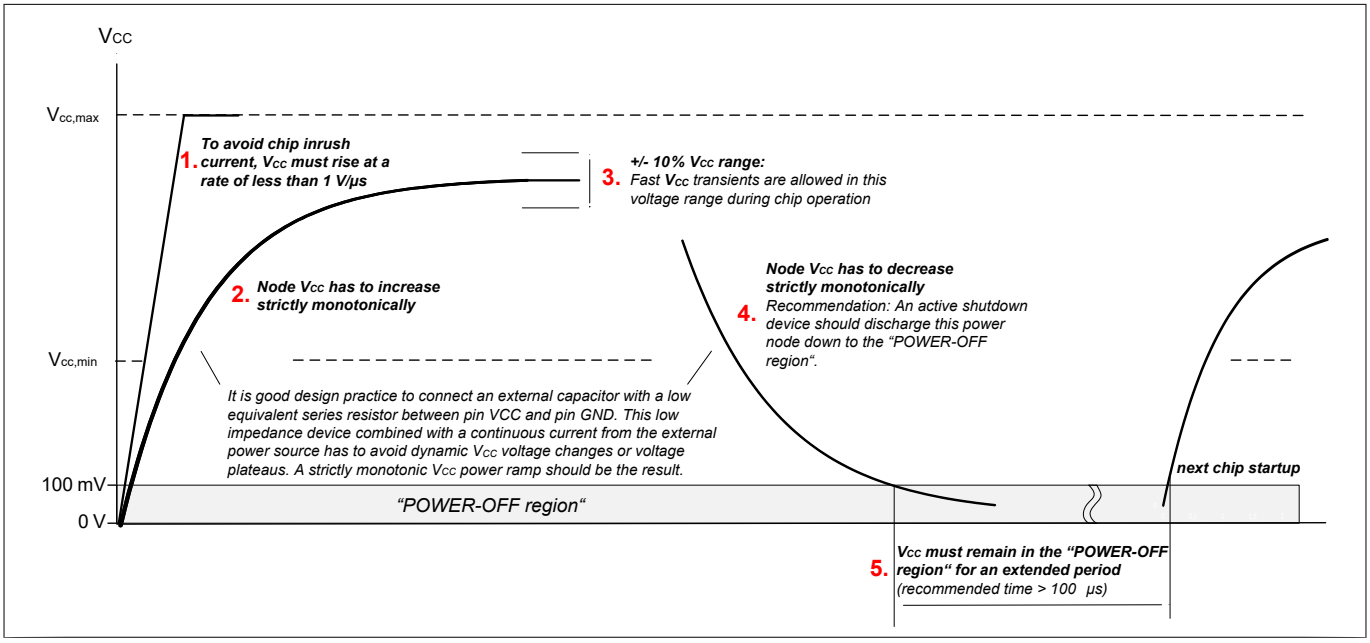


**Figure 6 Recommended power-up behavior**

## 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 ≤ $V_{IN\_GPIO}$ ≤ $V_{CC}$ − 0.5 V |
| Input current, pull-down (weak) enabled | $I_{PDW}$ | 3 | – | 20 | µA | 0.5 V ≤ $V_{IN\_GPIO}$ ≤ $V_{CC}$ |
| Pull-up (strong) resistance | $R_{PUS}$ | 2.5 | – | 5.5 | kΩ | 0 V ≤ $V_{IN\_GPIO}$ ≤ $V_{CC}$ − 0.5 V |
| Input leakage current | $I_{LI}$ | −2 | – | 2 | µA | Pull-up/down off, output stage off; 0 V ≤ $V_{IN\_GPIO}$ ≤ $V_{CC}$ |
| 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, $V_{CC}$ ≥ 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, $V_{CC}$ ≥ 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 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 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 7). 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. |

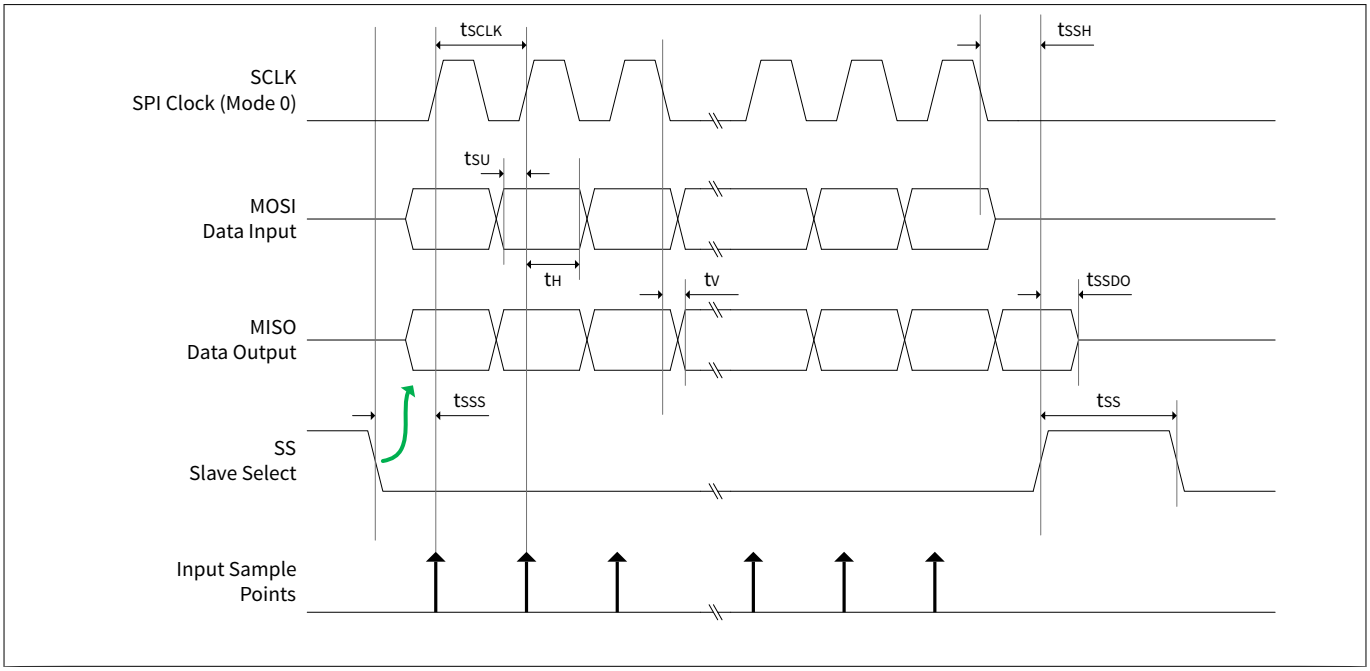


**Figure 7 SPI Mode 0**

*Note: A detailed timing diagram is shown in Figure 8 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 continues...)**

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

| 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 $0.6 * V_{CC}$ |

**(table continues...)**

**Table 15 (continued) 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. | | |
| SS inactive time | $t_{SS}$ | 30 | – | – | ns | For 3.3 V supply voltage range |
| | | 60 | – | – | ns | For 1.8 V supply voltage range |
| SS setup time | $t_{SSS}$ | 30 | – | – | ns | For 3.3 V supply voltage range:<br>Setup time SS to SCLK rising edge. |
| | | 60 | – | – | ns | For 1.8 V supply voltage range:<br>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:<br>Output valid delay time from SS active |
| | | – | – | 58 | ns | For 1.8 V supply voltage range:<br>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<br>Output valid delay time from SCLK falling edge<br>SCLK input $t_{slew}$ = 1 V/ns<br>MISO $C_{load}$ = 30 pF |
| | | – | – | 15 | ns | For 3.3 V supply voltage range<br>Output valid delay time from SCLK falling edge<br>SCLK input $t_{slew}$ = 1 V/ns<br>MISO $C_{load}$ = 30 pF |
| MISO output disable time | $t_{SSDO}$ | 0 | – | 30 | ns | For 3.3 V supply voltage range:<br>Output disable time from SS inactive |
| | | 0 | – | 60 | ns | For 1.8 V supply voltage range:<br>Output disable time from SS inactive |

**(table continues...)**

**Table 15 (continued) 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. | | |
| MISO hold time | $t_{HO}$ | 3.5 | – | – | ns | For 1.8 V supply voltage range<br>Output hold time to SCLK falling edge<br>SCLK input $t_{slew}$ = 4 V/ns<br>MISO $C_{load}$ = 10 pF |
| | | 1.5 | – | – | ns | For 3.3 V supply voltage range<br>Output hold time to SCLK falling edge<br>SCLK input $t_{slew}$ = 4 V/ns<br>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.*

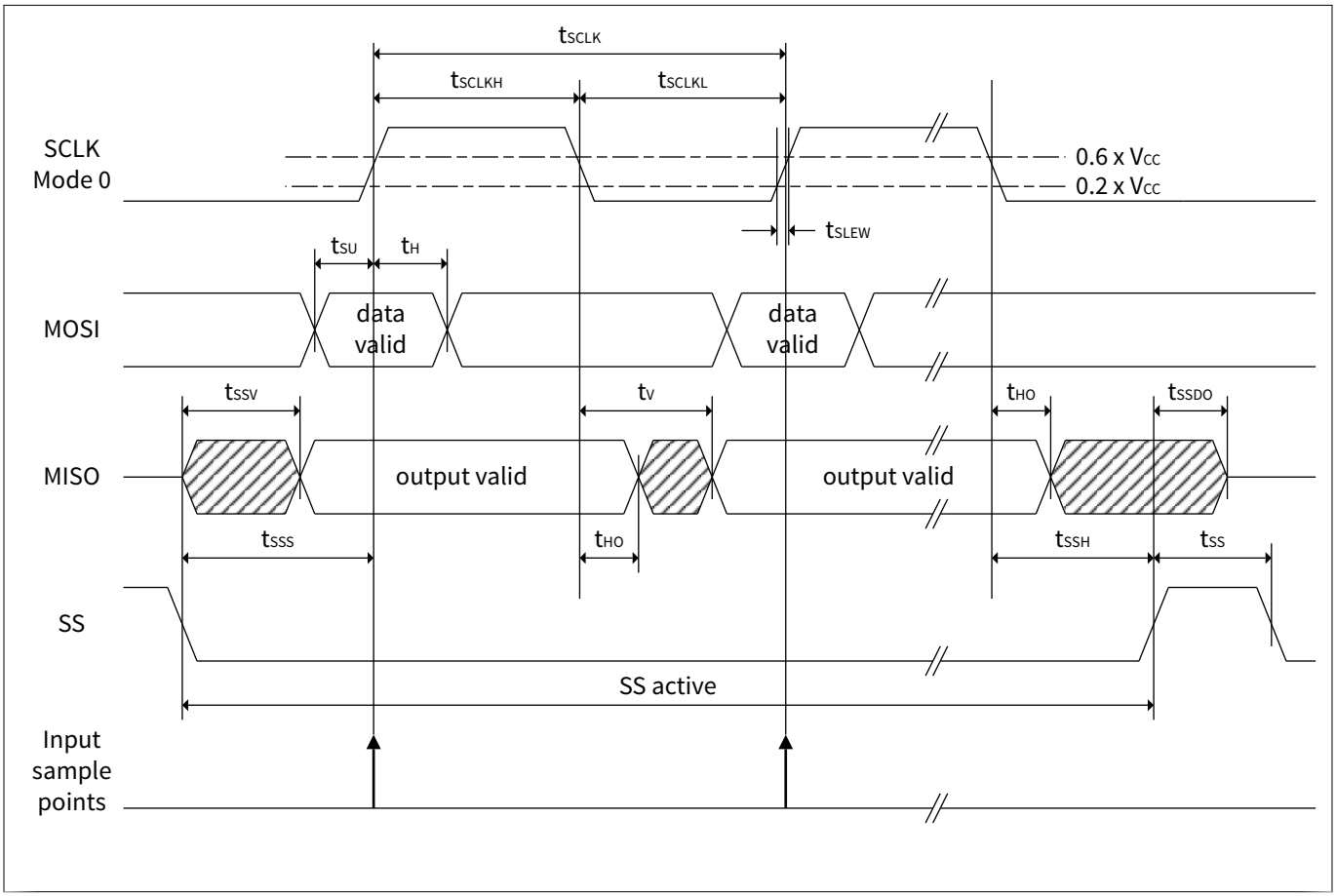


**Figure 8 Timing diagram Mode 0**

## 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 self-heating 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 (Barcode 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.

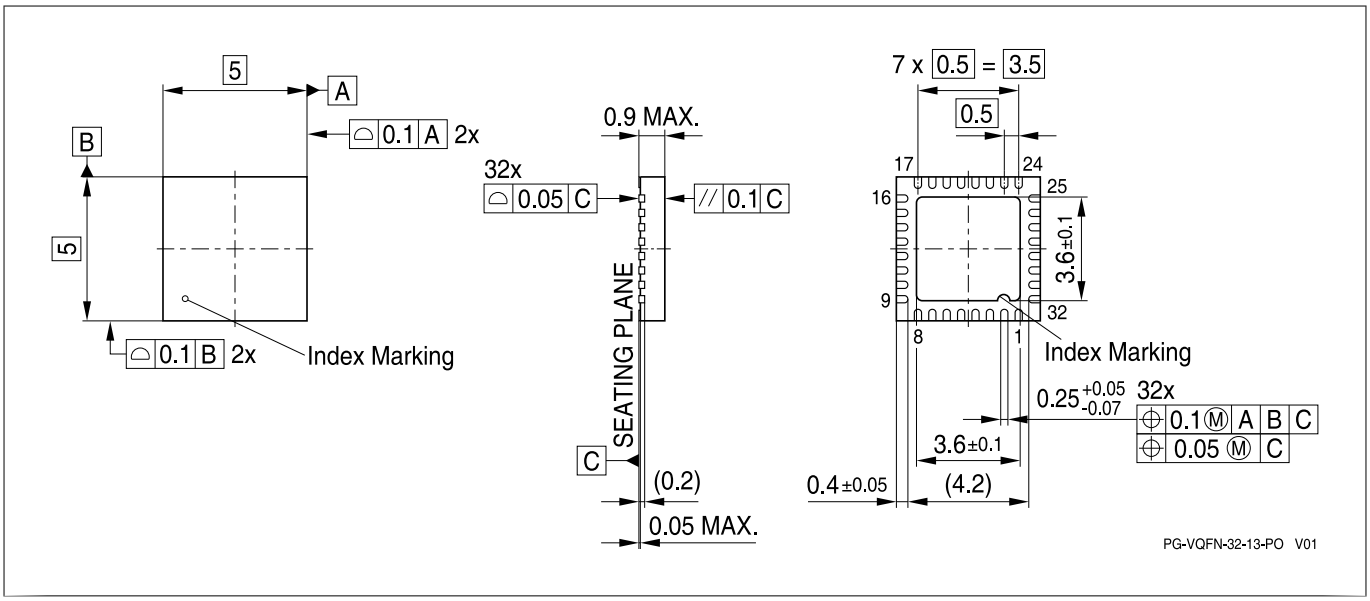


**Figure 9 PG-VQFN-32-13 package outline**

### 6.1.2 Package footprint

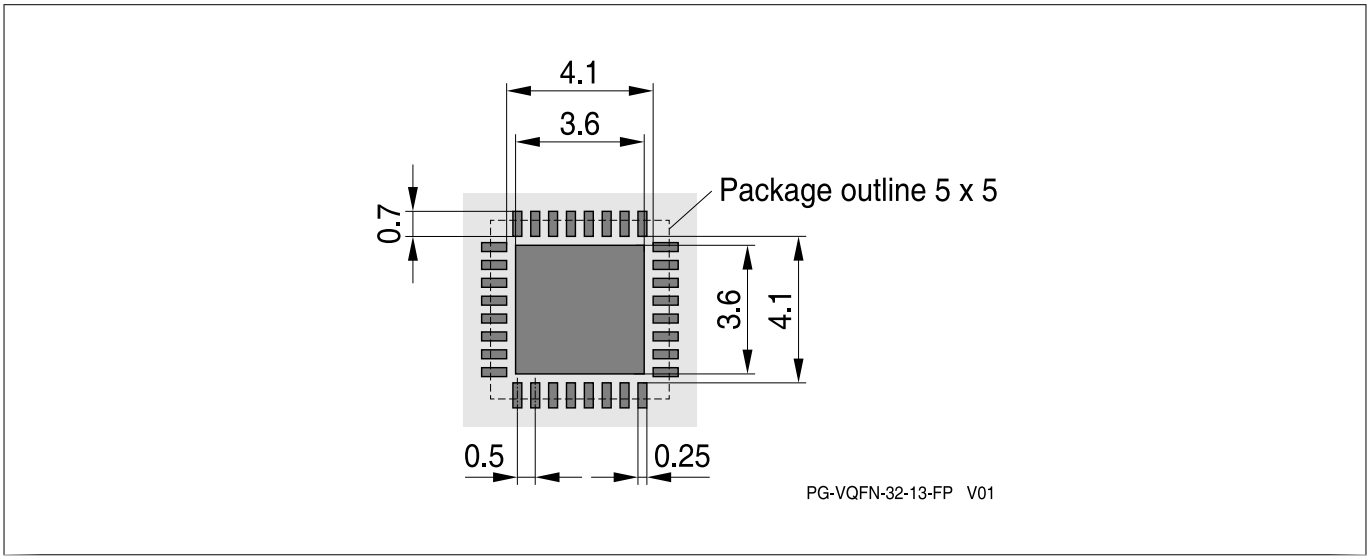


**Figure 10 PG-VQFN-32-13 package footprint**

### 6.1.3 Tape and reel packing

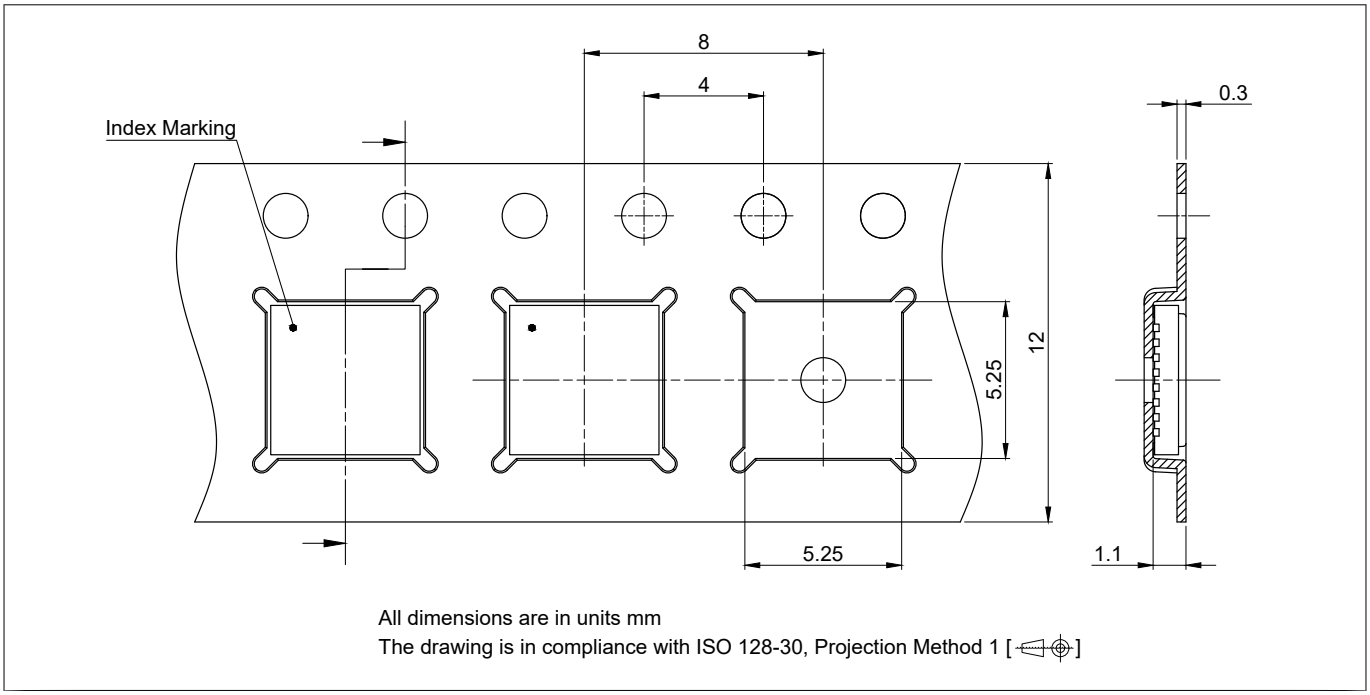


**Figure 11 PG-VQFN-32-13 tape and reel packing**

### 6.1.4 Production sample marking pattern

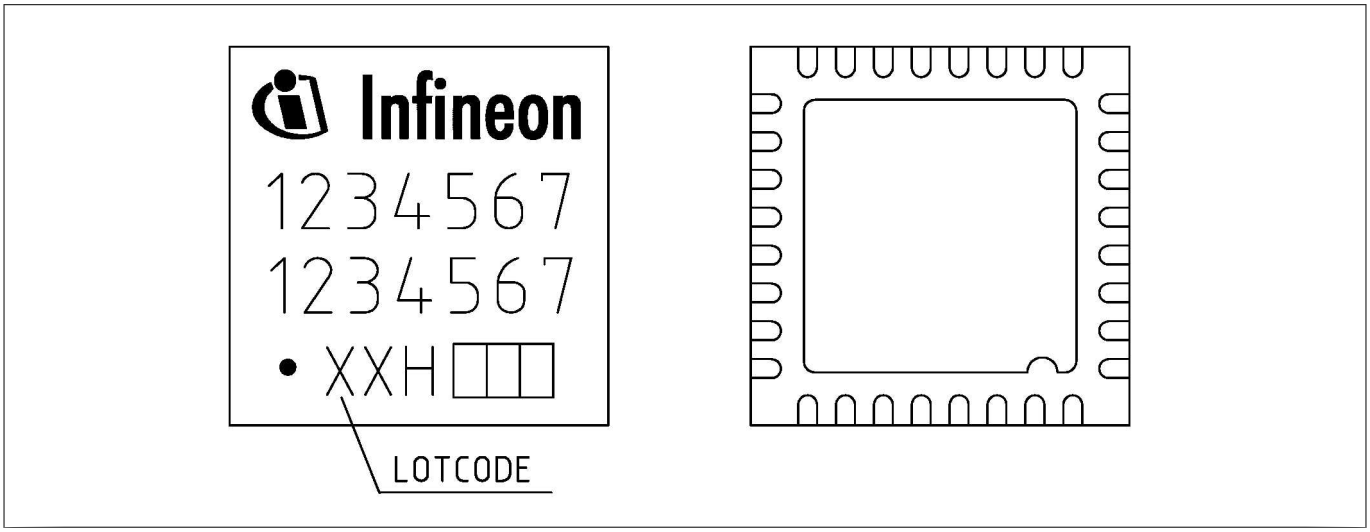


**Figure 12 PG-VQFN-32-13 sample marking pattern**

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 |
| SLS37TC (line 2) | Abbreviation for sales code SLS37CSAE20TC |
| OTCXXXA (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]** NIST FIPS 186-4: *Digital Signature Standard (DSS)*, July 2013
**[6]** RFC 2119: Bradner, Scott. "Key words for use in RFCs to Indicate Requirement Levels." RFC2119 (1997) https://tools.ietf.org/rfc/rfc2119.txt.
**[7]** Wireless Power Consortium: *Qi Specification – Authentication Protocol ( Version 1.3.1, Working Draft 1)*, January 2021

# Glossary

| | |
|---|---|
| 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 |
| BPL | Barcode Product Label |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| CA | Certificate Authority |
| CAD | Computer-Aided Design |
| CC | Common Criteria |
| CDM | Charged-Device Model |
| CMAC | Cipher-based Message Authentication Code |
| CMOS | Complementary Metal–Oxide–Semiconductor |
| CPHA | Clock Phase |
| CPOL | Clock Polarity |
| CPU | Central Processing Unit |
| CRC | Cyclic Redundancy Check |
| DC | Direct Current |
| DNC | Do Not Connect |
| EAL | Evaluation Assurance Level |
| ECC | Elliptic Curve Cryptography |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| ESD | Electrostatic Discharge |
| GND | Ground |
| GP | GlobalPlatform |
| GPIO | General Purpose Input Output |
| HBM | Human Body Model |
| HSM | Hardware Security Module |
| I/O | Input/Output |
| I2C | Inter-Integrated Circuit |
| IBIS | Input/Output Buffer Information Specification |
| IC | Integrated Circuit |

| | |
|---|---|
| IEC | International Electrotechnical Commission |
| IMM | Interface Management Module |
| IRQ | Interrupt Request |
| ISO | International Organization for Standardization |
| ISS | Instruction Stream Signature |
| MAC | Message Authentication Code |
| MED | Memory Encryption Device |
| MISO | Master In Slave Out |
| MOSI | Master Out Slave In |
| MPU | Memory Protection Unit |
| NCI | Not Connected Internally |
| NIST | National Institute of Standards and Technology |
| NVIC | Nested Vector Interrupt Control |
| NVM | Non-Volatile Memory |
| OEM | Original Equipment Manufacturer |
| PCB | Printed Circuit Board |
| PKI | Public Key Infrastructure |
| PP | Protection Profile |
| PPAP | Production Part Approval Process |
| PRNG | Pseudo Random Number Generator |
| PWR | Power |
| RAM | Random Access Memory |
| RFC | Request For Comments |
| RFU | Reserved for Future Use |
| RNG | Random Number Generator |
| ROM | Read-Only Memory |
| RST | Reset |
| SCLK | Serial Peripheral Interface Clock |
| SCP | Symmetric Co-Processor |
| SCP03 | Secure Channel Protocol 03 |
| SMD | Surface-Mounted Device |
| SPI | Serial Peripheral Interface |
| SS | Slave Select |
| TRNG | True Random Number Generator |
| Tx | Transmit |
| Typ | Typical |

| | |
|---|---|
| UMSLC | User Mode Security Life Control |
| VCC | Supply Voltage |
| VQFN | Very Thin Quad Flat No Leads |
| WDT | Watchdog Timer |

# Revision history

| Reference | Description |
|---|---|
| **Revision 1.0, 2023-01-20** | |
| All | 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 2023-01-20**

**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-nvm1670304102379**

**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.