Product Family	Part Number	Firmware Version	Interface		Package	Ambient Temperature		Applications
			SPI	I2C	QFN32	-20~+85°C	-40~+85°C	
Nations NS350 v32 TCM 2.0	NS350-KQAR-x0	32.06	○		○	○		PC and mobile computing with Intel x86 Trusted computing Servers
	NS350-KQBR-x0	32.06	○		○		○	ARM platforms and others Network equipment e.g. routers, gateways, switches, access points, multi-functions printers Industrial computing and programmable logic controllers embedded security
Nations NS350 v33 TCM 2.0	NS350-KQBR-x10	33.06		○	○		○	ARM platforms and others Network equipment e.g. routers, gateways, switches, access points, multi-functions printers Industrial computing and programmable logic controllers embedded security

The NS350 v32/v33 is a high-security, 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.

- Compliant to GM/T 0012-2020 Trusted computing – Trusted computing interface specification of trusted cryptography module
- SPI/I2C Interface
- 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