Sentinel LDK

SENTINEL HL BOARD FORM FACTOR – TECHNICAL SPECIFICATION GUIDE

Revision History

Part number 007-012421-002, Revision A, 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

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.

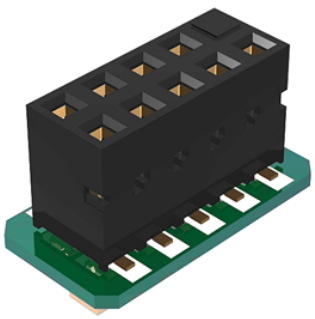
The Sentinel HL Max key is available using the Sentinel HL Board form factor. The Sentinel HL Board is embedded within your device, further enhancing security. This technical specifications guide describes the physical characteristics of the Sentinel HL Board form factor.

The Sentinel HL Board is compatible with Sentinel LDK v.7.1 and later.

Features

- High performance, low power SmartCard chip
- Connector: Socket, Pitch 2.54mm, 5 x 2Row
- Operation Ranges: from 3.0V to 5.5V
- Full-speed USB 2.0 interface, embedded pull-up resistor
- ESD Protection to 6000V of USB interface pin
- Hardware AES Engine
- Secure Tunnel
- Unique serial number for each chip
- RoHS & Lead Free compliant

Sentinel HL Board

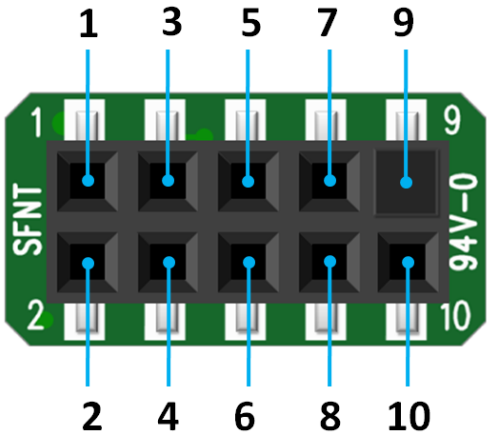


Security

- Dedicated hardware for protection against SPA/DPA/SEMA/DEMA attacks
- Advanced protection against physical attack, including active shield
- Environmental protection systems(voltage, frequency, temperature, light monitors …)
- Secure memory management/access protection (supervisor mode)

Characteristics

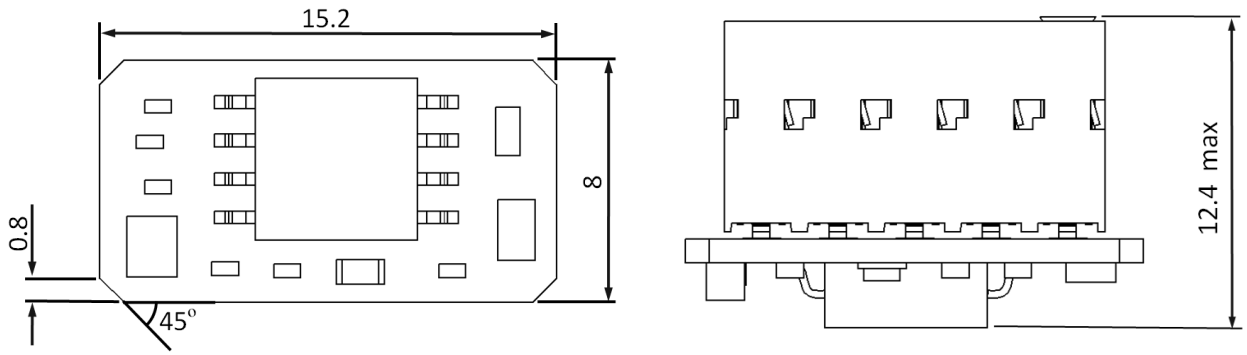
USB Interface Configuration

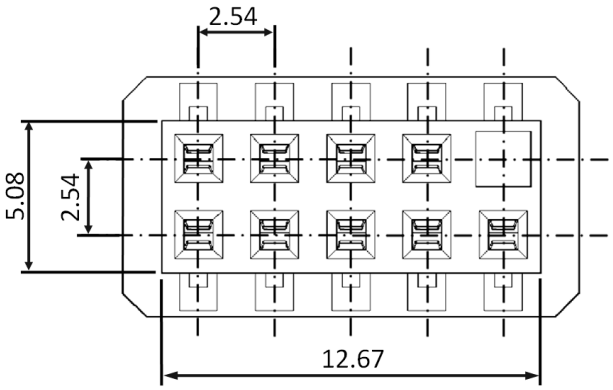


Contacts No.	Pin Name	Contacts No.	Pin Name
1	VBUS	2	NC
3	USB_Data-	4	NC
5	USB_ Data+	6	NC
7	GND	8	NC
9	Keyed	10	NC

Dimensions

(Unit = mm)





Maximum Ratings

Table 1: Absolute Maximum Ratings

Parameter	Symbol	Min.	Max.	Unit
Supply Voltage	V_{BUS}	-0.3	7.5	V
Input Voltage	V_{IN}	Vss-0.3	V_{BUS}+0.3	V
Operating Temperature	T_A	-25	+85	°C
EEPROM Endurance for Write/Erase Cycles	E_{EEPROM}		1 Million	Cycles
EEPROM Data Retention Virgin	$V_{DataRetention}$		10	Years
Electrostatic Discharge (HBM)	ESD		*2(Clock pin) *4(LED pin) *6(USB pin)	kV
Latch-up			+/- 200	mA

*The Clock pin, LED pin and USB pin are the pins of smart card chip on this board. These pins represent the most ESD-sensitive part in this board.

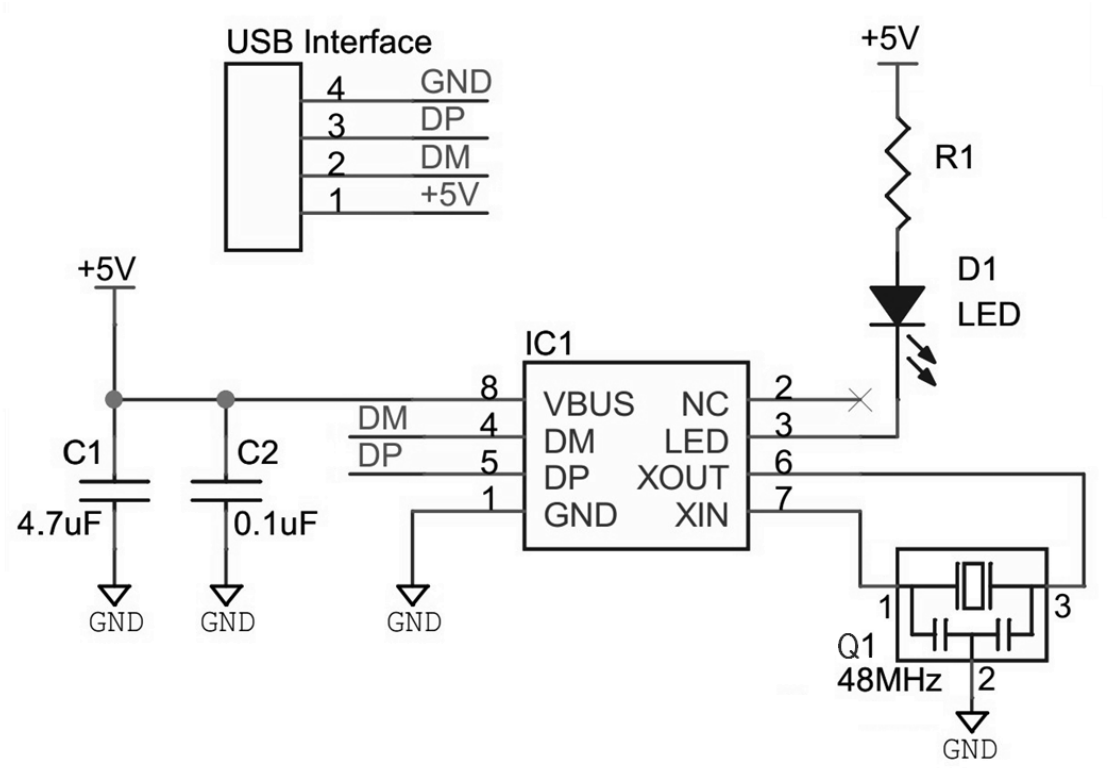
AC/DC Characteristics

Table 2: AC/DC Characteristics (Condition: VBUS=4.5V to 5.5V; T=–25°C to +85°C)

Symbol	Parameter	Min.	Typ.	Max.	Units
V_{BUS}	Supply Voltage	3.0	—	5.5	V
f_{CLK}	CPU Frequency (internal)	28	33	38.5	MHz
$I_{Run\ Mode}$	Supply Current in Run Mode			17	mA
$I_{Standby}$	Supply Current in Standby Mode			0.4	mA

Reference Design

Reference Schematic



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.