congatec Application Note

Affected Products	All SMARC products
Subject	SPI TPM Reference Design
Confidential/Public	Public
Author	SDA

Revision History

Revision	Date (yyyy-mm-dd)	Author	Changes
1.0	2020-10-28	SDA	First release

Preface

This application note provides the reference design and design notes for SPI TPM used on SMARC carrier boards.

Disclaimer

The information contained within this Application Note, including but not limited to any product specification, is subject to change without notice.

congatec AG provides no warranty with regard to this Application Note or any other information contained herein and hereby expressly disclaims any implied warranties of merchantability or fitness for any particular purpose with regard to any of the foregoing. congatec AG assumes no liability for any damages incurred directly or indirectly from any technical or typographical errors or omissions contained herein or for discrepancies between the product and the Application Note. In no event shall congatec AG be liable for any incidental, consequential, special, or exemplary damages, whether based on tort, contract or otherwise, arising out of or in connection with this Application Note or any other information contained herein or the use thereof.

Intended Audience

This Application Note is intended for technically qualified personnel. It is not intended for general audiences.

Electrostatic Sensitive Device

All congatec AG products are electrostatic sensitive devices and are packaged accordingly. Do not open or handle a congatec AG product except at an electrostatic-free workstation. Additionally, do not ship or store congatec AG products near strong electrostatic, electromagnetic, magnetic, or radioactive fields unless the device is contained within its original manufacturer's packaging. Be aware that failure to comply with these guidelines will void the congatec AG Limited Warranty.

Technical Support

congatec AG technicians and engineers are committed to providing the best possible technical support for our customers so that our products can be easily used and implemented. We request that you first visit our website at www.congatec.com for the latest documentation, utilities and drivers, which have been made available to assist you. If you still require assistance after visiting our website then contact our technical support department by email at support@congatec.com

Symbols

The following are symbols used in this application note.

Note

Notes call attention to important information that should be observed.

Caution

Cautions warn the user about how to prevent damage to hardware or loss of data.

Warning

Warnings indicate that personal injury can occur if the information is not observed.

Copyright Notice

Trademarks

Product names, logos, brands, and other trademarks featured or referred to within this user’s guide or the congatec website, are the property of their respective trademark holders. These trademark holders are not affiliated with congatec AG, our products, or our website.

Terminology

Term	Description
TPM	Trusted Platform Module
TCG	Trusted Computing Group
LPC	Low Pin Count
SPI	Serial Peripheral Interface

1 SPI TPM Reference Design

The Trusted Platform Module (TPM) is an international standard for security applications maintained by the Trusted Computing Group (TCG). The TCG considers the Intel Low Pin Count (LPC), Serial Peripheral Interface (SPI), and I²C interface for host communication. However, the SMARC 2.1 specification does not feature an Intel LPC interface and only non-x86 based platforms use the I²C interface for the TPM.

The reference design below shows how to design an SPI TPM to a SMARC 2.1 carrier board. The SPI TPM used in this reference design is an Infineon TPM SLB 9670VQ2.0. The SPI TPM is connected to the SMARC SPI0 interface.

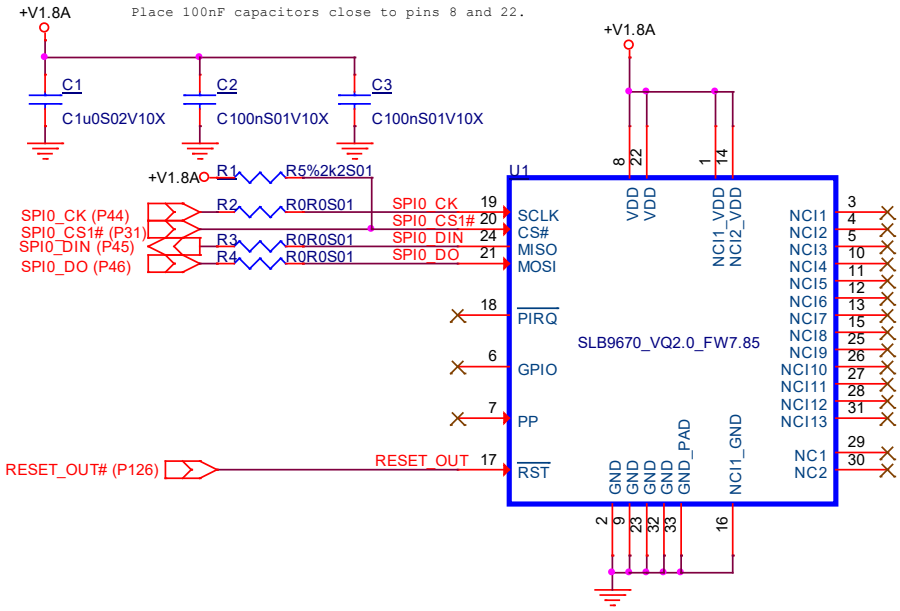

Figure 1: SPI TPM Reference Design

Design Notes:

- Typically, the on-module BIOS flash and the optional carrier board BIOS flash device are connected to SMARC **SPI0**.
- **SPI0_CS1#** (SMARC pin P31) must be used for the active low SPI chip select input of the TPM.
- A pull-up resistor **R1** is required to ensure the correct voltage level during start-up phase. congatec SMARC modules feature the required series resistors for SPI on the module. However, we recommend to place resistors **R2**, **R3** and **R4** on the carrier board for signal tuning purposes. Additionally, we recommend minimizing the routing length on the SMARC carrier board to less than 2500 mil.
- congatec SMARC modules do not support SPI TPM in the default configuration. Therefore, a **custom BIOS** version (e.g. SA50R916.bin for conga-SA5) must be used in order to enable SPI TPM support and to configure the required SPI clock frequency. Additionally, it is required to **disable the Intel Firmware-based TPM** (fTPM) in BIOS setup menu.