SPI TPM KIT
Evaluation Board for NS350 v32 Trusted Platform Module 2.0
Revision 1.01

Devices

- TPM2.0 FW 32.06

Board Rev. V1.2

About this document

Scope and purpose

This document describes the evaluation board for the NS350 v32 Trusted Platform Module 2.0 FW 32.06

The SPI TPM KIT board can be used to evaluate the functionality of NS350 v32 Trusted Platform Module 2.0(TPM 2.0) in a target system environment. The purpose of this document is also to help customers to use and integrate the NS350 v32 TPM2.0 into their system solutions.

Intended audience

This document has been written for system design and verification engineers, who use the NS350 v32 TPM2.0 FW32.06 evaluation board as a verification platform or reference design.

Revision History

Revision Date	Revision	Description
2025-05-23	1.00	First released
2025-05-30	1.01	Add logo

Table of Contents

List of figures

List of tables

1 Overview

1.1 Hardware

The Trusted Platform Module 2.0 (TPM 2.0) NS350 v32 TPM2.0 FW32.06 in QFN32 package is the main part of the SPI TPM KIT evaluation board with revision V1.2

The pinning of the NS350 v32 TPM2.0 FW32.06 is compliant to the follow specification:

- TCG PC Client Platform TPM Profile Specification for TPM 2.0 Version 1.05 Revision 14 September 4, 2020

1.2 Features

NS350 v32 TPM2.0 FW32.06 Trusted Platform Module 2.0 (TPM 2.0),

•QFN32 package,

• 1.8V or 3.3V power supply,

• Serial Peripheral Interface (SPI) accessible via 2x10 pin header connector,

• Small form factor PCB, 2 layer technology.

2 SPI TPM KIT Hardware Components

The main component on the SPI TPM KIT evaluation board is the NS350 v32 FW32.06

2.1 TPM Interfaces

2.1.1 Serial Peripheral Interface – SPI

This NS350 v32 TPM2.0 supports communication over an SPI interface.

For further details, please refer to NS350 v32 TPM2.0 Data Sheet.

2.2 Electrical Characteristics

For electrical characteristics of the NS350 v32 TPM2.0, please refer to the NS350 v32 TPM2.0 Data Sheet.

2.3 Pin Configuration of NS350 v32

Figure 1 shows pin configuration of NS350 v32 TPM2.0 FW32.06 in QFN 32 package.

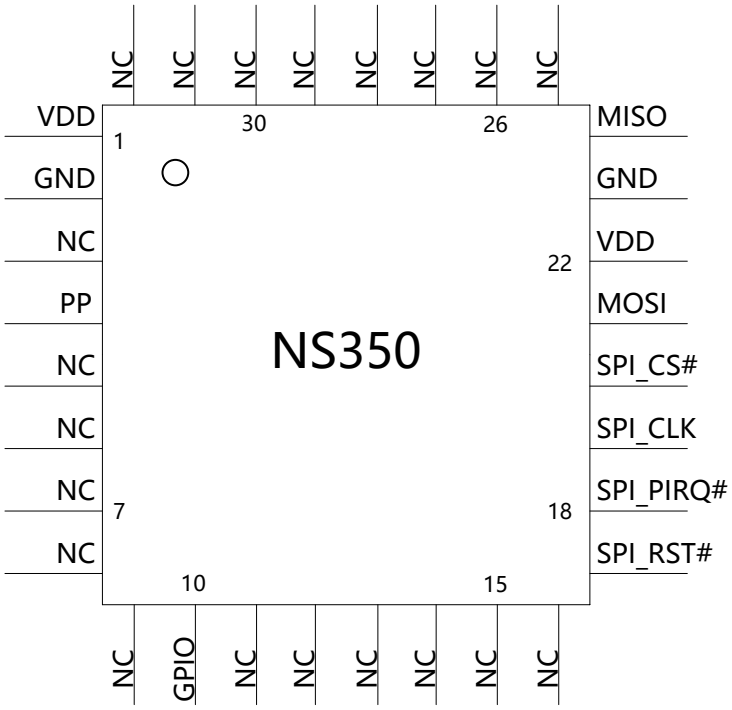

Figure 1 Pin Configuration of NS350 v32 (Top View)

Table 1 I/O Signals

Pin Name	Pin Number	Type	Description
VDD	1, 22	I	Power Supply, All VDD pins must be connected externally and should be bypassed to GND via 100 nF capacitors. This is a 3.3 volt or 1.8V DC power rail supplied by the motherboard to the module
GND	2, 23	I	Ground, All GND pins must be connected externally Zero volts. Expected to be connected to main motherboard ground
SPI_RST#	17	I	SPI_RST#: Active Low, internal weak pull up
SPI_PIRQ#	18	O	PIRQ#: SPI Interrupt, active low, open collector
SPI_CLK	19	I	SPI Clock, Only SPI mode 0 is supported (CPHA=0, CPOL=0), internal pull down
SPI_CS#	20	I	Chip Select, internal pull up
MOSI	21	I	Master output Slave input. SPI data which is received from the master
MISO	24	O	Master input Slave output. SPI data which is sent to the SPI bus master
NC	3,5,6,7,8,9,11,12, 13,14,15,16,25,26, 27,28,29,30,31,32		No Connected (can be connected externally)
PP	4	I	This pin may be left unconnected; Physical Presence, active high, internal pull-down. Used to indicate Physical Presence to the function

Pin Name	Pin Number	Type	Description
GPIO	10	I/O	This pin may be left unconnected; Input by default, internal pull up; It can be controlled via trusted GPIO functionality

Notes:

1. I - input only, O - output only
2. All pins must have the power at the same time in the whole life time when be used, include all VDD pins and IO pins
3. Make sure the SPI_CS# is high when the SPI_RST# is low
4. It is recommended to use an independent SPI bus on the CPU to connect to the chip
5. For SPI_CLK, external applications should be low by default.
6. For MOSI, external applications recommend be low by default.

2.4 Package

Package: QFN 32

For details on the package outline and the footprint, please refer to the NS350 v32 FW32.06 TPM2.0 datasheet.

3 Typical Schematic

3.1 SPI TPM KIT Connection Diagram

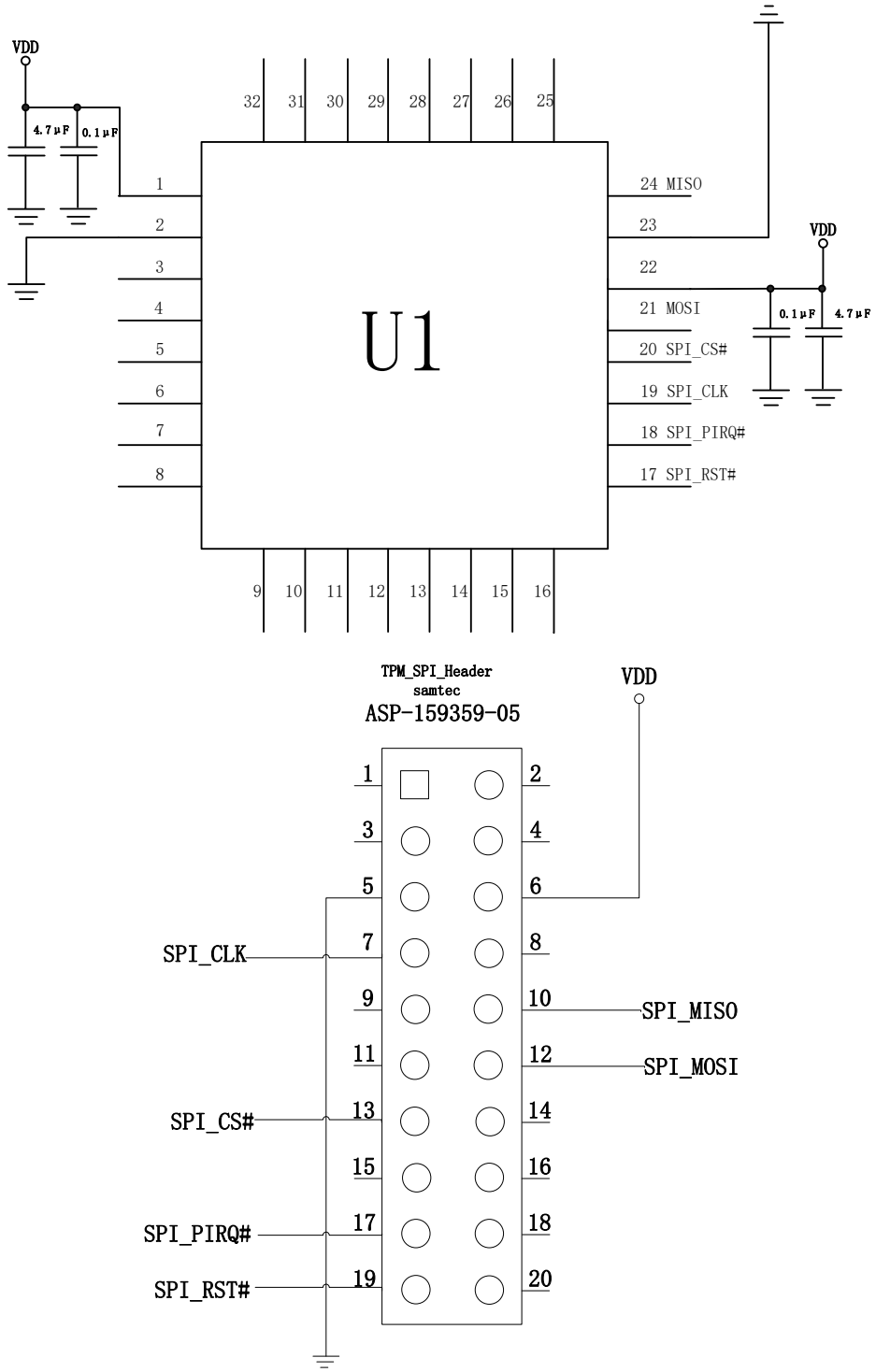

Figure 2 SPI TPM KIT board connection diagram

3.2 SPI TPM KIT Board Layout

- 2 Layers PCB design
- SMD and THT technologies

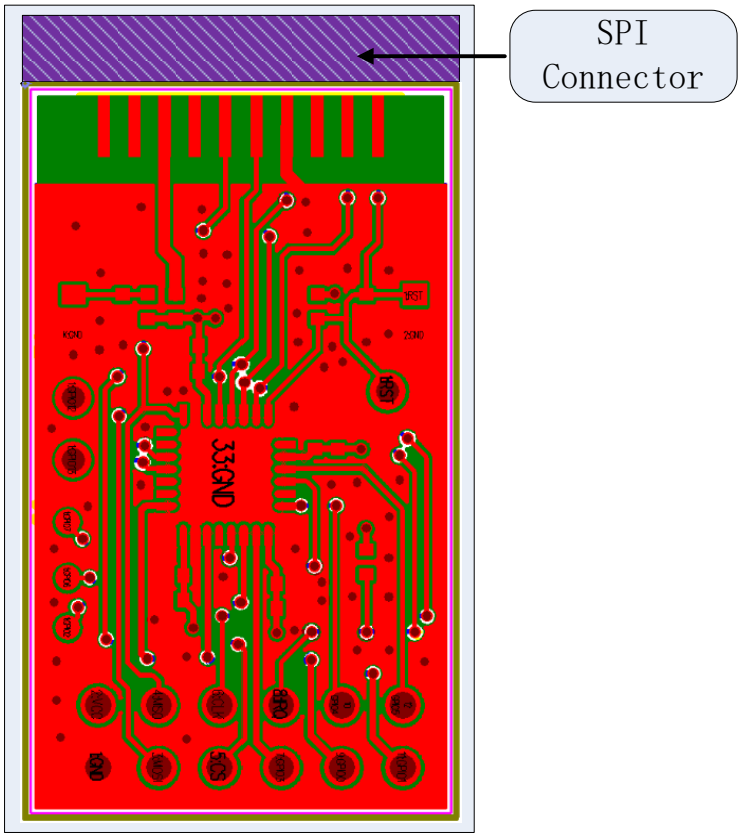

Figure 3 Top view of SPI TPM KIT board PCB for SPI TPM

4 SPI TPM KIT Board Details

4.1 Dimensions

- 17.4 mm x 34.7mm
- Thickness: 1.2 mm
- SPI accessible via 2x10 pin header (50mil / 1.27mm pin spacing)

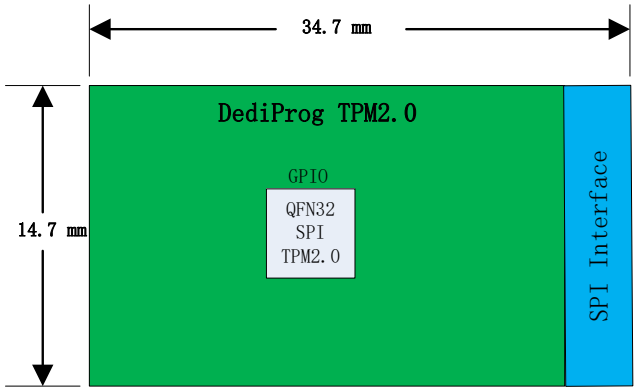

Figure 4 SPI TPM KIT board (V1.2)

4.2 SPI TPM KIT Pin Configuration

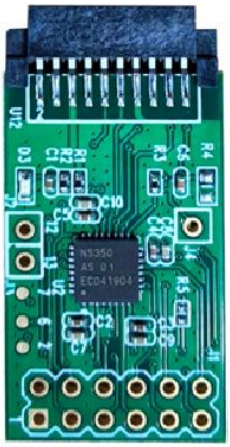

Figure 5 The picture for SPI TPM KIT

Table 2 I/O Signals for connector

Signal	Pin	Pin	Signal
KEY	1	2	-
NC	3	4	-
GND	5	6	VDD
CLK	7	8	-
-	9	10	MISO
-	11	12	MOSI
TPMCS2#	13	14	GND[1]
-	15	16	-
PIRQ#	17	18	-
PLT_RST#	19	20	-

[1] Note: Pin 14 – GND of the connector is not connected to GND on SPI TPM KIT Board.

Table 3 I/O Signals for J1 on board

Signal	Pin	Pin	Signal
GND	1	2	VDD
MOSI	3	4	MISO
TPMCS2#	5	6	CLK
-	7	8	PIRQ#
-	9	10	-
-	11	12	-

5 SPI TPM KIT Board Connectors

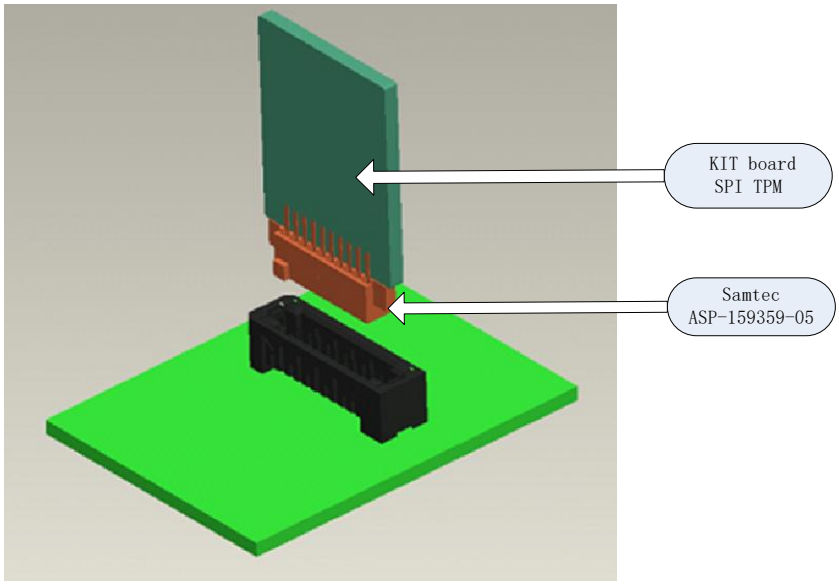

Figure 6 Pin Board connection SPI TPM KIT board with motherboard

The SPI TPM KIT board with the Samtec ASP-159359-05 connector can be plugged to a Samtec ASP 159358-01 (Through Hole Technology) or to a Samtec ASP-159358-03 (Surface Mount Technology)

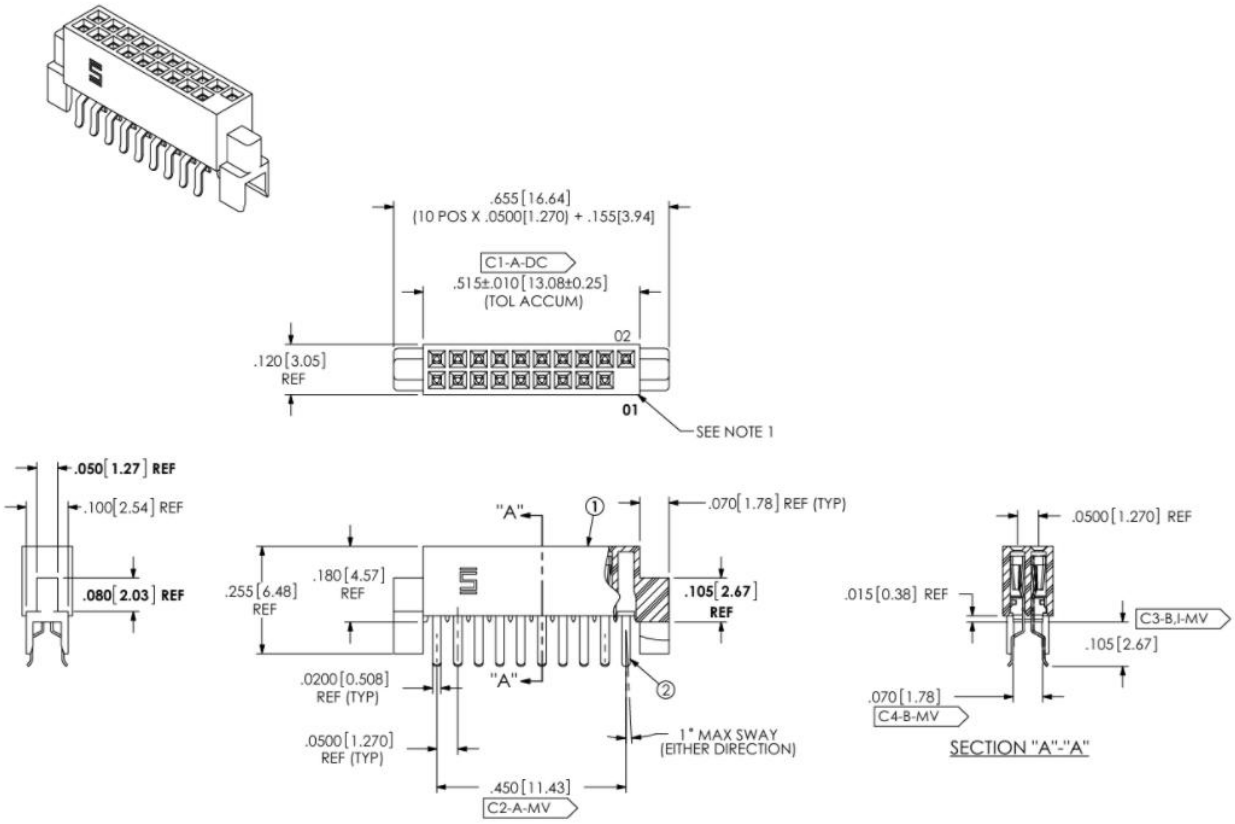

Figure 7 SPI TPM2.0 connector on SPI TPM KIT Board – Samtec ASP-159359-05

Table 4 SPI TPM KIT connector – Pin layout and description

Name	PIN	PIN	Name
Key	1	2	NC
NC	3	4	NC
GND	5	6	VDD3.3V(or 1.8V)-TPM power supply
CLK-TPM SPI clock	7	8	NC
NC	9	10	MISO-Master input Slave output, SPI data which is sent to the SPI bus master
NC	11	12	MOSI-Master output Slave input, SPI data which is received from the master
TPMCS2#-TPM SPI chip select signal	13	14	GND
NC	15	16	NC
PIRQ#-TPM interrupt signal, active low	17	18	NC
PLT_RST#-TPM reset signal, active low	19	20	NC

6 Board Ordering

Table 5 SPI TPM KIT board ordering information

Ordering Code(Part Number)	Firmware version
NS-SPITPM-KIT-T21	32.06

7 BOM Bill of Material

List of materials used for assembling the SPI TPM KIT board V1.2

Table 6 Bill of material for SPI TPM KIT board

Part ID	Value	Footprint	Description	Supplier
PCB	-	-	SPI TPM2.0 V1.2 PCB	NATIONS
U2	NS350 v32 TPM2.0 FW32.06	QFN32	TPM controller	NATIONS
C2/C3/C4/C5	0.1 μF	C_0402	Ceramic capacitor	-
C7/C8/C9/C10	4.7 μF	C_0402	Ceramic capacitor	-
R1	0 Ω	R_0402	-	-
R2/R3	4.7K Ω	R_0402	-	-
U12	-	-	Samtec ASP-159359-05 pin header (female)	Samtec

IMPORTANT NOTICE

Nations Technologies Inc. (“Nations”) can change, modify, enhance and improve its products and/or this document at any time without notice. It is advisable for purchasers to ensure they have the latest information about Nations’ products before placing orders. When purchasing Nations’ products, the responsibility solely lies on the purchaser to choose, select, and use the products, and Nations assumes no liability for any such responsibilities. Nations does not grant any license, whether express or implied, to any intellect property rights. If any purchaser resells Nations products with provisions that differ from the information stated in this document, such a resale shall void any warranty granted by Nations for the product. Nations and the Nations logo are their trademarks, and for more information on Nations’ trademarks, please see www.nationstech.com. All other product or service names belong to their respective owners. The information contained in this document supersedes and replaces the information supplied in any previous versions of the document.

Nations’ Products are intended solely for use in general-purpose electronic equipment and are not recommended, authorized, or warranted for use in military, aircraft, space, life-saving, or life-sustaining applications, nor in products or systems where failure or malfunction could result in personal injury, death, or significant property or environmental damage. Nations Products that are not specifically designated as “automotive grade” may be used in automotive applications only at the user’s own risk. Overall, it is important to use Nations Products only in the manner specified in the product documentation and as explicitly approved by an authorized Nations representative in writing.