OPTIGA™ Connect Consumer OC1230

Datasheet

5G-ready eSIM turnkey solution for cellular-connected consumer devices to support GSMA remote SIM provisioning (RSP)

Features

- Remote SIM provisioning (RSP) compatible with GSMA SGP.22 v2.5.0
- Multiple enabled profiles (MEP) compatible with GSMA SGP.22 v3
- Supports network technologies 3G, 4G (LTE), and 5G
- Supported network access applications: SIM, USIM, CSIM, and ISIM
- In-field OS update function
- Interoperable with worldwide commercial eSIM services following GSMA standards
- Up to 1.1 MB free memory for carrier profiles, applications, and data (additional applets integrable)
- Tiniest consumer eSIM solution with WLCSP (1.8 x 1.6 x 0.4 mm) and X2QFN20 (3.0 x 3.0 x 0.3 mm) packages
- Voltage classes: C (1.8 V), D (1.2 V)
- ETSI TS 102 221 and SPI interfaces
- Post-Quantum Cryptography ready
- Security evaluated according to the BSI-CC-PP-0100-2018 specified in GSMA SGP.25
- GSMA SAS-UP certified production process
- Temperature range: -25°C to +85°C
- Data retention: At least 10 years

Description

Infineon OPTIGA™ Connect Consumer OC1230 is an embedded universal integrated circuit card (eUICC) turnkey solution for embedded subscriber identity modules (eSIM) implementing GSMA's technical specification compatible with RSP GSMA SGP.22 v2.5.0 and MEP compatible with GSMA SGP.22 v3 for consumer mobile devices.

Potential applications

For embedding into cellular-connected mobile devices such as:

- Handsets
- Wearables
- Tablets
- Laptops

Support and services

- Design-in support for hardware and software
- End-to-end test support with the Infineon Test SM-DP+ profile server
- Support for software patches

About this document

Scope and purpose

This document describes the features, functionality and operational characteristics of OPTIGA™ Connect Consumer OC1230.

Intended audience

This document is primarily intended for OEM device integrators, system and application developers.

Table of contents

Features . . . 1
Description . . . 1
Potential applications . . . 1
Support and services . . . 2
About this document . . . 2
Table of contents . . . 3
List of tables . . . 5
List of figures . . . 6
1 Introduction . . . 7
2 eUICC OS . . . 9
2.1 GSMA eUICC framework . . . 9
2.1.1 Multiple enabled profiles (MEP) . . . 9
2.1.2 Logical secure element interfaces . . . 9
2.2 Telecom framework . . . 9
2.3 GlobalPlatform framework . . . 10
2.4 Java Card™ framework . . . 10
2.5 Android ready SE . . . 11
2.6 Patching mechanism . . . 11
2.7 Power management . . . 11
3 Java Card™ applets . . . 12
3.1 GlobalPlatform secure element access control applet . . . 12
3.2 Weaver applet . . . 12
3.3 Keymint applet . . . 12
3.4 OEM specific Java Card™ applets . . . 12
4 Security features . . . 13
5 Support and services . . . 14
5.1 Configuration and customization . . . 14
5.2 Design-in support for software . . . 14
5.2.1 Local profile assistant . . . 14
5.2.2 Patch agent . . . 14
5.2.3 Android ready SE integration . . . 14
6 Delivery forms and ordering . . . 15
6.1 SMD packages . . . 15
6.1.1 PG-X2QFN-20-1 . . . 16
6.1.2 SG-XFWLB-16-1 . . . 21

7 Electrical integration 25
7.1 Reference schematics for PG-X2QFN-20-1 25
7.2 Reference schematics for SG-XFWLB-16-1 27
8 Electrical characteristics 29
8.1 Key features 29
8.2 Absolute maximum ratings 29
8.3 Operational characteristics 29
8.3.1 DC characteristics 29
8.3.2 AC characteristics 30
8.3.2.1 Power-up guidelines 31
8.4 Interfaces 32
8.4.1 ISO 7816 interface characteristics 32
8.4.2 SPI interface characteristics 35
8.4.3 GPIO0.7 characteristics 37
8.4.3.1 GPIO0.7 as SPI interrupt (SPI IRQ) 37
8.4.3.2 GPIO0.7 as secure GPIO 38
9 Contact information 41
RoHS compliance 42
References 43
Glossary 44
Revision history 50
Disclaimer 51

List of tables

Table 1 Marking table for PG-X2QFN-20-1 packages 19
Table 2 Pinout for PG-X2QFN-20-1 20
Table 3 Marking table for SG-XFWLB-16-1 packages 23
Table 4 Pinout for SG-XFWLB-16-1 24
Table 5 Key features 29
Table 6 Absolute maximum ratings 29
Table 7 DC electrical characteristics 30
Table 8 AC electrical characteristics 30
Table 9 ISO/IEC 7816-3 card maximum ratings 32
Table 10 ISO/IEC 7816-3 card DC electrical characteristics 32
Table 11 ISO/IEC 7816-3 card DC electrical characteristics - UART_RST 33
Table 12 ISO/IEC 7816-3 card DC electrical characteristics - UART_CLK 33
Table 13 ISO/IEC 7816-3 card DC electrical characteristics - UART_IO 33
Table 14 ISO/IEC 7816-3 card AC electrical characteristics - UART_RST 34
Table 15 ISO/IEC 7816-3 card AC electrical characteristics - UART_CLK 34
Table 16 ISO/IEC 7816-3 card AC electrical characteristics - UART_IO 35
Table 17 ISO/IEC 7816-3 supported Fi/Di ratios 35
Table 18 DC characteristics 36
Table 19 AC characteristics 36
Table 20 DC characteristics for 1.8 V supply voltage range 38
Table 21 DC characteristics for 1.2 V supply voltage range 38
Table 22 AC characteristics 38
Table 23 Boot signal characteristics 39
Table 24 Secure GPIO operation supply and input voltages for (1.2 V and 1.8 V) supply voltage range 39
Table 25 Secure GPIO DC electrical characteristics 40

List of figures

Figure 1 Architecture of the OC1230 eUICC . . . 7
Figure 2 PG-X2QFN-20-1 package outline . . . 16
Figure 3 PG-X2QFN-20-1 package footprint . . . 17
Figure 4 PG-X2QFN-20-1 tape and reel packing . . . 18
Figure 5 PG-X2QFN-20-1 sample marking pattern . . . 18
Figure 6 PG-X2QFN-20-1 PIN layout . . . 19
Figure 7 SG-XFWLB-16-1 package outline . . . 21
Figure 8 SG-XFWLB-16-1 package footprint . . . 22
Figure 9 SG-XFWLB-16-1 tape and reel packing . . . 23
Figure 10 SG-XFWLB-16-1 sample marking pattern . . . 23
Figure 11 SG-XFWLB-16-1 PIN layout . . . 24
Figure 12 Reference schematics for PG-X2QFN-20-1 ISO + SPI + SPI IRQ . . . 25
Figure 13 Reference schematics for PG-X2QFN-20-1 ISO + SPI + SPI IRQ . . . 26
Figure 14 Reference schematics for PG-X2QFN-20-1 ISO + SPI + SECURE GPIO . . . 26
Figure 15 Reference schematics for SG-XFWLB-16-1 ISO only . . . 27
Figure 16 Reference schematics for SG-XFWLB-16-1 ISO + SPI + SPI IRQ . . . 28
Figure 17 Reference schematics for SG-XFWLB-16-1 ISO + SPI + SECURE GPIO . . . 28
Figure 18 Recommended power-up behavior . . . 31
Figure 19 Secure GPIO timing diagram . . . 39

1 Introduction

The OPTIGA™ Connect Consumer OC1230 eUICC is Infineon's next generation of embedded subscriber identity modules (eSIM) implementing GSMA's technical specification SGP.22 [16] for mobile consumer devices.

The main purpose of the OC1230 eUICC is to provide secure network authentication to a selected and subscribed carrier network. The OC1230 allows changing and adding of carrier profiles in full compliance to GSMA eSIM specifications. With up to 1.1 MB of free user memory, the OC1230 has ample space for multiple carrier profiles as well as additional applications and user data.

The OC1230 is a certified and tested solution:

- GSMA SAS-UP certified production process [18]
- GSMA eUICC functional compliant [15] [16]
- GSMA eSA security certified
- Common Criteria certified according to protection profile PP-0100 [17]
- Java Card™ functional compliant [25] [26]

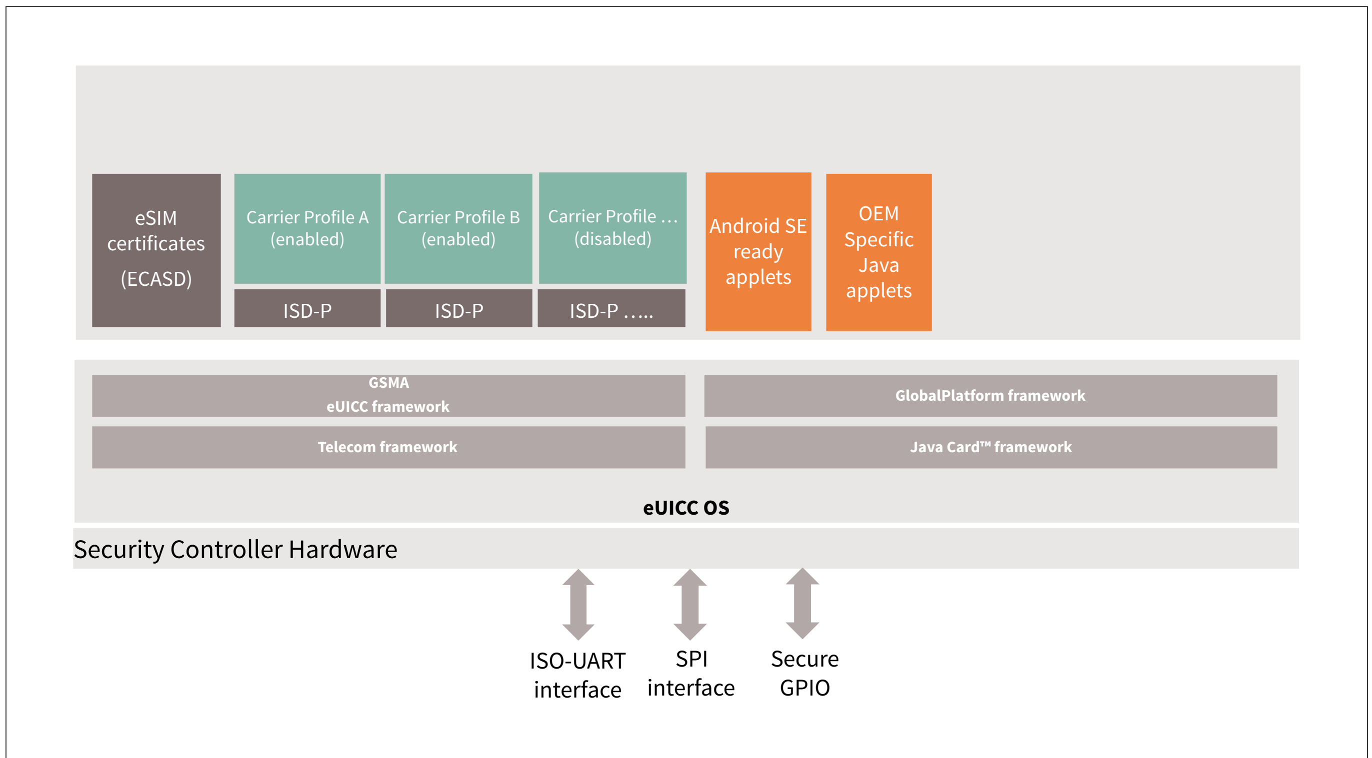

Figure 1 Architecture of the OC1230 eUICC

The OC1230 eUICC is a system composed of secure software and hardware. The eUICC OS resides on a security controller and forms a platform allowing to host carrier profiles, applications, and data.

The eUICC OS provides all services and features that make up the essence of an eUICC, respectively eSIM:

- GSMA eUICC framework to support remote SIM provisioning (RSP)
- A telecommunication framework with network access applications (NAAs), network authentication algorithms, file system services, and services for remote file management (RFM) and remote application management (RAM)

The eUICC OS serves as a foundation for user applications:

- The OS implements a comprehensive GlobalPlatform (GP) framework to allow for secure and interoperable application deployment
- The OS implements the Java Card™ platform, including virtual machine, runtime environment, and APIs, to support the execution of user applications in the format of Java Card™ applets

The capability to host Java Card™ applets allows to tailor the OC1230 for different use cases. The OC1230 is capable of securely storing sensitive data such as end-user credentials, consumer device configurations, cryptographic keys, certificates, and others.

Further, the OS cares for efficient power management and provides a patching mechanism that allows for applying OS updates in the field.

The OC1230 eUICC supports the following interfaces:

- ISO/IEC 7816-3 interface (conforming with ETS 102 221 [1]), to connect a baseband controller
- SPI interface, to connect an application processor
- Secure GPIO mechanism, to support Android secure boot

2 eUICC OS

2.1 GSMA eUICC framework

The OC1230 supports the following key features to support GSMA remote SIM provisioning:

- Compliance with GSMA SGP.22 v2.5.0 [16]
- Support for local profile assistant in the consumer mobile device (LPAd)
- Multiple Enabled Profiles (MEP), option MEP-B, according to GSMA SGP.22 v3 [16]
- eSIM ports, according to GSMA SGP.22 v3 [16], aka logical secure element interfaces (LSI)
- TCA profile package interoperable [24] (backward compatible with [23])
- Multiple public key certificate issuers (PK CI)
- EC domains NIST-P256 and brainpoolP256r1
- Profile metadata tag BF76

2.1.1 Multiple enabled profiles (MEP)

The OC1230 supports multiple enabled profiles in compliance with GSMA SGP.22 v3.

If supported by the connected baseband controller, the OC1230 allows to enable up to 2 carrier profiles to establish up to 2 cellular connections at the same time. Multiple enabled profiles correspond to dual-SIM capability as known from classic SIM legacy.

2.1.2 Logical secure element interfaces

Supporting multiple enabled profiles (MEP) requires the multiplexing of the APDU streams from an MEP-capable mobile device to concurrently enabled carrier profiles on a single physical interface. This ability is described by the ETSI (ETSI TS 102 221 [1]) as “logical secure element interface (LSI)”, and by the GSMA SGP.22 v3 as “eSIM port”. An “LSI” or “eSIM port” allows the mobile device to address a dedicated carrier profile on the eSIM.

The OC1230 supports the following mechanisms to address eSIM ports (respectively LSIs):

- For T=0, T=1, and T=1’: Via the APDU command MANAGE LSI
- For T=1 and T=1’: Via the NAD byte

For the selection of the ISD-R and the assignment of eSIM ports, the OC1230 supports option “MEP-B” of the GSMA SGP.22 v3 specification.

2.2 Telecom framework

The OC1230 OS offers a comprehensive telecom framework for supporting several network technologies, including 3G, 4G (LTE), and 5G. It also provides support for various network applications and authentication and key agreement algorithms.

Some of the key features supported by the telecom framework are:

- Compliance with network technologies, including 3G, 4G (LTE), and 5G
- Access to network applications, such as USIM, CSIM, and ISIM
- Authentication and key agreement algorithms, including:
    - Comp 128-2/3
    - MILENAGE (comp 128-4)

  - TUAK
  - CAVE
- 5G subscriber concealed identity (SUCI) protection scheme with on-chip SUCI generation, including a SUCI API
  - ECIES scheme, Profile A
  - ECIES scheme Profile B
  - Null scheme
- Remote applet management (RAM) and remote file management (RFM)
- Over-the-air (OTA) services via CAT_TP and HTTP
- Re-size files
- BER-TLV files
- High update activity supported for all files

2.3 GlobalPlatform framework

The OC1230 OS is compliant to the following GlobalPlatform standards:

- GlobalPlatform: Technology Card Specification, v2.3.1
- GlobalPlatform CIC: Card Common Implementation Configuration, v2.1
- GlobalPlatform UICC: UICC Configuration, v2.0
- GlobalPlatform Amdment A: Confidential Card Content Management Card Specification, v1.2
- GlobalPlatform Amendment B: Remote Application Management over HTTP Card Specification, v1.2
- GlobalPlatform Amendment C: Contactless Services Card Specification, v1.3
- GlobalPlatform Amendment D: Secure Channel Protocol 03 Card Specification, v1.0
- GlobalPlatform Amendment F: Technology Secure Channel Protocol '11' Card Specification, v1.3
- GlobalPlatform Amendment H: Executable Load File Upgrade Card Specification, v1.1
- GlobalPlatform SEAC: Device Technology Secure Element Access Control, v1.1
- GlobalPlatform APDU: APDU Transport over SPI/I2C, v1.0
- GlobalPlatform API: Card API - org.globalplatform, v1.7
- GlobalPlatform APIUPG: Card API - ELF Upgrade API org.globalplatform.upgrade, v1.1

2.4 Java Card™ framework

The OS implements a Java Card™ framework, that is compliant with the following standards:

- JCRE: Java Card™ runtime environment specification, Java Card™ platform classic edition v3.1
- JCVM: Java Card™ virtual machine specification, Java Card™ platform classic edition v3.1
- JCAPI: Java Card™ application programming interface, Java Card™ platform classic edition v3.1

The OS supports extended-length application protocol data units (APDUs) as defined in ISO/IEC 7816-4 [22], for Java Card™ applets that implement the Java Card™ interface `javacardx.apdu.ExtendedLength`. Extended-length APDUs are supported through both UART and SPI communication interfaces. The extended length APDUs allow for larger APDUs than the standard length of 256 bytes, enabling more data to be transferred in a single APDU exchange. This can be particularly beneficial for certain types of applications, such as those involving large data sets or files.

The OS also supports a large selection of standard and optional Java Card™ API packages. The APIs enable various functionalities such as cryptography, secure messaging, and key management, among others, to be implemented in Java Card™ applets running on the device. The standard APIs are mandated by the Java Card™

specifications, while the optional APIs provide additional functionality that can be used to extend the capabilities of Java Card™ applets beyond the standard features.

The Java Card™ applets can either reside on the OC1230 as an integral part of a carrier profile, or as so-called "transversal" applets, which are separate and independent from any carrier profile.

2.5 Android ready SE

The OC1230 supports the security architecture defined by Google for Android devices in the context of the Android ready SE program.

2.6 Patching mechanism

The OC1230 implements a patching mechanism that allows for applying OS patches remotely, when the product is already in the field. The patching mechanism is designed to minimize any potential interferences with the consumer device, guaranteeing the best possible user experience.

2.7 Power management

The OC1230 supports power management in order to conserve energy and improve the overall efficiency of the consumer device.

When the OC1230 is powered up, the OS checks if the ISO 7816 or the SPI interface have been activated.

- The ISO 7816 interface will get activated by active handling of the ISO-RST line in accordance to ISO/IEC 7816-3
- The SPI interface will get activated on assertion of the slave select signal

If no interface has been activated, the OS will switch the OC1230 to idle state. The idle state is left by command reception via:

- ISO 7816 interface
- SPI interface

The OC1230 re-enters the idle state after the transmission of the last response.

3 Java Card™ applets

Infineon offers a variety of Java Card™ applets for the OC1230.

3.1 GlobalPlatform secure element access control applet

The SEAC applet is used to manage and control the access of consumer device apps to the eSIM.

3.2 Weaver applet

Google Weaver is a secure inter-process communication (IPC) mechanism that is used to protect sensitive data in an Android-based mobile device OS. Weaver allows Android apps to communicate with each other securely, while preventing other Android apps or the Android OS from accessing the data.

3.3 Keymint applet

Google Keymint is a module within Android's security architecture that is responsible for managing the secure storage of cryptographic keys. It is designed to provide a hardware-backed keystore solution, allowing for secure storage and retrieval of keys.

3.4 OEM specific Java Card™ applets

The OC1230 allows to host OEM-specific applets, either loaded by the OEM via GlobalPlatform compliant content management means or preloaded by Infineon.

4 Security features

The OC1230 OS supports state-of-the-art security features:

- Security evaluated according to the BSI-CC-PP-0100-2018 specified in GSMA SGP.25 [17]
- GSMA SAS-UP certified production process
- All security-relevant methods are DPA/SPA/DFA-secured
- ANSI X9.17 software secure random number generator
- RSA coprocessor for RSA cryptography
- Post-quantum cryptography ready
- Secure GPIO mechanism

5 Support and services

5.1 Configuration and customization

The OC1230 can be configured in various ways and provides the option for individual customization, as follows:

- Preloading of test profiles
- Preloading and preinstallation of applets

Preloaded and preinstallation of content will be considered during the product configuration phase. The content will be added during Infineon's production process. This is a service that enables customers to have easy access to useful features right from the start, eliminating the need for later downloads and installations.

Further, Infineon's production process allows for chip individual diversification with respect to dedicated data elements.

5.2 Design-in support for software

Infineon offers a selection of reference software components, which allows for easy and seamless integration of the OC1230 into consumer devices. The reference software is available for host device architectures, based on the Android open source platform (AOSP) and Microsoft Windows.

5.2.1 Local profile assistant

Example implementations are provided to demonstrate the functionality of a local profile assistant (LPA). The LPA is responsible for profile management (for example, download, activation, and removal). Profile download can be demonstrated by using an activation code to retrieve a test profile from an SM-DP+ server.

Information of the available profiles and the eSIM details for example eID and supported specification versions and supported PKI IDs can be displayed in the user interface.

Depending on the host device architecture, either available system APIs are used or the required modules are delivered as part of the LPA SDK package.

5.2.2 Patch agent

The patch agent can be used to deploy in-field updates for the eSIM firmware. The example projects showcase the integration of the supplied libraries into an OEM application.

On the Android platform, this application would run as a system service and execute update scripts transparent to the user.

5.2.3 Android ready SE integration

Android ready SE provides native support for generic communication with the secure element (SE). This allows the Android system, as well as third-party apps to use specialized hardware for secured data storage (for example secret keys or access rules).

The example package contains implementations for the hardware abstraction layer (HAL) to communicate with the Keymint and Weaver applets installed on the SE. A generic HAL for low-level communication with the SE is also provided.

6 Delivery forms and ordering

This chapter provides information about available delivery forms and how the product's interfaces are assigned to the package pins.

6.1 SMD packages

The following packages are available:

- PG-X2QFN-20-1
- SG-XFWLB-16-1

The figures in the sections below show the following aspects of the package:

- **Package outline:** It shows the package dimensions of the device in the individual packages
- **Package footprint:** It shows footprint recommendations
- **Tape and reel packing:** It shows device orientation in the tape with pin or index marking
- **Sample marking pattern:** It describes the productive sample marking pattern on the package
- **Package layout:** It shows a simple layout with the pin numbers described in the pin-to-signal reference section

***Notes**:*

1. *The drawings are for information only and not drawn to scale. More detailed information about the package characteristics and assembly instructions are available on request.*

2. *Unless specified otherwise, all figure dimensions are given in mm.*

6.1.1 PG-X2QFN-20-1

Package outline

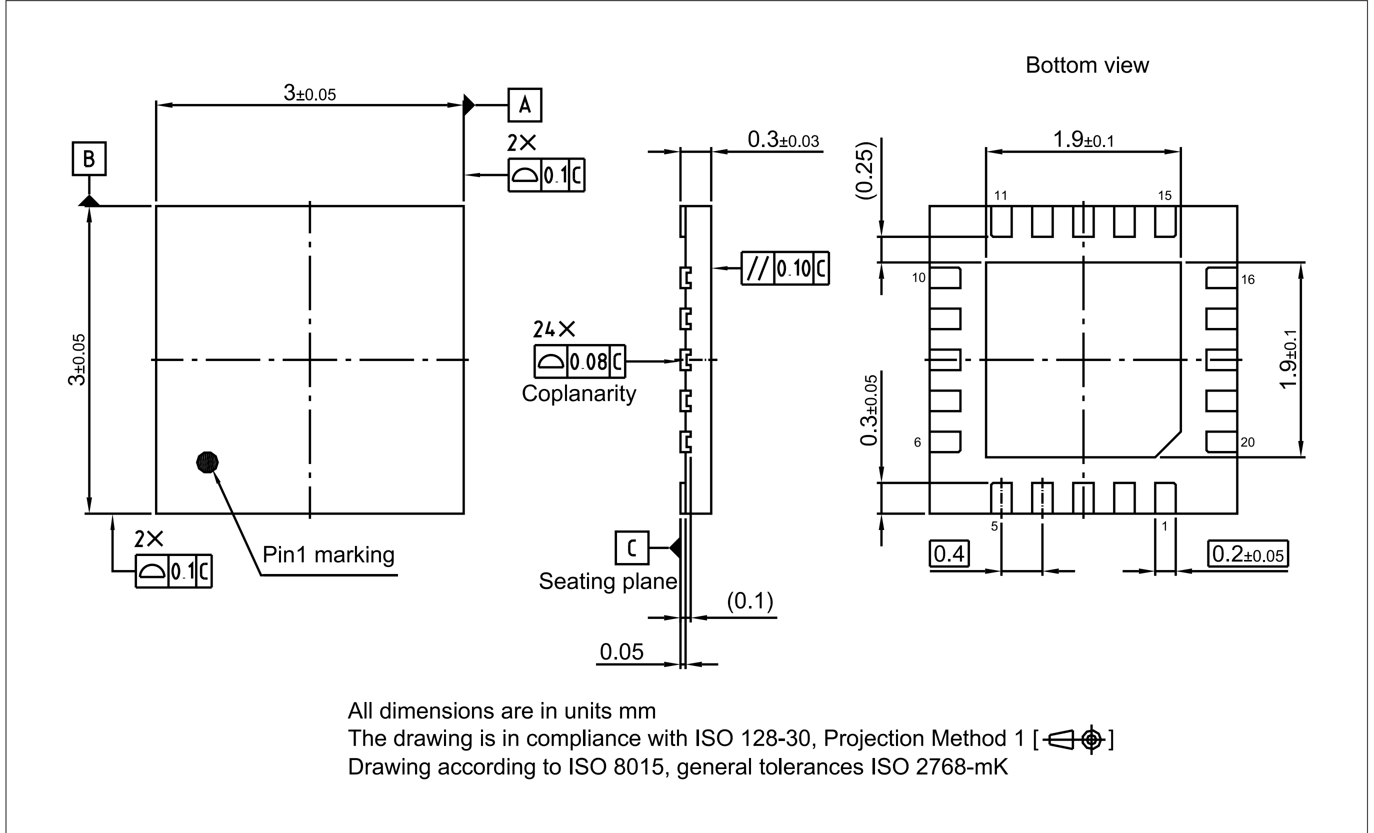

Figure 2 **PG-X2QFN-20-1 package outline**

Package footprint

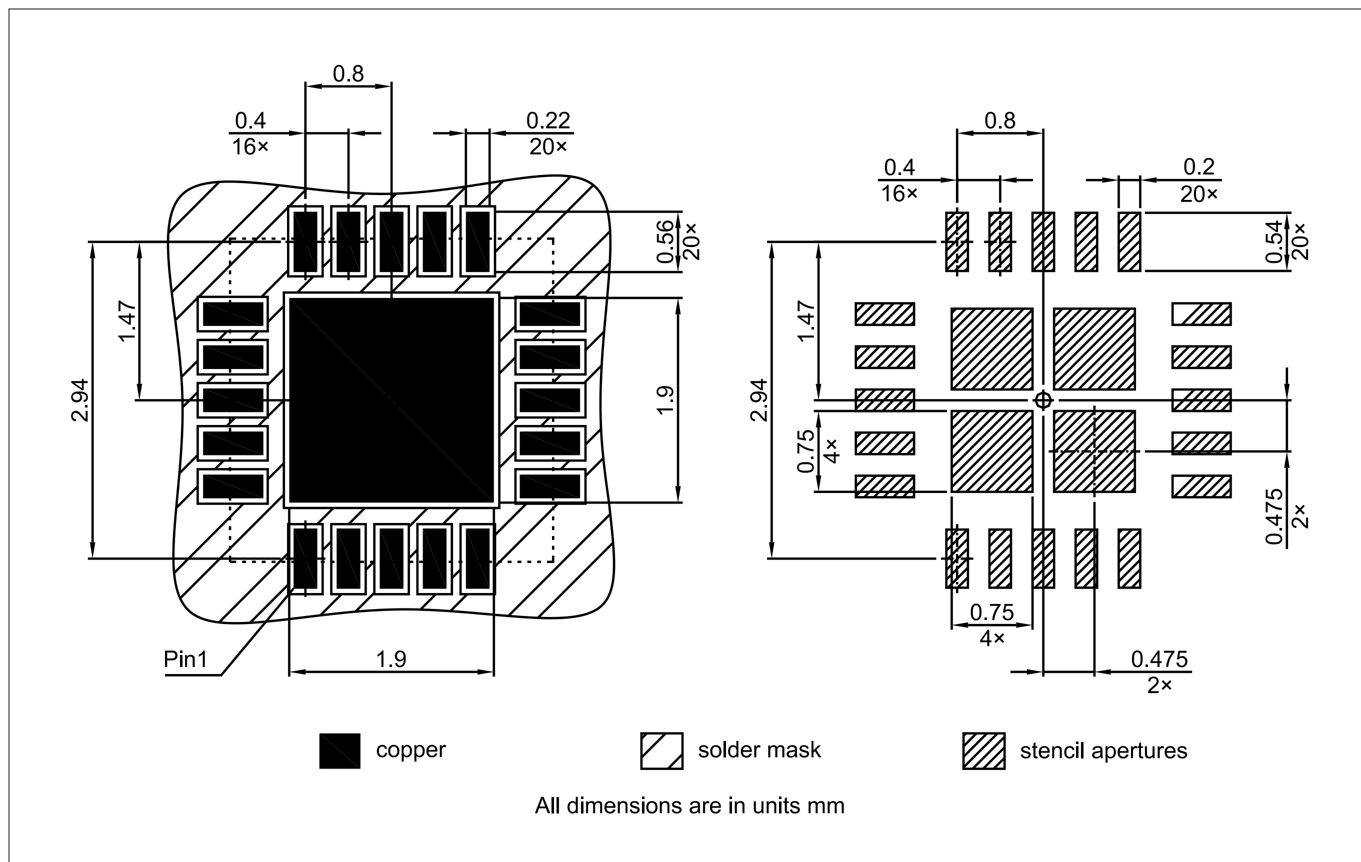

Figure 3 **PG-X2QFN-20-1 package footprint**

Tape and reel packing

Pin1 marking

8

4

0.25

5.5

12

3.25

3.25

0.5

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

Figure 4 **PG-X2QFN-20-1 tape and reel packing**

Production sample marking pattern

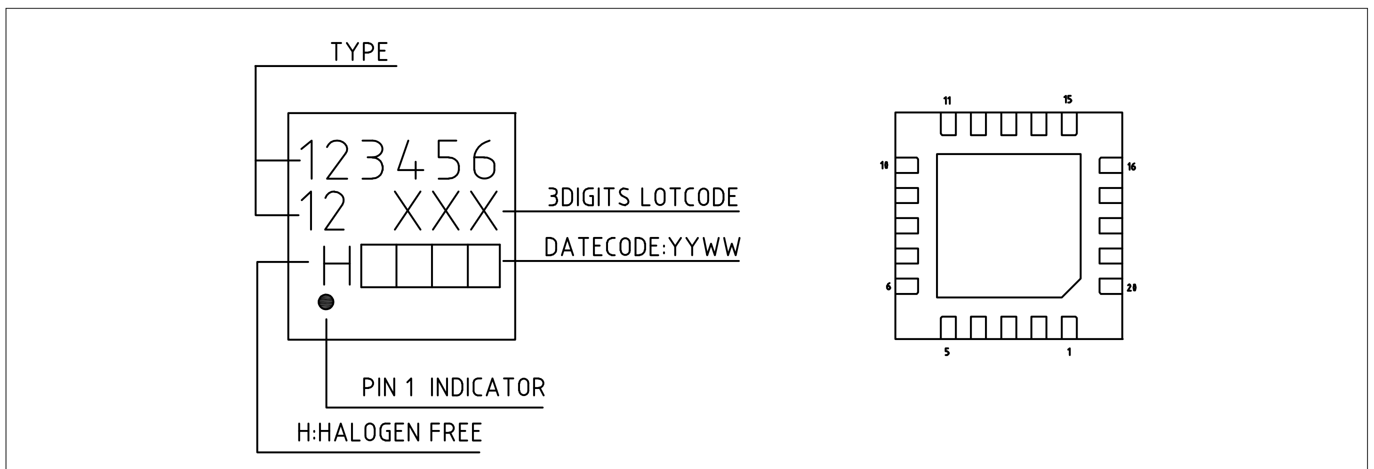

Figure 5 **PG-X2QFN-20-1 sample marking pattern**

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

Table 1 Marking table for PG-X2QFN-20-1 packages

Indicator	Description
123456 (1st line)	Type code
12 (2nd line)	Type code
XXX (2nd line)	Lot code, defined and inserted during fabrication, issued by the packaging site
H□□□□	Engineering samples: “HE<YWW>”: • Halogen-free • Engineering Sample • <YY>: 2nd digit of production year • <WW>: Production week Qualified production parts: “H<YYWW>”: • Halogen-free • <YY>: Production year • <WW>: Production week

PIN layout

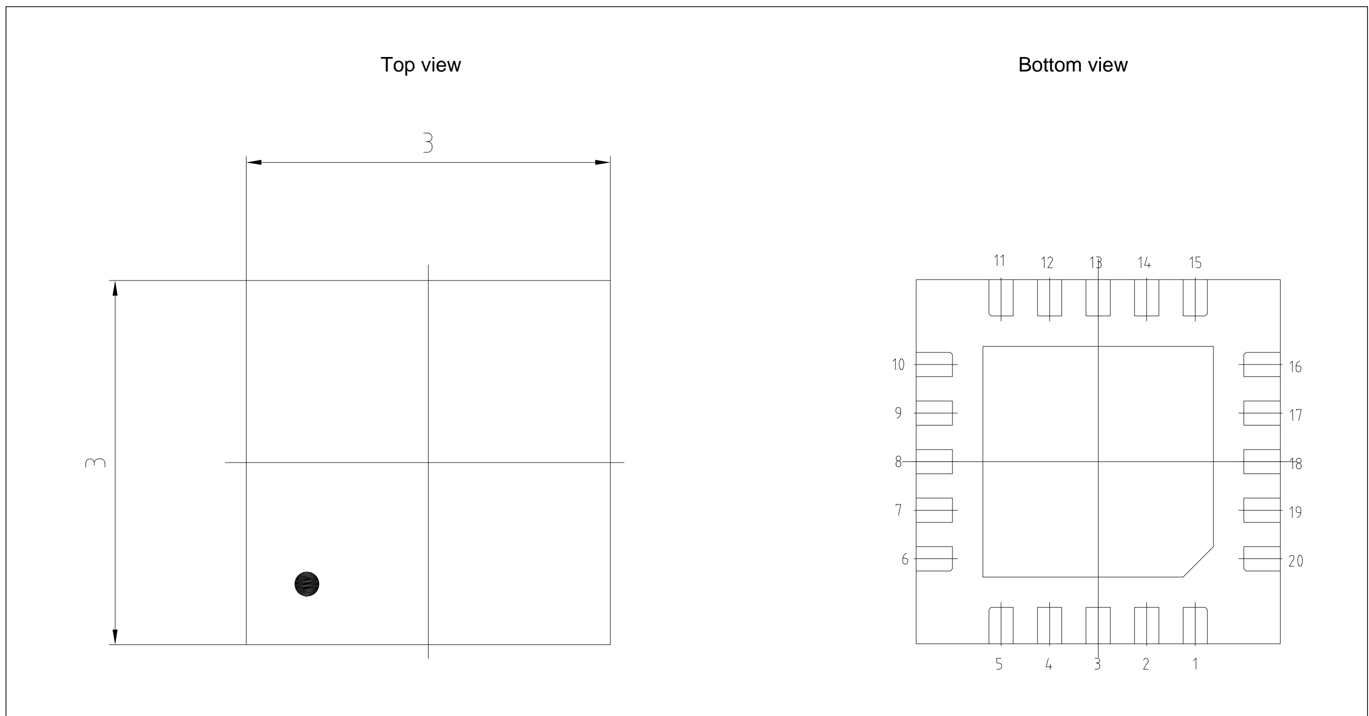

Figure 6 PG-X2QFN-20-1 PIN layout

***Note**: It is recommended to connect the exposed die pad to the common ground reference (GND) for heat distribution.*

Pad-to-signal reference

Table 2 Pinout for PG-X2QFN-20-1

Pin no.	Name	Pin type	Function
1	NC	NA	No internal connection
2	RFU	NA	Do not connect
3	ISO_IO	I/O	ISO7816-3 IO signal
4	NC	NA	No internal connection
5	V_{DD}	PWR	**Power supply**: V_{DD}
6	V_{SS}	GND	**Power supply**: Common ground reference
7	V_{DD}	PWR	**Power supply**: V_{DD}
8	V_{SS}	GND	**Power supply**: Common ground reference
9	GPIO0.7	OUT	If OC1230 is configured to support the SPI interrupt, then this pin acts as an SPI interrupt (SPI IRQ) signal. Do not connect if not used
		IN	If OC1230 is configured to support the secure boot mechanism, then this pin acts as a secure GPIO signal. Do not connect if not used
10	SPI_MISO	OUT	SPI slave data output signal; do not connect if not used
11	V_{DD}	PWR	**Power supply**: V_{DD}
12	NC	NA	No internal connection
13	ISO_CLK	IN	ISO/IEC 7816-3 clock signal
14	ISO_RST	IN	ISO/IEC 7816-3 reset signal
15	SPI_CLK	IN	SPI clock signal; connect to V_{DD} if not used
16	SPI_MOSI	IN	SPI slave data input signal; connect to V_{DD} if not used
17	SPI_SS	IN	SPI slave select signal; connect to V_{DD} if not used
18	V_{DD}	PWR	**Power supply**: V_{DD}
19	V_{SS}	GND	**Power supply**: Common ground reference
20	NC	NA	No internal connection

6.1.2 SG-XFWLB-16-1

Package outline

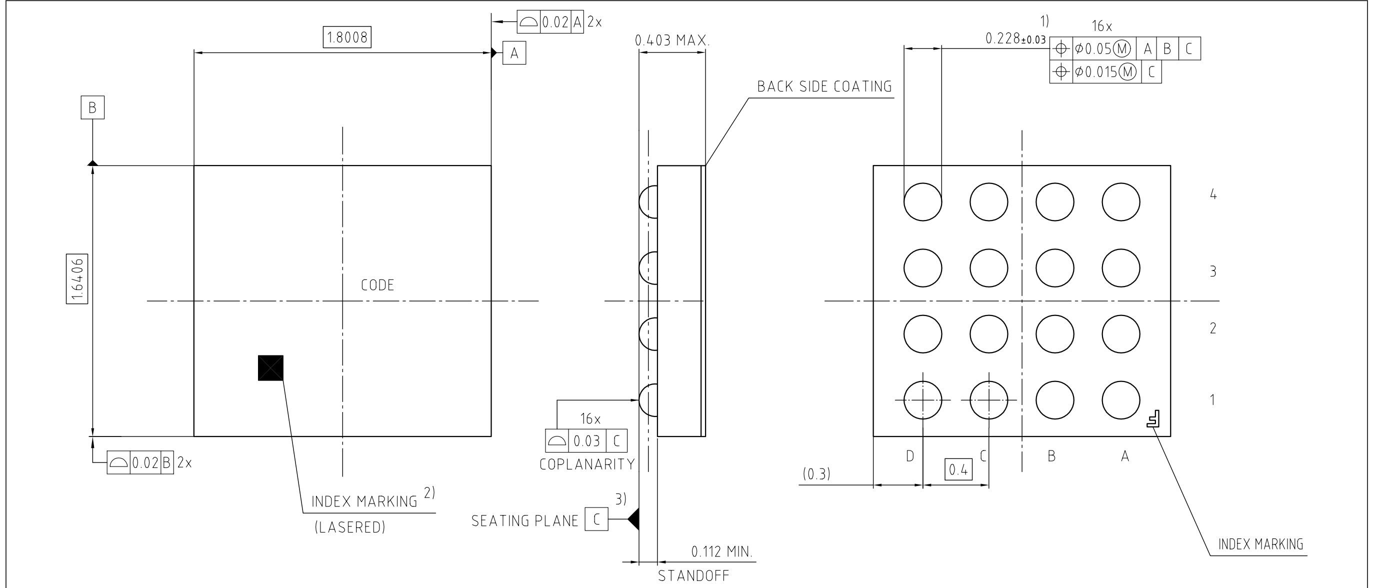

Figure 7 **SG-XFWLB-16-1 package outline**

Package footprint

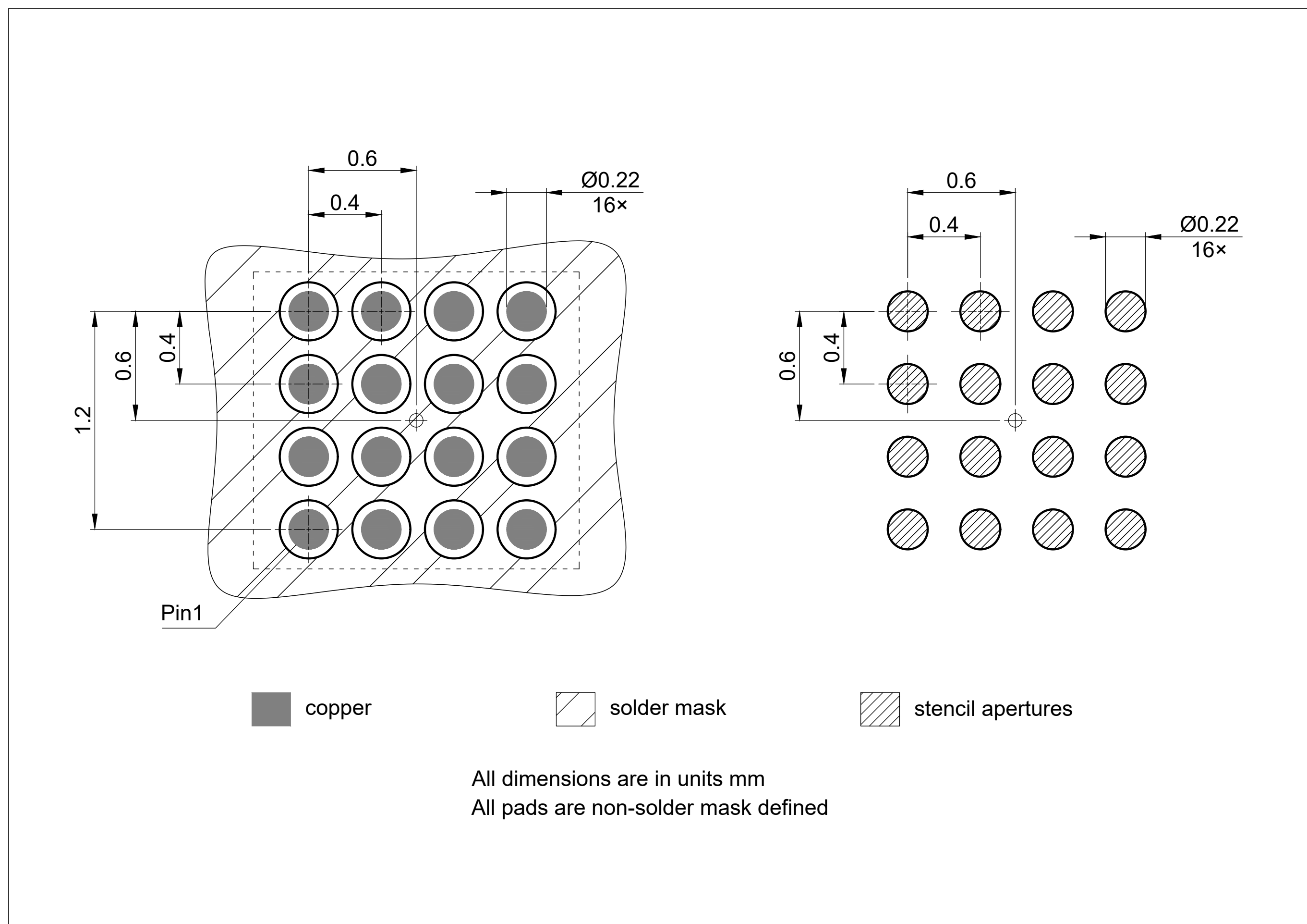

Figure 8 SG-XFWLB-16-1 package footprint

Tape and reel packing

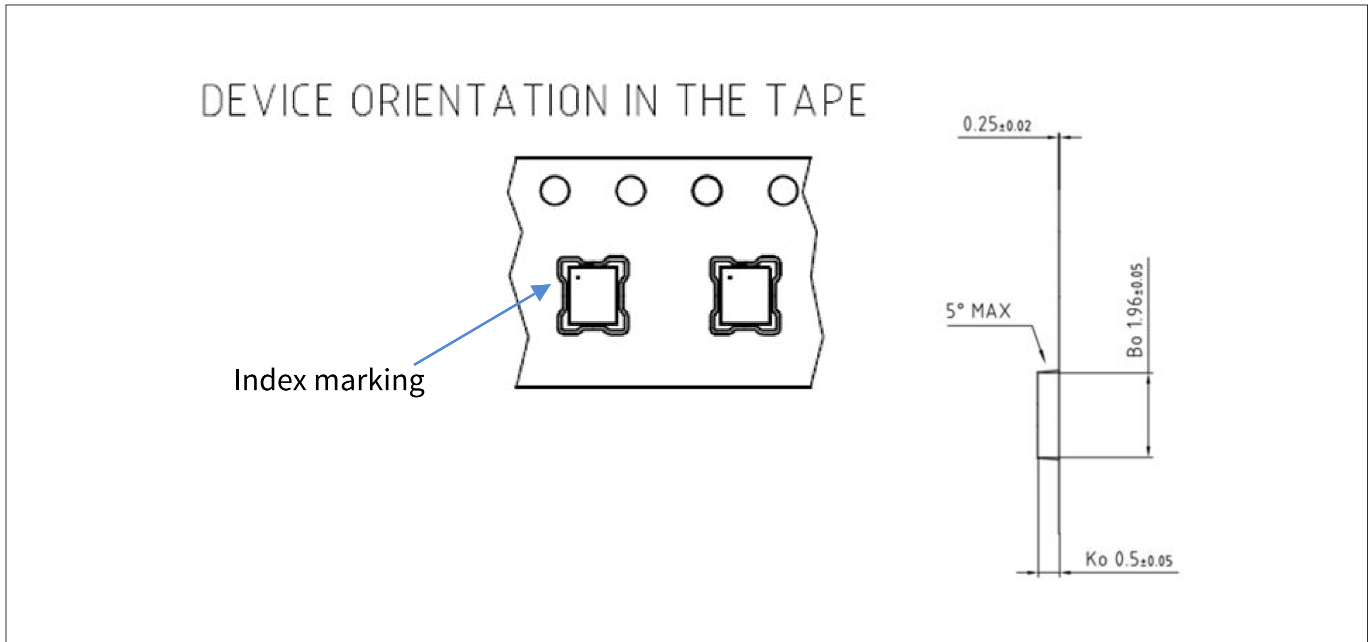

Figure 9 SG-XFWLB-16-1 tape and reel packing

Production sample marking pattern

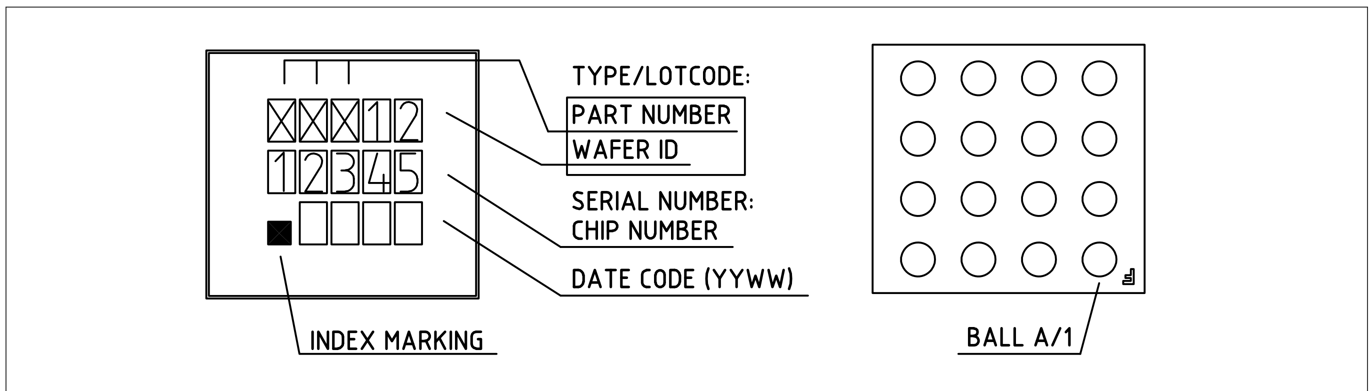

Figure 10 SG-XFWLB-16-1 sample marking pattern

The square indicates ball A/1 for the chip.

Table 3 Marking table for SG-XFWLB-16-1 packages

Indicator	Description
XXX (1st line)	Lot code, defined and inserted during fabrication, issued by the packaging site
12 (1st line)	Type code
12345 (2nd line)	Serial number, defined and inserted during fabrication, issued by the packaging site
□□□□	Date code: “YYWW>”: • <YY>: Production year • <WW>: Production week

PIN layout

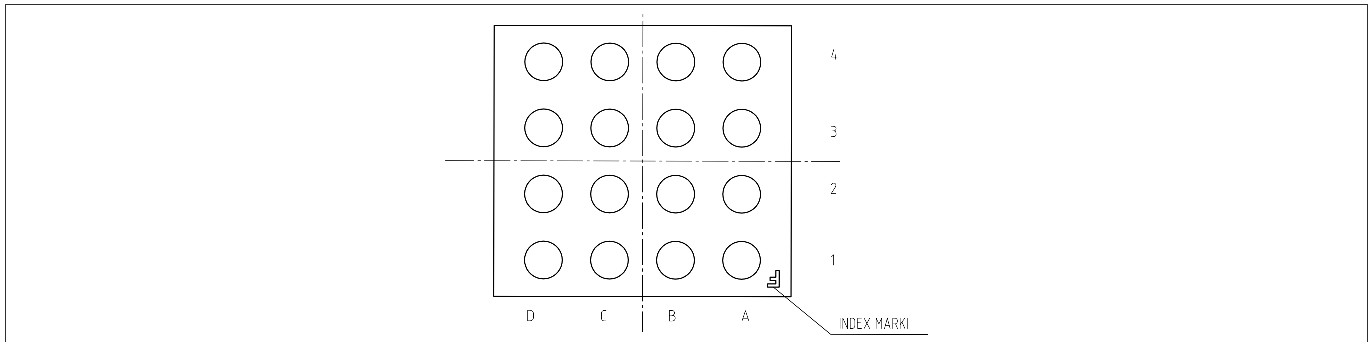

Figure 11 **SG-XFWLB-16-1 PIN layout**

Note*:* *It is recommended to connect the exposed die pad to the common ground reference (GND) for heat distribution.*

Pad-to-signal reference

Table 4 **Pinout for SG-XFWLB-16-1**

Pin no.	Name	Pin type	Function
A1	V_{DD}	PWR	**Power supply**: V_{DD}
A2	V_{SS}	GND	**Power supply**: Common ground reference
A3	GPIO0.7	OUT	If OC1230 is configured to support the SPI interrupt, then this pin acts as an SPI interrupt (SPI IRQ) signal. Do not connect if not used
		IN	If OC1230 is configured to support the secure boot mechanism, then this pin acts as a secure GPIO signal. Do not connect if not used
A4	ISO_CLK	IN	ISO/IEC 7816-3 clock signal
B1	ISO_IO	I/O	ISO/IEC 7816-3 IO signal
B2	V_{DD}	PWR	**Power supply**: V_{DD}
B3	SPI_MISO	OUT	SPI slave data output signal; do not connect if not used
B4	ISO_RST	IN	ISO/IEC 7816-3 reset signal
C1	RFU	NA	Do not connect
C2	V_{SS}	GND	**Power supply**: Common ground reference
C3	V_{DD}	PWR	**Power supply**: V_{DD}
C4	SPI_MOSI	IN	SPI slave data input signal; connect to V_{DD} if not used
D1	V_{SS}	GND	**Power supply**: Common ground reference
D2	V_{DD}	PWR	**Power supply**: V_{DD}
D3	SPI_SS	IN	SPI slave select signal; connect to V_{DD} if not used
D4	SPI_CLK	IN	SPI slave clock signal; connect to V_{DD} if not used

7 Electrical integration

This chapter provides information about the electrical integration of the product into a host device.

7.1 Reference schematics for PG-X2QFN-20-1

This chapter provides reference schematics for the OC1230 in the package type PG-X2QFN-20-1. It refers to a selection of typical use cases. For further recommendations on how to connect the OC1230, refer to Table 2.

Electrical schematics for the use case "ISO/IEC 7816-3 only"

These schematics refer to the use case, in which the OC1230 is only connected to the baseband controller via the ISO/IEC 7816-3 interface. The SPI interface is not connected. The GPIO0.7 is not connected. These schematics refer to the OC1230 configuration, in which the GPIO0.7 acts as SPI interrupt, as well as the configuration in which the GPIO0.7 acts as secure GPIO.

Note: *SPI connection is optional, GPIO0.7 connection is optional.*

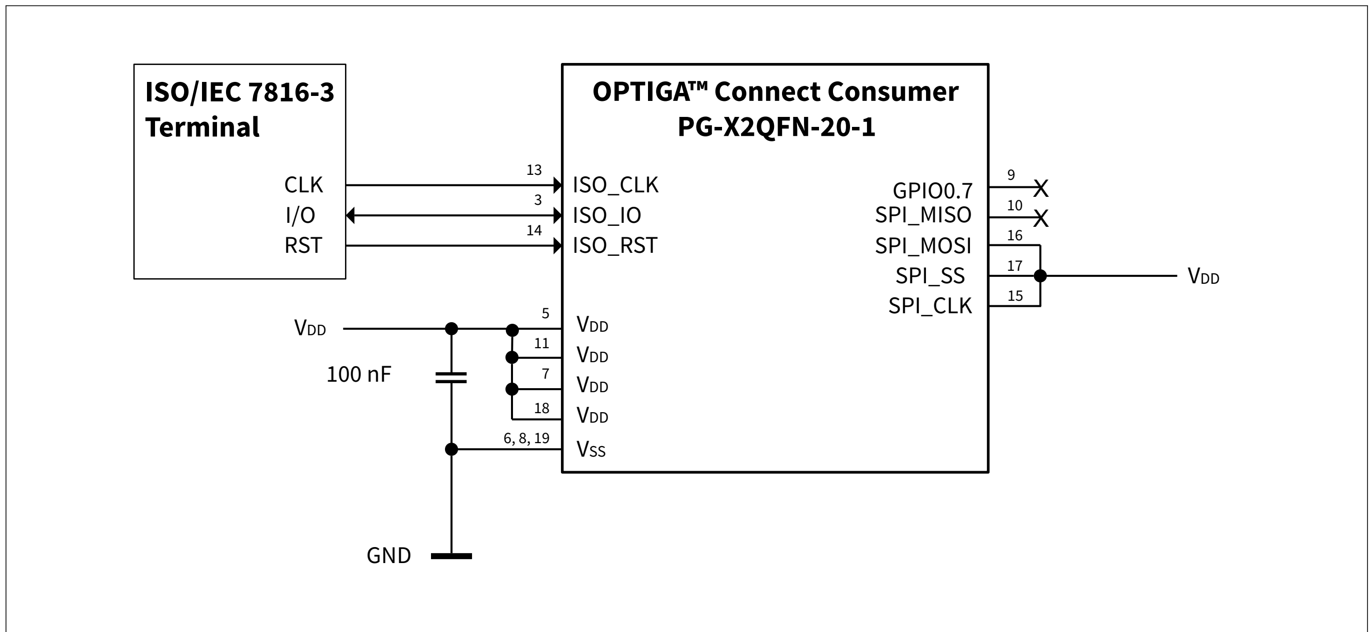

Figure 12 **Reference schematics for PG-X2QFN-20-1 ISO + SPI + SPI IRQ**

Electrical schematics for the use case "ISO/IEC 7816-3, SPI with SPI IRQ"

These schematics refer to the use case, in which the OC1230 is connected to the baseband controller via the ISO/IEC 7816-3 interface, and to the application processor via SPI. These schematics refer to the OC1230 configuration, in which the GPIO0.7 acts as an SPI interrupt. The GPIO0.7 as SPI interrupt is connected to the SPI master.

Note: *SPI connection is optional, SPI IRQ connection is optional.*

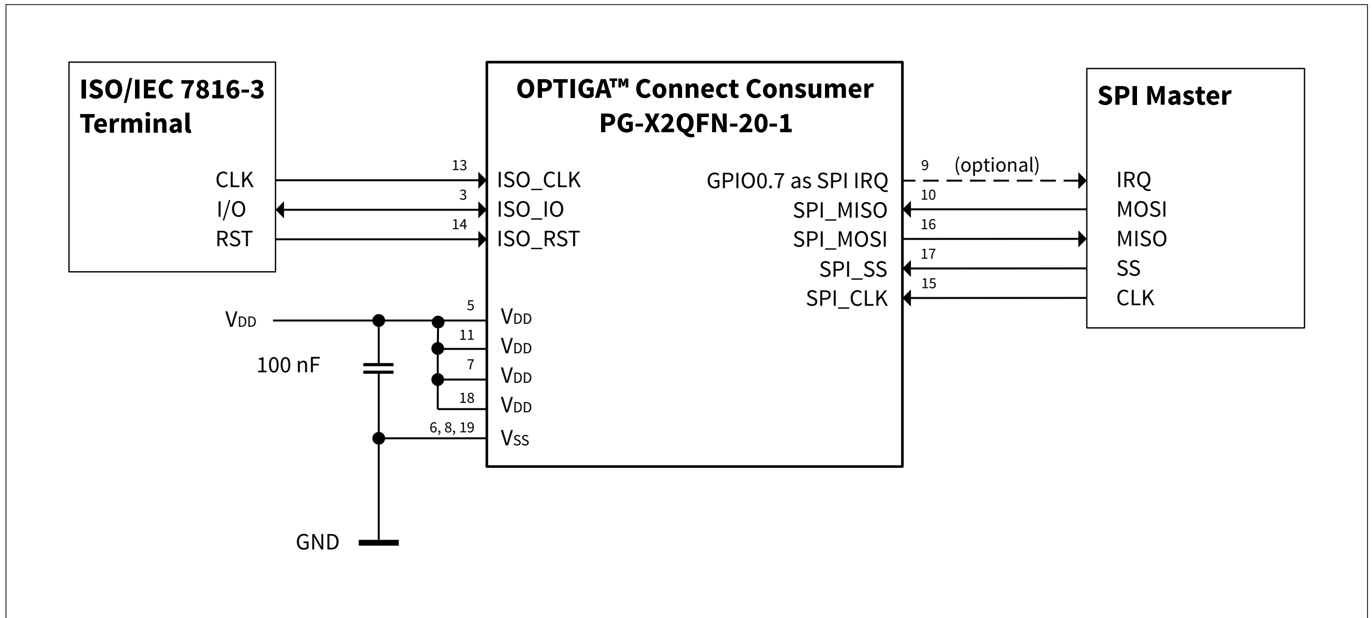

Figure 13 Reference schematics for PG-X2QFN-20-1 ISO + SPI + SPI IRQ

Electrical schematics for the use case "ISO/IEC 7816-3, SPI and secure GPIO"

These schematics refer to the use case, in which the OC1230 is connected to the baseband controller via the ISO/IEC 7816-3 interface, and to the application processor via SPI. These schematics refer to the OC1230 configuration, in which the GPIO0.7 acts as a secure GPIO. The GPIO0.7 as a secure GPIO is connected to the application processor boot loader.

***Note**:* *SPI connection is optional, secure GPIO connection is optional.*

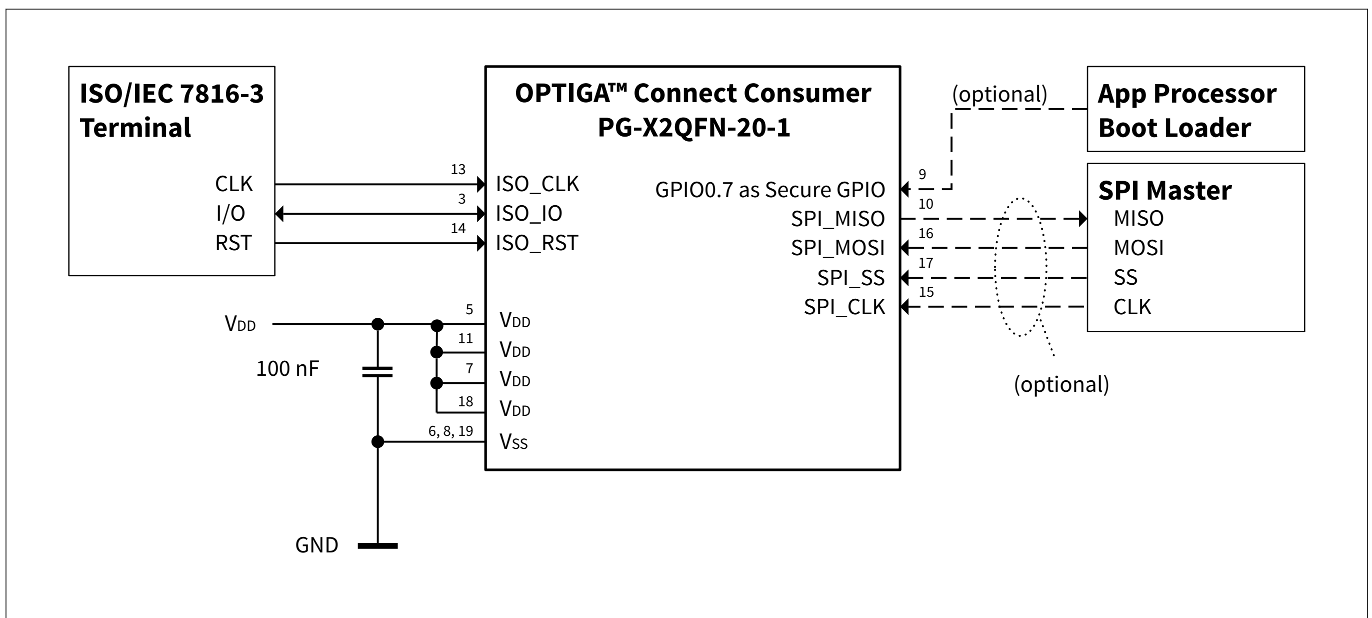

Figure 14 Reference schematics for PG-X2QFN-20-1 ISO + SPI + SECURE GPIO

7.2 Reference schematics for SG-XFWLB-16-1

This chapter provides reference schematics for the OC1230 in the package type SG-XFWLB-16-1. It refers to a selection of typical use cases. For further recommendations on how to connect the OC1230, refer to Table 4.

Electrical schematics for the use case "ISO/IEC 7816-3 only"

These schematics refer to the use case, in which the OC1230 is only connected to the baseband controller via the ISO/IEC 7816-3 interface. The SPI interface is not connected. The GPIO0.7 is not connected. These schematics refer to the OC1230 configuration, in which the GPIO0.7 acts as SPI interrupt, as well as the configuration in which the GPIO0.7 acts as secure GPIO.

***Note**: SPI connection is optional, GPIO0.7 connection is optional.*

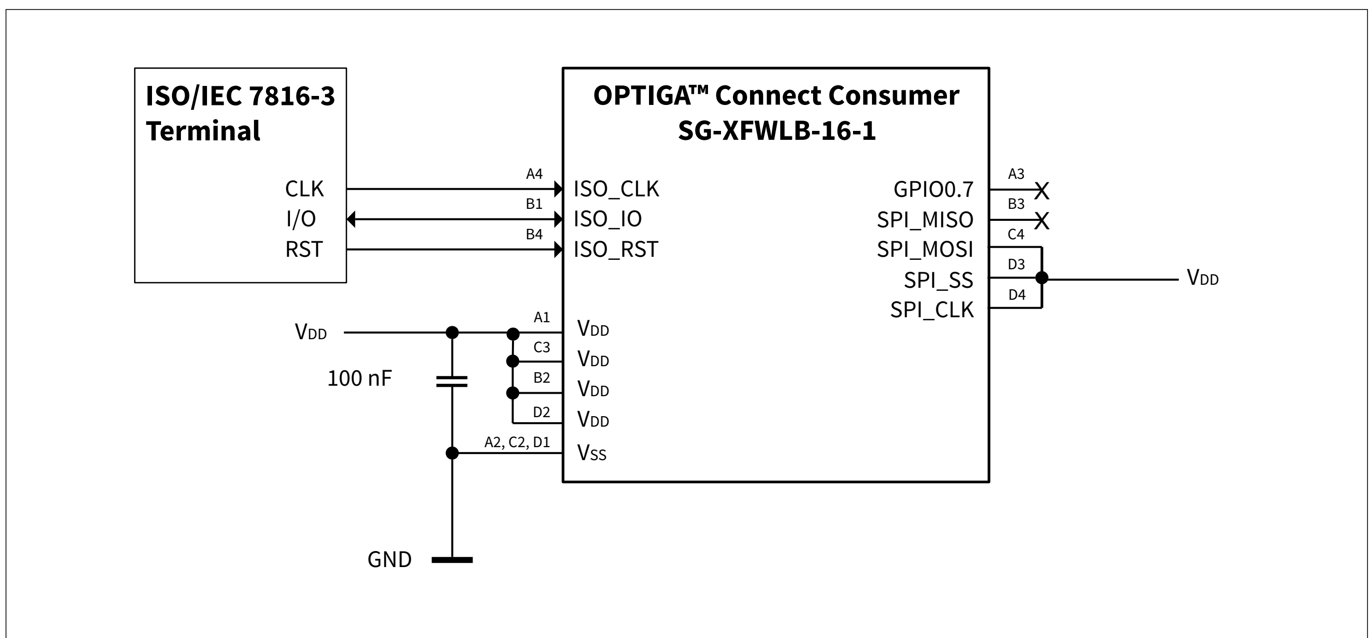

Figure 15 Reference schematics for SG-XFWLB-16-1 ISO only

Electrical schematics for the use case "ISO/IEC 7816-3, SPI with SPI IRQ"

These schematics refer to the use case, in which the OC1230 is connected to the baseband controller via the ISO/IEC 7816-3 interface, and to the application processor via SPI. These schematics refer to the OC1230 configuration, in which the GPIO0.7 acts as an SPI interrupt. The GPIO0.7 as SPI interrupt is connected to the SPI master.

***Note**: SPI connection is optional, SPI IRQ connection is optional.*

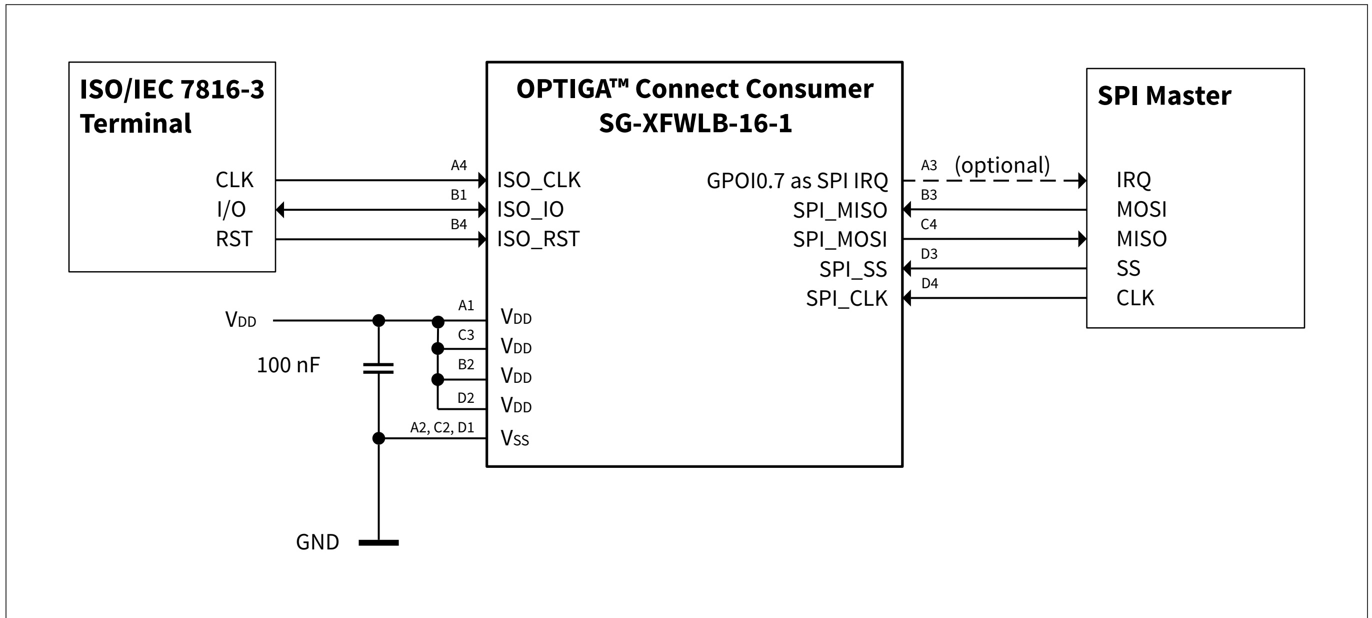

Figure 16 Reference schematics for SG-XFWLB-16-1 ISO + SPI + SPI IRQ

Electrical schematics for the use case "ISO/IEC 7816-3, SPI and secure GPIO"

These schematics refer to the use case, in which the OC1230 is connected to the baseband controller via the ISO/IEC 7816-3 interface, and to the application processor via SPI. These schematics refer to the OC1230 configuration, in which the GPIO0.7 acts as a secure GPIO. The GPIO0.7 as a secure GPIO is connected to the application processor boot loader.

***Note**:* *SPI connection is optional, secure GPIO connection is optional.*

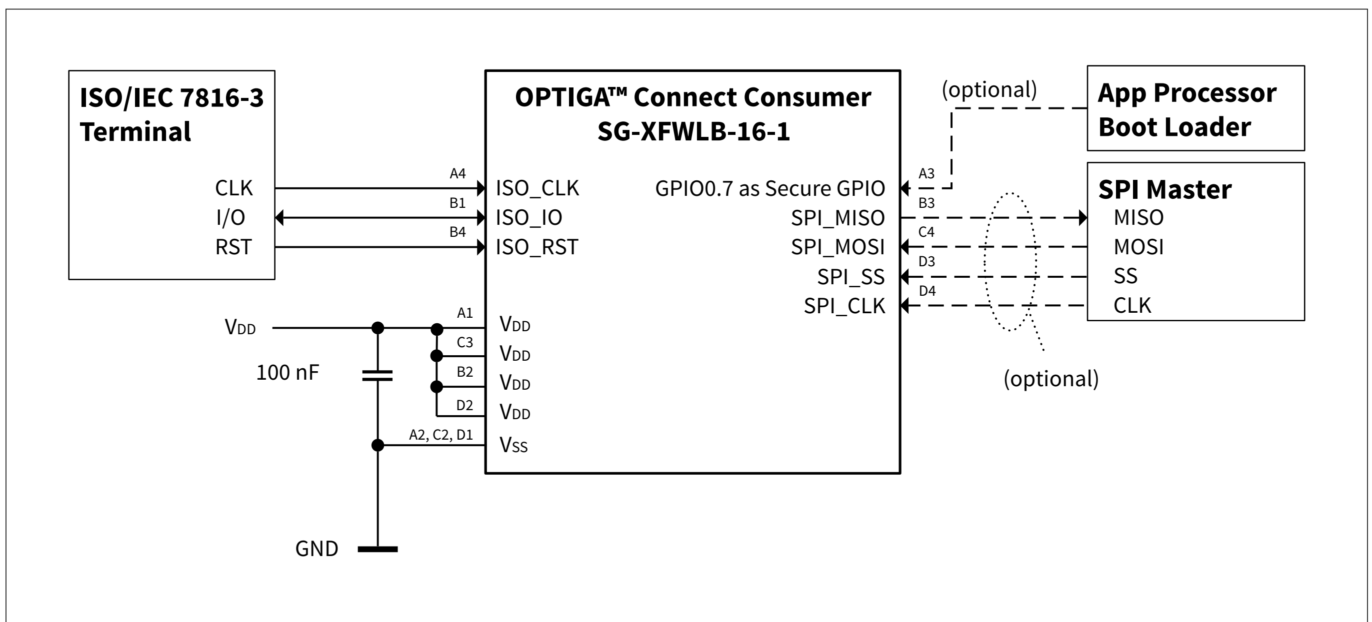

Figure 17 Reference schematics for SG-XFWLB-16-1 ISO + SPI + SECURE GPIO

8 Electrical characteristics

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

***Notes**:*

1. *T_A as given for the operating temperature range of the controller unless otherwise stated.*
2. *All currents flowing into the controller are considered positive.*

8.1 Key features

Table 5 Key features

Voltage class	Class C (1.8 V) Class D (1.2 V)
Data retention	10 years at room temperature

8.2 Absolute maximum ratings

This section defines the absolute maximum ratings. Stresses exceeding the values listed in Table 6 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 specification is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability, including NVM data retention and programming endurance.

All voltages are referenced to common ground (GND) reference, unless otherwise specified.

Table 6 Absolute maximum ratings

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Operating temperature, ambient	T_A	-25	-	+85	°C	T_J (max) must not be exceeded
Junction temperature	T_J	-	-	+110	°C	-
Supply voltage	V_{DD}	-0.3	-	2.5	V	-

8.3 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.

8.3.1 DC characteristics

T_A as given for the security controller’s operating ambient temperature range unless otherwise stated.

All currents flowing into the security controller are considered positive.

Table 7 DC electrical characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Supply voltage	V_{DD}	1.08	-	1.98	V	Overall functional range of V_{DD}
Supply voltage variation during operation	V_{DD_op}	V_{DD_nom} * 0.90	-	V_{DD_nom} * 1.10	V	In operation and idle state phases, the supply voltage must stay within this range around the nominal supply voltage. Max operating voltage must stay below V_{DD_max}.
Supply current, operating state	$I_{1V2_operating}$	-	12.75	-	mA	V_{DD} = 1.2 V, ISO/IEC 7816
Supply current, operating state	$I_{1V8_operating}$	-	12.90	-	mA	V_{DD} = 1.8 V, ISO/IEC 7816
Supply current, idle state	I_{1V2_idle}	-	141	-	µA	V_{DD} = 1.2 V, via ISO/IEC 7816 connected
Supply current, idle state	I_{1V8_idle}	-	142	-	µA	V_{DD} = 1.8 V, via ISO/IEC 7816 connected

8.3.2 AC characteristics

T_A as given for the security controller's operating ambient temperature range unless otherwise stated.
All currents flowing into the security controller are considered positive.

Table 8 AC electrical characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
V_{DD} ramp-up time	t_{VDD}	2[1]	-	-	µs	0% to 100% of the target voltage ramp
System oscillator frequency	f_{OSC}	-	100	-	MHz	Average system frequency for a nominally adjusted oscillator at T_j = +25°C and zero lifetime (without silicon aging). The actual oscillator frequency may vary due to dynamic on-chip power management functions (for example voltage drop monitor) and environmental conditions.
System oscillator frequency temperature drift	f_{OSC_T}	-	-30	-	kHz/°C	Average system oscillator frequency drift as a function of junction temperature
System clock frequency	f_{SYSCLK}	$f_{OSC}/32$	-	f_{OSC}	MHz	-

1) At a faster supply ramp-up time the chip internal ESD elements cause temporarily a cross current between V_{DD} and GND, which would be larger than the allowed I_{CC} for the relevant voltage class.

8.3.2.1 Power-up guidelines

The rampup times given in AC 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.

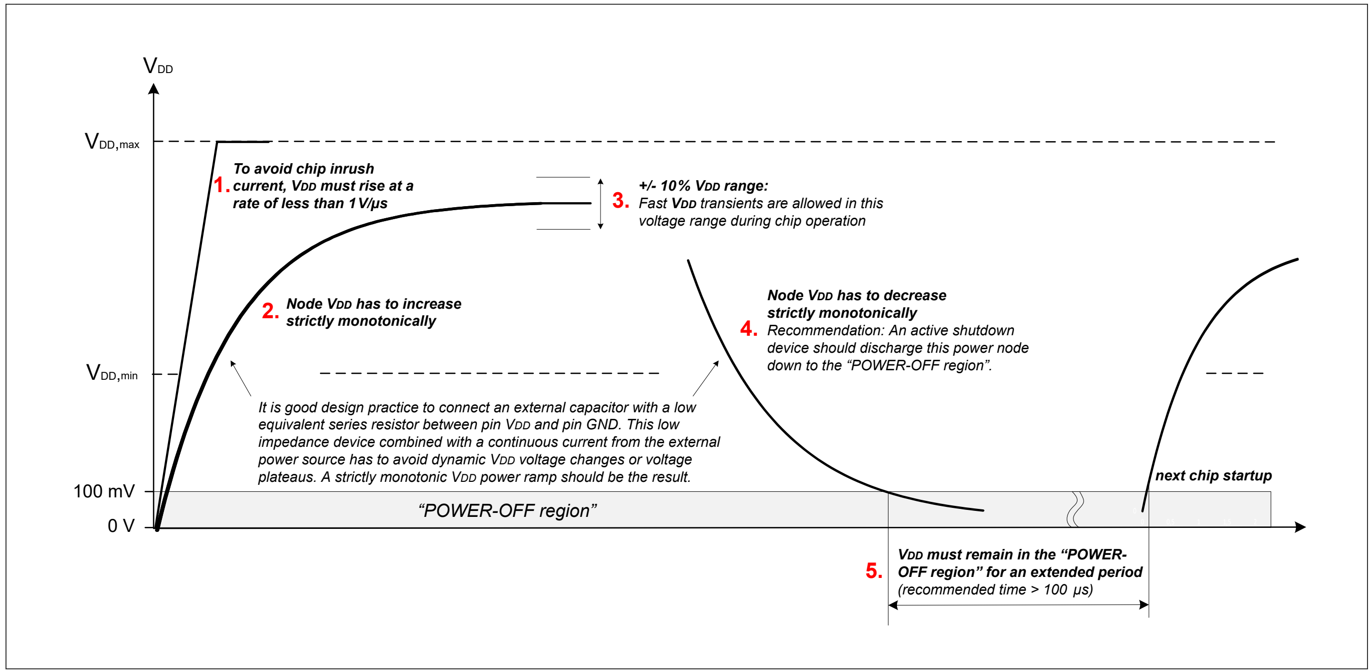

Figure 18 **Recommended power-up behavior**

8.4 Interfaces

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!*

The general characteristics of GPIO pins are stated at first covering the full operational range and various configuration options. The characteristics of a particular interfaces are stated with respect to the specific interface standards.

8.4.1 ISO 7816 interface characteristics

The ISO 7816 interface conforms with the ISO/IEC 7816-3, integrated circuit card (ICC) side, implementing the transport protocols T=0 and T=1.

This interface supports APDU multiplexing, allowing for efficient communication in context with multiple enabled carrier profiles. For more information please refer to Multiple enabled profiles (MEP) and Logical secure element interfaces.

This interface supports logical channels according to ISO/IEC 7816-4. Logical channels allow multiple application protocols to share the same physical connection, enabling the consumer device to manage multiple applications simultaneously.

***Notes**:*

1. *All currents flowing out of the pad are considered to be positive.*
2. *Symbol T_A describes the ambient temperature range.*
3. *ISO/IEC 7816-3 defines Class C as lowest supply voltage. Since this product supports lower voltages the requirements and limits from Class C are used for the whole voltage range below Class C.*

Absolute maximum ratings

Table 9 ISO/IEC 7816-3 card maximum ratings

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Pad input voltage	V_I	-0.3	-	V_{DD} +0.3	V	

DC electrical characteristics

Table 10 ISO/IEC 7816-3 card DC electrical characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Supply voltage	V_{DD}	1.08	-	1.98	V	Note: V_{DD} includes: V_{DD_C}

Table 11 ISO/IEC 7816-3 card DC electrical characteristics - UART_RST

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Input high voltage	V_{IH}	0.8 * V_{DD}	-	V_{DD}	V	-150 µA < I_{IH} < +20 µA T_A = 0°C … 50°C
Input high voltage	V_{IH}	0.7 * V_{DD}	-	V_{DD}	V	T_A = 0°C … +50°C
Input high voltage	V_{IH}	0.8 * V_{DD}	-	V_{DD}	V	-20 µA ≤ I_{IH} T_A = -25°C … +85°C
Input low voltage	V_{IL}	0	-	0.12 * V_{DD}	V	-20 µA < I_{IL} < 200 µA T_A = 0°C … +50°C
Input low voltage	V_{IL}	0	-	0.2 * V_{DD}	V	T_A = 0°C … +50°C
Input low voltage	V_{IL}	0	-	0.2 * V_{DD}	V	I_{IL} ≤ 200 µA T_A = -25°C … +85°C

Table 12 ISO/IEC 7816-3 card DC electrical characteristics - UART_CLK

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Input high voltage	V_{IH}	0.7 * V_{DD}	-	V_{DD}	V	-100 µA < I_{IH} < +20 µA T_A= 0°C … +50°C
Input high voltage	V_{IH}	0.7 * V_{DD}	-	V_{DD}	V	T_A= 0°C … +50°C
Input high voltage	V_{IH}	0.7 * V_{DD}	-	V_{DD}	V	-20 µA ≤ I_{IH} T_A= -25°C … +85°C
Input low voltage	V_{IL}	0	-	0.2 * V_{DD}	V	-20 µA < I_{IL} < 100 µA T_A= 0°C … +50°C
Input low voltage	V_{IL}	0	-	0.2 * V_{DD}	V	T_A= 0°C … +50°C
Input low voltage	V_{IL}	0	-	0.2 * V_{DD}	V	I_{IL} ≤ 20 µA T_A= -25°C … +85°C

Table 13 ISO/IEC 7816-3 card DC electrical characteristics - UART_IO

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Input high voltage	V_{IH}	0.7 * V_{DD}	-	V_{DD}	V	-20 µA < I_{IH} < 300 µA T_A= 0°C … +50°C
Input high voltage	V_{IH}	0.7 * V_{DD}	-	-	V	T_A= 0°C … +50°C
Input high voltage	V_{IH}	0.7 * V_{DD}	-	V_{DD} + 0.3	V	-20 µA < I_{IH} < 20 µA T_A= -25°C … +85°C
Input low voltage	V_{IL}	0	-	0.15 * V_{DD}	V	-20 µA < I_{IL} < 1000 µA T_A= 0°C … +50°C
Input low voltage	V_{IL}	0	-	0.2 * V_{DD}	V	T_A= 0°C … +50°C
Input low voltage	V_{IL}	-0.3	-	0.2 * V_{DD}	V	I_{IL} ≤ 1000 µA T_A= -25°C … +85°C

(table continues...)

Table 13 (continued) ISO/IEC 7816-3 card DC electrical characteristics - UART_IO

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Output high voltage	V_{OH}	0.7 * V_{DD}	-	V_{DD}	V	-20 µA < I_{OH} 20 kΩ to V_{DD} T_A= 0°C … +50°C
Output high voltage	V_{OH}	0.7 * V_{DD}	-	V_{DD}	V	0 µA < I_{OH} < 20 µA 20 kΩ to V_{DD} T_A= 0°C … +50°C
Output high voltage	V_{OH}	0.7 * V_{DD}	-	V_{DD}	V	Voltage class C I_{OH} = 20 µA 20 kΩ to V_{DD} T_A= -25°C … +85°C
Output low voltage	V_{OL}	0	-	0.15 * V_{DD}	V	-500 µA = I_{OL} T_A= 0°C … +50°C
Output low voltage	V_{OL}	0	-	0.15 * V_{DD}	V	Voltage class C -500 µA < I_{OL} < 0 µA T_A= 0°C … +50°C
Output low voltage	V_{OL}	0	-	0.3	V	-1000 µA = I_{OL} T_A= -25°C … +85°C

ISO/IEC 7816-3 card AC electrical characteristics

Table 14 ISO/IEC 7816-3 card AC electrical characteristics - UART_RST

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Rise/fall time	t_R, t_F	-	-	1	µs	T_A= 0°C … +50°C
Rise/fall time	t_R, t_F	-	-	400	µs	T_A= -25°C … +85°C
Input load capacitance	C_{LOAD}	-	-	30	pF	-

Table 15 ISO/IEC 7816-3 card AC electrical characteristics - UART_CLK

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
External frequency	f_{UART_CLK}	1	-	15	MHz	@ duty cycle 40% … 60% V_{IL} < 0.1 * V_{DD} V_{IH} > 0.9 * V_{DD}
Rise/fall time	t_R, t_F	-	-	0.9 * 1/ f_{UART_CLK}	µs	T_A= 0°C … +50°C Measured between 10% and 90% of signal amplitude
Rise/fall time	t_R, t_F	-	-	50	ns	T_A= -25°C … +85°C measured between 10% and 90% of signal amplitude

(table continues...)

Table 15 (continued) ISO/IEC 7816-3 card AC electrical characteristics - UART_CLK

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Input load capacitance	C_{LOAD}	-	T_A= -25°C … +85°C	30	pF	-

Table 16 ISO/IEC 7816-3 card AC electrical characteristics - UART_IO

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Rise/fall time	t_R, t_F	-	-	1	µs	T_A= 0°C … +50°C
Rise/fall time	t_R, t_F	-	-	-	µs	T_A= -25°C … +85°C
Input load capacitance	C_{LOAD}	-	-	30	pF	-
Output load capacitance	C_{LOAD}	-	-	30	pF	-

Table 17 ISO/IEC 7816-3 supported Fi/Di ratios

Fi-Di	F/D	Baud rate
0x01 (%0000 0001)	372	9600 Bd @3.579 MHz
0x02 (%0000 0010)	186	19200 Bd @3.579 MHz
0x03 (%0000 0011)	93	38400 Bd @3.579 MHz
0x08 (%0000 1000)	31	115200 Bd @3.579 MHz
0x11 (%0001 0001)	372	9600 Bd @3.579 MHz
0x12 (%0001 0010)	186	19200 Bd @3.579 MHz
0x13 (%0001 0011)	93	38400 Bd @3.579 MHz
0x18 (%0001 1000)	31	115200 Bd @3.579 MHz
0x38 (%0011 1000)	62	57600 Bd @3.579 MHz
0x93 (%1001 0011)	128	31250 Bd @4.000 MHz
0x94 (%1001 0100)	64	56000 Bd @3.579 MHz
0x95 (%1001 0101)	32	156250 Bd @5.000 MHz
0x96 (%1001 0110)	16	312500 Bd @5.000 MHz
0x97 (%1001 0111)	8	625000 Bd @5.000 MHz

8.4.2 SPI interface characteristics

The SPI interface on the OC1230 is compliant with the GlobalPlatform APDU Transport protocol T=1', as defined in [GP22_APDU] [12], implementing the “SPI slave” role, supporting the following details:

- Configuration "mode 0"
- Null-byte value '00'
- Polling mode

Depending on the configuration of the OC1230, the SPI interface may also support the SPI interrupt mode. If supported, the interrupt mode can optionally be used to manage the flow of data and optimize the efficiency of the communication between the OC1230 and the consumer device. For more details refer to GPIO0.7 as SPI interrupt (SPI IRQ).

The electrical characteristics of the SPI interface lines SCL, MOSI, MISO, and SS are given below.

This interface supports logical channels according to ISO/IEC 7816-4. Logical channels allow multiple application protocols to share the same physical connection, enabling the consumer device to manage multiple applications simultaneously.

***Notes**:*

1. *All currents flowing into the pad are considered to be positive*
2. *T_A as given for the controller's operating temperature range unless otherwise stated*

Table 18 **DC characteristics**

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Pad supply voltage	V_{DD}	1.08	-	1.98	V	
Input high voltage	V_{IH}	0.7 * V_{DD}	-	V_{DD} + 0.3	V	
Input low voltage	V_{IL}	-0.3	-	0.3 * V_{DD}	V	
Output high voltage	V_{OH}	0.9 * V_{DD}	-	-	V	I_{OH} = -100 µA
Output low voltage	V_{OL}	-	-	0.1 * V_{DD}	V	I_{OL} = 1.5 mA
Pad leakage	I_L	-2	-	2	µA	0 V < V_{PAD} < V_{DD}
Pad leakage	I_L	-1	-	0.02	mA	-0.3 V < V_{PAD} < V_{DD} + 0.3 V

Table 19 **AC characteristics**

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
SCLK frequency, mode 0	f_{SCLK}	-	-	8	MHz	
SCLK clock period	t_{SCLK_range}	1/f_{SCLK} -5%	-	1/f_{SCLK} +5%	µs	Measured at input pad voltage of 0.5 * V_{DD}
SCLK nominal clock period	t_{SCLK}	-	1/ f_{SCLK}	-	µs	-
SCLK low time	t_{SCLKL}	0.45 * t_{SCLK}	-	-	µs	Measured at input pad voltage of 0.5 * V_{DD}
SCLK high time	t_{SCLKH}	0.45 * t_{SCLK}	-	-	µs	Measured at input pad voltage of 0.5 * V_{DD}
SCLK input slew rate	t_{SLEW}	1	-	4	V/ns	SCLK input voltage slew rate measured between 0.2 * V_{DD} and 0.6 * V_{DD}
SS inactive time	t_{SS}	40	-	-	ns	

(table continues...)

Table 19 (continued) AC characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
SS setup time	t_{SSS}	40	-	-	ns	Setup time SS to SCLK leading[1] edge
SS hold time	t_{SSH}	5	-	-	ns	Hold time SCLK trailing edge to SS inactive
MOSI setup time	t_{SU}	5	-	-	ns	Data setup time to SCLK latching edge
MOSI hold time	t_H	3	-	-	ns	Data hold time to SCLK latching edge
MISO valid delay time from SS active, mode 0	t_{SSV}	-	-	30	ns	Output valid delay time from SS active
MISO valid delay time from SCLK edge	t_V	0	-	0.7 * t_{SCLKL}	ns	Output valid delay time from SCLK shifting edge
MISO output disable time	t_{SSDO}	0	-	40	ns	Output disable time from SS inactive
MISO hold time	t_{HO}	3	-	-	ns	Output hold time to SCLK shifting edge
Input capacitance (package pin[2])	C_{IN}	-	-	10	pF	-
Output load capacitance	C_{LOAD}	-	-	30	pF	-

1) Depending on the SPI mode, the relevant SCLK edge is either the rising or the falling edge, refer to for a description of the SPI modes
2) Bare die + typical package, for example X2QFN.

8.4.3 GPIO0.7 characteristics

The OC1230 is available in 2 different configurations with regards to the functionality that is supported by GPIO0.7: Pin GPIO0.7 can either serve as an interrupt output line for the SPI interrupt (SPI IRQ), or as an input line to support a "Secure GPIO" mechanism, as defined by Google within the Android ready SE program. These two configuration options are mutually exclusive. This configuration is applied pre-issuance by Infineon and is persistent for the lifetime of the product.

8.4.3.1 GPIO0.7 as SPI interrupt (SPI IRQ)

The following section describes the electrical characteristics of the pin GPIO0.7, when used as an SPI interrupt line (SPI IRQ).

The GPIO0.7 can optionally be used to optimize the efficiency of the SPI communication between the OC1230 and the consumer device. If configured to support the SPI interrupt mechanism, the OC1230 will use the pin GPIO0.7 to indicate, that there is response data available to be retrieved by the SPI master. As an improvement over the [GP22_APDU] [12] the handling of the SPI interrupt was modified for better robustness: In contrast to the [GP22_APDU] [12], the OC1230 will not clear the interrupt signal as soon as the SS line is asserted by the SPI

master. Instead, the OC1230 will keep the interrupt line on a high active voltage level, until all available response data has been retrieved by the SPI master.

The electrical characteristics of the GPIO0.7 as SPI IRQ are given below.

***Notes**:*

1. *All currents flowing into the pad are considered to be positive*
2. *T_A as given for the controller's operating temperature range unless otherwise stated*

Table 20 DC characteristics for 1.8 V supply voltage range

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Pad supply voltage	V_{DD}	1.62	-	1.98	V	
Output low voltage	V_{OL}	-	-	0.28	V	
Output low current	I_{OL}	750	-	-	µA	
Output high voltage	V_{OH}	V_{DD} - 0.27	-	-	V	
Output high current	I_{OH}	750	-	-	µA	

Table 21 DC characteristics for 1.2 V supply voltage range

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Pad supply voltage	V_{DD}	1.08	-	1.32	V	
Output low voltage	V_{OL}	-	-	0.18	V	
Output low current	I_{OL}	500	-	-	µA	
Output high voltage	V_{OH}	V_{DD} - 0.18	-	-	V	
Output high current	I_{OH}	500	-	-	µA	

Table 22 AC characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Output load capacitance	C_{LOAD}	-	-	30	pF	-

8.4.3.2 GPIO0.7 as secure GPIO

The following section describes the electrical characteristics of the pin GPIO0.7, when used as a secure GPIO.

If configured to support the secure GPIO mechanism, the OC1230 monitors pin GPIO0.7 for the boot signal from the boot loader of the application processor of an embedding device. The boot signal is an impulse, that indicates the boot phase of the application processor boot loader. It ensures physically that BOOT parameters can only be set in the Keymint applet at device boot time. The OC1230 will detect the boot signal on the rising edge of the GPIO0.7 pin, according to the following timing diagram:

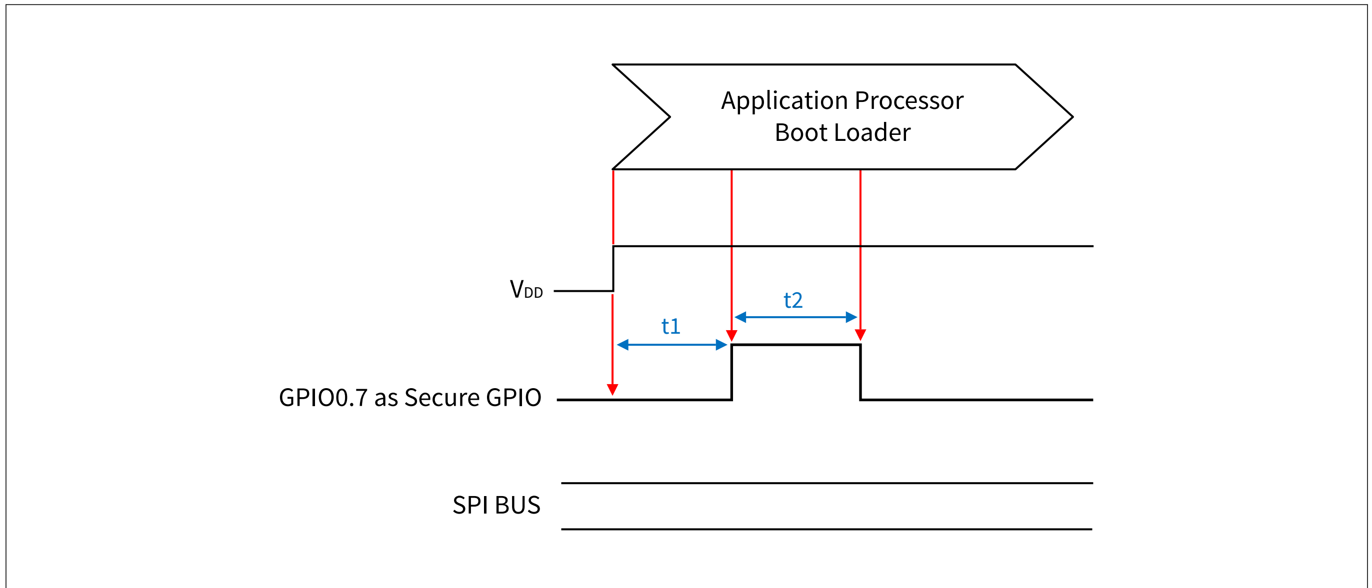

Figure 19 **Secure GPIO timing diagram**

Table 23 **Boot signal characteristics**

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Time from V_{DD} on, to rising edge	t1	1	-	-	ms	-
Duration of high state	t2	1	-	-	µs	OC1230 triggers on the rising edge

The electrical characteristics of the GPIO0.7 are given below.

***Notes**:*

1. *All currents flowing into the pad are considered to be positive*
2. *T_A as given for the controller's operating temperature range unless otherwise stated*

Table 24 **Secure GPIO operation supply and input voltages for (1.2 V and 1.8 V) supply voltage range**

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Supply voltage	V_{DD}	1.08	-	1.98	V	
GPIO pad input voltage	V_{IN_GPIO}	-0.3	-	V_{DD} + 0.3	V	V_{DD} is in the operational supply range
GPIO pad input voltage	V_{IN_GPIO}	-0.3	-	1.98	V	V_{DD} is switched off See Attention below

Attention: ***The pin used for operating the secure GPIO is provided with an "indirect supply avoidance" feature (ISA) which allows to switch off the supply voltage of the security controller regardless of the input voltage V_{IN_GPIO} at these pins and without drawing a significant pad input current.***

Table 25 Secure GPIO DC electrical characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Input current	I_{PUW}	-20	-	-3	µA	0 V ≤ V_{IN_GPIO} ≤ V_{DD} -0.5 V; pin is configured as pull-up (weak)
Input low voltage	V_{IL}	-0.3	-	0.3 * V_{VDD}	V	-
Input high voltage	V_{IH}	0.7 * V_{VDD}	-	V_{VDD} +0.3	V	-
Input capacitance	C_{IN}	-	-	10	pF	-

9 Contact information

For contact information, sales and office addresses please visit http://www.infineon.com.

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.

References

ETSI

[1] ETSI TS 102 221: *Smart Cards; UICC-Terminal interface; Physical and logical characteristics*

GlobalPlatform

[2] GPCS: GPC_SPE_034: *GlobalPlatform Technology Card Specification*, v2.3.1
[3] GPCIC: GPC_GUI_080: *GlobalPlatform Card Common Implementation Configuration*, v2.1
[4] GPC_UICC: GPC_GUI_010: *GlobalPlatform UICC Configuration*, v2.0
[5] GP2X_AMDTA: GPC_SPE_007: *GlobalPlatform Confidential Card Content Management Card Specification – Amendment A*, v1.2
[6] GP2X_AMDTB: GPC_SPE_011: *GlobalPlatform Remote Application Management over HTTP Card Specification – Amendment B*, v1.2
[7] GP2X_AMDTC: GPC_SPE_025: *GlobalPlatform Contactless Services Card Specification – Amendment C*, v1.3
[8] GP22_AMDTD: GPC_SPE_014: *GlobalPlatform Secure Channel Protocol 03 Card Specification – Amendment D*, v1.0
[9] GP2X_AMDTF: GPC_SPE_093: *GlobalPlatform Technology Secure Channel Protocol '11' Card Specification – Amendment F*, v1.3
[10] GP2X_AMDTH: GPC_SPE_120: *GlobalPlatform Technology Executable Load File Upgrade Card Specification – Amendment H*, v1.1
[11] GPD_SEAC: GPD_SPE_013: *GlobalPlatform Device Technology Secure Element Access Control*, v1.1
[12] GP2X_APDU: GPC_SPE_172: *GlobalPlatform Technology APDU Transport over SPI/I2C*, v1.0
[13] GPC_API: *GlobalPlatform Card API - org.globalplatform*, v1.7
[14] GPC_APIUPG: *GlobalPlatform Card API - ELF Upgrade API org.globalplatform.upgrade*, v1.1

GSMA

[15] GSM Association SGP.21: *RSP Architecture Specification*
[16] GSM Association SGP.22: *RSP Technical Specification*; v2.5.0 and v3
[17] GSM Association SGP.25: *Embedded UICC for Consumer Devices Protection Profile*
[18] GSM Association FS.04: *Security Accreditation Scheme (SAS) for UICC Production - Standard*

Infineon Technologies AG

[19] 32-bit Security Controller: *V07 Integration Guide*
[20] Recommendations: *For Board Assembly of Infineon Wafer Level Ball Grid Array Packages*

ISO/IEC

[21] ISO/IEC 7816-3:2006: *Identification cards - Integrated circuit cards - Part 3: Cards with contacts - Electrical interface and transmission protocols*
[22] ISO/IEC 7816-4:2020: *Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange*

TCA

[23] TCA_EUICCPP_v2: eUICC Profile Package: *Interoperable Format Technical Specification*
[24] TCA_EUICCPP_v3: eUICC Profile Package: *Interoperable Format Technical Specification*; 2022

Oracle Java Card™

[25] JCRE: *Java Card™ Platform Runtime Environment Specification, Classic Edition*; v3.1
[26] JCVM: *Java Card™ Platform Virtual Machine Specification, Classic Edition*; v3.1
[27] JCAPI: *Java Card™ Platform Application Programming Interface (API) Classic Edition*; v3.1

Glossary

AES

Advanced Encryption Standard (AES)

The standard for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. The algorithm described by AES is a symmetric-key algorithm (the same key is used for both encryption and decryption).

AOSP

Android open source platform (AOSP)

APDU

application protocol data unit (APDU)
The communication unit between a smart card reader and a smart card.

API

application programming interface (API)

BER

basic encoding rules (BER)

BSI

Bundesamt für Sicherheit in der Informationstechnik (BSI)
German Federal Office for Information Security.

CAVE

cellular authentication and voice encryption (CAVE)

CC

Common Criteria for Information Technology Security Evaluation (CC)
An international standard (ISO/IEC 15408) for computer security certification.

CDMA

code-division multiple access (CDMA)

CLF

contactless front end (CLF)

CLK

clock (CLK)

CPU

central processing unit (CPU)

CSIM

CDMA subscriber identity module (CSIM)

DFA

differential fault analysis (DFA)
A class of side channel attacks in the field of cryptography, specifically cryptographic analysis. Faults are induced into cryptographic implementations with the intention of revealing information about their internal states.

DPA

differential power analysis (DPA)
A class of attacks against smart cards and secure cryptographic tokens. The attack involves monitoring how much power a microprocessor uses as it functions, then using advanced statistical methods to determine secret keys or personal identification numbers involved in the computations.

ECASD

eUICC controlling authority security domain (ECASD)

ECIES

elliptic curve integrated encryption scheme (ECIES)

eSA

eUICC security assurance (eSA)

ESD

electrostatic discharge (ESD)
The sudden draining of electrostatic charge. Even with small charges, it poses a considerable risk to small semiconductor structures, in particular MOS structures. It is therefore essential to take precautions when dealing with unprotected semiconductors.

eSIM

embedded SIM (eSIM)

An eUICC that hosts one or several MNO profiles.

ETSI

European Telecommunications Standards Institute (ETSI)

eUICC

embedded UICC (eUICC)

A removable or non-removable UICC that enables the remote and/or local management of profiles in a secure way.

GND

ground (GND)

GP

GlobalPlatform (GP)

GPIO

general purpose input/output (GPIO)

GSMA

GSM Association (GSMA)

GSM

Global System for Mobile communications (GSM)
A standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation digital cellular networks used by mobile devices.

HAL

hardware abstraction layer (HAL)

HTTP

hypertext transfer protocol (HTTP)

I2C

inter-integrated circuit (I2C)

I3C

improved inter-integrated circuit (I3C)

An industry standard for multidrop serial data buses, developed under the guidance of the MIPI Alliance.

ICC

integrated card circuit (ICC)

IEC

International Electrotechnical Commission (IEC)
The international committee responsible for drawing up electrotechnical standards.

IPC

inter-process communication (IPC)

IRQ

interrupt request (IRQ)
A type of exception that breaks the linear flow of a program. The requesting module needs a software service routine to evaluate its current state and take the necessary actions.

ISD-R

issuer security domain-root (ISD-R)

ISIM

IP multimedia services identity module (ISIM)

ISO

International Organization for Standardization (ISO)

JC

Java Card™ (JC)

JCVM

Java Card™ virtual machine (JCVM)

LPAd

local profile assistant device (LPAd)
Local profile assistant when LPA is in the device.

LPA
local profile assistant (LPA)

LSI
logical secure element interface (LSI)

LTE
long-term evolution (LTE)

LUId
local user interface device (LUId)
Local user interface when LPA is in the device.

MAC
message authentication code (MAC)
Used to prove message integrity.

MEP
multiple enabled profiles (MEP)

MISO
master in slave out (MISO)

MOSI
master out slave in (MOSI)

NAA
network access application (NAA)
An application located on a UICC, that provides access to a telecommunication network.

NIST
National Institute of Standards and Technology (NIST)

NVM
non-volatile memory (NVM)

OEM
original equipment manufacturer (OEM)

OS
operating system (OS)

OTA
over-the-air (OTA)

PK CI
public key certificate issuers (PK CI)

PPS
protocol and parameters selection (PPS)

PWR
power (PWR)

RAM
remote application management (RAM)

RFM
remote file management (RFM)

RFU
reserved for future use (RFU)

RoHS
Restriction of Hazardous Substances in Electrical and Electronic Equipment (RoHS)
EU rules restricting the use of hazardous substances in electrical and electronic equipment to protect the environment and public health.

RSA
Rivest Shamir Adleman (RSA)
An asymmetric cryptographic algorithm in which the encryption key is public and differs from the decryption key, which is kept secret (private).

RSP
remote SIM provisioning (RSP)

RST
reset (RST)

RUIM
removable user identity module (RUIM)

SCL
serial clock line (SCL)

SEAC
secure element access control applet (SEAC)

SE
secure element (SE)

SIM
subscriber identity module (SIM)

SM-DP+
subscription manager-data preparation + (SM-DP+)
A profile server for MNO profiles over interface ES9+.

SMD
surface-mounted device (SMD)

SPA
simple power analysis (SPA)

SPI
serial peripheral interface (SPI)

SS
slave select (SS)

SUCI
schemes including subscriber concealed identity (SUCI)

SW
status word (SW)

TAF
Technical Assistance Facility (TAF)

TCA
Trusted Connectivity Alliance (TCA)

TLV
tag length value (TLV)

UART
universal asynchronous receiver/transmitter (UART)
A universal asynchronous receiver transmitter is used for serial communications over a peripheral device serial port by translating data between parallel and serial forms.

USIM
universal subscriber identity module (USIM)

WEEE
Waste from Electrical and Electronic Equipment (WEEE)
EU rules on treating waste electrical and electronic equipment to contribute to sustainable production and consumption.

Revision history

Reference	Description
Revision 1.0, 2024-02-15	
All	Initial release

Trademarks

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

Edition 2024-02-15

Published by

Infineon Technologies AG

81726 Munich, Germany

© 2024 Infineon Technologies AG

All Rights Reserved.

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

Email: **CSSCustomerService@infineon.com**

Document reference
IFX-ghj1691726447751

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.