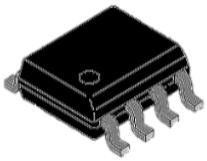
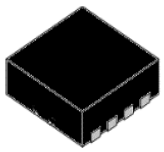
HQS6003E/HQS6004E
Brief Datasheet V1.4

HQS6003E/HQS6004E is a Low Power Secure Coprocessor. Its NIST Certified DRBG, Entropy Source and SHA Technologies can produce high quality entropy for secret key generation servers, HSMs, Linux & crypto applications.

Package Type



SOP8



8-Lead DFN (3mmx3mm)

- Basic Information
  - Operating Voltage: 2.0V ~ 5.5V
  - Operating Temperature: -40°C ~ 85°C
- Communication
  - HQS6003E supports standard I2C (Max: 1MHz)
  - HQS6004E supports standard SPI (Max: 10MHz@MODE3)
- Security Features
  - NIST CAVP DRBG, SP800-90A Standard Certified
  - NIST ESV(Entropy Source Validation) SP800-90B Standard Certified and CMVP FIPS 140-3 Complied
  - NIST FIPS180-4 Standard Certified, SHA-256
  - Active Tamper Detection and Reacts to Perturbation Attacks.
  - Independent Internal Clock to Prevent Glitch Attack
  - 128-bit Unique ID (UID)
- Applications
  - Financial transactions / POS (Point of Sales)
  - Secure IPSEC / TLS / SSL / SSH protocols
  - Networking / Smart Home
  - AIoT Device Security
  - Cloud Computing
  - Gaming and Lotteries
  - Secret Key Generation
  - Accessory Authentication
  - End-to-End Encryption
  - Scientific

1. Preface

The Random Number Generator is essential for system security and especially for providing the randomness and robustness of the keys for the cryptography. HQS600xE provides highest quality random numbers through TRNG, DRBG and SHA-256. Its Entropy Source is NIST ESV (SP800-90B) certified, the DRBG (SP800-90A) and SHA-256 are NIST CAVP certified.

HQS600xE is suitable for building highest level-security applications, such as IoT, Mobile Phone, Laptop, Tablet, SmartHome, SmartCity, Server, NAS, Gaming, etc.

IMQ Certifications

2. Pin Assignment

2.1 HQS6003E Pin Assignment/Description

PRODUCT: HQS6003ESP008C00R:

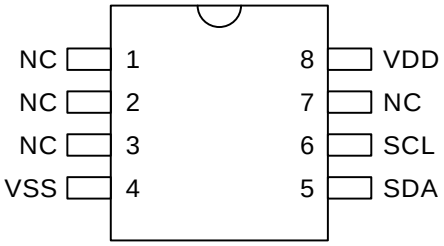


Figure 2-1 Pin Assignment of HQS6003E SOP8

PRODUCT: HQS6003EN3008C00R

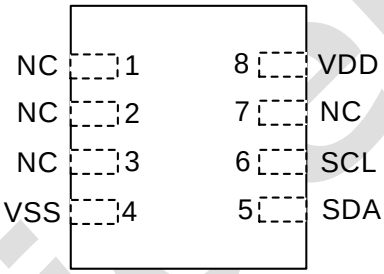


Figure 2-2 Pin Assignment of HQS6003E 8-Lead DFN

Pin No.	Pin Name	I/O Type	Description
1	NC	-	No Connect
2	NC	-	No Connect
3	NC	-	No Connect
4	VSS	GND	Ground
5	SDA	I/O	I2C Serial Data
6	SCL	I	I2C Serial Clock Input
7	NC	-	No Connect
8	VDD	Power	VDD power Supply

2.2 HQS6004E Pin Assignment/Description

PRODUCT: HQS6004ESP008S00R:

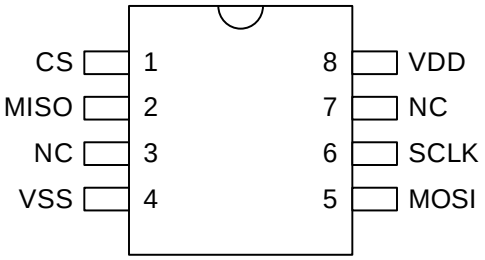


Figure 2-3 Pin Assignment of HQS6004E SOP8

PRODUCT: HQS6004EN3008S00R

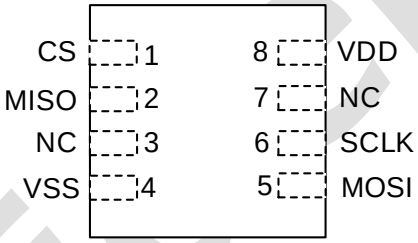


Figure 2-4 Pin Assignment of HQS6004E 8-Lead DFN

Pin No.	Pin Name	I/O Type	Description
1	CS	I	SPI Chip Select
2	MISO	O	Data Out
3	NC	-	No Connect
4	VSS	GND	Ground
5	MOSI	I	Data In
6	SCLK	I	Clock Input
7	NC	-	No Connect
8	VDD	Power	VDD power Supply

3. Electrical Characteristics

3.1 Absolute Maximum Rating

The absolute maximum ratings are rated values which must not be exceeded during operation, even for an instant. Any one of the ratings must not be exceeded. If any absolute maximum rating is exceeded, a device may break down or its performance may be degraded, causing it to catch fire or explode resulting in injury to the user. Thus, when designing products which include this device, ensure that no absolute maximum rating value will ever be exceeded.

(Vss=0V)

Parameter	Symbol	Pins	Ratings	Unit
Supply Voltage	V_{DD}		-0.3 to 6.0	V
Input Voltage	V_{IN}	All I/O pins	-0.3 to VDD+0.3	V
Output Current(Total)	I_{OL}	All I/O pins	100	mA
Storage Temperature	T_{STG}		-50 to 125	℃

3.2 Operation Conditions

The following defines the electrical characteristics of the device when it is operated at voltage and temperature maximum/minimum values. Unless otherwise stated, the standard conditions were determined at "operating temperature 25°C and operating voltage VDD = 3.3 V".

3.2.1 Operation Conditions

Parameter	Symbol	Condition	Min.	Typ.	Max.	Unit
Supply Voltage	V_{DD}		2.0	3.3	5.5	V
Operating Temperature	Ta		-40	25	85	℃

3.2.2 I/O Characteristics

Parameter	Symbol	Condition	Min.	Typ.	Max.	Unit
Input Low Voltage	V_{IL}	VDD=5V, temperature=25°C	0		0.3 VDD	V
Input High Voltage	V_{IH}	VDD=5V, temperature=25°C	0.7 VDD		VDD	V
Output Low Voltage	V_{OL}	VDD=5V, temperature=25°C IOL= 3 mA	0		0.1 VDD	V
Output High Voltage	V_{OH}	VDD=5V, temperature=25°C IOH= -3 mA	0.9VDD		VDD	V

3.3 DC Characteristics

Parameter	Symbol	Min.	Typ.	Max.	Unit
Supply Current in Operation Mode (Waiting for Command)	IDD_N1		3.7		mA
Supply Current in Operation Mode (During Command Execution)	IDD_N2		4.3		mA
Supply Current in Sleep Mode	IDD_DS	-	0.3	-	uA

3.4 Power-on Reset Characteristics

Ta=-40~85℃					
Symbol	**Description**	**Min.**	**Typ.**	**Max.**	**Unit**
tPPW	Power-on reset minimum pulse width	1	-	-	ms
tPWUP	Warming-up time after a reset is clear and device ready	-	4	-	ms
tVDD	Power supply rise time	0.5	-	5	ms

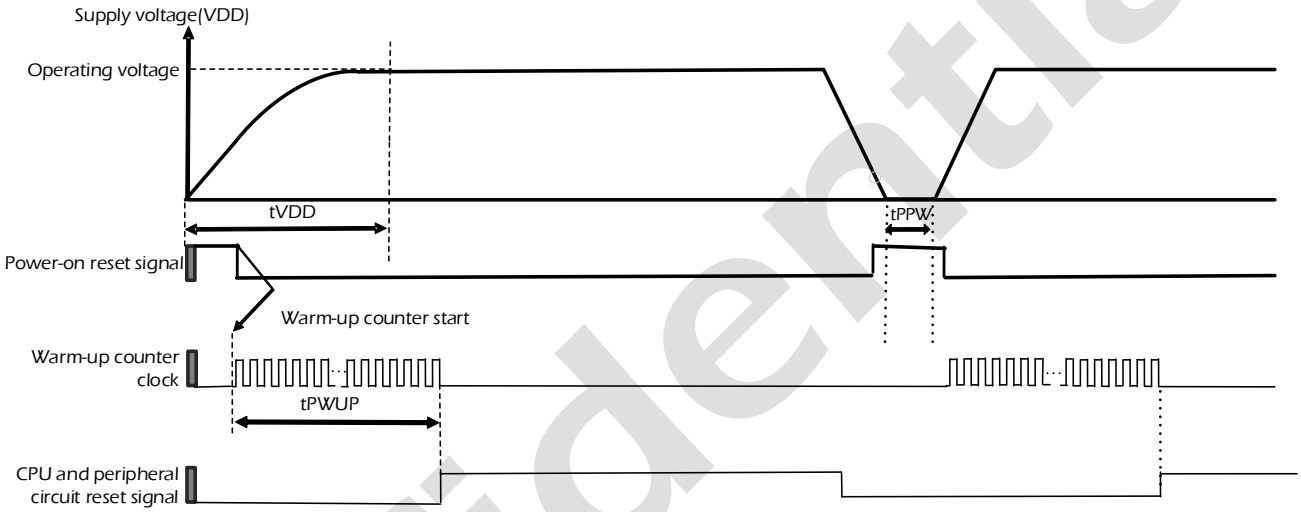


Figure 3-1 Operation Timing of Power-on Reset

Note：In power-down process, the VDD must be 0 V, then re-power-on to ensure the IC operating normal.

3.5 BROR Characteristics

Ta=-40~85℃

Parameter	Symbol	Condition	Min.	Typ.	Max.	Unit
BROR detected voltage	VBROR_Falling	VDD fall time > tVDD (tVDD please refer to Power-on Reset Characteristics)	1.85	1.90	1.95	V

3.6 AC Characteristics

3.6.1 AC Parameters

Parameter	Symbol	Min.	Typ.	Max.	Unit
Power-Up Delay	T_{PU_RDY}	-	1200	1500	us
Standby Time, Entering the deep sleep mode	T_{STB}	-	55	90	us
Wake-Up Ready Time, deep sleep mode	TW_{DS_RDY}	-	300	-	us

Note: The "Typ." value is based on 25°C room temperature, and the Sleep command will change this value.

3.6.2 I2C Characteristics

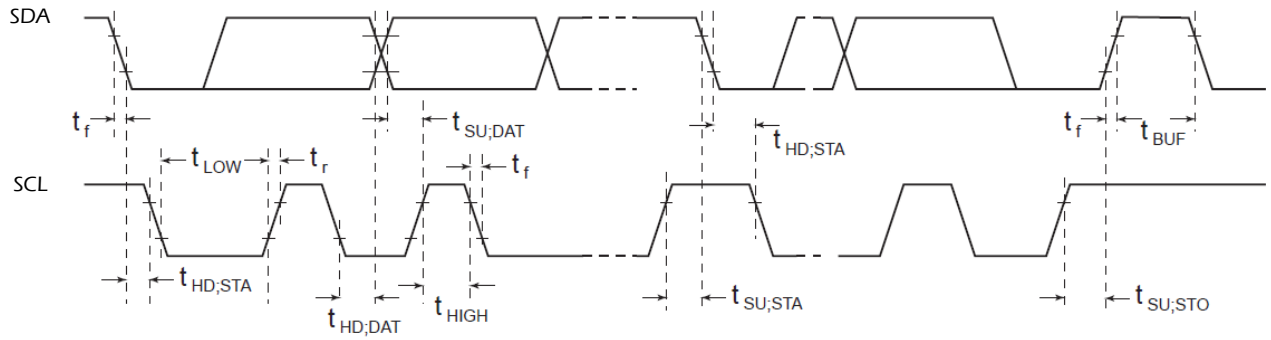


Figure 3-2 I2C Timing Sequence

Parameter	Symbol	Min.	Max.	Unit
Clock Frequency	f_{SCL}	-	1	MHz
Hold Time Repeated START Condition	$t_{HD;STA}$	0.45	-	us
Low Period of SCL Clock	t_{LOW}	0.65	-	us
High Period of SCL Clock	t_{HIGH}	0.35	-	us
Setup Time for a Repeated START Condition	$t_{SU;STA}$	0.35	-	us
Data Hold Time	$t_{HD;DAT}$	-	0.5	us
Data Setup Time	$t_{SU;DAT}$	0.1	-	us
Rise Time of Both SDA and SCL	t_r	20	300	ns
Fall Time of both SDA and SCL	t_f	20	300	ns
Setup Time of STOP Condition	$t_{SU;STO}$	0.6	-	us
Bus Free Time Between a STOP and START Condition	t_{BUF}	1.3	-	us
Capacitive Load for Each Bus Line	C_b	-	400	pF

3.6.3 SPI Characteristics

Mode 3

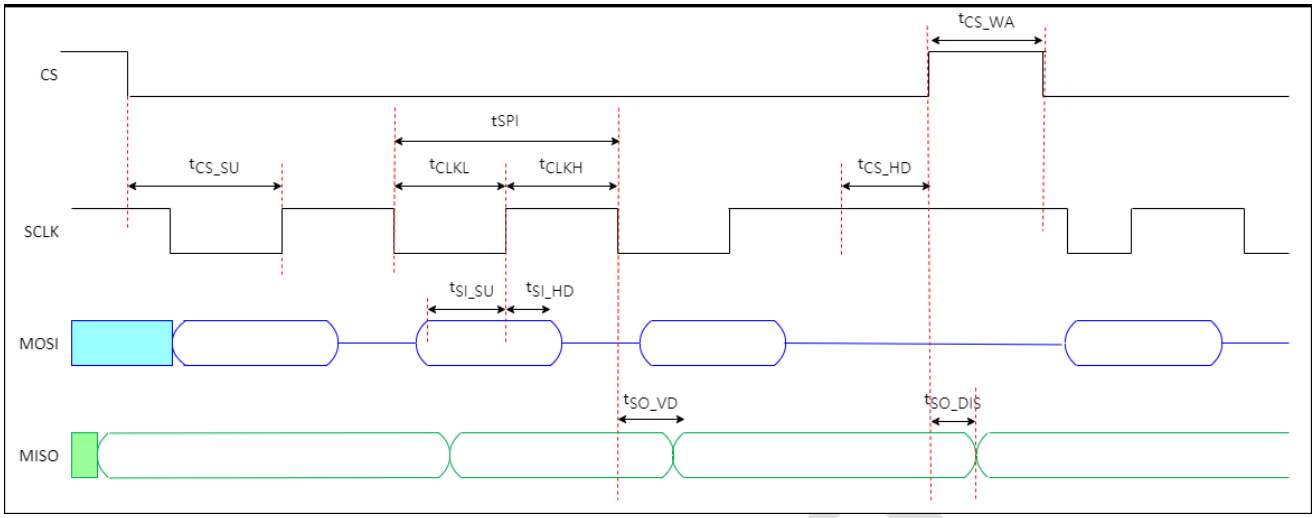


Figure 3-3 SPI mode 3 Timing Sequence

Parameter	Symbol	Min.	Max.	Unit
SPI Frequency	fSPI	-		
(VDD=2.7V~5.5V)			10	MHz
(VDD=2.0V~2.7V)			5	MHz
SPI Period	tSPI	1/fSPI	-	ns
High period of the SCLK pin	tCLKH	0.4 tSPI	-	ns
Low period of the SCLK pin	tCLKL	0.4 tSPI	-	ns
From SPICS active to first sample edge	tCS_SU	50	-	ns
From last SCLK shift edge to SPICS inactive	tCS_HD	50	-	ns
Time between SPI transaction	tCS_WA	3 tSPI	-	ns
Data Input Setup Time	tSI_SU	5	-	ns
Data Input Hold time	tSI_HD	5	-	ns
Data Output Valid Time	tSO_VD	-	20	ns
Data Output Disable Time	tSO_DIS	-	20	ns

4. Command Information

This section provides information on command, response format, and response status codes used in this device. The following terms are used in this document.

Table 4-1 Document Termsw

Term	Meaning
Var.bit	Use to specify one bit in a variable. For example, MODE.2, refers to bit 2 of MODE.
Var.a:b	Use to specify multiple bits in a variable. For example, MODE.2:0 refers to bits 2:0 of MODE.
MVar[a:b]	For a multiple byte variable, this notation specifies multiple bytes of the variable. For example DIN[5:0], refers to Byte 0 to Byte 5 of DIN.

4.1 Initial Sequence

After any reset or wake from sleep mode, Host should sent RDSR command to device until device return 'READY'. Next, host should send the Info – Error Status to enquire if any error has been detected. Failure condition such as Self Test failure will restrict the device to respond to a limited set of commands.

After any reset, host shall send SelfTest command to ensure that Random Number Generator is operated properly before issuing the Random Command.

4.2 Byte and Bit Ordering

All multi-byte elements are treated as arrays of bytes and are processed in the order received or transmitted with most significant byte first. Within a byte, the most significant bit is transmitted first.

In this document, the most-significant byte appears towards the left hand side of the page.

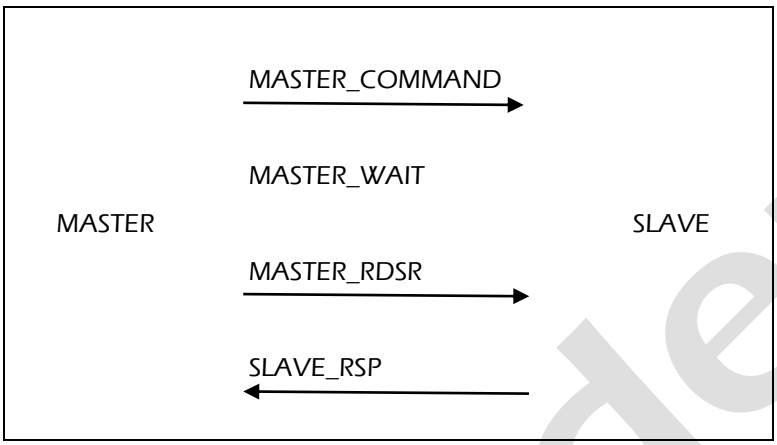
4.3 Command Sequence

Host communicated with the device via the following supported communication interface:

- I2C (HQS6003E)
- SPI (HQS6004E)

This device supports communication in the form of Command and Response.

A typical command sequence is as follow



Master is an external host while slave is HQS6003E/HQS6004E.

Master issues a command (MASTER_COMMAND) to Slave

Master waits for Slave to execute the command (MASTER_WAIT)

Master issues a Read Status command (MASTER_RDSR)

Slave sends a Slave Response (SLAVE_RSP)

All the commands follow the above protocol. RESET and RDSR are special cases and are described in details in the later sessions.

For data integrity, all commands and responses are appended with a CRC16 checksum with initial value set to 0xFFFF. The CRC is computed over the entire packets starting from the first byte to the byte before the CRC Checksum.

The polynomial use is CRC-16: X^16 + X^12 + X^5 + 1 (0x1021)

The first CRC byte transmitted (N-1) is the Most Significant Byte of the CRC value, so the last byte of the group is the Least Significant Byte of the CRC.

4.4 Command Format

Regardless of the interface selected, all commands and responses are constructed in manner described in this session.

Command Packet:

Table 4-2 Command Format

Size (Byte)	Name	Description
1	LEN	Number of bytes in the command including LEN byte. Minimum value is 7, up to supported by the individual command.
1	COMMAND	Command Code
1	MODE	Mode
2	PARAM	Parameters
LEN - 7	DIN	Data Input (Optional) depending on command
2	CRC16	CRC16 Checksum. Computed over the entire command sequence from LEN to DIN.

If any of the command field values differs from the command definition or LEN value does not match the command length received, then the device may response with either an error indication or some input bytes may be silently ignored. Any values not currently defined in the command are reserved for future use. Application should not use them in their system.

After a complete error-free command is received, the device status is changed to BUSY and command execution starts. Only RDSR status command is accepted while device is BUSY. All other command will be ignored. Command execution result is available after the status is changed from BUSY to Success.

4.5 Response Format

The command response is retrieved by the Read Status Command (RDSR). The device response is divided into two response packets. The first packet (Response Length) returns the length of command result output while the second packet (Response Data) return command result. Please refer to each command for the response data information.

CRC and LEN errors indicate a communication interface issue. Command may be resent to the device. All the other errors should be resolved first before resending command to the device. If multiple error occurs, only one of them will be reported. In the case of an error condition, no Response Data response will be returned.

Table 4-3 Response Length Format

Size (Byte)	Name	Description
1	LEN	Number of bytes in Response Length from LEN to CRC16. This Response packet has a fixed length of 5.
1	STATUS	Status. 0x00 if command execute successfully. An error status code if command fails.
1	RSP LEN	Response Length. For command with no output data, this field has a value of 0x00. For command with output data, this field contains the total length of the Response Data Packet.
2	CRC16	CRC16 Checksum. Computed over the entire command sequence from LEN to RSP LEN.

Table 4-4 Response Data Format

Size (Byte)	Name	Description
1	RSP_LEN	Number of bytes in Response Data from RSP LEN to CRC16. This field has the same value as RSP LEN in the Response Length above.
RSP_LEN - 3	DOUT	Data Output depending on command
2	CRC16	CRC16 Checksum. Computed over the entire command sequence from LEN to DOUT.

4.6 Response Status Codes

The device status is listed in Table 4-5 Device Status. The device is ready to receive a new command if it is not BUSY.

Table 4-5 Device Status

Status Code	State Description	Description
0x00	Successful Command Execution	Command executed successfully.
0x01	READY	The device is now idle and is ready for a new command.
0x03	CRC or Other Communications Error	Communication Error. Invalid command CRC16 value or invalid length (LEN < 7). The command is ignored.
0x04	Invalid Command/Parse Error	Command was properly received. However, command fields are invalid. Correction of the command fields must be made before command is resent.
0x07	Failure Error	Failure condition occurs. This will restrict the device to respond to a limited set of commands. Use Info – Error Status to retrieve the error source.
0x0F	Execution error	Command was properly received but could not be executed by the device in its current state. Changes in the device state or the command field values must be made before command is resent.
0x7F	BUSY	Device Busy. Device is not ready to receive any command. Device is either executing a command or during initialization.

4.7 I2C Format

The I2C supports the following features:

- Slave Only
- 7-bit address
- Up to 1MHz

The I2C adds Start(S), Slave Address (ADDR) R/W and Stop (P) condition to the basic protocol format.

I2C address default value is 0xC8.

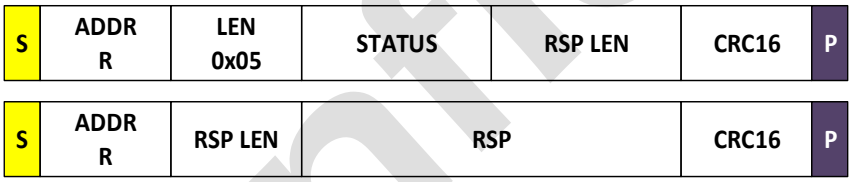
The command packet is terminated by a STOP condition.

In between the two response packets, a STOP condition must be sent.

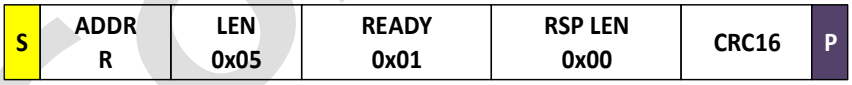
I2C Command Format

RDSR Command Format:

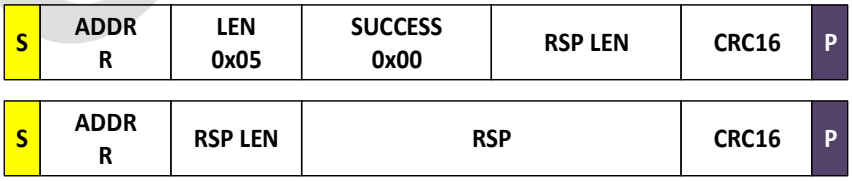
Response Format



Response Format – Ready:



Response Format – Success:



Response Format – Busy:

S	ADDR R	LEN 0x05	BUSY 0x7F	RSP LEN 0x00	CRC16	P

Response Format –Communication Error:

S	ADDR R	LEN 0x05	COMERR 0x03	RSP LEN 0x00	CRC16	P

4.8 SPI Format

This device uses the SPI serial interface for communication. The SPI supports the following features:

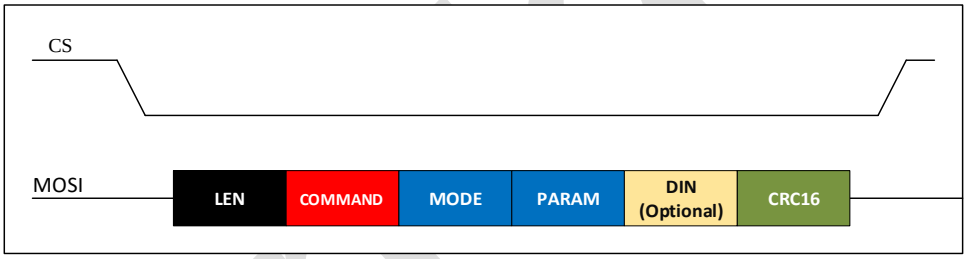
- Slave Only
- Mode 3
- Up to10MHz

SPI supports Slave mode only. The SPI interface is composed of four signals:

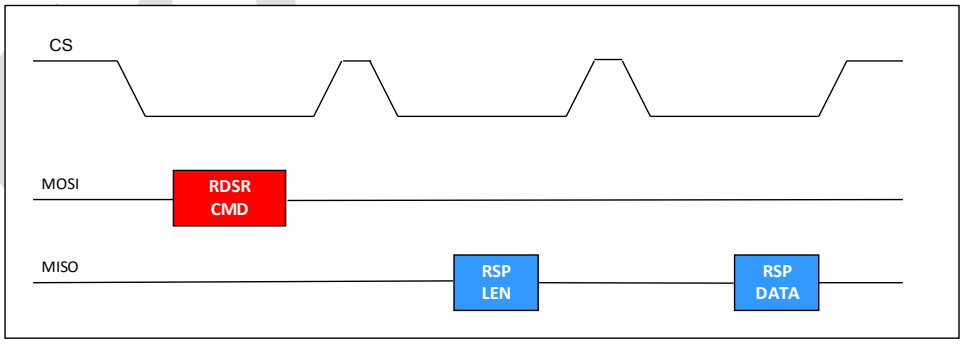
SCLK	SPI CLK :	SPI clock output driven by master and input to the slave.
MOSI	Master Out Slave In :	A unidirectional output driven by master and input to the slave.
MISO	Master In Slave Out:	A unidirectional input to the master and output driven by slave.
CS	Chip Select :	The SPI Chip Select is an output driver by master and input to the slave.

An SPI transaction starts when the master asserts the slave chip select and ends when the slave chip select is deasserted. After CS is asserted, if available, output data is shifted out by the first shift edge. Data is shifted out by the output device on the shift edge and sampled by the recipient at the sample edge.

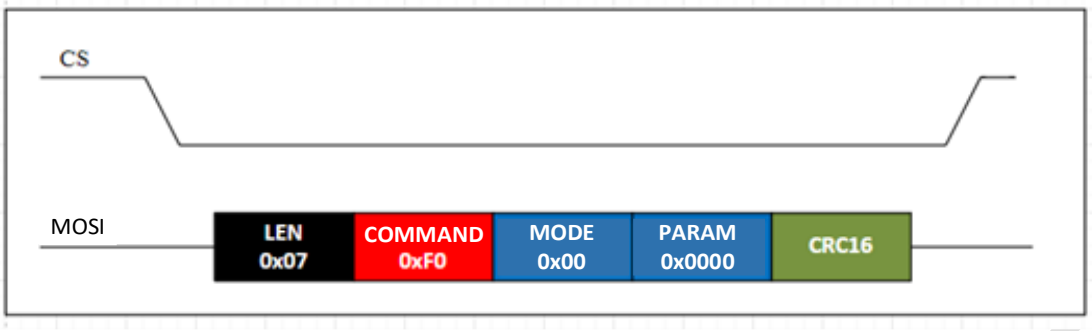
SPI Command Format



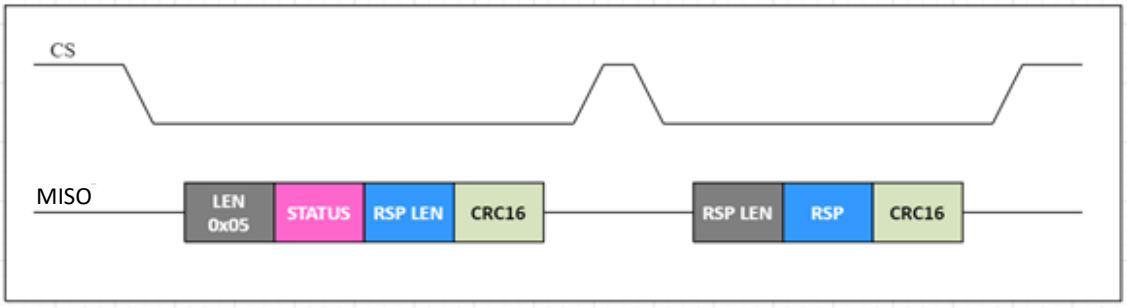
SPI Read Status Command and Response Format



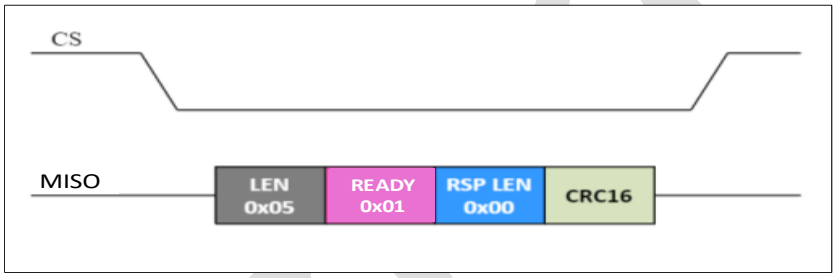
RDSR Command Format



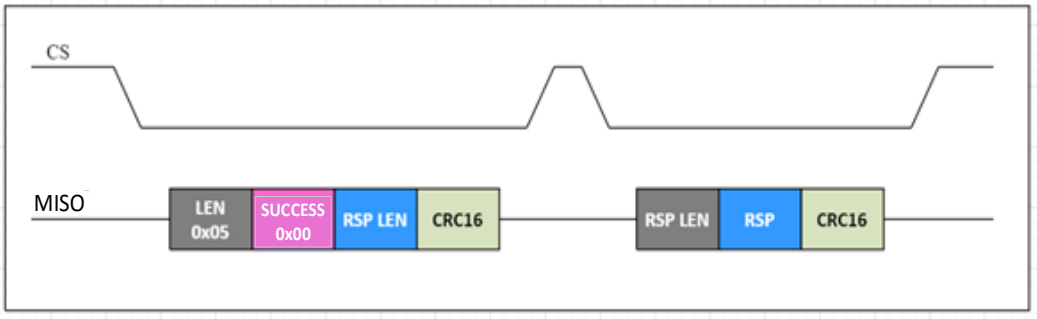
Response Format



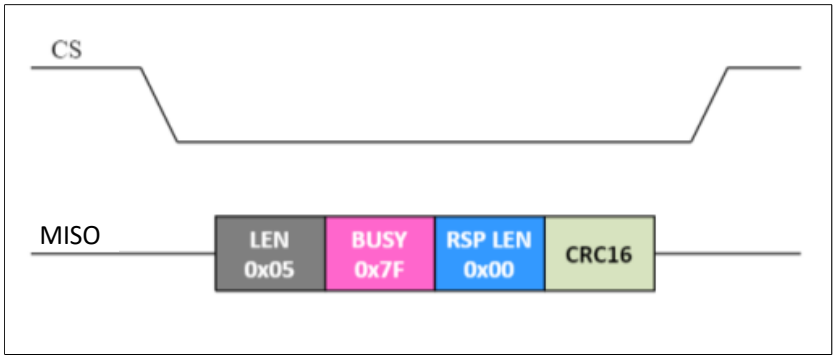
Response Format – Ready



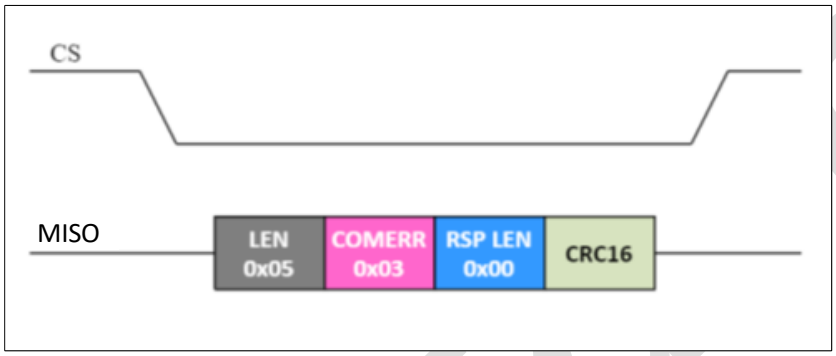
Response Format – Success



Response Format – Busy

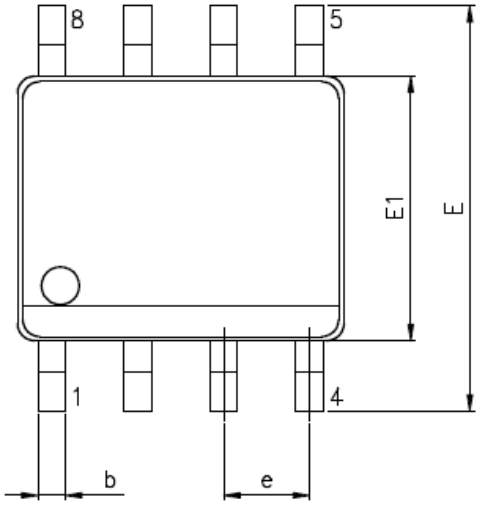


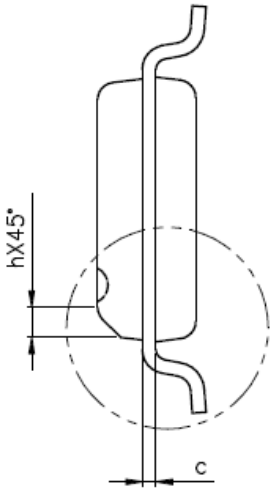
Response Format – Communication Error

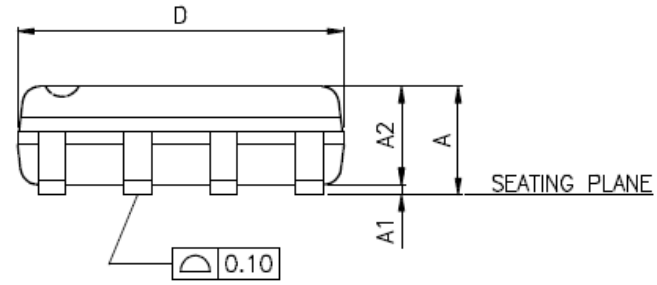


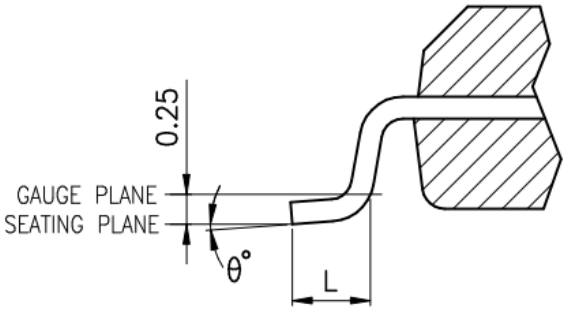
Appendix A. Package Information

SOP8



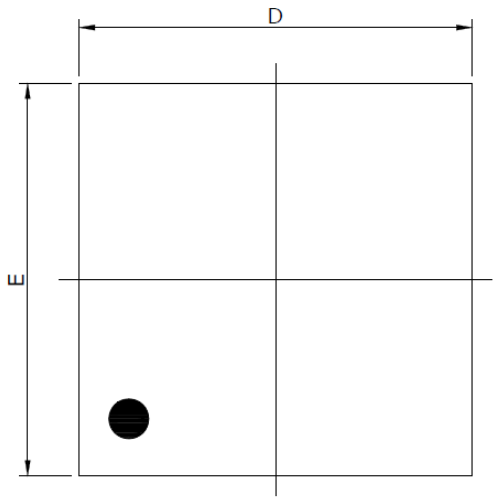




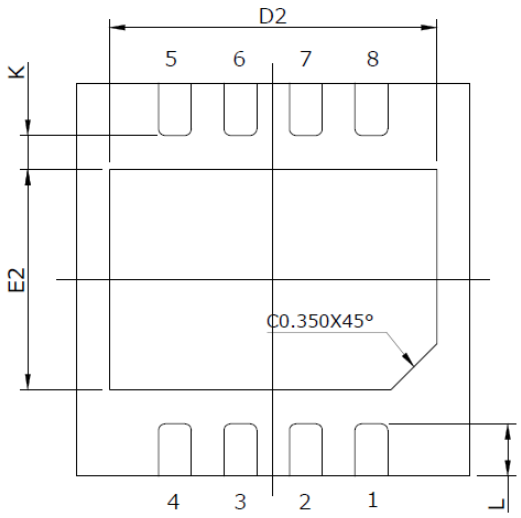


Symbol	mm		
	Min.	Typ.	Max.
A	–	–	1.75
A1	0.10	–	0.25
A2	1.25	–	–
b	0.31	–	0.51
c	0.10	–	0.25
D	4.90 BSC		
E	6.00 BSC		
E1	3.90 BSC		
e	1.27 BSC		
L	0.40	–	1.27
h	0.25	–	0.50
θ	0°	–	8°

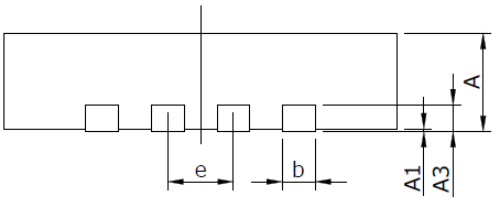
8-Lead DFN (3mm x3mm)



TOP VIEW



BOTTOM VIEW



Symbol	mm		
	Min.		Max
A	0.70	0.75	0.80
A1	0.00	0.02	0.05
A3	0.203 REF.		
b	0.20	0.25	0.30
D	2.90	3.00	3.10
E	2.90	3.00	3.10
e	0.50 BSC		
L	0.35	0.40	0.45
D2	2.45	2.50	2.55
E2	1.63	1.68	1.73
K	0.20	–	–

Appendix B. Ordering Information

When ordering products, please provide the following details:

Ordering Information	Product	Packing	Description
Example	HQS6003ESP008C00R	T	I2C, SOP8, Tape & Reel, 85℃, A5
	HQS6003EN3008C00R	T	I2C, DFN 3x3, Tape & Reel, 85℃, A5
	HQS6004ESP008S00R	T	SPI, SOP8, Tape & Reel, 85℃, A5
	HQS6004EN3008S00R	T	SPI, DFN 3x3, Tape & Reel, 85℃, A5
	HQS6003ESP008C01R	T	I2C, SOP8, Tape & Reel, 85℃, A5.1
	HQS6003EN3008C01R	T	I2C, DFN 3x3, Tape & Reel, 85℃, A5.1
	HQS6004ESP008S01R	T	SPI, SOP8, Tape & Reel, 85℃, A5.1
	HQS6004EN3008S01R	T	SPI, DFN 3x3, Tape & Reel, 85℃, A.5.1

Note 1: "Packing"- T: Tape & Reel; B: Tube/Tray

Appendix C. Product Number Information

Example： **HQS 60 04E SP 008 S 01 R T**

iMQ HQS product

Product Series

Sub Series

Package Type

Code	Package Type
SP	SOP
N3	DFN 3x3

Pin Count

Code	Pin
008	8

Communication Interface

Code	Type.
C	I2C
S	SPI
W	SWI

Designator

Code	Version
00	A5
01	A5.1

Operating Temp

Code	Operating Temp.
R	-40~85°C

Packing

Code	Packing
T	T&R
B	Tube

Revision History

Version	Approved Date	Description
V1.4	2025/02/24	1. Add "Preface" Section
V1.3	2025/02/20	1. Modify Security Features "NIST CAVP Certified DRBG Technology" to "NIST CAVP DRBG, SP800-90A Standard Certified" 2. Modify Security Features "NIST SP800 -90A/B/C compliant test" to "NIST ESV(Entropy Source Validation) SP800-90B Standard Certified and CMVP FIPS 140-3 Complied" 3. Remove Security Features "NIST SP800-22 test suite compliance" 4. Modify Security Features "NIST 180-4 SHA-256" to "NIST "FIPS180-4 Standard Certified, SHA-256"
V1.2	2025/02/04	1. Add Packing (T) in Appendix C. Product Number Information 2. Add "Designator" example description in Appendix B. Ordering Information 3. Correct typo "Packaging" to "Packing" in Appendix B. Ordering Information
V1.1	2024/12/24	1. Sync with full version datasheet
V1.0	2024/12/6	1. Initial release based on HQS6003E/HQS6004E Datasheet, TDDS02-H6004-EN