OPTIGA™ Connect Consumer OC1120

Datasheet

5G-ready eSIM turnkey solution for consumer applications compliant to GSMA SGP.22 specification

Key features

- Remote SIM Provisioning (RSP) compliant with GSMA SGP.22 v2.2.2
- Allows to accommodate multiple MNO profiles - up to 800 KB free user memory
- Supports 2G, 3G, 4G (LTE), 5G network technologies
- Supported Network Access Applications SIM, USIM, CSIM, RUIM and ISIM
- Trusted Connectivity Alliance (TCA) eUICC Profile Package V2.3.1 compliant
- Over-the-air (OTA) functionality for Remote File Management (RFM) and Remote Applet Management (RAM)
- Java Card™ 3.0.5 classic and GlobalPlatform 2.2.1 Runtime Environment
- APIs for Java Card™ 3.0.5 classic, GlobalPlatform, UICC and USIM functionality
- ISO 7816 UART interface
- Certified and tested solution according to GSMA

Potential applications

For embedding into cellular-connected mobile devices such as:

- Smartphones
- Tablets
- Wearable devices
- Mobile terminals
- Laptops

Description

Infineon OPTIGA™ Connect Consumer OC1120 is an embedded universal integrated circuit card (eUICC) turnkey solution for embedded subscriber identity modules (eSIM) implementing GSMA's technical specification SGP.22 for mobile consumer devices. It is available with 3 different memory configurations (see Ordering information).

Support and services

- Design-in support for hardware and software
- End-to-End test support with the Infineon Test SM-DP+ Profile Server

About this document

Scope and purpose

This datasheet provides the following information about the OPTIGA™ Connect Consumer OC1120:

- Hardware and software features
- Support services
- Supported interfaces and connectivity
- Electrical characteristics and other technical information
- SMD packages (PG-VQFN-8-4) and chip scale packages (SG-XFWLB-25-3)

Intended audience

This document is primarily intended for device integrators.

Table of contents

Table of contents

List of tables

List of figures

1 General description

The OPTIGA™ Connect Consumer OC1120 eUICC is Infineon's next generation of embedded subscriber identity modules (eSIM) implementing GSMA's technical specification SGP.22 [11] for mobile consumer devices.

The main purpose of the OPTIGA™ Connect Consumer OC1120 eUICC is to provide secure network authentication to a selected and subscribed carrier network. Changing or adding carrier profiles by means of Remote SIM Provisioning (RSP) Over-the-Air is possible via LPA on supporting devices. With up to 800 KB of free user memory, the OPTIGA™ Connect Consumer OC1120 has ample space for resident multiple subscriptions as well as additional applications and user data.

The OPTIGA™ Connect Consumer OC1120 is a certified and tested solution according to GSMA and Common Criteria certification according to protection profile PP0084:

- GSMA eUICC statement of security evaluation
- GSMA SAS-UP certified production process
- GlobalPlatform eUICC TCA Interoperable Profile Test
- GlobalPlatform eUICC Consumer Compliance Test

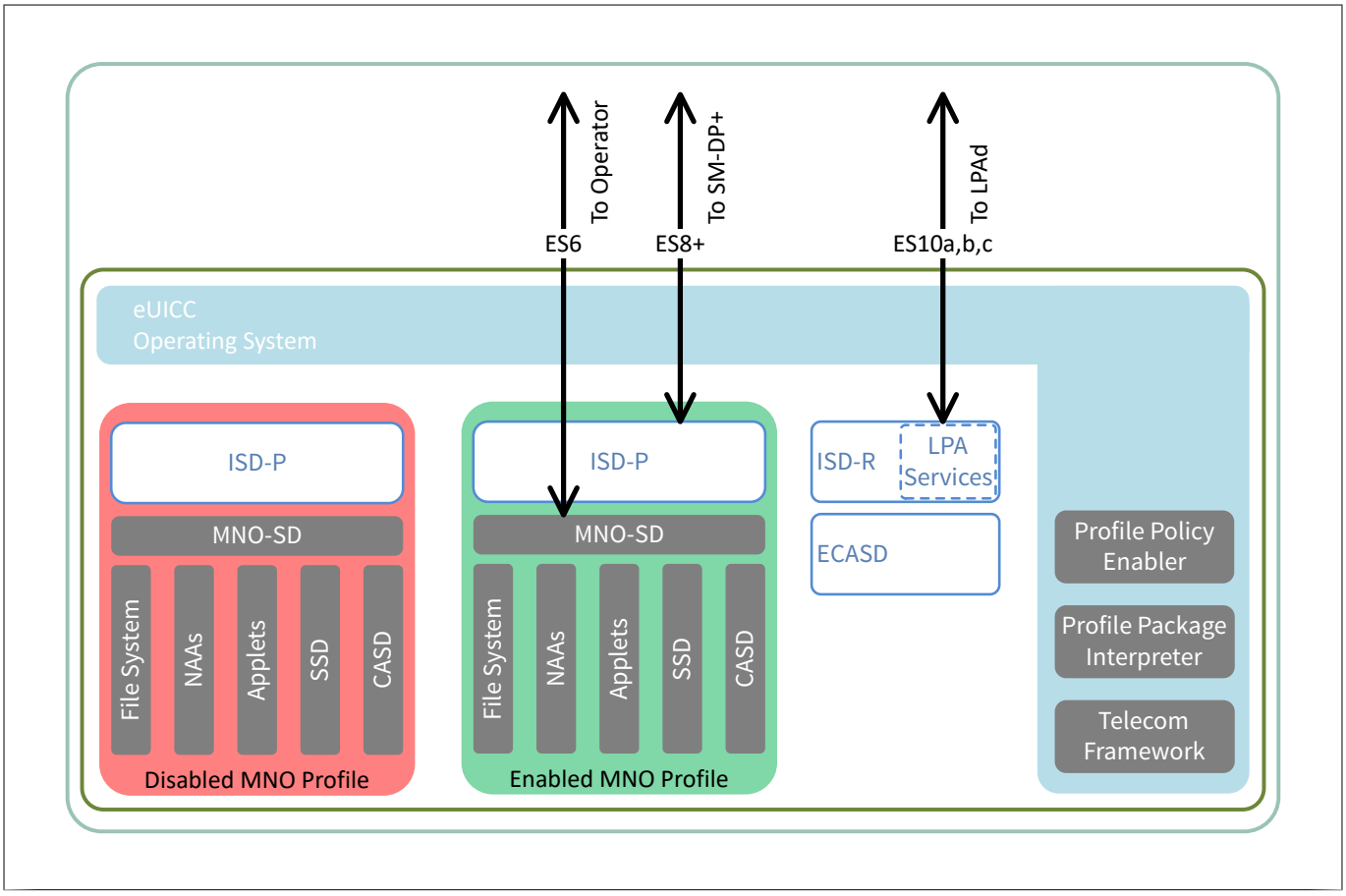


Figure 1 Embedded subscriber identity module (eSIM) overview

OPTIGA™ Connect Consumer OC1120 supports all interfaces according to GSMA SGP.22 [11]:

- ES6: OTA interface between eUICC and MNO for the management of MNO services
- ES8+: Secure end-to-end channel between eUICC and SM-DP+ for the protected download of the bound profile package
- ES10a: Local interface between eUICC and LDSd (part of LPAd) for management of profile discovery

- ES10b: Local interface between eUICC and LPDd (part of LPAd) for the download of the bound profile package
- ES10c: Local interface between eUICC and LUId (part of LPAd) for local profile management by the end user

1.1 Hardware features

The OPTIGA™ Connect Consumer OC1120 is available in SMD packages (PG-VQFN-8-4) and Chip scale packages (SG-XFWLB-25-3) to provide flexibility for the device design.

Table 1 Hardware features

Voltage Class	Class B (2.7 V - 3.3 V) Class C (1.6 V - 1.98 V)
CPU	32-bit Arm® SecurCore® SC300, Optimized for Secure SIM/UICC applications
Internal clock	Up to 100 MHz
External clock	From 1 MHz to 10 MHz
Operating temperature range	-25°C to +85°C
Data retention	10 years at room temperature

1.2 OS features

1.2.1 Supported standards

- GSMA SGP.21 v2.2 [10] and GSMA SGP.22 v2.2.2 [11] compliant
- Trusted Connectivity Alliance (TCA) eUICC Profile Package V2.3.1 [17] compliant
- Java Card™ v3.0.5 classic [32] compliant
- GlobalPlatform v2.2.1 [9] compliant including amendments related to Remote Subscription Management functionality
- UICC Framework:
  - UICC platform according to ETSI TS 102 221 [1]
  - Over-the-air functionality (OTA) for Remote File Management (RFM) and Remote Application Management (RAM) according to 3GPP TS 31.115 [21], ETSI TS 102 225 [3], ETSI TS 102 226 [4]
  - Card Application Toolkit (CAT) for UICC according to ETSI TS 102 223 [2]
  - USIM Application Toolkit (USAT) according to 3GPP TS 31.111 [20]
- Application Programming Interfaces (APIs):
  - Java Card™ 3.0.5 classic
  - GlobalPlatform API org.globalplatform v1.6
  - UICC API according to ETSI TS 102 241 [5]
  - (U)SIM API according to 3GPP TS 31.130 [23], 3GPP TR 31.919 [25]
  - ISIM API according to 3GPP TS 31.133 [24]

1.2.2 Network access applications

- (U)SIM (2G/3G/4G/LTE/5G) as defined in 3GPP TS 31.102 [18], 3GPP TS 51.011 [28] etc.
- RUIM as defined in 3GPP2 C.S0023-D [29]
- CSIM as defined in 3GPP2 C.S0065-B [30]
- ISIM as defined in 3GPP TS 31.103 [19], with support for the following services:
  - Generic Bootstrapping Architecture (GBA)
  - P-CSCF addressing
  - P-CSCF discovery for IMS Local Break Out

The OPTIGA™ Connect Consumer OC1120 supports multimode systems such as USIM, RUIM, CSIM and ISIM applications in all combinations to support most types of network technology systems such as CDMA2000 1x, CDMA2000 HRPD, GERAN (GSM), UTRAN (UMTS), EUTRAN (LTE).

1.2.3 Network algorithms

The OPTIGA™ Connect Consumer OC1120 supports the following Authentication and Key Agreement algorithms (AKA):

- Comp 128-2/3
- Milenage (Comp128-4) according to ETSI TS 135 208 [6]
- TUAK, according to 3GPP TS 35.231 [27]
- CAVE, according to 3GPP2 MAP [31]
- 5G protection schemes including subscriber concealed identity (SUCI) schemes according to 3GPP TS 33.501 [26]
  - ECIES scheme, Profile A
  - ECIES scheme, Profile B
  - Null scheme
- EAP-SIM, EAP-AKA

1.2.4 Security features

The OPTIGA™ Connect Consumer OC1120 supports the following security features:

- All security-relevant methods are DPA/SPA/DFA-secured
- ANSI X9.17 software secure random number generator
- DES coprocessor for DES cryptography
- RSA coprocessor for RSA cryptography
- Elliptic Curve Cryptography (ECC):
  - NIST P-256
  - BrainpoolP256r1
  - FRP256V1
- Digital Signature Algorithm (DSA)
- Hash-Based Message Authentication Code (HMAC)
- Scalable crypto API with DES encryption
- SHA-1, SHA-256 and MD5 hash algorithms
- Main crypto services provided by the Java Card v3.0.5 classic API:
  - AES (128, 192 and 256 bit)

- CRC (16 and 32 bit)
- DES (CBC and ECB modes)
- RSA (up to 2048 bit)
- ECC (up to 521 bit)

1.2.5 Additional features

- Support of BF76 Tag in profile metadata for carrier privilege rules in Android

1.2.6 Communication features

UART interface, with ISO 7816-3 T=0 protocol.

1.2.7 Remote SIM provisioning (RSP)

The Infineon OPTIGA™ Connect Consumer OC1120 supports Remote SIM Provisioning according to GSMA SGP.22 v2.2.2 [11] via a LPA in the device (LPAd).

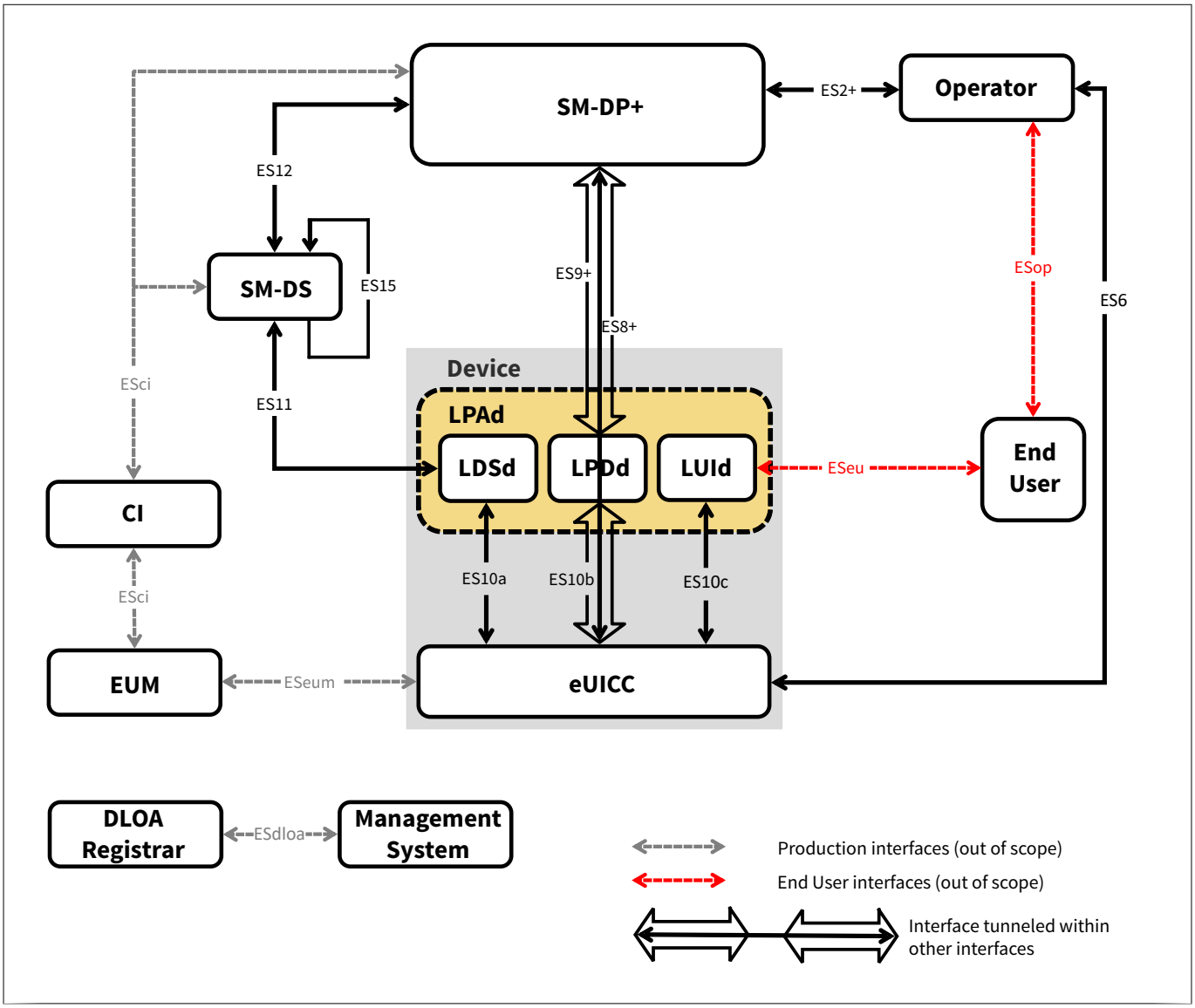


Figure 2 Remote SIM provisioning system, LPA in the device (source: GSMA SGP.22 v2.2.2 [11])

1.2.8 Over-the-air (OTA) functionality

The OPTIGA™ Connect Consumer OC1120 supports the following Over-the-Air (OTA) functions:

- Remote Application Management (RAM)
- Remote File Management (RFM)

According to ETSI TS 102 225 [3], ETSI TS 102 226 [4], 3GPP TS 31.115 [21] and 3GPP TS 31.116 [22]. These specifications define transport mechanisms and formats for communication over-the-air (OTA).

The Infineon OPTIGA™ Connect Consumer OC1120 supports the following bearers for OTA functions:

- Over the SMS channel using the Short Message Services Center (SMSC)
- Over HTTP

1.2.9 Memory management

For information about the available memory configurations, please refer to Ordering information .

1.3 Support and services

To support the design-in process, the following sets of configurations are available:

- GSMA SGP.26 (GCF) test configuration for early engineering tests
- GSMA live configuration for volume production tests

Additionally, Infineon provides support for the smooth integration of the OPTIGA™ Connect Consumer OC1120 eUICC into customer devices with:

- Getting Started Guide
- End-to-End test support for profile downloads
  - Customer access to the Infineon Test SM-DP+ Profile Server for the end-to-end test of profile downloads with GSMA test profiles[1)]

[1] eSIM samples with GSMA SGP.26 certificates required

2 Connectivity

2.1 Power supply schematic

The following figure illustrates the power supply circuit for the controller.

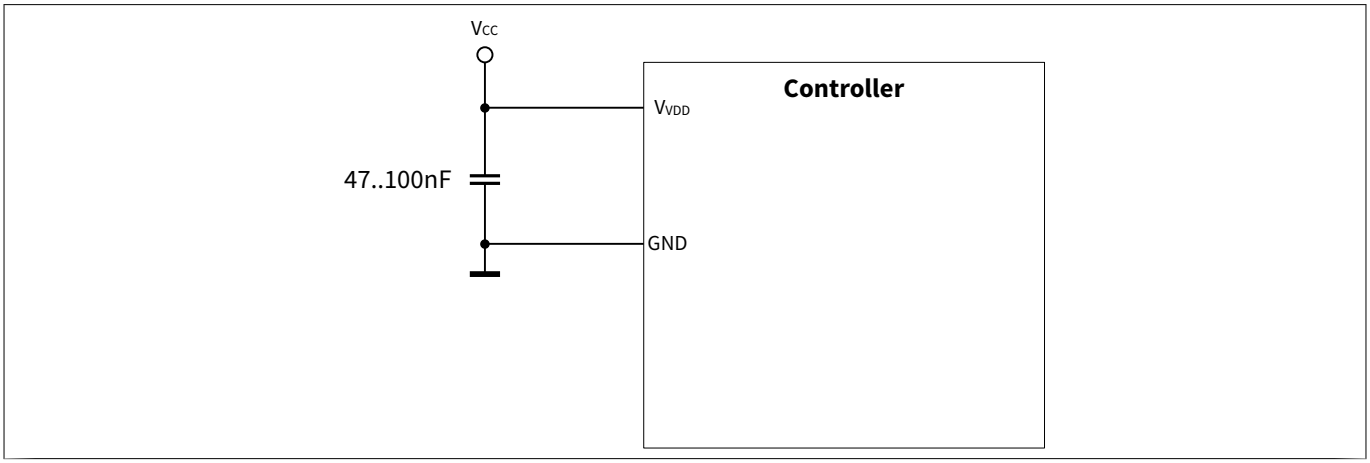


Figure 3 Power supply diagram

Contrary to other areas of application in which different types of capacitors are switched in parallel to stabilize the power supply, here normally only one capacitor is required. This is due to the wide variation limits of the supply voltage and the additional internal measures to handle sudden changes in load. For this decoupling capacitor, use a ceramic type with a low equivalent series resistance.

2.2 Interfaces

This section shows how the interfaces are to be connected.

2.2.1 ISO 7816-3 UART interface

Figure 4 illustrates how the OPTIGA™ Connect Consumer OC1120 is to be connected to a host via the UART interface. In the sense of the ISO/IEC 7816-3 the OPTIGA™ Connect Consumer OC1120 takes the role of the ICC, and the host takes the role of the terminal.

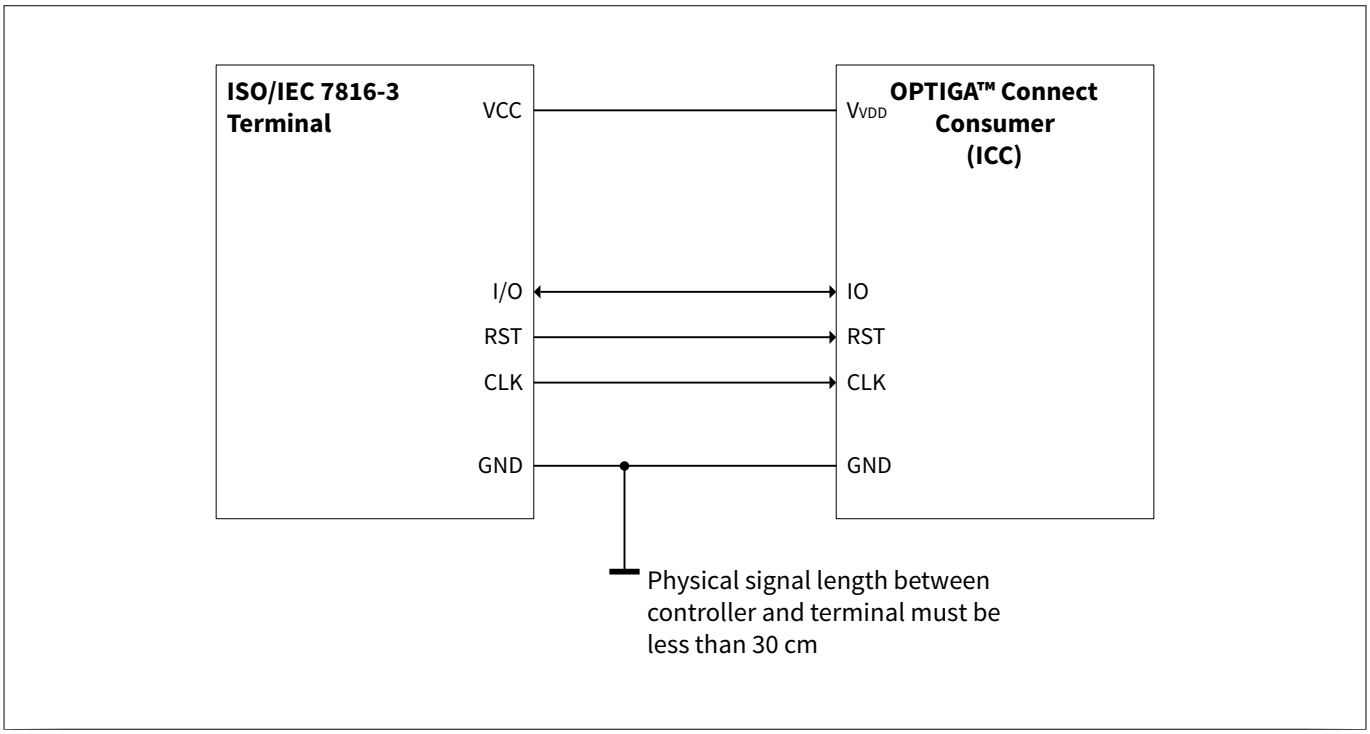


Figure 4 ISO/IEC 7816-3 terminal connection

3 Electrical characteristics

3.1 Absolute maximum ratings

Note: This section defines the absolute maximum ratings. Stresses exceeding the values listed in Table 2 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 write/erase endurance.

The values stated in the Table 2 may be further restricted for particular products (i.e., sales codes). All voltages are referenced to common ground (GND) reference, unless otherwise specified.

Table 2 Absolute maximum ratings

Parameter	Symbol	Values			Unit	Signal function/ remarks	Applicable pins
		Min.	Typ.	Max.			
Operating temperature, ambient	T_A	-25	-	+85	°C		
Supply voltage	V_{VDD}	-0.3	-	7.0	V	-	
Input voltage	V_{IN}	-0.3	-	7.0	V	-	ISO_RST, ISO_CLK, ISO_IO

3.2 Operational characteristics

3.2.1 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.

Differentiation is done according to ETSI TS 102 221 [1] to adapt to required current consumption limits. Certain values in the tables below may depend on the applied voltage class.

Table 3 DC characteristics

Parameter	Symbol	Values			Unit	Signal function/remarks
		Min.	Typ.	Max.		
Supply voltage	V_{VDD_B}	2.70	3.00	3.30	V	Supply voltage range for operation of ISO/IEC 7816-3 Class B
	V_{VDD_C}	1.62	1.80	1.98	V	Supply voltage range for operation of ISO/IEC 7816-3 Class C
Average supply current	I_{VDD}	-	-	10	mA	While running an encryption/ decryption
Supply current spikes[1)]	I_{VDD_B}	-	-	50	mA	Q ≤ 10 nAs; V_{VDD} in ISO/IEC 7816-3 Class B supply voltage range
Supply current spikes[1)]	I_{VDD_C}	-	-	30	mA	Q ≤ 6 nAs; V_{VDD} in ISO/IEC 7816-3 Class C supply voltage range
Supply current, power saving mode	I_{psm}	-	70 - 100	200[2)]	µA	T_A = +25°C, f_{ISO_CLK} stopped, all other inputs at V_{VDD}, No other interface activity, max value chosen in accordance with ETSI TS 102 221 [1]

1) The maximum spike amplitude and spike charge defined by ETSI TS 102 221 [1] and ETSI TS 102 613 [8] are kept within the specified range. The maximum spike length which is technically irrelevant for terminal regulator and voltage stability is typically kept within the specified range.
2) Up to 600 µA for PG-VQFN-8-4.

3.2.2 AC characteristics

Power-up considerations

It is recommended to follow the voltage characteristics shown in the figure below to limit current spike effects.

Note: The power-up consideration applies to V_{VDD}, see also Chapter 2.1.

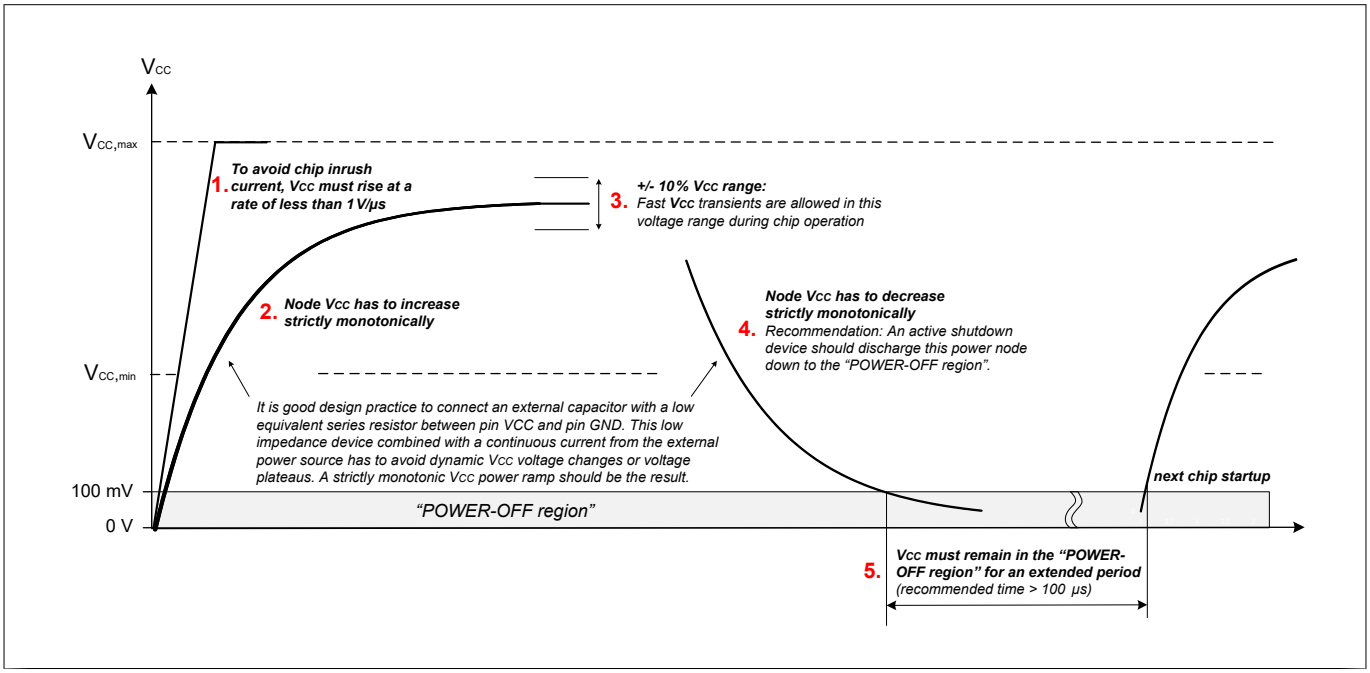


Figure 5 Recommended power-up behavior

3.3 Interface characteristics

3.3.1 ISO 7816-3 UART interface

The electrical characteristics of the pads described below comply with the following standards ISO/IEC 7816-3 [16], ETSI TS 102 221 [1].

Note: All currents flowing out of the pad are considered to be positive. T_A as given for the controller's operating temperature range unless otherwise stated.

Table 4 ISO/IEC 7816-3 maximum ratings

Parameter	Symbol	Values			Unit	Signal function/ remarks	Applicable pins
		Min.	Typ.	Max.			
Pad input voltage	V_I	-0.3	-	V_{VDD} + 0.3	V		

Table 5 ISO/IEC 7816-3 DC electrical characteristics

Parameter	Symbol	Values			Unit	Signal function/ remarks	Applicable pins
		Min.	Typ.	Max.			
ISO_RST Input high voltage	V_{IH}	0.8 * V_{VDD}	-	V_{VDD}	V	Voltage Class B, C, -20 µA ≤ I_{IH}	ISO_RST
ISO_RST Input low voltage	V_{IL}	0	-	0.2 * V_{VDD}	V	Voltage Class B, C, I_{IL} ≤ 200 µA	ISO_RST
ISO_CLK Input high voltage	V_{IH}	0.7 * V_{VDD}	-	V_{VDD}	V	Voltage Class B, C, -20 µA ≤ I_{IH}	ISO_CLK
ISO_CLK Input low voltage	V_{IL}	0	-	0.2 * V_{VDD}	V	Voltage Class B, C, I_{IL} ≤ 20 µA	ISO_CLK
ISO_IO Input high voltage	V_{IH}	0.7 * V_{VDD}	-	V_{VDD} + 0.3	V	Voltage Class B, C, -20 µA < I_{IH} < 20 µA	ISO_IO
ISO_IO Input low voltage	V_{IL}	-0.3		0.2 * V_{VDD}	V	Voltage Class B, C, I_{IL} < 1000 µA	ISO_IO
ISO_IO Output high voltage	V_{OH}	0.7 * V_{VDD}		V_{VDD}	V	Voltage Class B, C, I_{OH} = 20 µA, 20 kΩ to V_{VDD}	ISO_IO
ISO_IO Output low voltage	V_{OL}	0		0.4	V	Voltage Class B, -1 mA = I_{OL}	ISO_IO
	V_{OL}	0		0.3	V	Voltage Class C, -1 mA = I_{OL}	ISO_IO

Table 6 ISO/IEC 7816-3 AC electrical characteristics

Parameter	Symbol	Values			Unit	Signal function/ remarks	Applicable pins	Supported data rates
		Min.	Typ.	Max.				
ISO_CLK External frequency	f_{ISO_CLK}	1	-	-	MHz	@duty cycle 40%..60%	ISO_CLK	1)

1) A protocol parameter select (PPS) procedure defined according to ISO/IEC 7816-3 [16] can be conducted after the ATR to set the appropriate communication speed. The supported clock rate conversion factors are 16, 32, 64, 93, 128, 186, 256, 372 and 512.

4 Delivery forms and ordering

This chapter describes the details about delivery forms, package descriptions and other ordering information for PG-VQFN-8-4 and SG-XFWLB-25-3.

In addition to the packages for volume production described in the following sections, Infineon also offers engineering samples as convenient 4FF/2FF/1FF breakout cards. Please approach your local Infineon representative for more details.

4.1 SMD packages

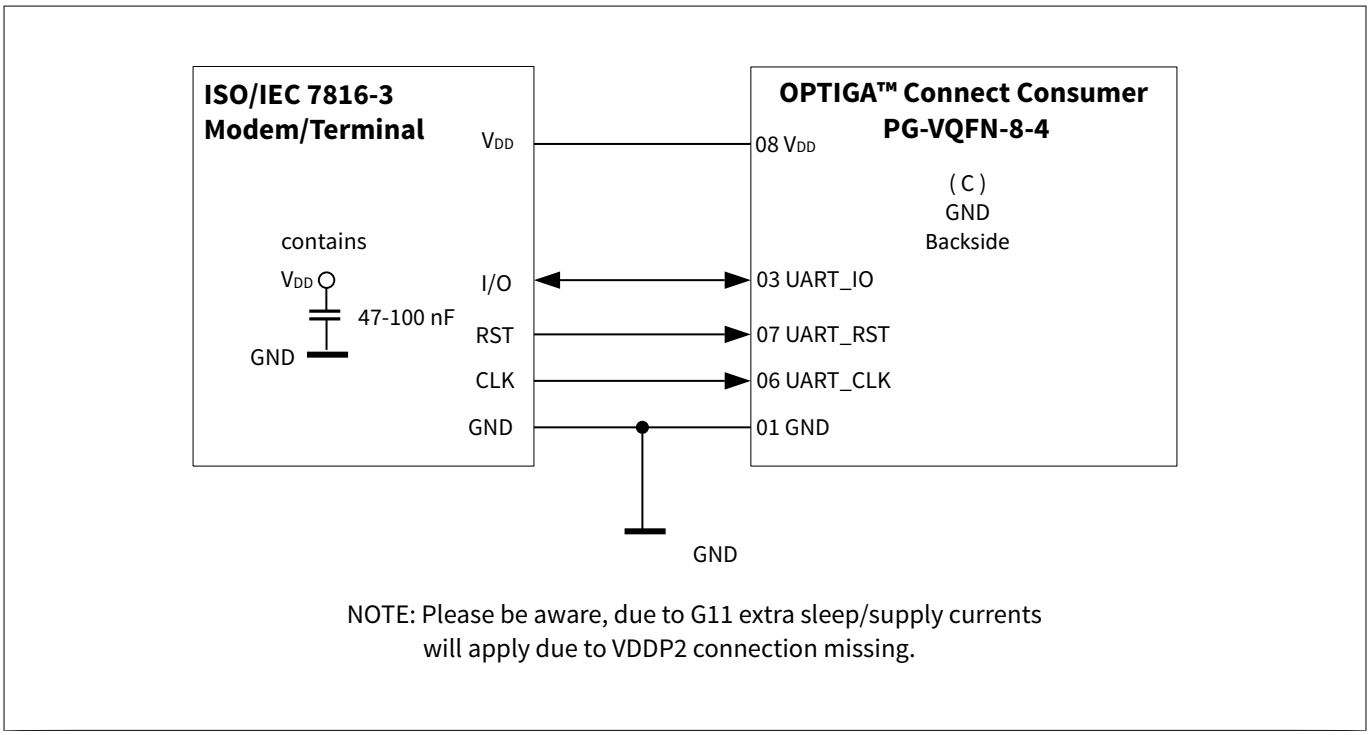


Figure 6 PG-VQFN-8-4 schematic diagram

The following packages are available:

- PG-VQFN-8-4

A detailed description of the PG-VQFN-8-4 package can be found in the following link:

https://www.infineon.com/cms/en/product/packages/PG-VQFN/PG-VQFN-8-4/

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

- Package outline: Shows the package dimensions of the controller in the individual packages
- Package footprint: Shows footprint recommendations
- Tape and reel packing
- Sample marking pattern: Describes the productive sample marking pattern on the package
- Package layout: Shows a simple layout with the pin numbers described in the pad-to-signal reference section

Note: Unless specified otherwise, all figure dimensions are given in mm.

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

4.1.1 Package outline

The package dimensions (in mm) of the controller in PG-VQFN-8-4 packages are given below.

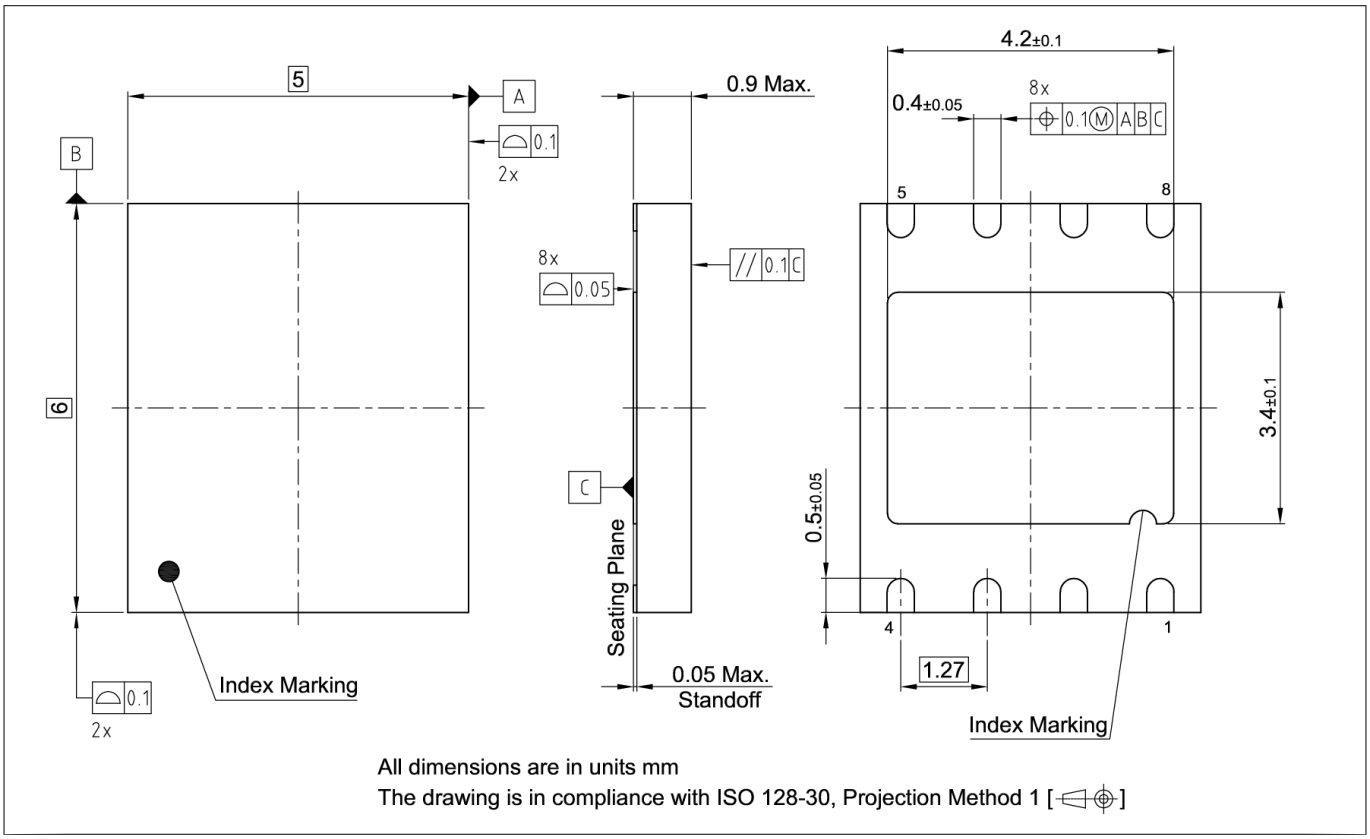


Figure 7 PG-VQFN-8-4 package outline

4.1.2 Package footprint

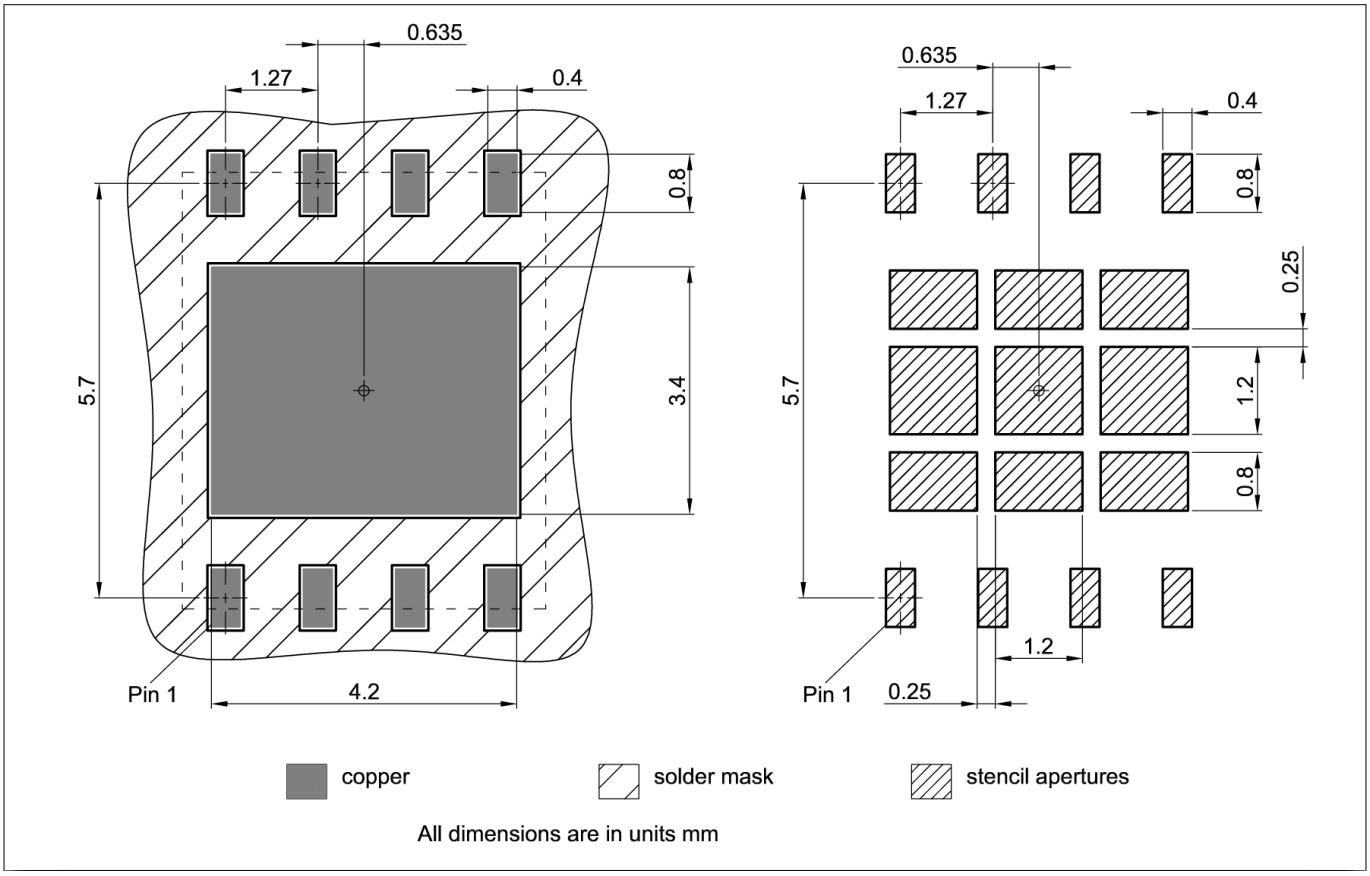


Figure 8 PG-VQFN-8-4 package footprint

4.1.3 Tape and reel packing

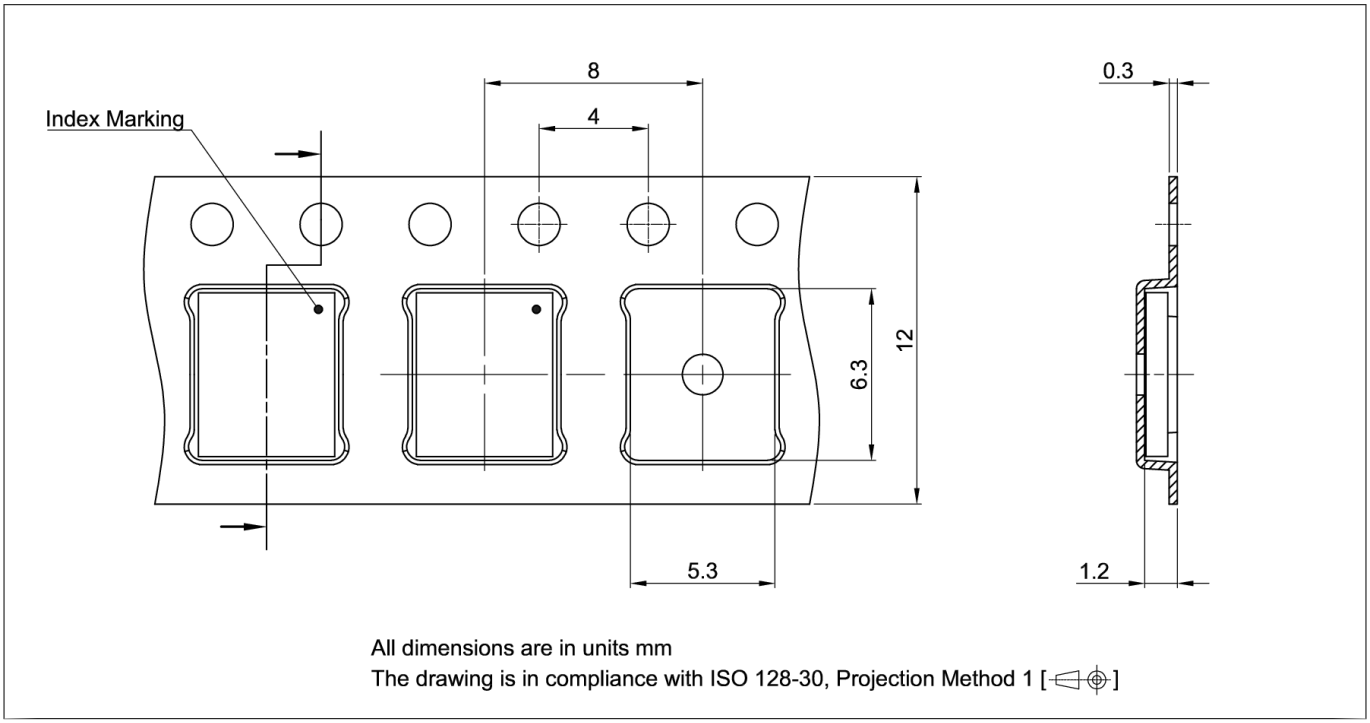


Figure 9 PG-VQFN-8-4 tape and reel packing

4.1.4 Production sample marking pattern

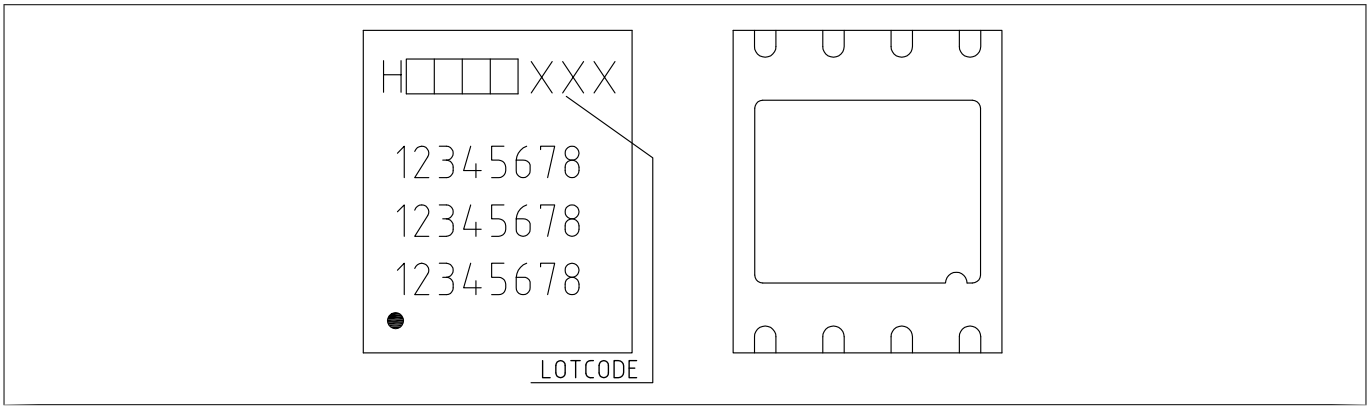


Figure 10 PG-VQFN-8-4 sample marking pattern

The dot indicates pin 01 for the chip. The “lot code” and “serial number” are defined and inserted during fabrication.

The following table describes the sample marking pattern:

Table 7 Marking table for PG-VQFN-8-4 packages

Indicator	Description
H□□□□	Engineering samples: “HE<YWW>”: • Halogen-free • Engineering Sample • <Y>: 2nd digit of production year • <WW>: Production week (calendar week) Qualified production parts: “H<YYWW>”: • Halogen-free • <YY>: Production year • <WW>: Production week (calendar week)
XXX	Lot code, defined and inserted during fabrication, issued by the packaging site
12345678	Product name (example: OC1120)
12345678	Configuration (example: OC101, OC102)
12345678	Empty (reserved for future use)

4.1.5 Package layout

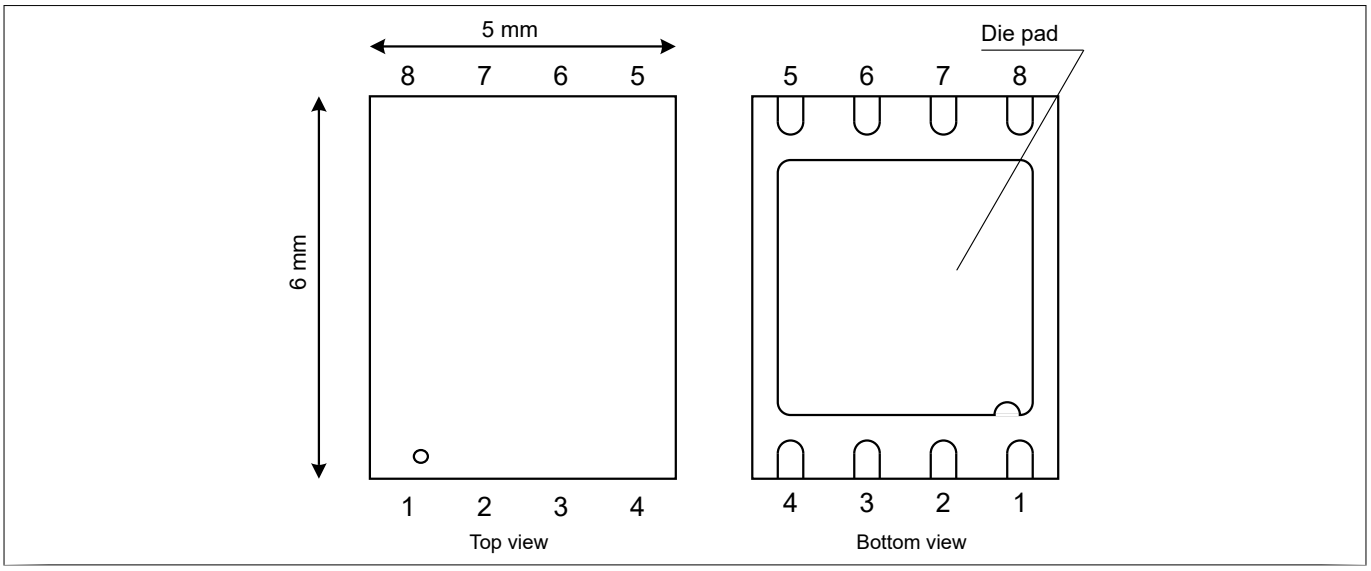


Figure 11 PG-VQFN-8-4 package layout

Pad-to-signal reference

The contacts and their functionality are given in the table below.

Table 8 Pad-to-signal reference for PG-VQFN-8-4

Pad	Symbol	Pin type	Buffer type	Signal function/remarks
01	GND	GND	-	Power supply: Common ground reference (V_{SS})
02	NC	-	-	No internal connection/do not connect externally
03	UART_IO	I/O	GPIO_IO	UART_IO according to ISO/IEC 7816-3 [16]

(table continues...)

Table 8 (continued) Pad-to-signal reference for PG-VQFN-8-4

Pad	Symbol	Pin type	Buffer type	Signal function/remarks
04	NC	-	-	No internal connection/do not connect externally
05	NC	-	-	No internal connection/do not connect externally
06	UART_CLK	I	GPIO_I	UART_CLK according to ISO/IEC 7816-3 [16]
07	UART_RST	I	GPIO_I	UART_RST according to ISO/IEC 7816-3 [16]
08	V_{DD}	PWR	-	Power supply: Chip power and pad supply (V_{DD})

4.2 Chip scale packages

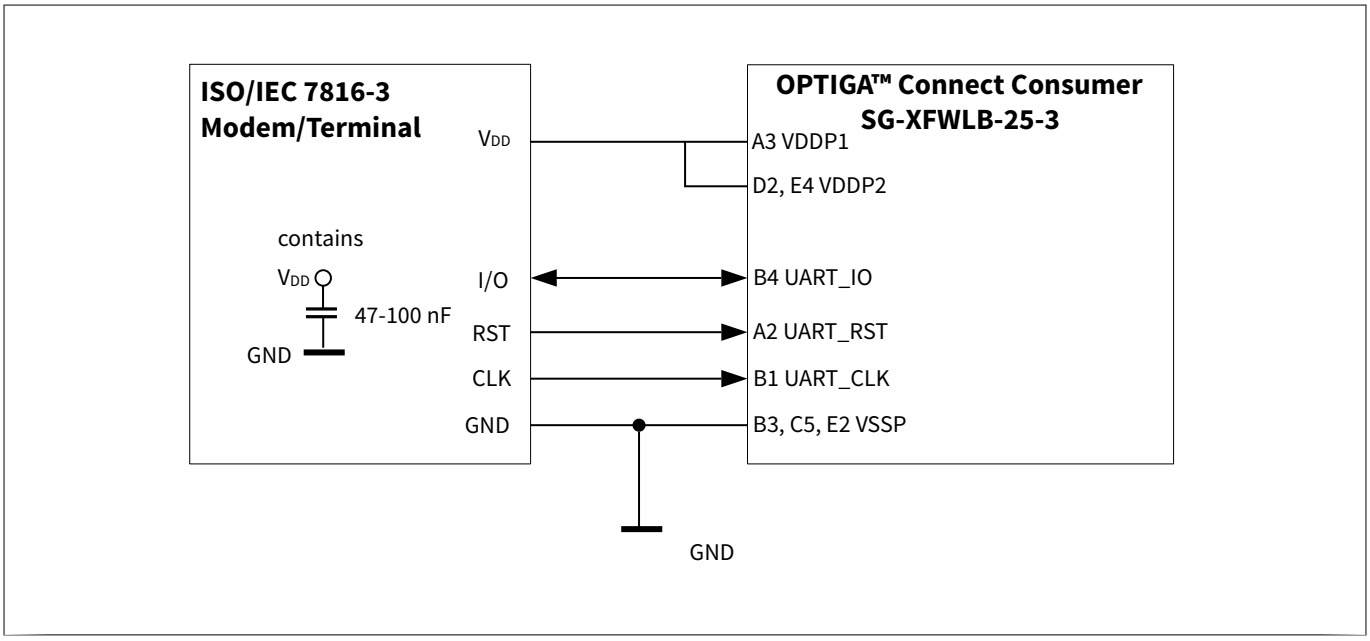


Figure 12 SG-XFWLB-25-3 schematic diagram

The following packages are available:

- SG-XFWLB-25-3[2)]

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

- Package outline: Shows the package dimensions of the controller in the individual packages
- Package footprint: Shows footprint recommendations
- Tape and reel packing
- Sample marking pattern: Describes the productive sample marking pattern on the package
- Package layout: Shows a simple layout with the pin numbers described in the pad-to-signal reference section

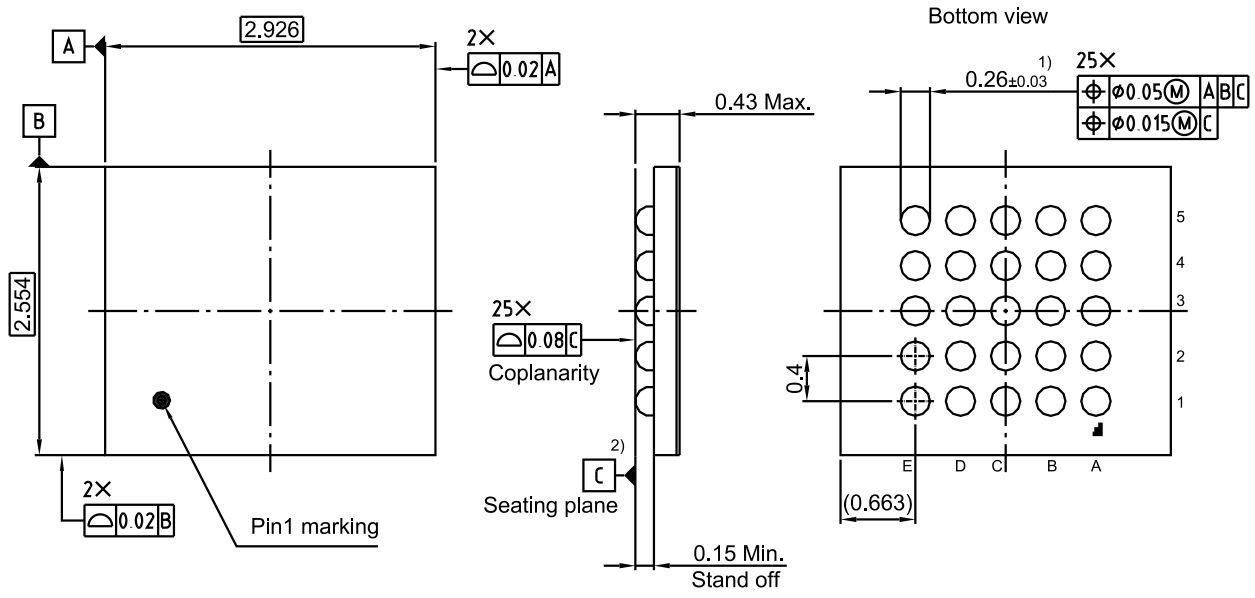
Note: Unless specified otherwise, all figure dimensions are given in mm.

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

2 -3 = with Back Side Protection.

4.2.1 Package outline

The package dimensions (in mm) of the controller in SG-XFWLB-25-3 packages are given below.



1) Dimension is measured at the maximum solder ball diameter, parallel to primary datum c
2) Primary datum c and seating plane are defined by the domed crowns of the balls
All dimensions are in units mm
The drawing is in compliance with ISO 128-30, Projection Method 1 [ ]
Drawing according to ISO 8015, general tolerances ISO 2768-mK

Figure 13 SG-XFWLB-25-3 package outline

4.2.2 Package footprint

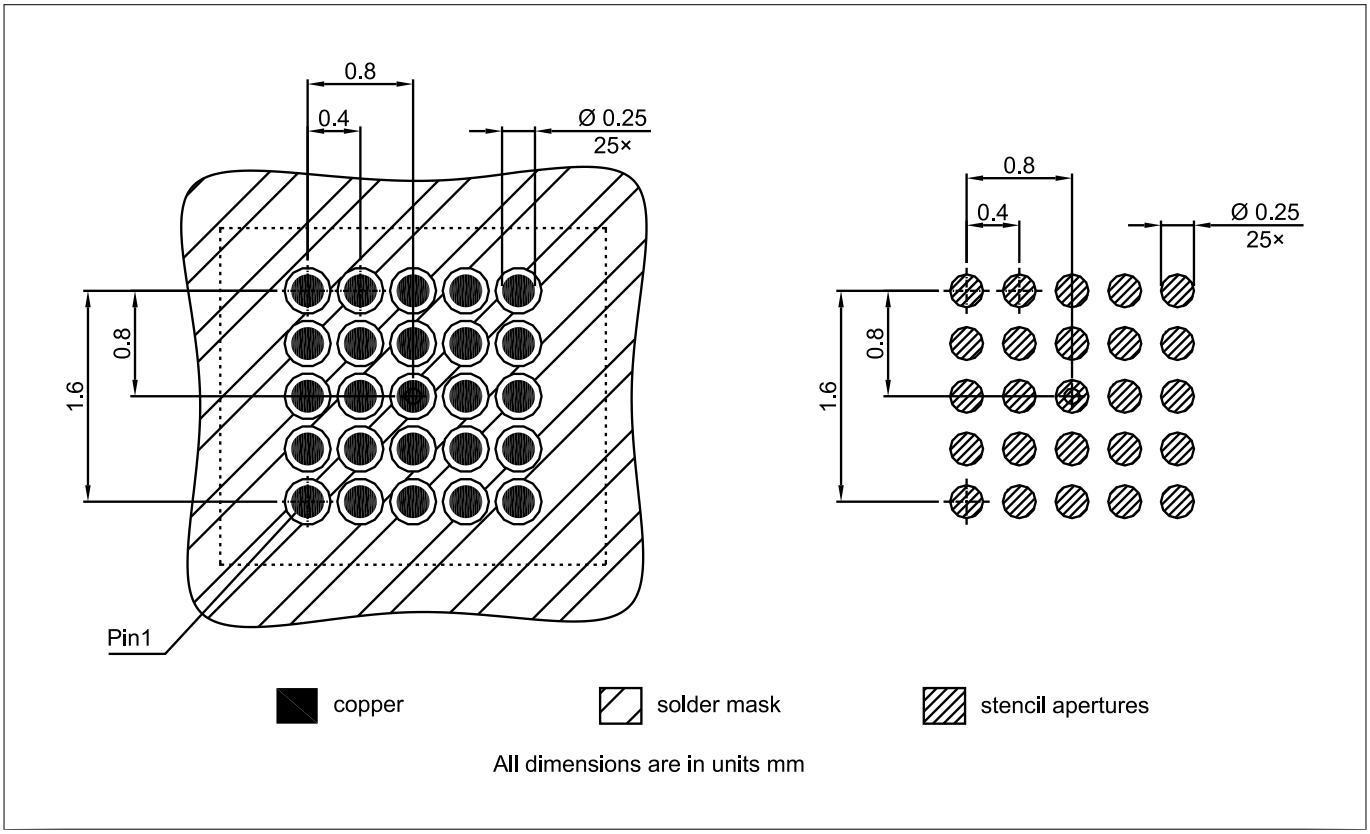


Figure 14 SG-XFWLB-25-3 package footprint

4.2.3 Tape and reel packing

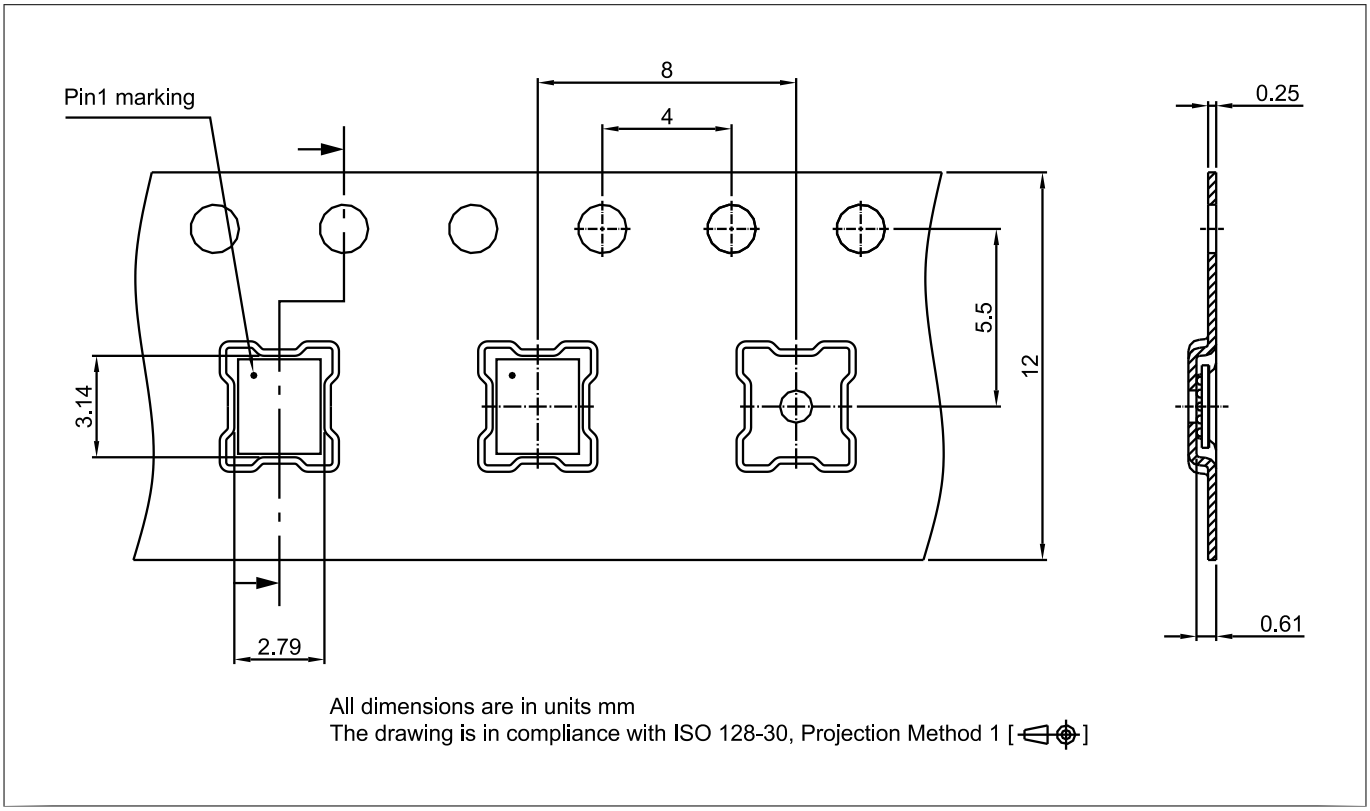


Figure 15 SG-XFWLB-25-3 tape and reel packing

4.2.4 Production sample marking pattern

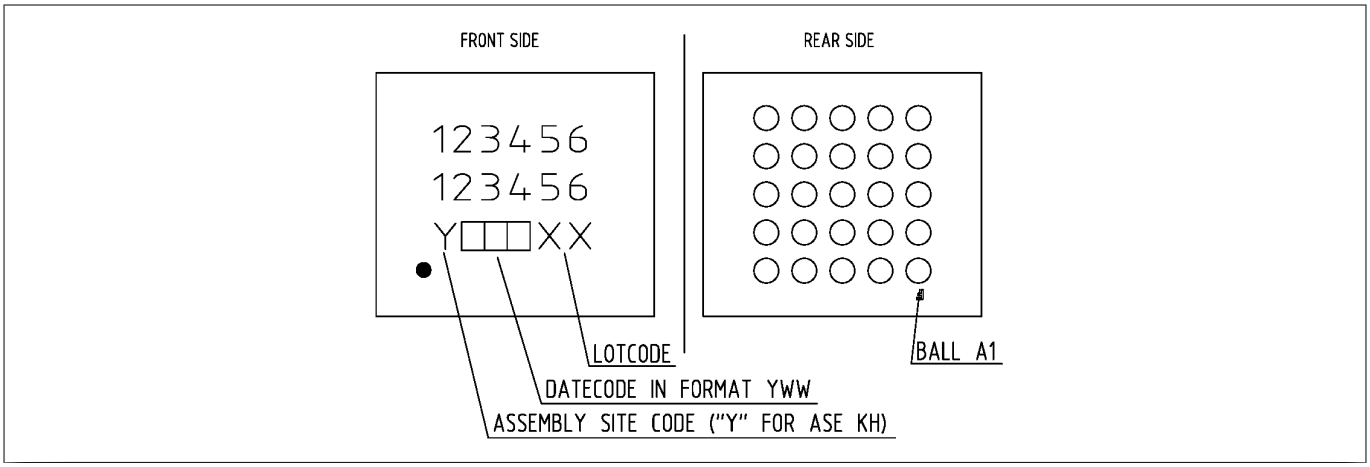


Figure 16 SG-XFWLB-25-3 sample marking pattern

The dot indicates pin 01 for the chip. The “lot code” and “serial number” are defined and inserted during fabrication.

The following table describes the sample marking pattern:

Table 9 Marking table for SG-XFWLB-25-3 packages

Indicator		Description
Y□□□XX	Y	Assembly site code • Y = ASE KH
	□□□	Date code • □: 2nd digit of production year • □□: Production week
	XX	Lot code, defined and inserted during fabrication, issued by the packaging site
123456		Product name (example: OC1120)
123456		Configuration (example: OC101, OC102)

4.2.5 Package layout

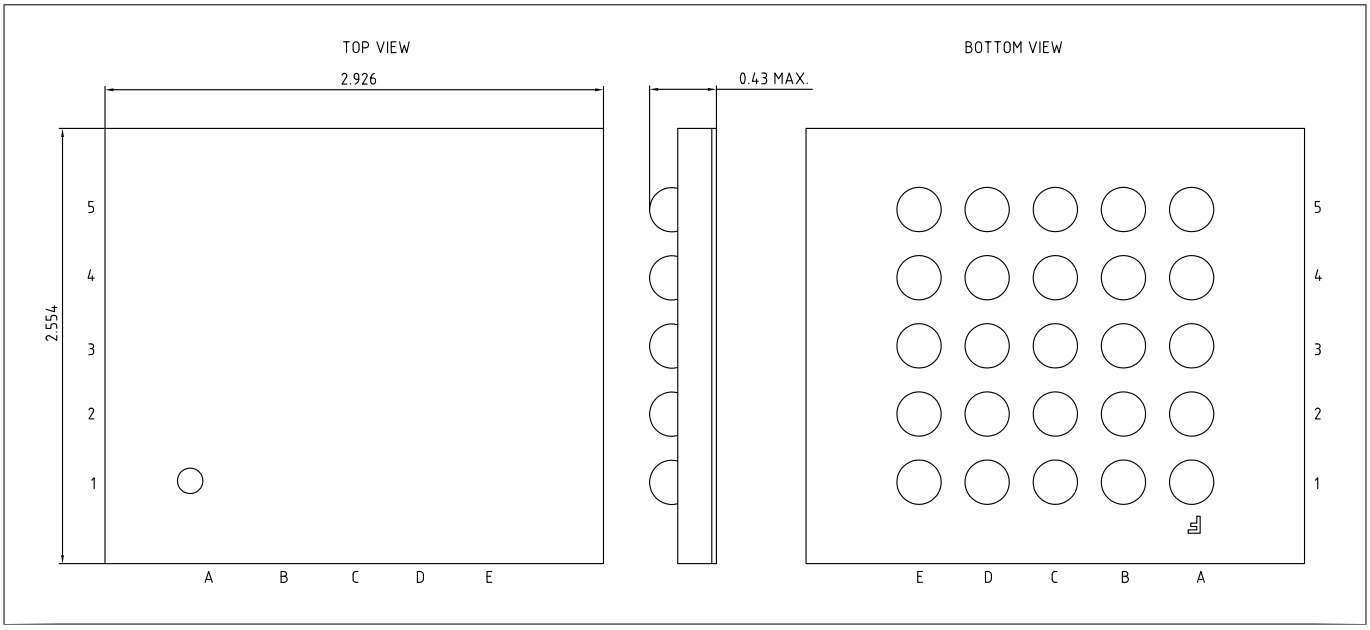


Figure 17 SG-XFWLB-25-3 package layout

Pad-to-signal reference

The contacts and their functionality are given in the table below.
Balls not listed in the following table are not connected.

Table 10 Pad-to-signal reference for SG-XFWLB-25-3

Ball	Symbol	Pin type	Buffer type	Signal function/remarks
A2	UART_RST	I	GPIO_IO	UART_RST according to ISO/IEC 7816-3 [16]
B1	UART_CLK	I	GPIO_IO	UART_CLK according to ISO/IEC 7816-3 [16]
B4	UART_IO	I/O	GPIO_IO	UART_IO according to ISO/IEC 7816-3 [16]
B3, C5, E2	VSSP	GND	-	Power supply: Common ground reference (V_{SS})
A3	VDDP1	PWR	-	Power supply: Chip power and pad supply usage Connect to common supply voltage

(table continues...)

Table 10 (continued) Pad-to-signal reference for SG-XFWLB-25-3

Ball	Symbol	Pin type	Buffer type	Signal function/remarks
D2, E4	VDDP2	PWR	-	Power supply: Chip power and pad supply usage Connect to common supply voltage
A1, A5, B2, C3, E1, E5	NC	-	-	No internal connection. Do not connect externally!
A4, B5, C1, C2, C4, D1, D3, D4, D5, E3	RFU	-	-	Reserved for future use. Do not connect externally!

4.3 Ordering information

The OPTIGA™ Connect Consumer OC1120 is available with the following sales codes:

Table 11 Sales codes described in this document

Sales code	Free user NVM[1)]	Package	Key characteristics
OC1120-0810WLB25	800 KB	XFWLB-25-3	GSMA SGP.21 v2.2 [10] and GSMA SGP.22 v2.2.2 [11] compliant TCA eUICC Profile Package V2.3.1 [17] compliant
OC1120-0810VQFN8	800 KB	VQFN-8-4	

1) Actual free user memory may differ and depends on configuration, pre-installed profiles and pre-installed applets.

5 Contact information

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

References

ETSI

[1] ETSI TS 102 221: *Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release-12)*; 2014-12
[2] ETSI TS 102 223: *Technical Specification; Smart Cards; Card Application Toolkit (CAT) (Release-11)*
[3] ETSI TS 102 225: *Secured packet structure for UICC based applications (Release-11)*
[4] ETSI TS 102 226: *Remote APDU structure for UICC based applications (Release-11)*
[5] ETSI TS 102 241: *UICC Application Programming Interface (UICC API) for Java Card™ (Release-11)*
[6] ETSI TS 135 208: *Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design conformance test data (Release-15)*
[7] ETSI TS 135 208: *Technical Specification; Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Specification of the TUAK algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: Algorithm specification (Release-15)*
[8] ETSI TS 102 613: *Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics (Release 11)*; 2012-09

GlobalPlatform

[9] GlobalPlatform: *Card Specification V2.2.1*; January-2011

GSMA

[10] GSM Association SGP.21: *Architecture Specification V2.2,*; 2017-09-01
[11] GSM Association SGP.22: *RSP Technical Specification, version 2.2.2*; 2020-06-05
[12] GSM Association FS.04: *Security Accreditation Scheme for UICC Production - Standard (Version 9.0)*; 2019-06-26

Infineon Technologies AG

[13] 32-bit Security Controller: *V07 Integration Guide, Revision 1.5*; 2018-04-11
[14] Package Specification: *SG-XFWLB-25-3, Edition 02*; July-2019
[15] Recommendations: *For Board Assembly of Infineon Wafer Level Ball Grid Array Packages, Revision 4.0*; 2019-03-15

ISO/IEC

[16] ISO/IEC 7816-3:2006: *Identification cards - Integrated circuit cards - Part 3: Cards with contacts - Electrical interface and transmission protocols (Third edition)*; 2006-11

TCA

[17] Trusted Connectivity Alliance (TCA) eUICC Profile Package: *Interoperable Format Technical Specification, Version 2.3.1*; November-2019

3GPP

[18] 3GPP TS 31.102: *Characteristics of the Universal Subscriber Identity Module (USIM) application (Release-15)*
[19] 3GPP TS 31.103: *Characteristics of the IP Multimedia Services Identity Module (ISIM) application (Release-11)*
[20] 3GPP TS 31.111: *Universal Subscriber Identity Module (USIM) Application Toolkit (USAT), (Release-15)*
[21] 3GPP TS 31.115: *Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications (Release-15)*

References

[22] 3GPP TS 31.116: *Remote APDU Structure for (U)SIM Toolkit applications (Release-15)*
[23] 3GPP TS 31.130: *(U)SIM Application Programming Interface (API); (U)SIM API for Java Card™ (Release-13)*
[24] 3GPP TS 31.133: *IP Multimedia Services Identity Module (ISIM) Application Programming Interface (API); ISIM API for Java Card™ (Release-10)*
[25] 3GPP TR 31.919: *2G/3G Java Card™ API based applet interworking (Release-8)*
[26] 3GPP TS 33.501: *5G Security architecture and procedures for 5G System (Release-15)*; 2019-05
[27] 3GPP TS 35.231: *Universal Mobile Telecommunications System (UMTS); LTE; Specification of the TUAK algorithm set: A second example algorithm set (Release-15)*
[28] 3GPP TS 51.011: *Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (Release-5)*

3GPP2

[29] 3GPP2 C.S0023-D: *Rev.D V1.0 Removable User Identity Module for Spread Spectrum Systems*
[30] 3GPP2 C.S0065-B: *Rev.B V2.0 cdma2000 Application on UICC for Spread Spectrum Systems*
[31] 3GPP2 X.S0004-000-E: *v9.0, Mobile Application Part (MAP)*; June-2009

Java Card

[32] Oracle: Java Card™ Platform Specification, Classic Edition 3.0.5, including: *Java Card™ Platform Virtual Machine Specification, Java Card™ Platform, Runtime Environment Specification, Java Card™ Platform, API Classic Edition 3.0.5*; June-2015

Glossary

3GPP

3rd Generation Partnership Project (3GPP)

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 (i.e. the same key is used for both encryption and decryption).

API

application programming interface (API)

CAVE

cellular authentication and voice encryption (CAVE)

CBC

cipher block chaining (CBC)

CLK

clock (CLK)

CRC

cyclic redundancy check (CRC)
A procedure that uses a checksum to check the validity of a data transfer.

DES

Data Encryption Standard (DES)
The standard referring to a symmetric-key algorithm for the encryption of electronic data.

DSA

Digital Signature Algorithm (DSA)
Federal Information Processing Standard for digital signatures based on the mathematical concept of modular exponentiation and the discrete logarithm problem.

ECC

elliptic curve cryptography (ECC)

eSIM

embedded subscriber identity module (eSIM)

ESSC

enhanced synchronous serial slave controller (ESSC)
This module provides an SPI slave-compatible interface.

ETSI

European Telecommunications Standards Institute (ETSI)

eUICC

embedded universal integrated circuit card (eUICC)

GP
GlobalPlatform (GP)

GPIO
general purpose input/output (GPIO)

GSMA
GSM Association (GSMA)

ICC
integrated card circuit (ICC)

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

ISIM
IP multimedia services identity module (ISIM)

ISO
International Organization for Standardization (ISO)

ITL
image trusted loader (ITL)

LTE
long-term evolution (LTE)

MNO
mobile network operator (MNO)

NVM
non-volatile memory (NVM)

OTA
over-the-air (OTA)

RAM
remote application management (RAM)

RFM
remote file management (RFM)

RFU
reserved for future use (RFU)

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)

SGP.2x
GSMA consumer eSIM specifications

SIM
subscriber identity module (SIM)

SMS
short message service (SMS)

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.

UICC
universal integrated circuit card (UICC)

USIM
universal subscriber identity module (USIM)

Revision history

Reference	Description
Revision 1.1, 2023-05-17	
Updated	Network algorithms
Revision 1.0, 2022-04-07	
All	Initial release

Trademarks

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

Edition 2023-05-17

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-snb1649313962745

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.