NSING

NS350 v30 Trusted Platform Module 2.0
Data Brief Revision 1.03

Key Features

- Compliant to TCG TPM Main Specification, Family "2.0", Level 00, Revision 01.59 - errata 1.4 and PC Client Specific TPM Platform Specification 1.05 revision 14
- Targeted certifications:
  - Common Criteria (CC), Version 3.1 Revision 5, Level EAL4+, AVA_VAN.4, ALC_FLR.1, according to TCG PC Client TPM 2.0 Protection Profile Version 1.3
  - FIPS 140-2 level 2 (physical security level 3)
  - TCG certification
- SPI Interface
- Standard (-20~+85°C) and Enhanced (-40~+85°C) temperature range
- QFN32 package
- 1.8v or 3.3v supply voltage range
- Optimized for battery operated devices: low standby low power consumption (typical 75uA)
- Active shield and environmental sensors
- Monitoring of environmental parameters (power, temperature)
- Hardware and software protection against fault injection
- Random Number Generator (RNG) implemented according to NIST SP800-90A using entropy source according to NIST SP800-90B
- 24 PCRs (SHA1, SHA-256 or SHA384)
- RSA key generation (2048, 3072 and 4096 bit)
- ECC (NIST P_256, NIST P_384)
- SHA1, SHA256, SHA384
- Full personalization with 3 EK certificates (RSA 2048, RSA 3072, ECC NIST P384)
- Compliant with the TCG test suite for TPM 2.0
- Field Upgrade - allows secure firmware updates

NSING

Table of Contents

1 Scope

1.1 Device Information

The NS350 v30 is a cost-effective and high-performance Trusted Platform Module 2.0 (TPM 2.0) targeting PCs, server platforms and embedded systems. It is available in QFN32 package. It supports an SPI interface.

Table 1 Part Number

Part Number	Firmware Version	Description
NS350-KQAR-x2	30.30	Standard temperature range (-20~+85°C) TCG profile, SPI interface, QFN32-package, Tape & Reel delivery
NS350-KQBR-x2	30.30	Enhanced temperature range (-40~+85°C) TCG profile, SPI interface, QFN32-package, Tape & Reel delivery

Note:

1. x as customer-specific letter: A, D, G, H, I, J, L, M, N, R, S, V, or T
2. Part Number is ordering code
3. The minimum ordering quantity is 3000, smaller sampling quantities can be ordered through the sales channel

1.2 Scope and purpose

This datasheet describes the NS350 v30 TPM2.0 Trusted Platform Module together with its features, functionality and programming interface. It is primarily intended for system developers.

1.3 Support and information

Additional information regarding this device can be obtained from the www.nsing.com.sg.

For any specific support information, you can contact through the following e-mail: tpm@nsing.com.sg.

2 Pin Description

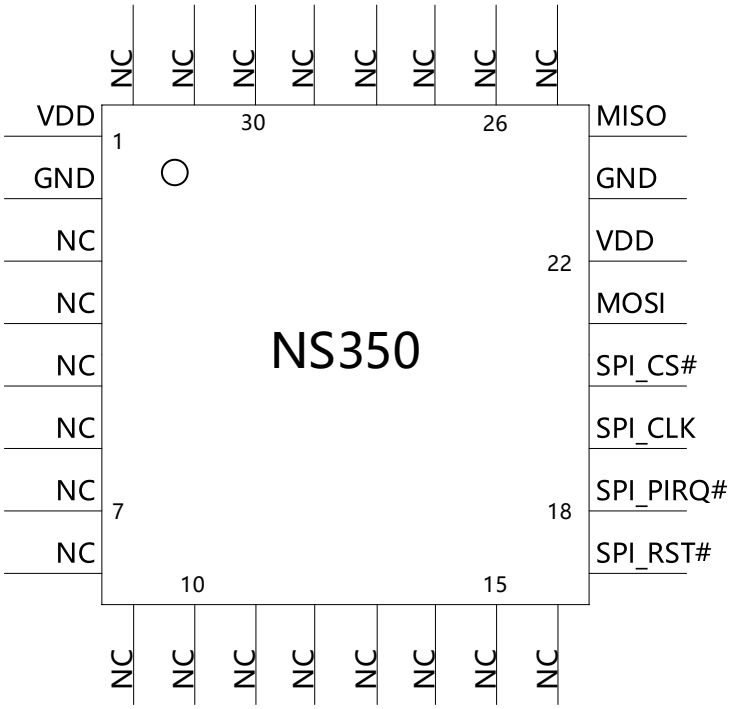

Figure 1 Pinout of NS350 (Top View)

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#: External reset signal 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)
SPI_CS#	20	I	Chip Select, active low
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	3,4,5,6,7,8,9,10,11,12, 13,14,15,16,25,26, 27,28,29,30,31,32		No Connect Internally (can be connected externally)

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 TPM
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. The power supply pins should be bypassed to GND with capacitors located close to the device.

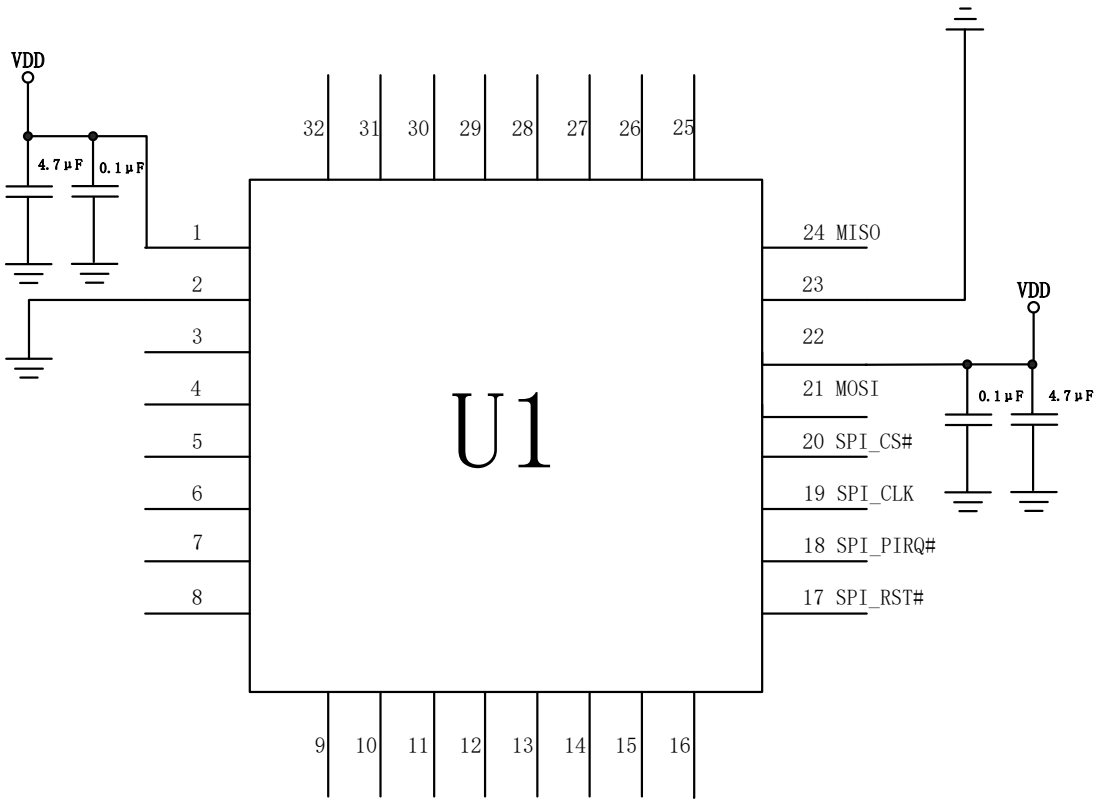

Figure 2 Typical Schematic

4 Embedded Software

Properties defined within the TPM can be read with the command TPM2_GetCapability. The following properties are returned by the NS350. (capability = TPM_CAP_TPM_PROPERTIES):

Table 3 NS350 TPM Property Values

TPM_PT_MANUFACTURER	0x4E534700 ("NSG")
TPM_PT_VENDOR_STRING_1	0x4E533335 ("NS35")
TPM_PT_VENDOR_STRING_2	0x30000000 ("0")
TPM_PT_VENDOR_STRING_3	NULL
TPM_PT_VENDOR_STRING_4	NULL
TPM_PT_FIRMWARE_VERSION_1	0x001E001E (30.30)
TPM_PT_FIRMWARE_VERSION_2	0x24042510 (9220.9488)
TPM_PT_MODES	0x00000001

Table 4 FIFO Configuration Registers

Register	Value	Comments
TPM_VID	0x9999	Vendor identification of NSING
TPM_DID	0x0701	Device identification
TPM_RID	0x01	Revision identification register

5 Electrical Characteristics

5.1 Power Supply

Table 5 Power Supply

Symbol	Parameters	Unit	Min	Typical	Max
VDD	Supply Voltage 3.3V mode	V	3.0	3.3	3.6
	Supply Voltage 1.8V mode	V	1.65	1.8	1.95

5.2 Electrostatic Discharge (ESD)

Table 6 Electrostatic Discharge

Symbol	Parameters	Unit	Min	Typical	Max
$V_{ESD(HBM)}$	Electrostatic discharge (Human body model)	V	-	-	4000
$V_{ESD(CDM)}$	Electrostatic discharge (Charged device model)	V	-	-	750

5.3 Latchup Immunity

Table 7 Latchup Immunity

Parameters	Unit	Min	Typical	Max
Latchup Immunity	mA	-	-	200

5.4 Temperature Range

Table 8 Temperature Range

Symbol	Parameters	Unit	Min	Typical	Max
T_A	Operating Temperature (Standard)	℃	-20	-	85
T_A	Operating Temperature (Extended)	℃	-40	-	85
T_S	Storage Temperature	℃	-40	-	125

5.5 Operating Lifetime

Table 9 Operating Lifetime

Parameters	Unit	Min	Typical	Max
Useful lifetime	Year	-	-	10
Operating lifetime	Year	-	-	10

Note: typical average temperature over time is 55 ℃

5.6 DC Characteristics

TA = 25℃, VDD = 3.3V±0.3V or VDD = 1.8V±0.15V unless otherwise noted

Table 10 Current Consumption

Symbol	Parameters	Unit	Min	Typical	Max
$I_{VDD(RUN)}$	TPM Current Consumption in Active Mode	mA	-	-	30
$I_{VDD(Idle)}$	TPM Current Consumption in S0 idle state	μA	-	75	-

Table 11 DC Characteristics of SPI Interface Pins (SCLK, CS#, MISO, MOSI, RST#, PIRQ#) 1.8V

Symbol	Parameters	Unit	Min	Typical	Max
V_{IH}	Input voltage high	V	0.7*VDD	-	0.3+VDD
V_{IL}	Input voltage low	V	-0.3	-	0.3*VDD
V_{OH}	Output high voltage	Iout=-100 μA	0.9*VDD		
V_{OL}	Output low voltage	1.5 mA			0.15*VDD

Note : Conditions VDD=1.65V – 1.95V

Table 12 DC Characteristics of SPI Interface Pins (SCLK, CS#, MISO, MOSI, RST#, PIRQ#) 3.3V

Symbol	Parameters	Unit	Min	Typical	Max
V_{IH}	Input voltage high	V	0.7*VDD	-	0.5+VDD
V_{IL}	Input voltage low	V	-0.5	-	0.3*VDD
V_{OH}	Output high voltage	Iout=-100 μA	0.9*VDD		
V_{OL}	Output low voltage	1.5 mA			0.15*VDD

Note : Conditions VDD=3.0V – 3.6V

5.7 AC Characteristics

TA = 25℃, VDD = 3.3V±0.3V or VDD = 1.8V±0.15V unless otherwise noted

Table 13 Device Reset

Symbol	Parameters	Unit	Min	Typical	Max
t_{POR}	Cold (Power-On) Reset	μs	120	-	-
t_{WRST}	Warm Reset	μs	2	-	-

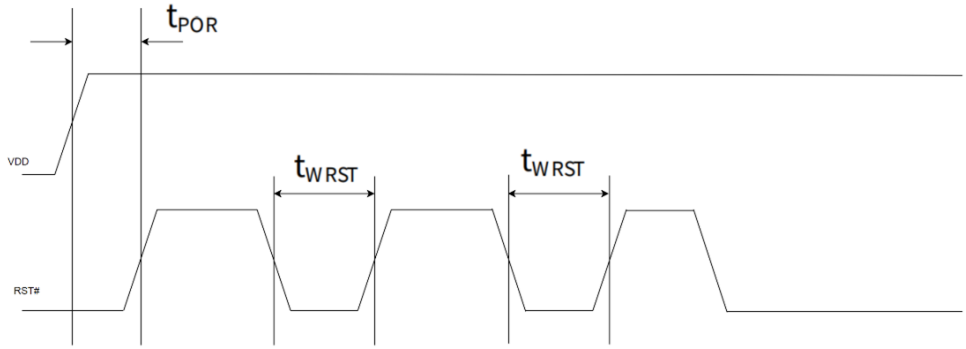

Figure 3 Reset Timing

Table 14 SPI Bus Frequency

Symbol	Parameters	Unit	Min	Typical	Max
f_{CLK}	SPI Bus Frequency	MHz	-	-	25

Table 15 AC Characteristics of SPI Interface

SCLK Frequency f_{CLK} = 5Mhz~25MHz

Symbol	Parameters	Conditions	Unit	Min	Max
t_{CLKf}	Clock Period	Rising Edge to Rising Edge	ns	$1/f_{CLK}$-5%	$1/f_{CLK}$+5%
t_{CLKr}	Nominal Clock Period	Nominal Clock Period	ns	$1/f_{CLK}$	
t_{CLKL}	Clock Low Time	Clock Low Time	ns	$0.45t_{CLKr}$	-
t_{CLKH}	Clock High Time	Clock High Time	ns	$0.45*t_{CLKr}$	-
$t_{CLKslew}$	Clock Slew Rate	f_{CLK} >= 20MHz, $0.2*V_{CC}$ – $0.6*V_{CC}$	V/ns	1	4

		f_{CLK} < 20MHz, 0.2*V_{CC} – 0.6*V_{CC}	V/ns	0.5	4
t_{CS}	CS# High Time	Rising Edge to Falling Edge	ns	50	
t_{CSS}	CS# Setup to clock	CS Setup time	ns	5	
t_{CSH}	CS# Hold to clock	CS Hold time	ns	5	
t_{SU}	MOSI Setup to clock	Data Setup time	ns	2.5	
t_H	MOSI Hold to clock	Data Hold time	ns	3	
t_{HO}	Clock to MISO valid	Output Hold time	ns	0	
t_{Vmin}	Output valid from clock falling edge minimum	Output Valid Min	ns	0	
t_{Vmax}	Output valid from clock falling edge maximum	Output Valid Max	ns		0.7* t_{CLKL}
	TPM SPI Pin Capacitance		pF		10

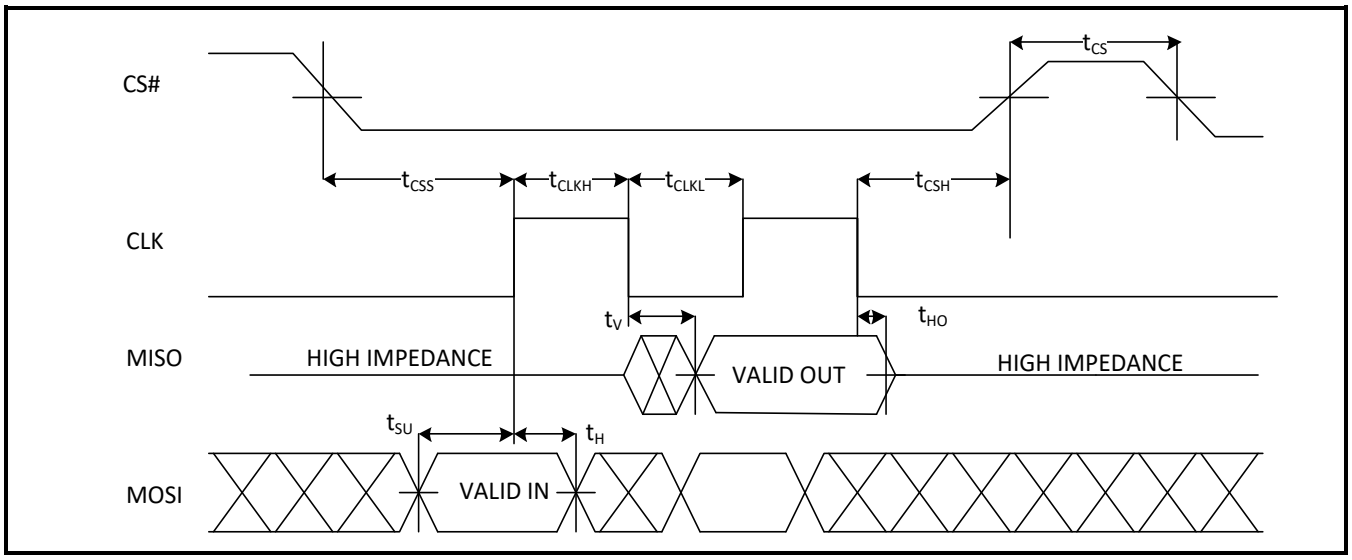

Figure 4 Timing Diagram

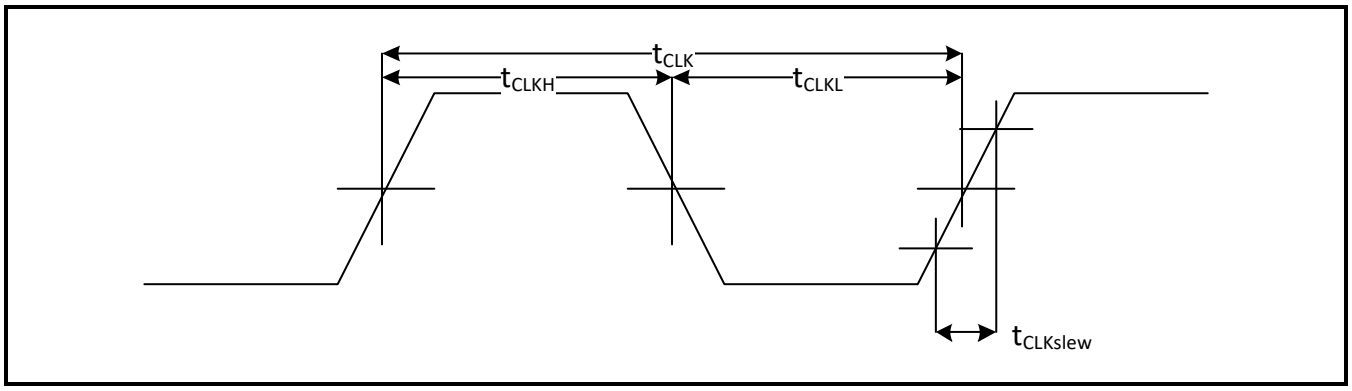

Figure 5 Clock Timing Diagram

6 Package Information

6.1 Package Dimensions

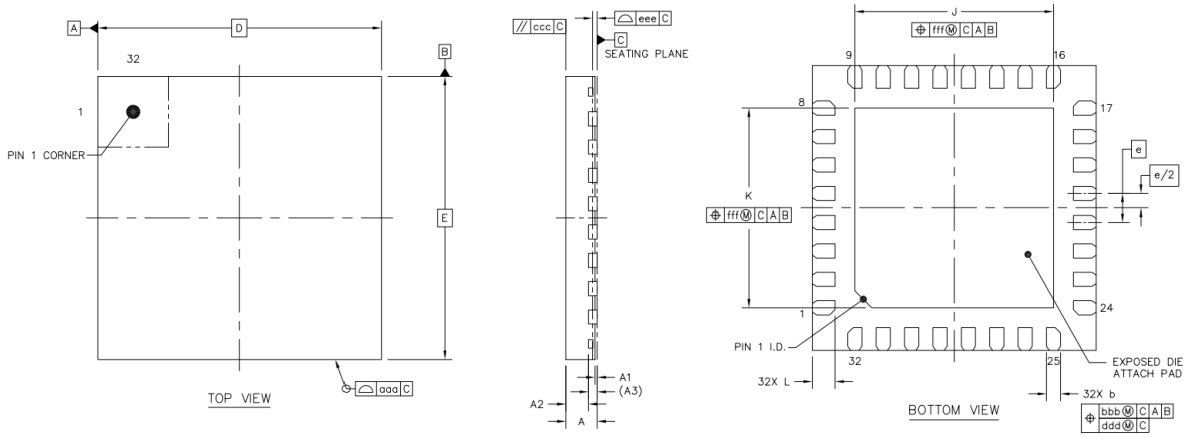

Figure 6 Package Symbol

Table 16 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		

Note:

1. PIN 1# on the figure 6 is Pin 1

2. The tolerance is equal Nor.-Min./Max.-Nor.
3. Coplanarity applies to leads, corner leads and die attach pad.
4. Total thickness not include SAW BURR.

6.2 Delivery packing

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

All dimensions to meet the requirement of EIA-481-C.

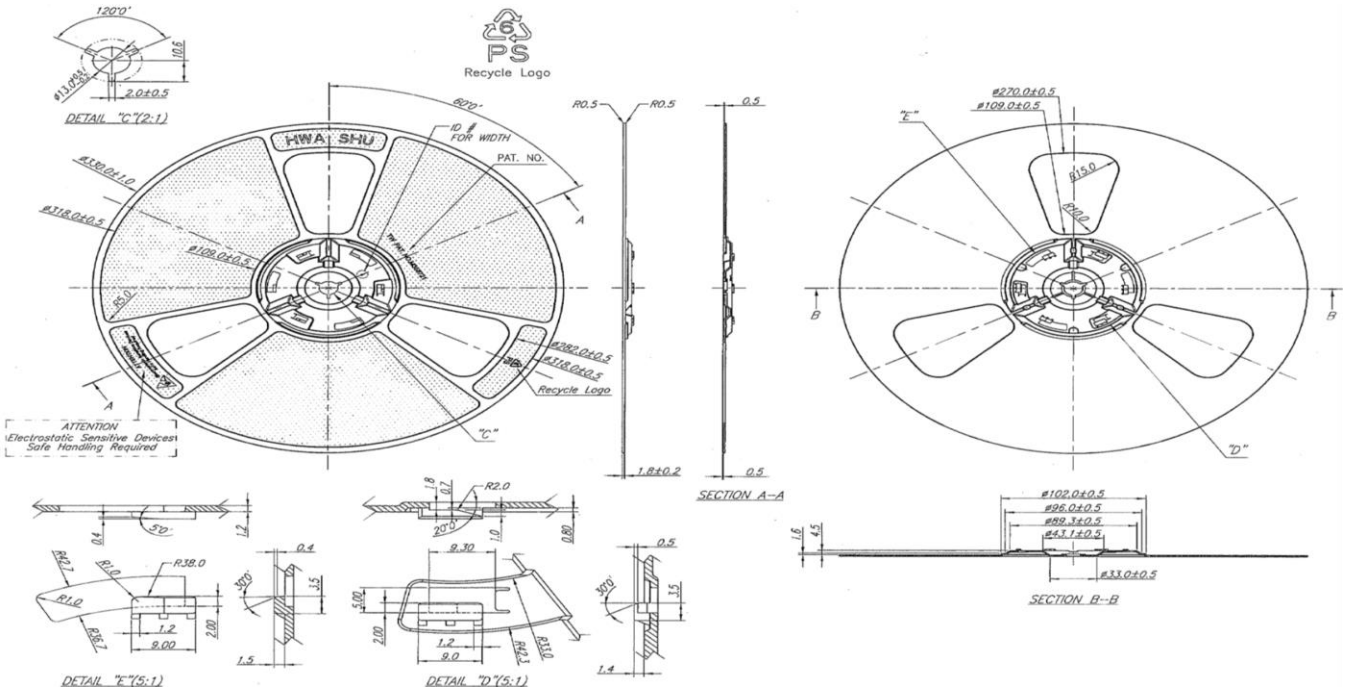

Figure 7 Reel diagram

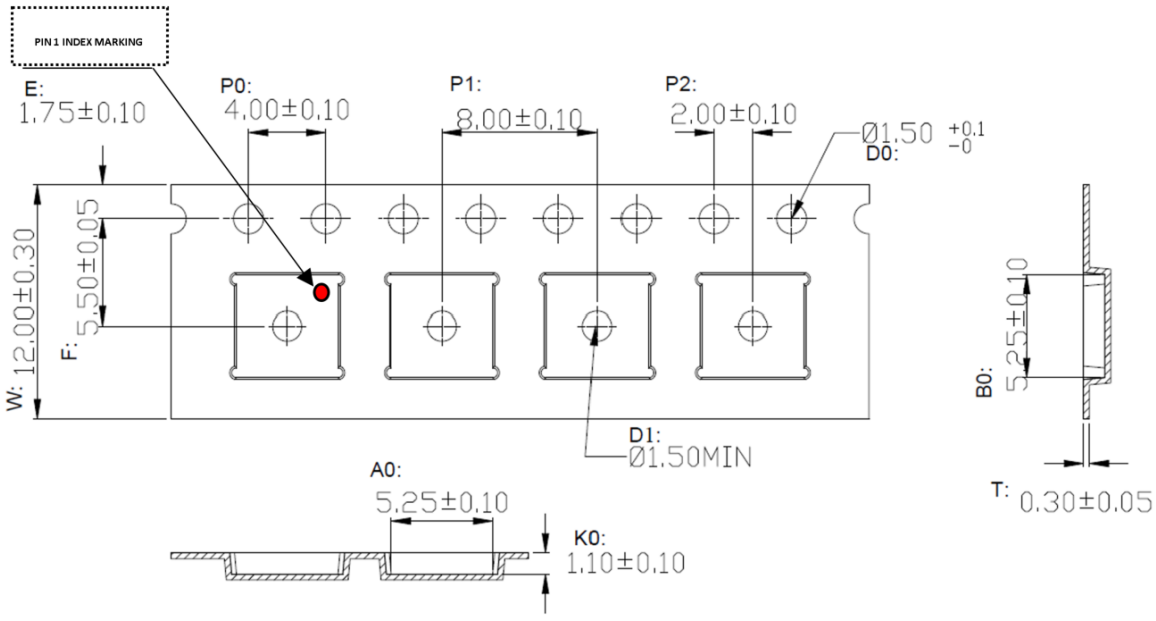

Figure 8 Embossed carrier tape

6.3 Recommended footprint

Below figure shows the recommended footprint for the package.

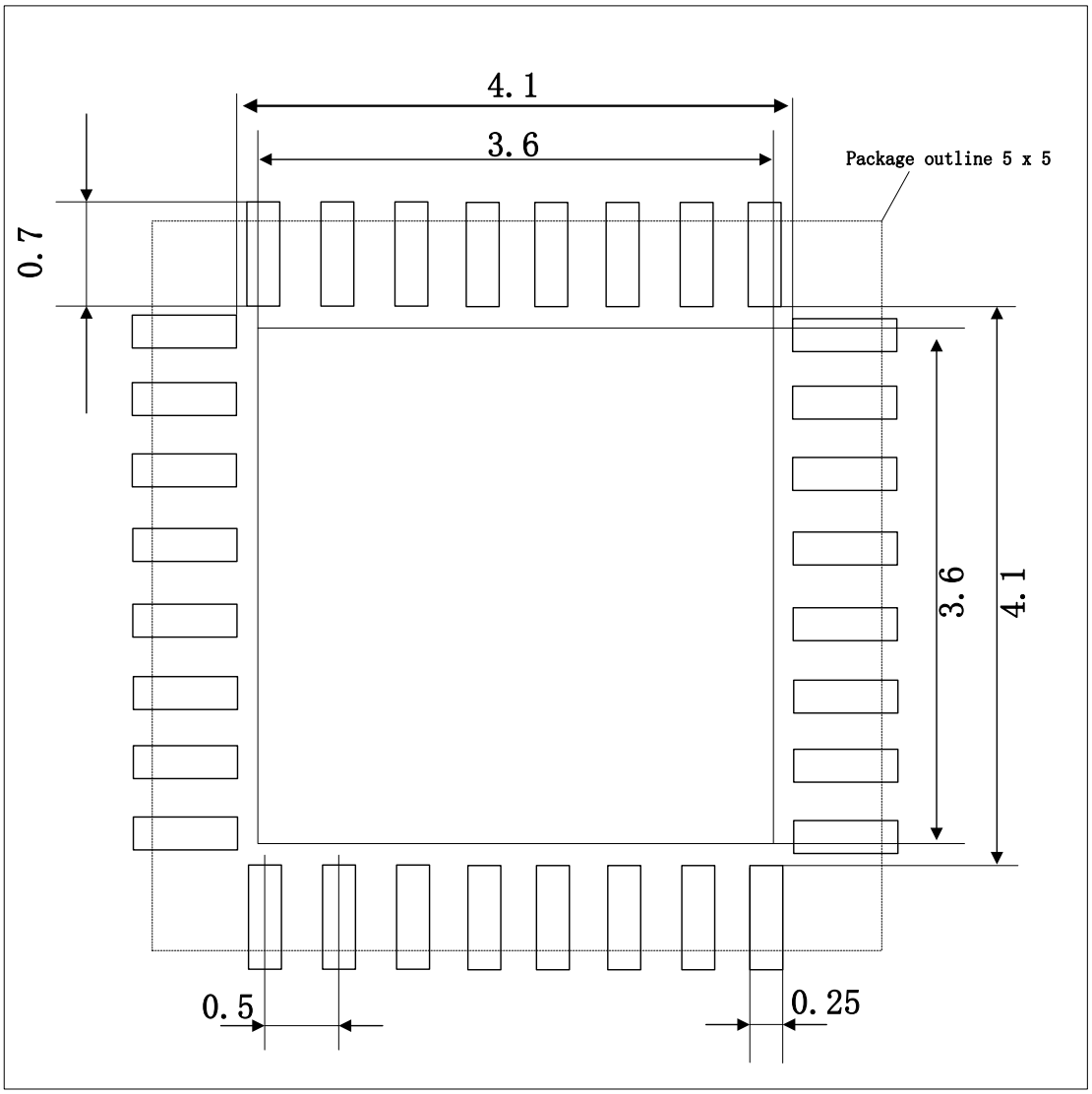

Figure 9 Recommended Footprint

6.4 Chip Marking

Figure 10 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 17 symbol and firmware version

Symbol	Firmware version
YY = 02	30.30

(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.

6.5 Reflow

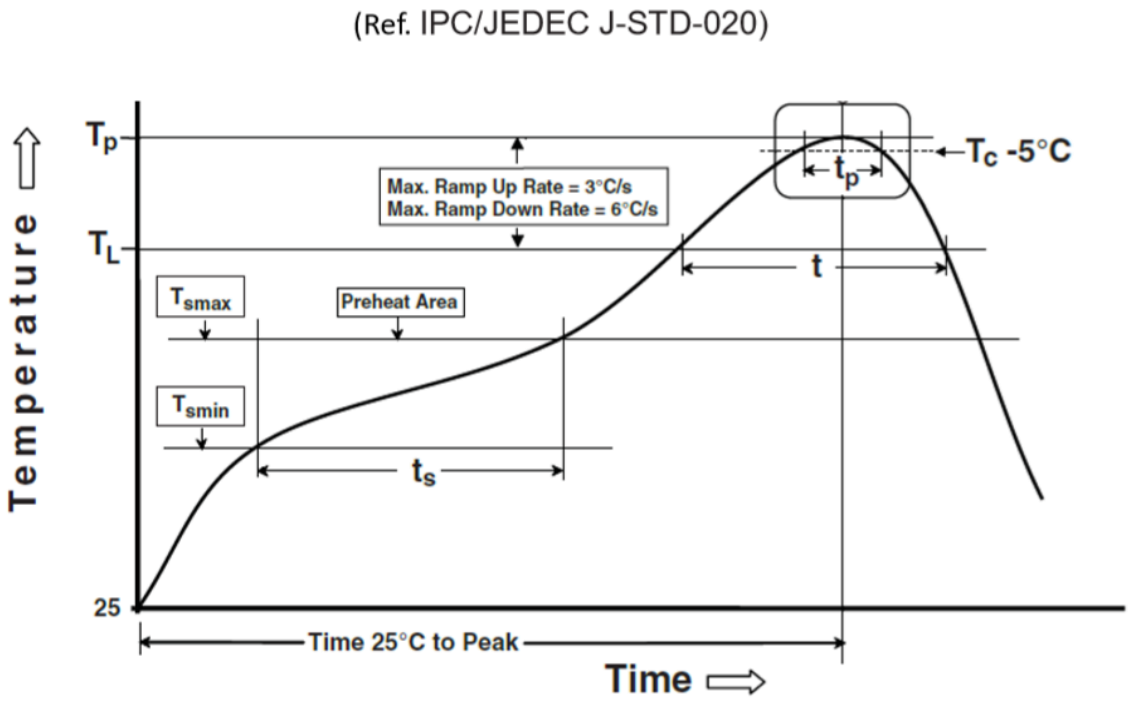

Figure 11 Reflow

Table 18 Classification Reflow Profiles

Profile Feature	Reflow
Preheat/Soak	
Temperature Min (T_{smin})	150 °C
Temperature Max (T_{smax})	200 °C
Time (t_s) from T_{smin} to T_{smax}	60-120 seconds
Ramp-up rate (T_L to T_p)	3 °C/second max.
Liquidous temperature (T_L)	217 °C
Time (t_L) maintained above T_L	60-150 seconds
Peak package body temperature (T_p)	245-260 °C
Time (t_p) within 5 °C of actual peak temperature	20-30 seconds
Ramp-down rate (T_p to T_L)	6 °C/second max.
Time 25 °C to peak temperature	8 minutes max.

6.6 Moisture sensitivity

MSL Moisture sensitivity levels Classifications is level 3.

6.7 RoHS/REACH/HALOGEN information

Table 19 RoHS/REACH/HALOGEN information

Name	Declaration
RoHS	We hereby certify that NS350 is compliant with all requirement and exemption set by the European RoHS 2.0, Directive 2011/65/EU & the European Delegated Directive (EU) 2015/863. NS350 is also compliant with China RoHS 2.
HALOGEN-Free	We hereby declare that NS350 delivered by us are complying with Halogen free requirements.
REACH	We hereby also certify that NS350 are fully comply with the related requirements of European Union Regulation (EC) 1907/2006 concerning the Registration, Evaluation, Authorization and Restriction of Chemicals (REACH).

Revision History

Table 20 Revision History

Revision Date	Revision	Description
2024-05-15	1.03	Update Electrical Characteristics
2024-04-21	1.02	Update information
2024-04-19	1.01	Update firmware information
2024-04-02	1.00	First release

IMPORTANT NOTICE

NSING Technologies Pte. Ltd. (“NSING”) 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 NSING’s products before placing orders. When purchasing NSING’s products, the responsibility solely lies on the purchaser to choose, select, and use the products, and NSING assumes no liability for any such responsibilities. NSING does not grant any license, whether express or implied, to any intellect property rights. If any purchaser resells NSING’s products with provisions that differ from the information stated in this document, such a resale shall void any warranty granted by NSING for the product. NSING and the NSING logo are their trademarks, and for more information on NSING’s trademarks, please see www.nsing.com.sg. 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.

NSING’s 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. NSING’s 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 NSING’s Products only in the manner specified in the product documentation and as explicitly approved by an authorized NSING’s representative in writing.