NS350 v33 Trusted Cryptography Module 2.0

Data brief Revision 1.00

Key Features

- Compliant to GM/T 0012-2020 Trusted computing – Trusted computing interface specification of trusted cryptography module
- I2C Interface, fast mode (400kbs)
- Enhanced (-40~+85°C)
- QFN16 and QFN32 package
- 1.8 V or 3.3 V supply voltage range
- 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

Table of Contents

1 Scope

1.1 Device Information

The NS350 v33 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-KQBR-x10	33.05	Enhanced temperature range (-40~+85°C) TCM 2.0 profile, I2C 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 v33 TCM2.0 together with its features and functionality. It is primarily intended for system developers.

2 Pin Description

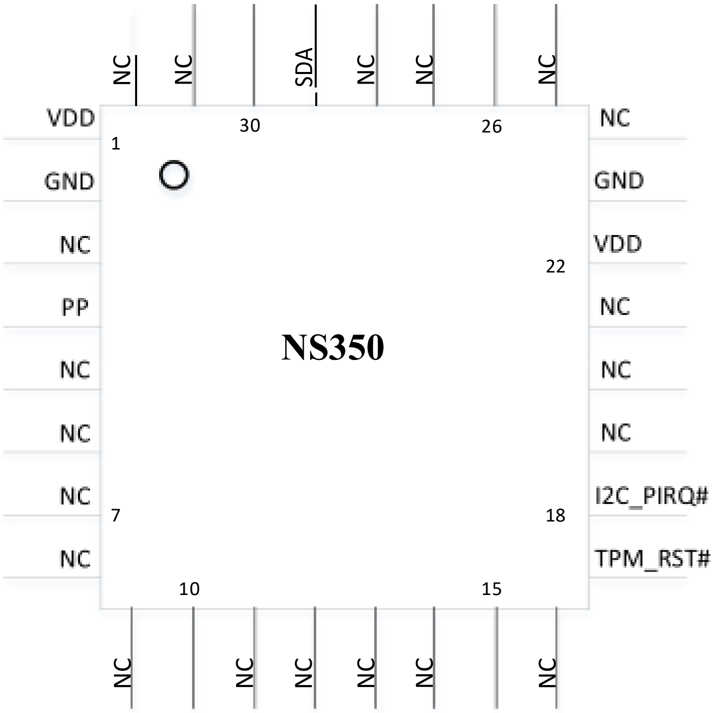


Figure 1 Pinout of NS350 v33 (Top View)

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
TPM_RST#	17	I	TPM_RST#: Active Low, internal weak pull up
I2C_PIRQ#	18	O	I2C_PIRQ#: Optional location for I2C PIRQ#, active low, open drain.
SDA	29	I/O	I2C Data pin
SCL	30	O	I2C Clock pin
NC	3,5,6,7,8,9,		No Connected (can be connected externally)

	11,12,13,14, 15,16,19,20, 21,24,25,26, 27,28,31,32		
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 Typical Schematic

Figure 2 shows the typical schematic for the NS350 v33. The power supply pins should be bypassed to GND with capacitors located close to the device.

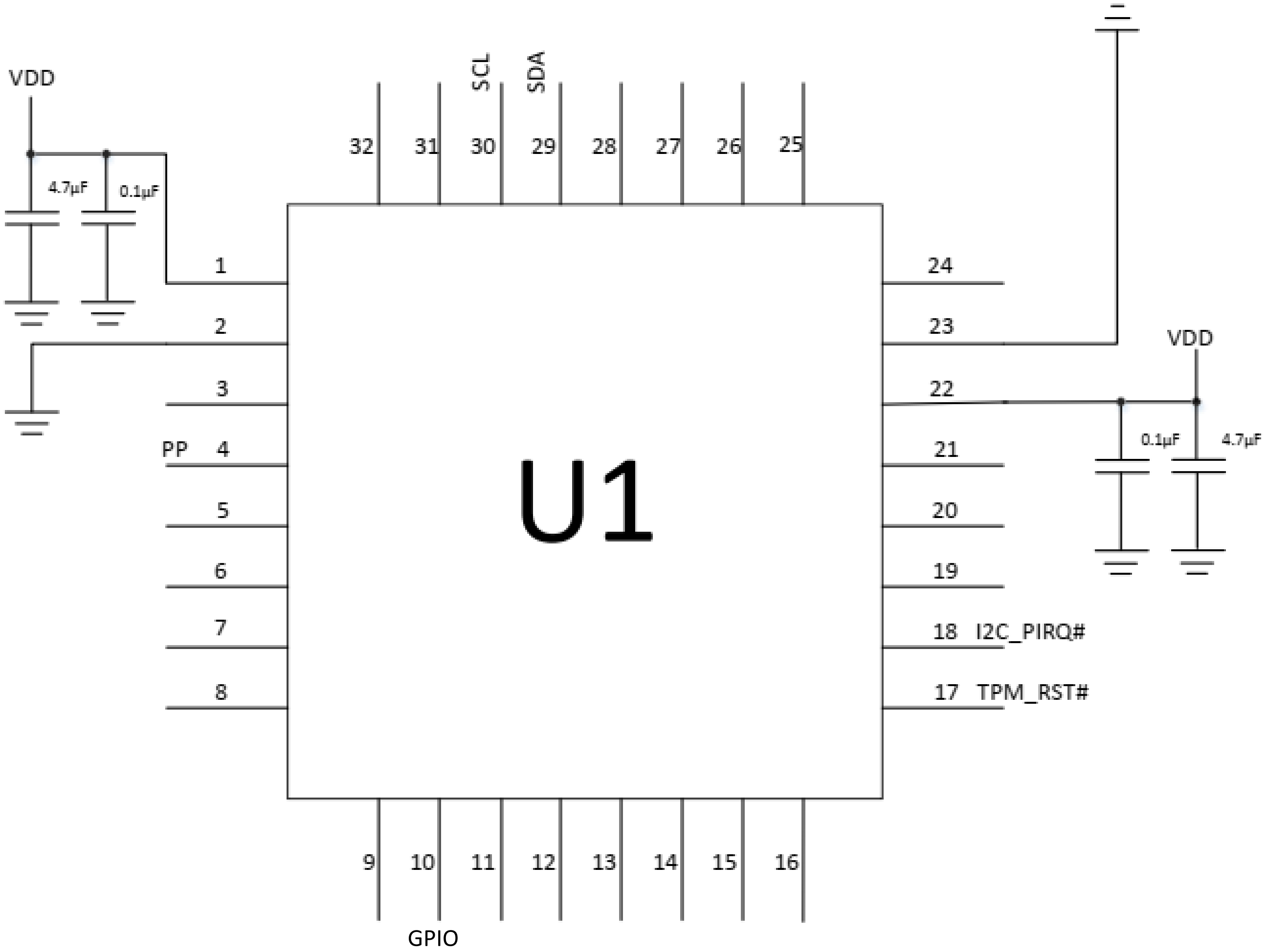


Figure 2 Typical Schematic

4 Package Information

4.1 Package Dimensions

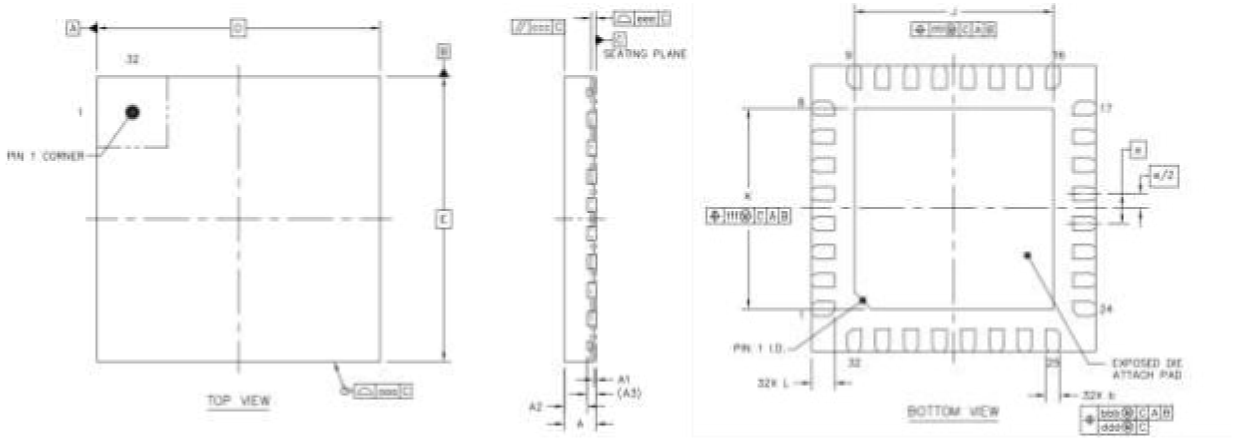
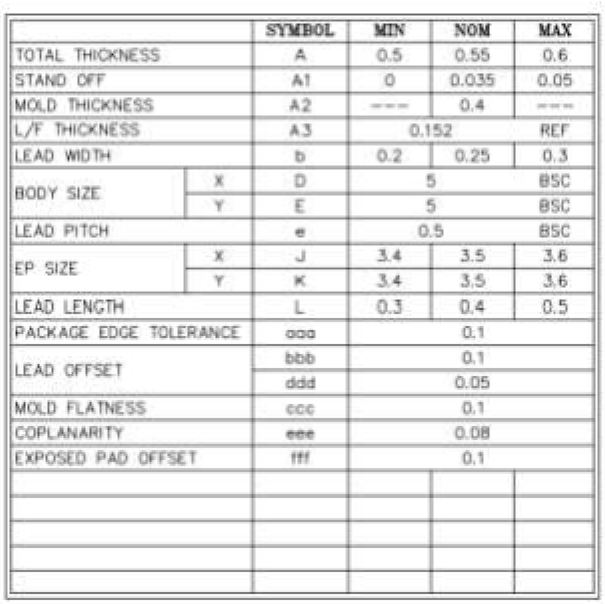


Figure 3 Package Symbol

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

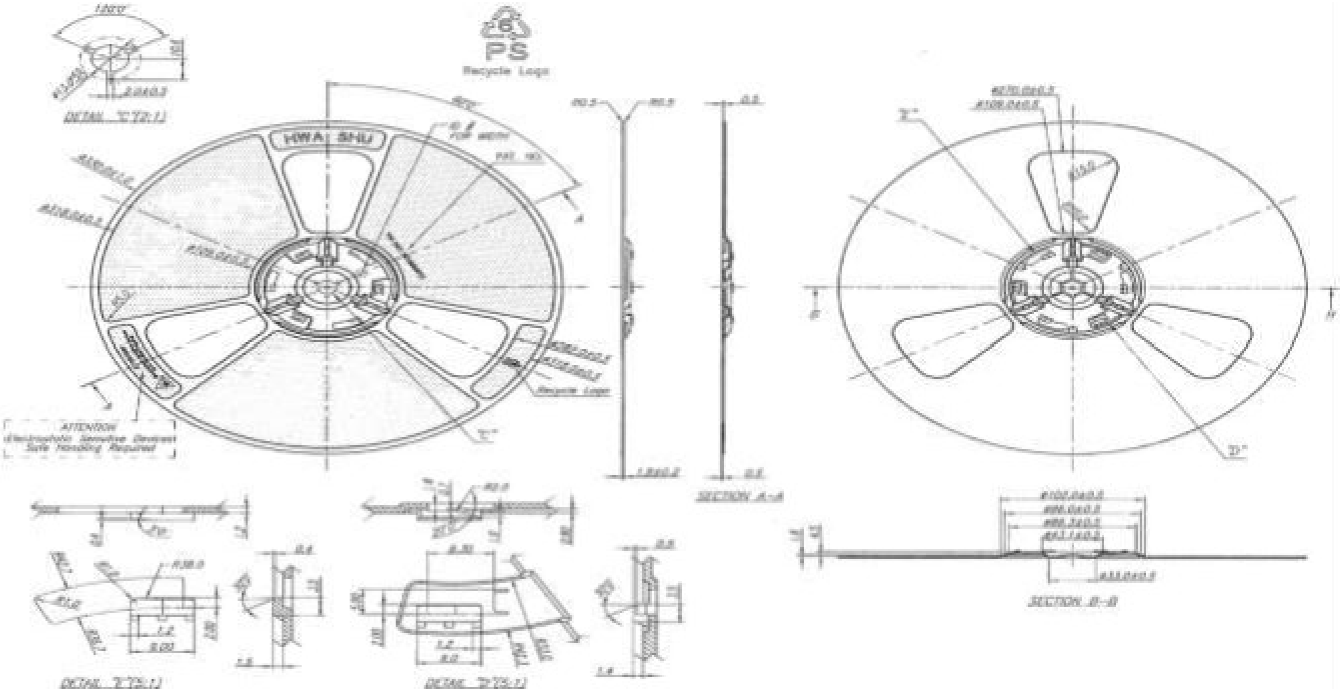


Figure 4 Reel diagram

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

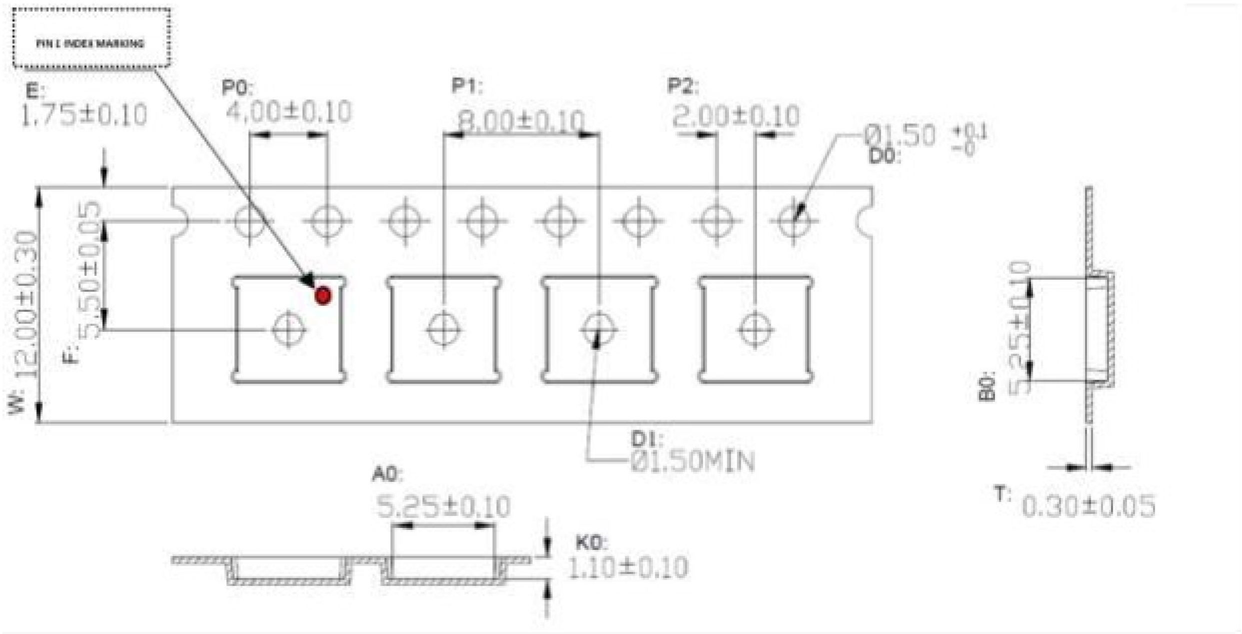


Figure 5 Packing Type

4.3 Recommended footprint

Figure shows the recommended footprint for the package.

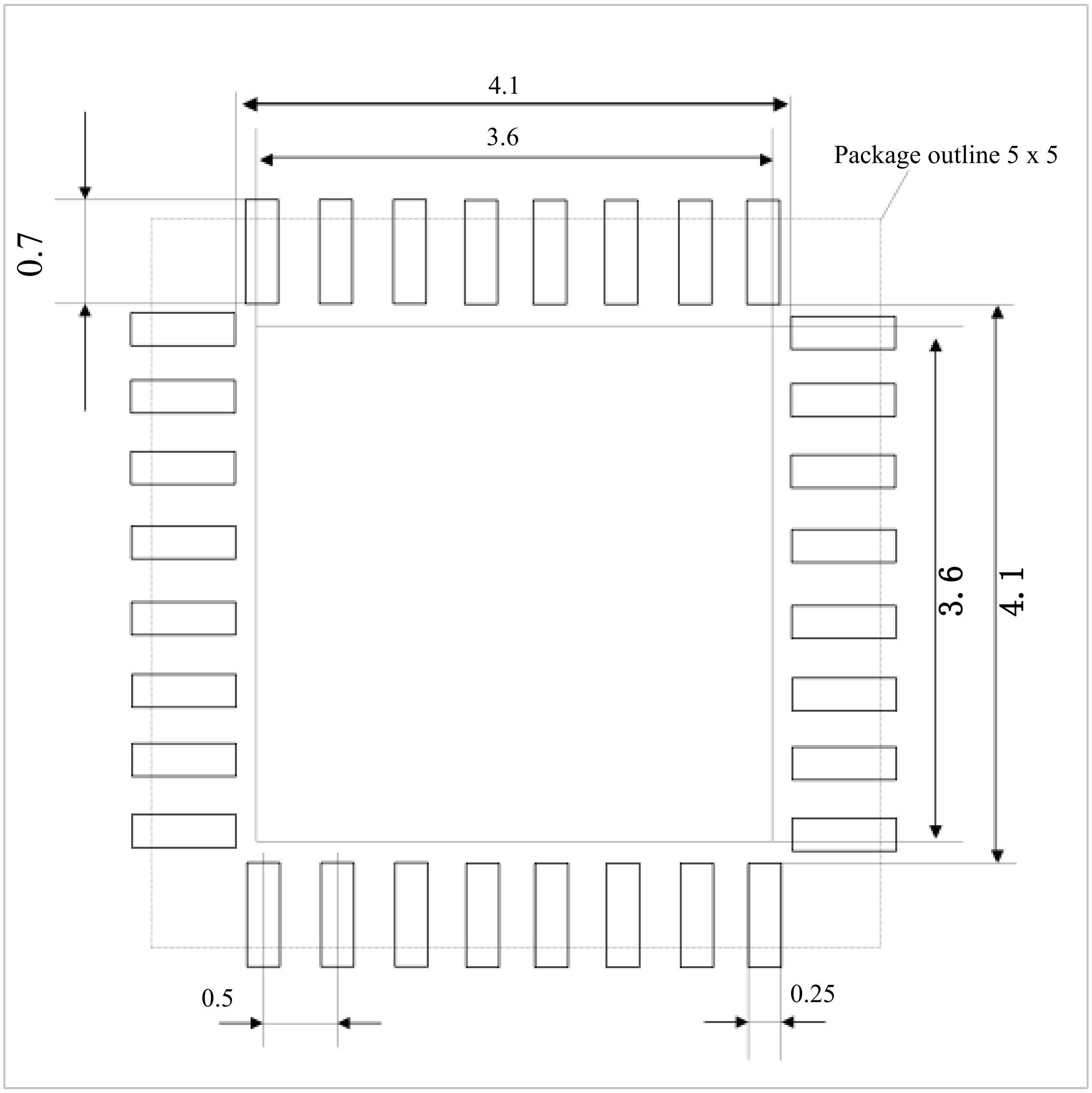


Figure 6 Recommended Footprint

4.4 Chip Marking

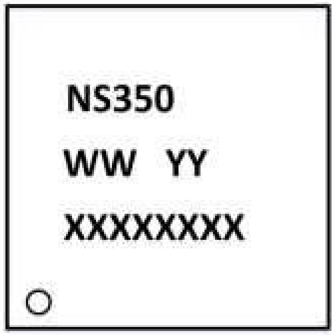


Figure 7 chip Marking

Description

(1) Line 1 - Hardware Technology name

NS350 is the name of the hardware technology.

(2) Line 2 - Device model

WW=BI means support temperature from -40˚C to 85˚C, I2C interface.

YY is the symbol for firmware version.

Table 4 symbol and firmware version

Symbol	Firmware version
YY = 03	33.05

(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.

5. Revision History

Revision	Date	Description
1.00	2024-03-29	First released

6. Disclaimer

This document is the exclusive property of NSING TECHNOLOGIES PTE. LTD. (Hereinafter referred to as NSING). This document, and the product of NSING described herein (Hereinafter referred to as the Product) are owned by NSING under the laws and treaties of Republic of Singapore and other applicable jurisdictions worldwide.

The intellectual properties of the product belong to Nations Technologies Inc. and Nations Technologies Inc. does not grant any third party any license under its patents, copyrights, trademarks, or other intellectual property rights. Names and brands of third party may be mentioned or referred thereto (if any) for identification purposes only.

NSING reserves the right to make changes, corrections. enhancements, modifications, and improvements to this document at any time without notice. Please contact NSING and obtain the latest version of this document before placing orders.

Although NATIONS has attempted to provide accurate and reliable information, NATIONS assumes no responsibility for the accuracy and reliability of this document. It is the responsibility of the user of this document to properly design, program, and test the functionality and safety of any application made of this information and any resulting product.
In no event shall NATIONS be liable for any direct, indirect, incidental, special, exemplary, or consequential damages arising in any way out of the use of this document or the Product.

NATIONS Products are neither intended nor warranted for usage in systems or equipment, any malfunction or failure of which may cause loss of human life, bodily injury or severe property damage. Such applications are deemed, Insecure Usage’. Insecure usage includes, but is not limited to: equipment for surgical implementation, atomic energy control instruments, airplane or spaceship instruments, all types of safety devices, and other applications intended to supporter sustain life. All Insecure Usage shall be made at user's risk. User shall indemnify NATIONS and hold NATIONS harmless from and against all claims, costs, damages, and other liabilities, arising from or related to any customer's Insecure Usage Any express or implied warranty with regard to this document or the Product, including, but not limited to. The warranties of merchantability, fitness for a particular purpose and non-infringement are disclaimed to the fullest extent permitted by law. Unless otherwise explicitly permitted by NATIONS, anyone may not use, duplicate, modify, transcribe or otherwise distribute this document for any purposes, in whole or in part.