Sentinel LDK

SENTINEL HL CHIP FORM FACTOR VQFN32 – TECHNICAL SPECIFICATION GUIDE

Revision History

Part number 007-13274-001, Revision C, 2209-1

Disclaimer and Copyrights

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.
Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as “Thales”) information.
This document can be used for informational, non-commercial, internal and personal use only provided that:
• The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
• This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.
Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.
The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein. The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.
Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.
Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

CONTENTS

SENTINEL HL CHIP FORM FACTOR VQFN32 TECHNICAL SPECIFICATIONS GUIDE

Introduction

Description

Sentinel HL keys protect software against piracy and illegal copying. Access to and execution of the protected software is permitted only when the protected software communicates with the Sentinel HL key. A secure communications channel is established for each communication session between the highly secure, impenetrable AES 128-bit encryption engine on the Sentinel HL key and the application. The secure communication channel between the Sentinel HL key and the application offers powerful resistance to “man-in-the-middle” and brute force attacks. A secure, non-external storage device stores licenses, passwords, strings, and application dependent data in its own internal protected read/write memory.

A secure, trusted execution environment (AppOnChip) inside the keys is supplied to run customer’s application code.

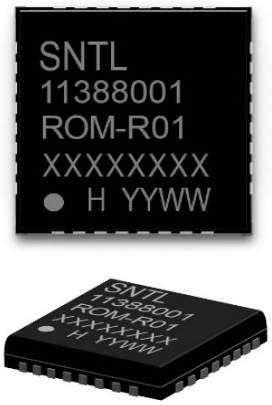
Certain Sentinel HL keys are available using the Sentinel HL Chip form factor. The Sentinel HL Chip is embedded within your device, further enhancing security. This technical specifications guide describes the physical characteristics of the Sentinel HL Chip form factor.

The Sentinel HL Chip is compatible with Sentinel LDK v7.8 or later.

Features

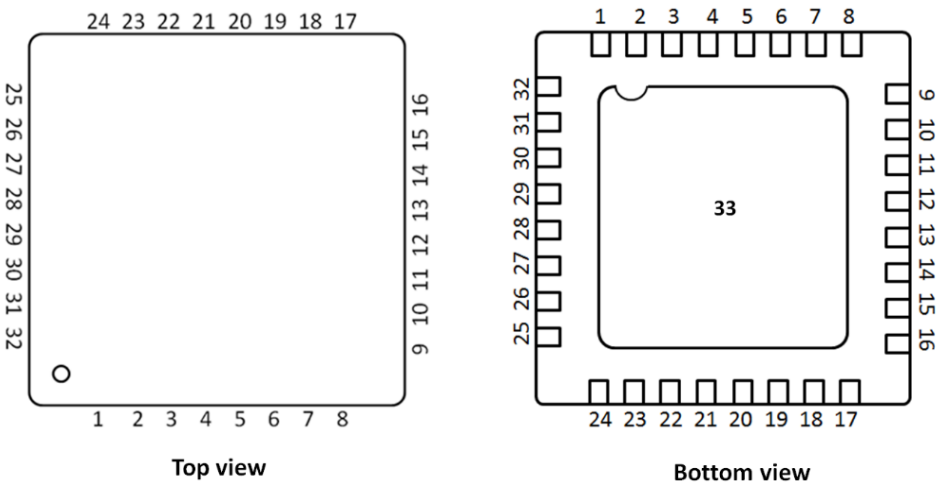
- High performance, low power SmartCard chip
- Supply voltage: from 3.0V to 3.6V
- Operating temperature range: -40°C ~ +105°C
- Full-speed USB 2.0 interface, embedded pull-up resistor
- (Optional) SPI interface upon request
- ESD Protection up to 2000V for LED pin and 4000V for USB interface pins
- Hardware AES Engine
- AES/ECC based Secure Tunnel
- Unique serial number for each chip
- VQFN Package (RoHS compliant)
- An on-chip oscillator generates the system clock.
- AppOnChip

Sentinel HL Chip



VQFN-32-13
(Reference Only)

Pin Configuration



Pin Number	Pin Name	Description
Pin 5	DP	USB D+ differential data
Pin 7	I/F_Config	Interface configuration: If this pin is connected to VCC, the SPI interface is enabled. If this pin is connected to GND, the USB interface is enabled. **Note:** This pin must not be left open.
Pin 8	VCC	Power supply input
Pin 10	MOSI	SPI slave input
Pin 11	MISO	SPI slave output
Pin 12	SCLK	SPI slave clock
Pin 13	/SS	SPI slave select (low active)
Pin 17, 33	GND	Common ground reference

Pin Number	Pin Name	Description
Pin 20	DM	USB D- differential data
Pin 1-4, 6, 9, 14-16, 18-19, 21-32	NC	These pins should be left open.

Characteristics

Maximum Ratings

Table 1: Absolute Maximum Ratings

Parameter	Symbol	Min.	Max.	Unit
Supply Voltage	V_{CC}	-0.3	+7.0	V
Signal DP/DM, Input Voltage	V_{IN_USB}	-0.3	V_{CC}+0.3	V
Storage Temperature	T_S	-40	+125	°C
Junction Temperature	T_J	-40	+110	°C
Operating Temperature (T_J must be kept)	T_A	-40	+105	°C
NVM Endurance for Write/Erase Cycles	E_{NMV}	—	1 Million	Cycles
NVM Data Retention Virgin	$V_{DataRetention}$	—	10	Years
Pad Group “USB”, Pulse Voltage (ESD protection)	$V_{ESD\_USB,HBM}$	—	4000	V
	$V_{ESD\_USB,CDM}$	—	500	V
LED Pin, Pulse Voltage (ESD protection)	$V_{ESD\_USB,HBM}$	—	2000	V
	$V_{ESD\_USB,CDM}$	—	500	V

.

AC/DC Characteristics

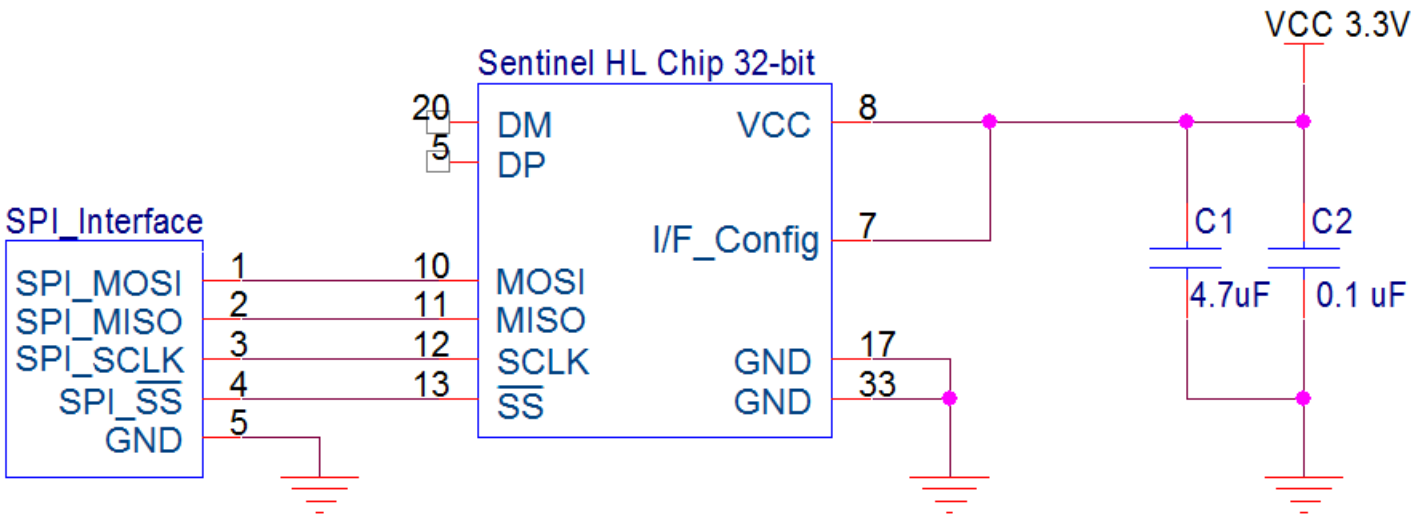
Table 2: AC/DC Characteristics (Condition: VBUS=4.4V to 5.25V; TA=25^{O}C)

Symbol	Parameter	Min.	Max.	Units
V_{CC}	Supply Voltage	3.00	3.60	V
V_{OH_USB}	Output High Voltage of USB DP/DM	2.8	3.6	V
V_{OL_USB}	Output Low Voltage of USB DP/DM	0	0.3	V
V_{IH_USB}	Input High Voltage of USB DP/DM	2.0	—	V
V_{IL_USB}	Input Low Voltage of USB DP/DM	-0.3	0.8	V
C_{LOAD_USB}	Load Capacitance	—	50	pF
Z_{IN_USB}	Input Impedance	300	—	KΩ
$I_{CC\_Run\_Mode}$	Supply Current in Running Mode	—	21	mA
I_{CC_SLEEP}	Supply Current in Sleep Mode	—	200	uA

Reference Design

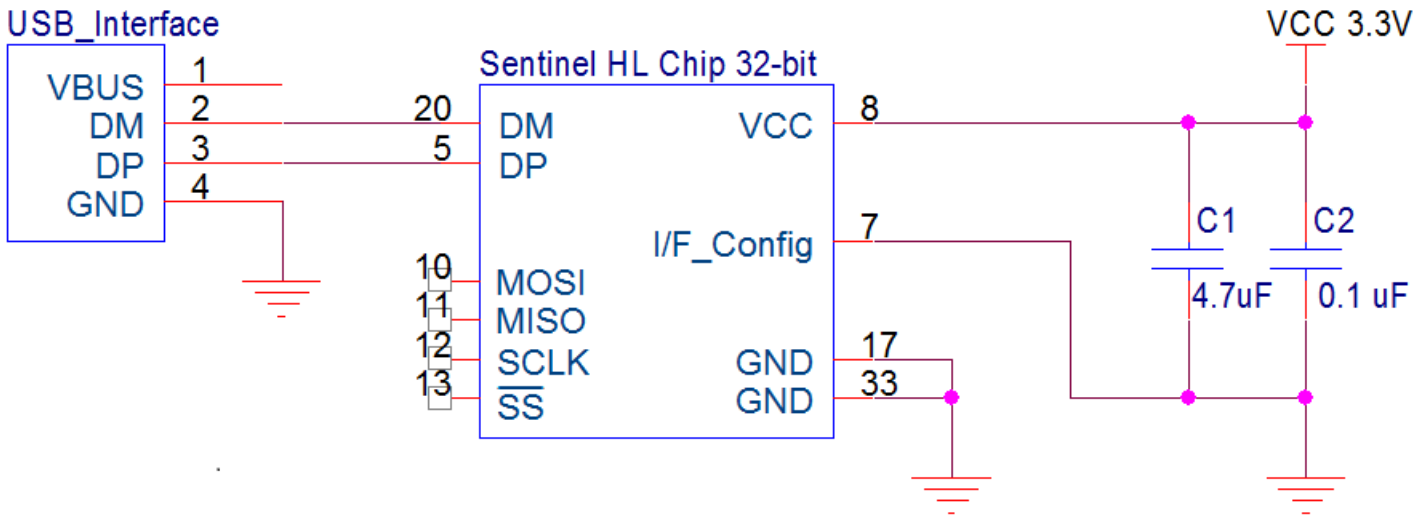
Reference Schematic

Application of SPI Interface



* Pin 5 and Pin 20 can be left open in this application.

Application of USB Interface



* Pin 10 to Pin 13 can be left open in this application.

Recommended BOM

Ref.	Description	Quantity	Manufacture P/N	Manufacturer
IC1	Sentinel HL Chip	1	942-001251-001	Thales
C1	CAP, 4.7uF, X5R,16V	1	– –	– –
C2	Ceramic capacitor, 0.1uF, X5R, 10V, 10%	1	– –	– –

Recommended PCB Layout

USB Signals

1. Place the Sentinel HL Chip on the signal layer adjacent to the GND plane.
2. Route D+ and D– on the signal layer adjacent to the GND plane.
3. Route D+ and D– before other signals.
4. Applying the ESD protection chip with Low capacitance TVS array could improve the ESD Immunity level on USB Signals. (Recommended ESD protection chips: ON Semiconductor/ESDR0502NMUTBG, SEMTECH/RCLAMP0502N)
5. Keep the GND plane solid under D+ and D–. Splitting the GND plane underneath these signals introduces impedance mismatch and increases electrical emissions.
6. Avoid routing D+ and D– through vias; vias introduce impedance mismatch. Where vias are necessary, keep them small (25-mil pad, 10-mil hole) and keep the D+ and D– traces on the same layers.
7. Keep the length of D+ and D– as short as possible.
8. Match the lengths of D+ and D– to be within 50 mils (1.25 mm) of each other to avoid skewing the signals and affecting the crossover voltage.
9. Keep constant trace spacing between D+ and D- along their route. Varying trace separation creates impedance mismatch.
10. Keep at least 250 mil (6.5 mm) distance between D+/D- and other non-static traces wherever possible.
11. Use two 45° bends or round corners instead of 90° bends.
12. Keep a minimum of five trace widths between D+ and D– and any adjacent copper pour. When placed too close to these signals, copper pour affects their impedance.

Capacitor

The decoupling capacitor C2 should be placed as close as possible to Pin_8 of the Sentinel HL Chip.

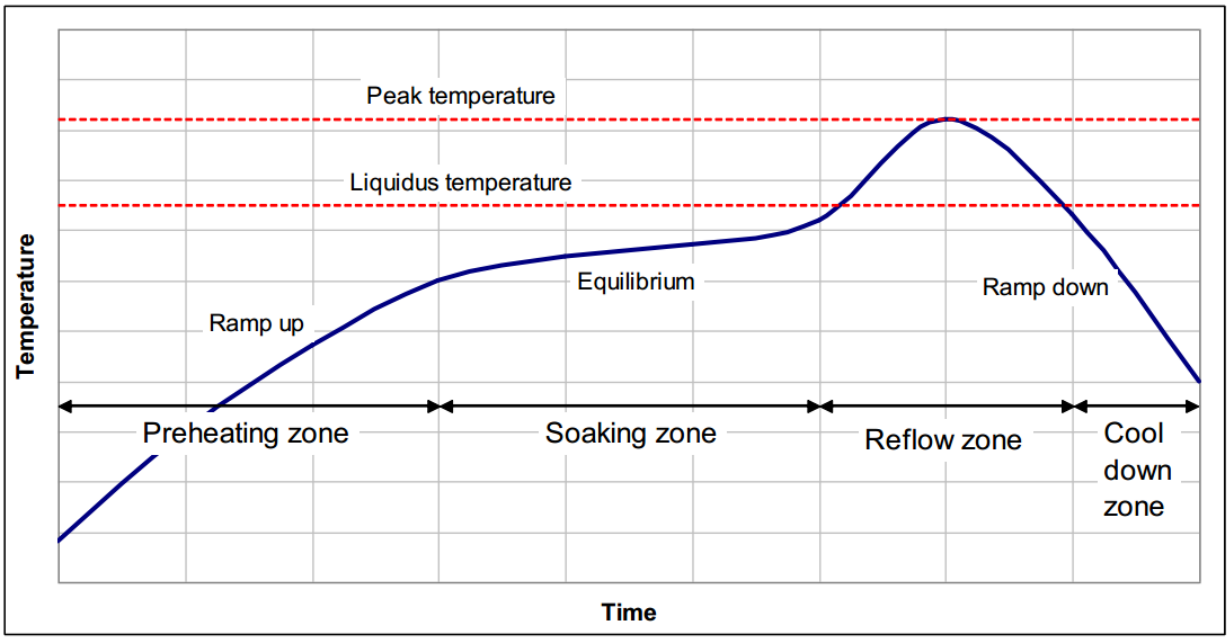
ESD Caution

ESD (electrostatic discharge) sensitive device.

Charged devices and circuit boards can discharge without detection. Although this product contains ESD circuitry, damage may occur on devices subjected to high energy ESD. Therefore, proper ESD precautions should be taken to avoid performance degradation or loss of functionality.

Soldering Reflow Temperature Profile

General forced-convection reflow solder profile



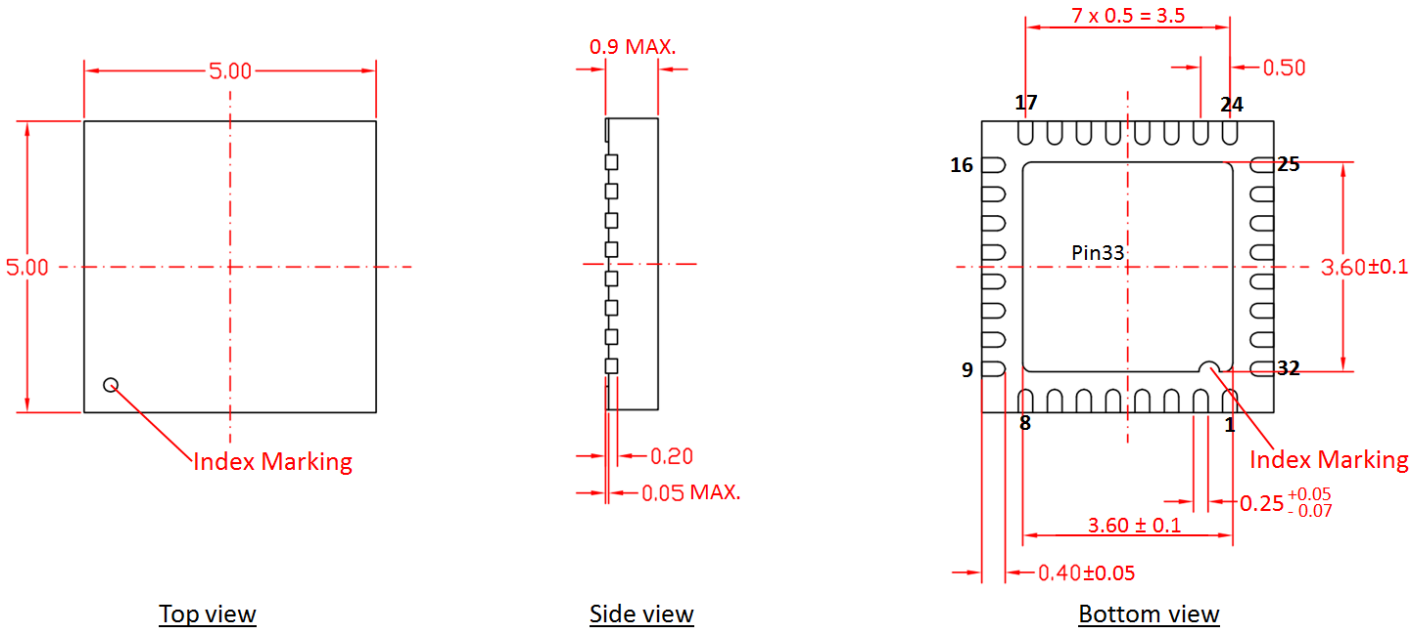
Example of the key data for a forced-convection reflow solder profile

Parameter	Minimum Value	Typical Value	Max Value (acc. IPC/JEDEC J-STD-020)	Main Influence
Preheating Rate	1.0 K/s	2.5 K/s	3.0 K/s	flux system (solder paste)
Soaking Temperature	140 – 170°C	140 – 170°C	150 – 200°C	flux system (solder paste)
Soaking Time	50 s	80 s	120 s	flux system (solder paste)
Peak Temperature	230°C	245°C	260°C	alloy (solder paste)

Parameter	Minimum Value	Typical Value	Max Value (acc. IPC/JEDEC J-STD-020)	Main Influence
Reflow Time Above Melting Point (liquidus)	40 s	60 s	150 s	alloy (solder paste)
Cool-down	1.0 K/s	2.5 K/s	8.0 K/s	

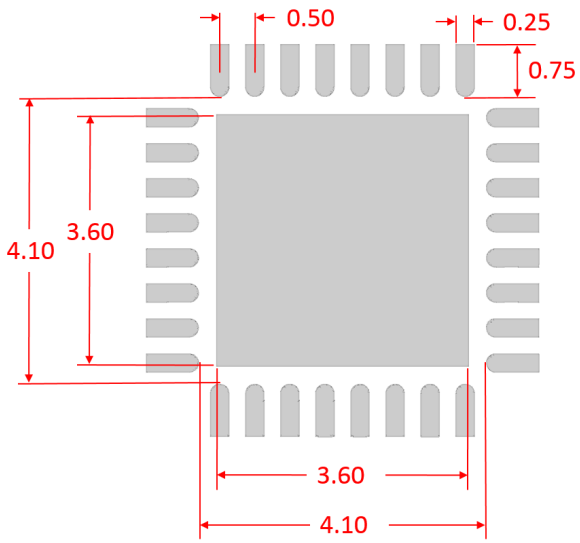
Package Configuration

Figure 1: VQFN32-13 Package Characteristics (Unit: mm)

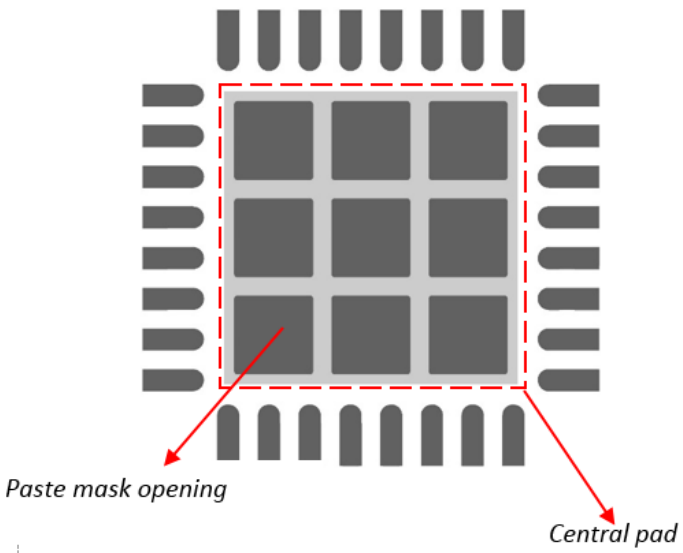


Top view Side view Bottom view

Figure 2: Recommended Land Pattern (Unit: mm)



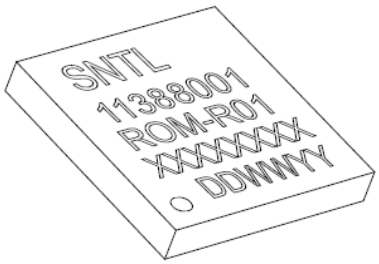
Recommended Land Pattern



Recommended Paste Mask Opening Pattern

The area of paste mask openings should account for more than 60% of the whole area in the central pad.

Marking Instructions



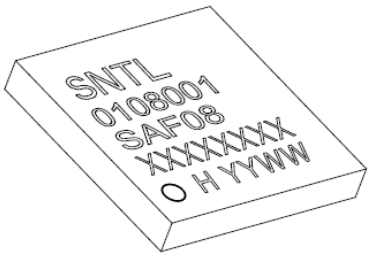


Table 3: Marking Definition

	Comment	Description
Line 1	SNTL	Logo
Line 2	11388001(Existing) 0108001(New release)	Chip ID number
Line 3	ROM-R01 (Existing) SAF08 (New release)	FW-HW version or revision
Line 4	XXXXXXXX	Lot number
Line 5	Dot, YYWW	Pin 1, Production date code in YYWW format

Packaging

Sentinel HL Chips are packaged using a tube packing system.

Two types of tubes are available:

- Tube 1: 160mm, containing 25 chips each
- Tube 2: 381mm, containing 70 chips each

For more information on packaging, contact your Thales representative.

Tube Packaging Specifications

A tube packing system protects the IC from damage during shipping and storage and is designed for automatic pick-and-place equipment.

Figure 3: Tube 1 Dimensions (mm)

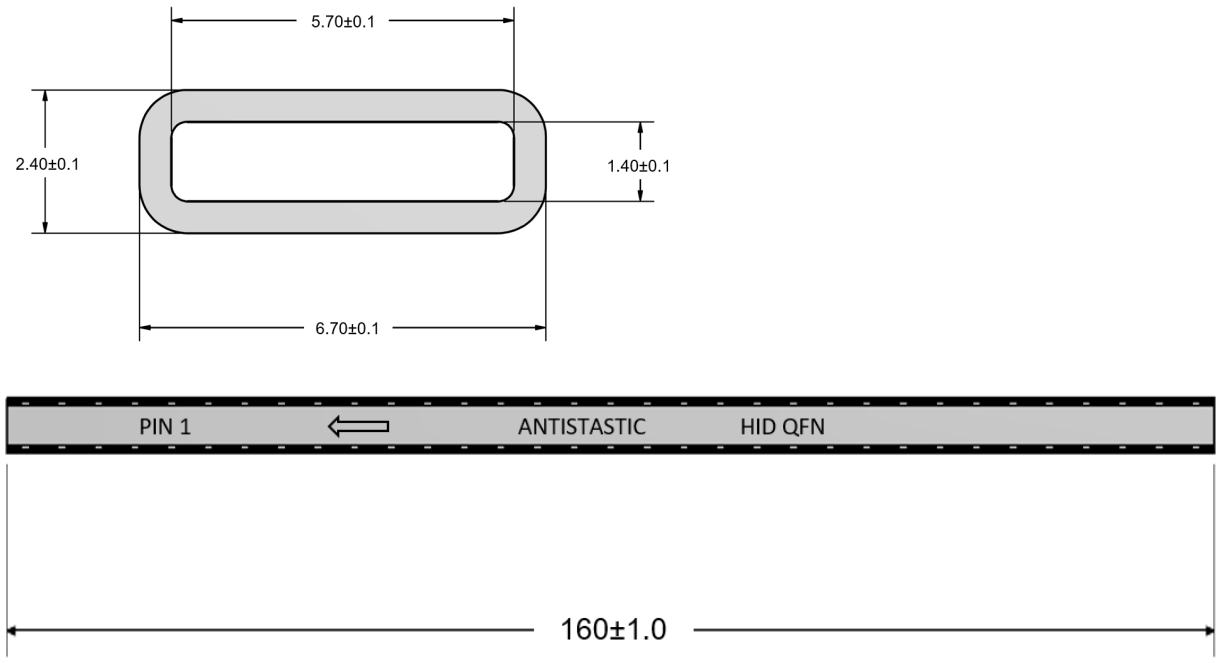
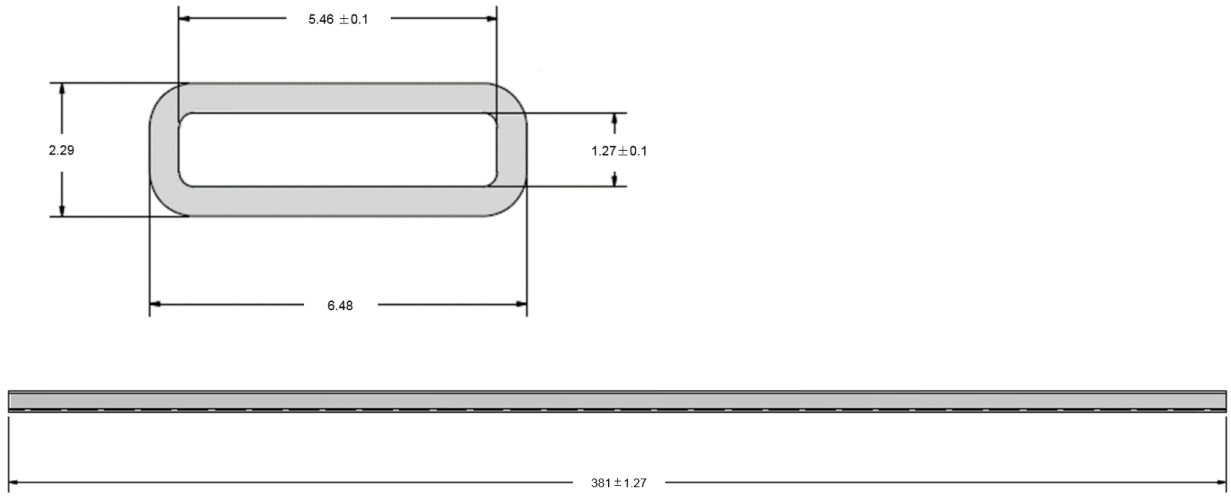


Figure 4: Tube 2 Dimensions (mm)



Labels On Packaging

Package content labels and MSL labels are provided as described in this section.

Package Content Label

Human-readable and machine-readable labels are provided on the packaging bag and carton box. The contents of each label are listed below:

- P/N: Manufacturer Part Number and Revision
- IPN: Internal (Thales) Part Number
- Date Code: Programming Date Code
- IC Lot No.
- Quantity
- COO: Country of Origin
- MSL: Moisture Sensitive Level
- Max. Reflow Temp.: Maximum Reflow Temperature
- Package
- ESD Protection, RoHS compliance, China RoHS LOGO

Refer to the figure below for details.

Figure 5: Packaging Label

MSL Label

An MSL label is affixed on the packaging bag with following information:

Figure 6: MSL Label