NS350 v32 Trusted Cryptography Module 2.0
Data Brief Revision 1.02

Key Features

- Compliant to GM/T 0012-2020 Trusted computing – Trusted computing interface specification of trusted cryptography module
- SPI Interface
- Standard (-20~+85°C) and Enhanced (-40~+85°C) temperature range
- QFN16 and QFN32 package
- 1.8 V or 3.3 V supply voltage range
- Optimized for battery operated devices: low standby low power consumption (typical 100 uA)
- Active shield and environmental sensors
- Monitoring of environmental parameters (power, temperature)
- Hardware and software protection against fault injection
- Random Number Generator (RNG) implemented according the requirements of GM/T 0062
- 24 PCRs (SM3)
- SM2, SM3, SM4
- Full personalization Endorsement Key (EK) certificates
- Field Upgrade - allows secure firmware updates

Revision History

Revision Date	Revision	Description
2024-05-31	1.02	Update information
2024-04-15	1.01	Update firmware information
2024-03-22	1.00	First released

Table of Contents

1 Scope

1.1 Device Information

The NS350 v32 is a cost-effective and high-performance Trusted Cryptography Module 2.0 (TCM 2.0) targeting PCs, server platforms and embedded systems. It is available in QFN32 package.

Table 1 Part Number

Part Number	Firmware Version	Description
NS350-KQAR-x0	32.06	Standard temperature range (-20~+85°C) Support TCM 2.0 profile, SPI interface, QFN32-package, Tape & Reel delivery
NS350-KQBR-x0	32.06	Enhanced temperature range (-40~+85°C) TCM 2.0 profile, SPI interface, QFN32-package, Tape & Reel delivery

Note: x as customer-specific letter: A, D, G, H, I, J, L, M, N, R, S, V, or T

1.2 Scope and purpose

This document describes the NS350 v32 TCM2.0 together with its features and functionality. It is primarily intended for system developers.

2 Pin Description

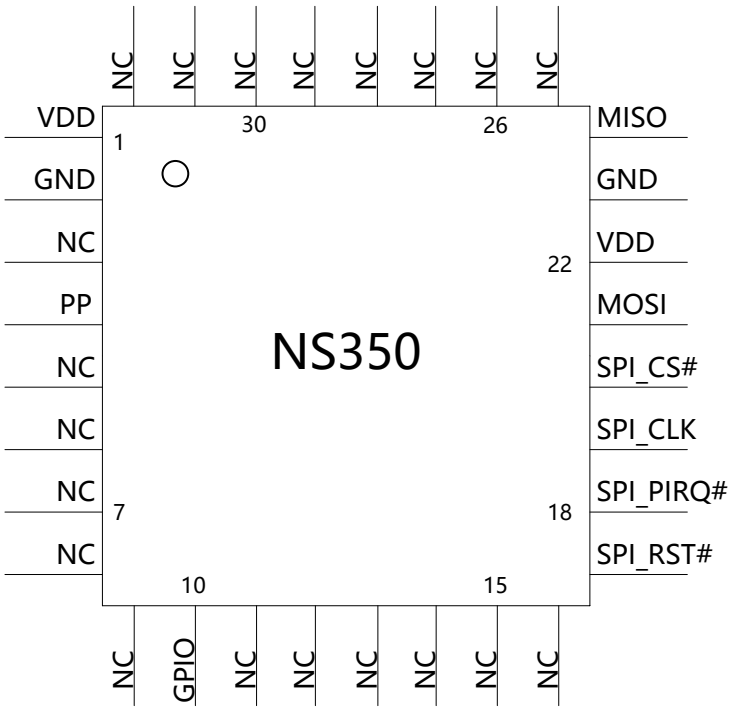

Figure 1 Pinout of NS350 v32 (Top View)

Table 2 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
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.

3 Typical Schematic

Figure 2 shows the typical schematic for the NS350 v32. The power supply pins should be bypassed to GND with capacitors located close to the device.

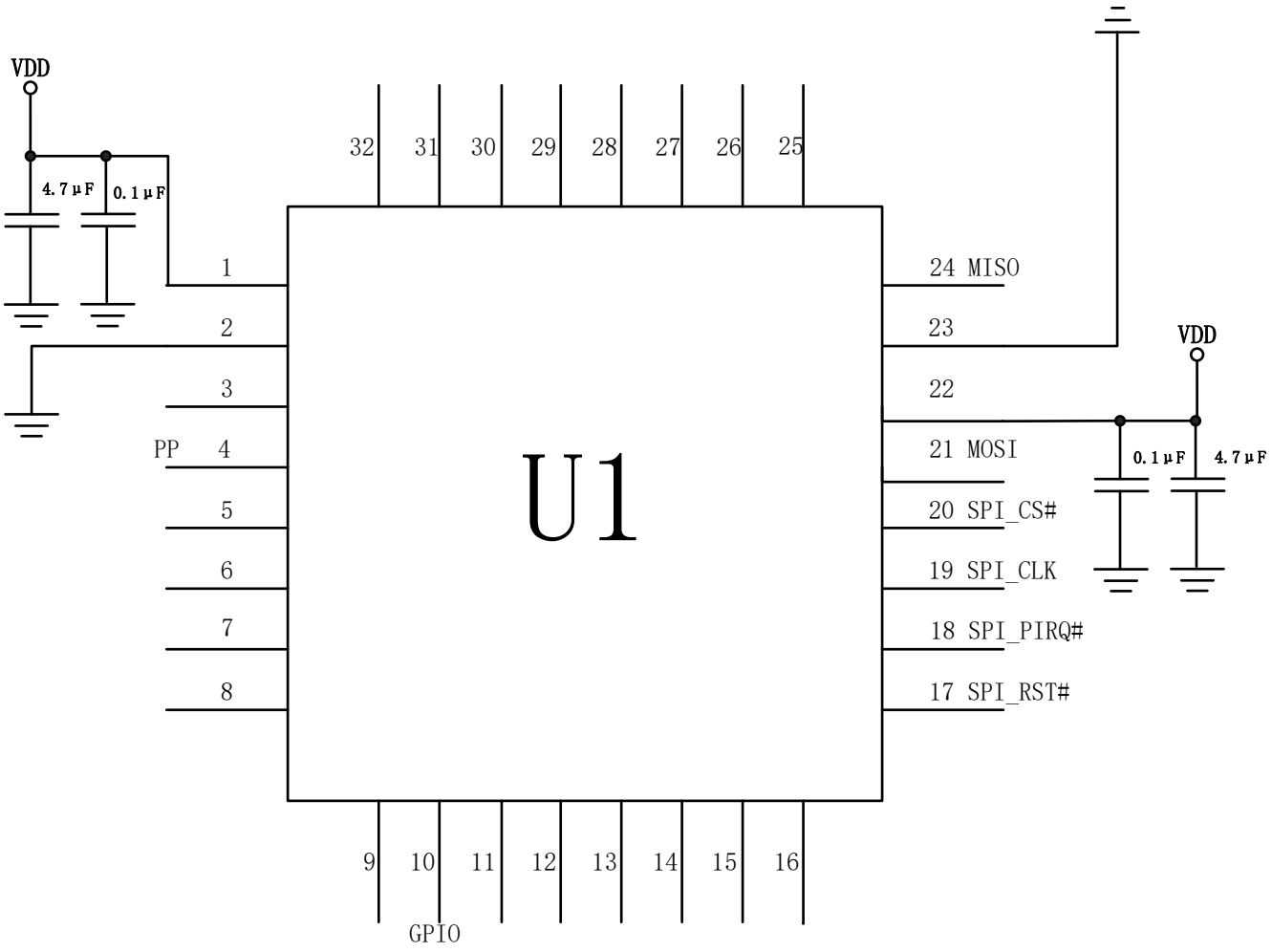

Figure 2 Typical Schematic

4 Package Information

4.1 Package Dimensions

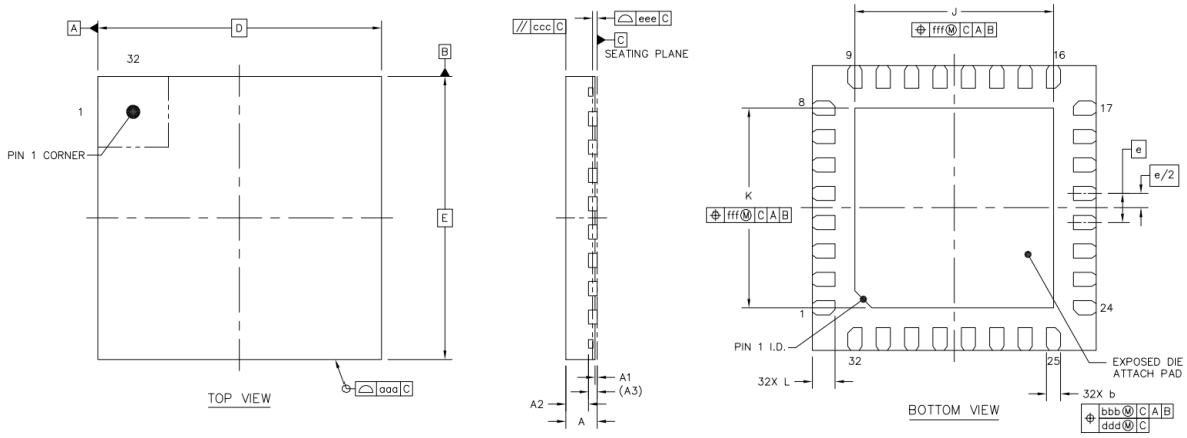

Figure 3 Package Symbol

Table 3 Symbol and Dimension

		SYMBOL	MIN	NOM	MAX
TOTAL THICKNESS		A	0.5	0.55	0.6
STAND OFF		A1	0	0.035	0.05
MOLD THICKNESS		A2	---	0.4	---
L/F THICKNESS		A3		0.152	REF
LEAD WIDTH		b	0.2	0.25	0.3
BODY SIZE	X	D		5	BSC
	Y	E		5	BSC
LEAD PITCH		e		0.5	BSC
EP SIZE	X	J	3.4	3.5	3.6
	Y	K	3.4	3.5	3.6
LEAD LENGTH		L	0.3	0.4	0.5
PACKAGE EDGE TOLERANCE		aaa		0.1	
LEAD OFFSET		bbb		0.1	
		ddd		0.05	
MOLD FLATNESS		ccc		0.1	
COPLANARITY		eee		0.08	
EXPOSED PAD OFFSET		fff		0.1	

NOTES:

1. Coplanarity applies to leads, corner leads and die attach pad.
2. Total thickness not include SAW BURR.

4.2 Packing Type

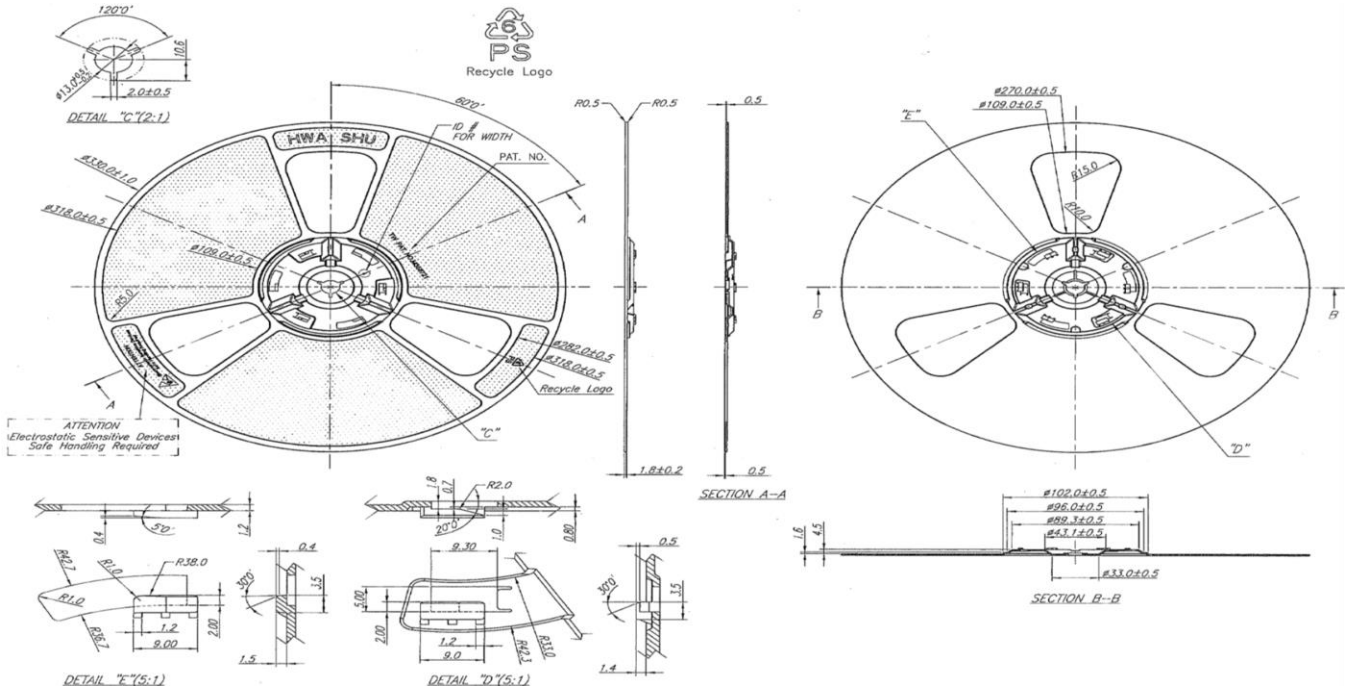

Figure 4 Reel diagram

Tape & Reel (reel diameter 330mm), 3000 pcs. per reel.

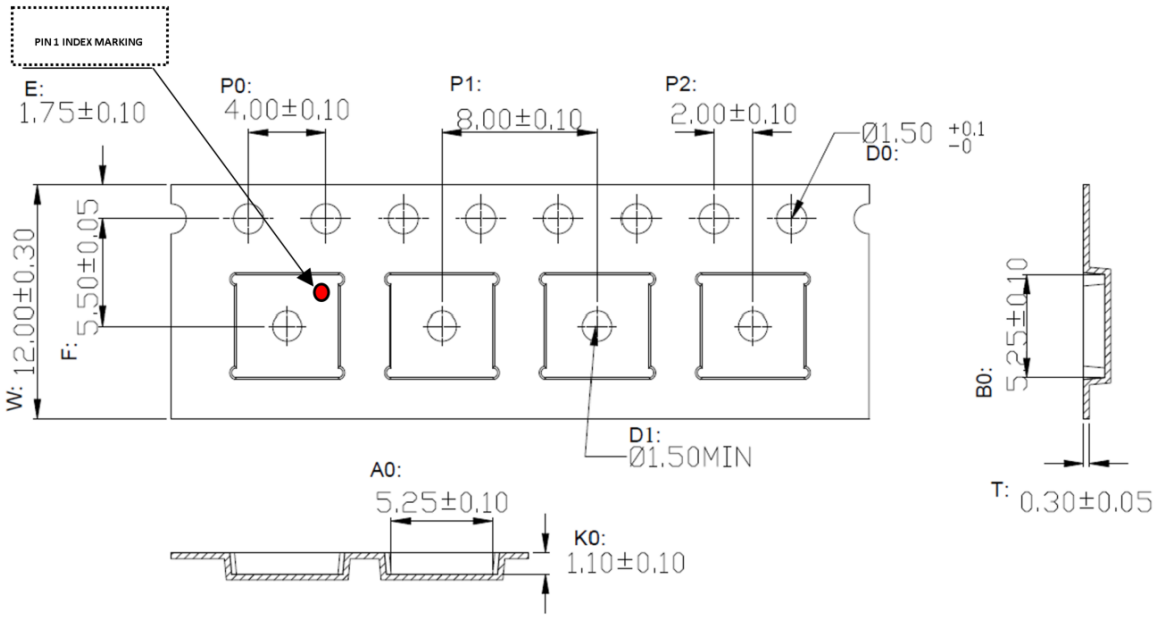

Figure 5 Packing Type

4.3 Recommended footprint

Figure 6 shows the recommended footprint for the package.

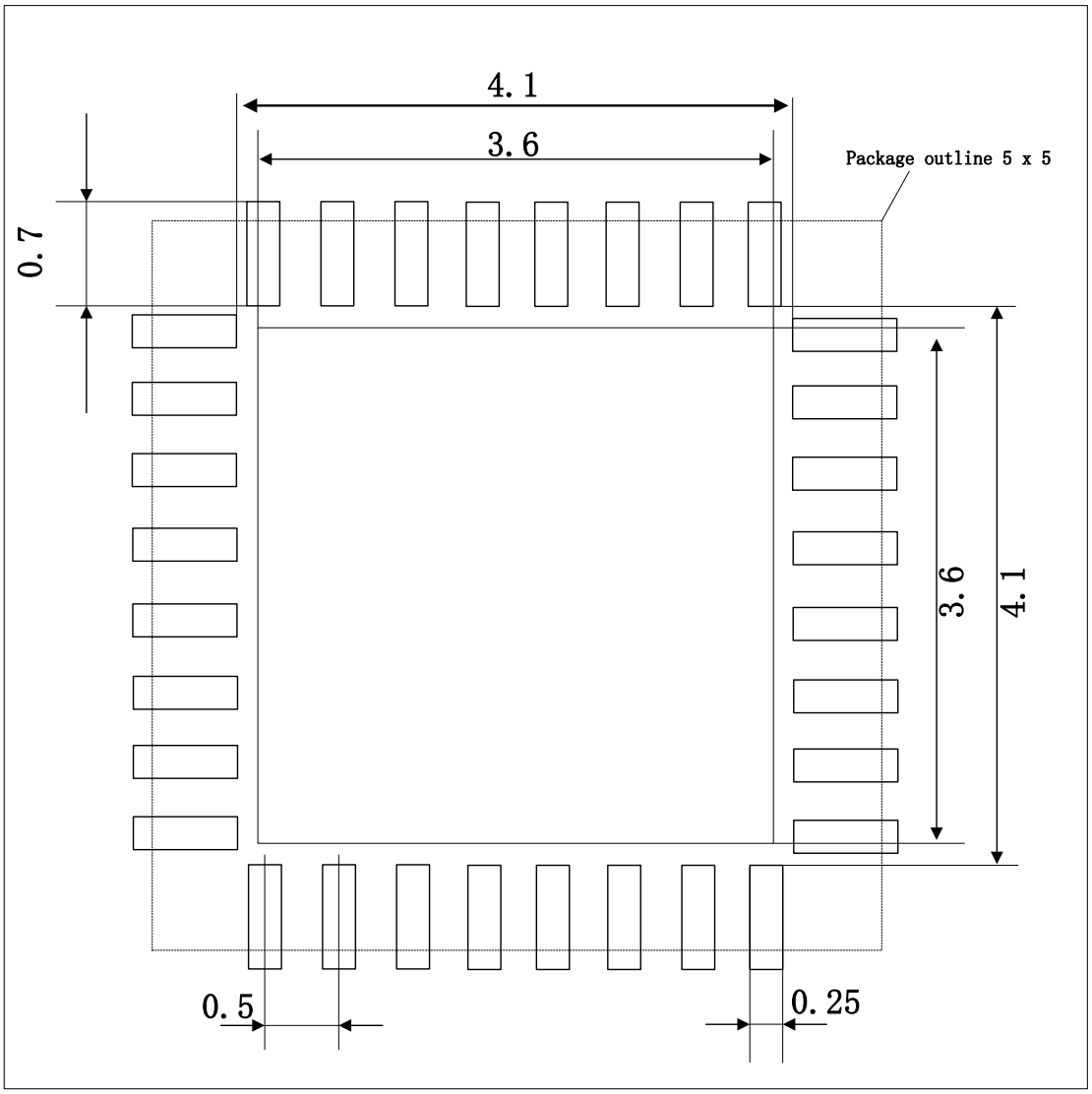

Figure 6 Recommended Footprint

4.4 Chip Marking

Figure 7 chip Marking

Description

(1) Line 1 - Hardware Technology name

NS350 is the name of the hardware technology.

(2) Line 2 - Device model

WW=AS means support temperature from -20℃ to 85℃, SPI interface.

WW=BS means support temperature from -40℃ to 85℃, SPI interface.

YY is the symbol for firmware version.

Table 4 symbol and firmware version

Symbol	Firmware version
YY = 01	32.06

(3) Line 3 - Device information

XXXXXXXX is production lot number.

XX(Reserved)+X[Year]+XX[Week]+XXX[Wafer Lot Number. 000~999].

(4) #1 Pin Position Mark

"○" indicates the position of #1 pin.

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.