Modsemi CryptoAuthentication

MOD208

Revision history

Document version	Date of release	Description of changes
1.42	2021-12-08	
1.40	2021-10-08	
1.30	2021-09-01	
1.00	2019-05-01	Initial Version

MOD208

MOD208 CryptoAuthentication：
Ensure device and software code is Trusted, Real, Untampered, and Traceable

Key features

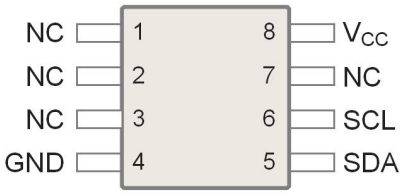
- Security co-processor with cryptographic algorithm and key storage
  - > High-end security controller
  - > Protected Storage for Keys
- Secure Symmetric Authentication Device Host and Client Operations
- High Security SHA-256 Hash Algorithm with Message Authentication Code (MAC) and Hash-Based Message Authentication Code (HMAC) Options
- High reliability and Security 256-bit Key Length; Storage for Up to 16 Keys
- Internal High-Quality NIST Standard Random Number Generator (RNG)
- Up to 5kB of user security NVM to store Keys and security Data
- 512 bit OTP (One Time Programmable) Bits for Fixed Information
- Interface Options Available400k/100K Hz Standard I2C Interface
- 1.65V to 3.6V Supply Voltage Range
- Secure Download and Boot
  - Ecosystem Control
  - Message Security
  - Anti-Cloning
- Fast and easy integration
- DFN8 and SOP8 Packages

Benefits

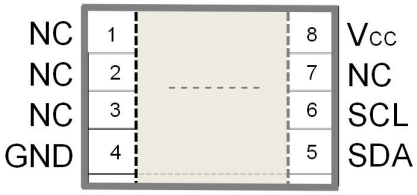
- Electronic equipment Anti-cloning.
- Authentication and Protect Code
- Secure Download and Boot
- Ecosystem Control Ensure Only OEM/Licensed Nodes and Accessories Work
- Prevent Building with Identical BOM or Stolen Code
- Message Security Authentication, Message Integrity, and Confidentiality of Network Nodes (IoT)
- Electronic accessories protection

Description of PIN

SOP8
(Top View)



DFN8
(Top View)



Pin	Function
GND	Ground
SDA	Serial Data
SCL	Serial Clock Input
VCC	Power Supply
NC	No Connect

Table of Contents

Intended audience

This Datasheet is intended for device integrators and board manufacturers.

1. Introduction

1.1 Introduction

The MOD208 is a high-security authenticator that provides a core set of cryptographic accelerators derived from integrated symmetric (SHA-256) security functions. In addition to the security services provided by the hardware implemented crypto engines,the device integrates a FIPS/NIST true random number generator (RNG), 5Kb of secured NVM,The MOD208 combine key storage with advanced hardware cryptographic accelerators to implement various authentication applications.

1.2 Features

The MOD208 based on an advanced security controller with built-in tamper proof NVM for secure storage and Symmetric crypto engines to support SHA-256. The MOD208 includes an security NVM which can be used for storage keysand private data， security read/write, read-only or secret data, consumption logging, and security configurations.This new security technology greatly enhances your overall system securit.The MOD208 features a wide array of defense mechanisms specifically designed to prevent physical attacks on the device itself or logical attacks on the data transmitted between the device and the system.

MOD208 has an I2C interface that supports secure communication, which can easily and fast integrate with host microcontroller software.

MOD208 covers a broad range of use cases necessary for many types of security applications that include the following:：

- **Secure Download and Boot**

  Authentication and Protect Code In-transit
- **Ecosystem Control**

  Ensure Only OEM/Licensed
  Nodes and Accessories protection
- **Anti-cloning**

  Prevent Building with Identical BOM or Stolen Code
- **Message Security**

  Authentication, Message Integrity, and Confidentiality of Network Nodes (IoT)

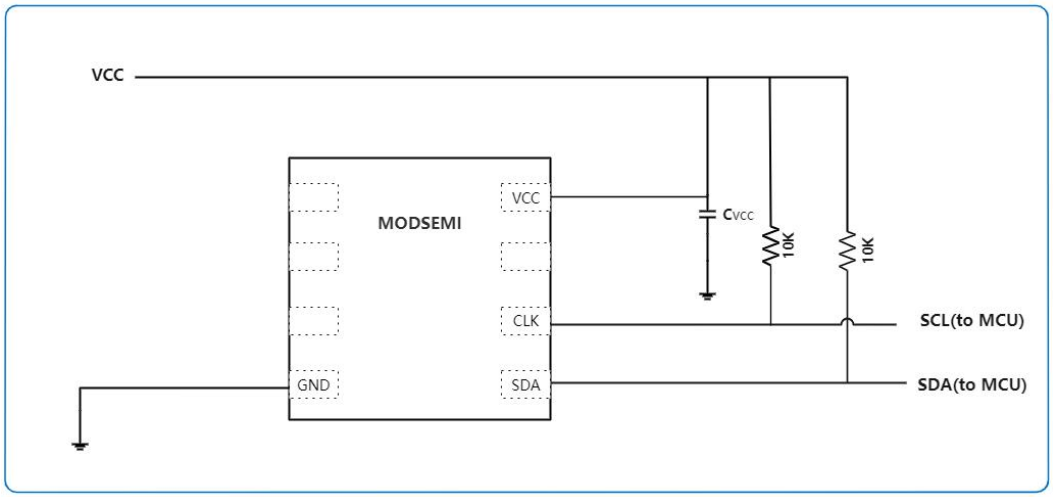
2. Interface and Schematics

This section explains the schematics of the product and gives some recommendations as to how the controller should be externally connected.

2.1 System Integration Schematics

The following figure illustrates how to integrate MOD208 with your local host.

Figure 2 -1 System Integration Schematic Diagram



Note: Value of the pull up resistors and Cvcc depend on the target application circuit and the targeted I2C frequency.

3. Electrical Characteristics

3.1 Absolute Maximum Ratings

Parameter	Description	Min.	Max.	Units
TS	Storage Temperature	-55	125	℃
TA	Operating Temperature	-40	85	℃
VCC	Operating Voltage	1.62	3.3	V
VESD	Human Body Model(HBM) ESD	-	4000	V

Note: Stresses beyond those listed under "Absolute Maximum Ratings" may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of this specification are not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

3.2 Reliability

The MOD208 is fabricated with high reliability NVM manufacturing technology.

Table 3-1. FLASH Reliability

Parameter	Min.	Typ.	Max.	Units
Write Endurance	100,000	—	—	Write Cycles
Data Retention	10	—	—	Years
Read Endurance	Unlimited			Read Cycles

3.3 DC Parameters: All I/O Interfaces

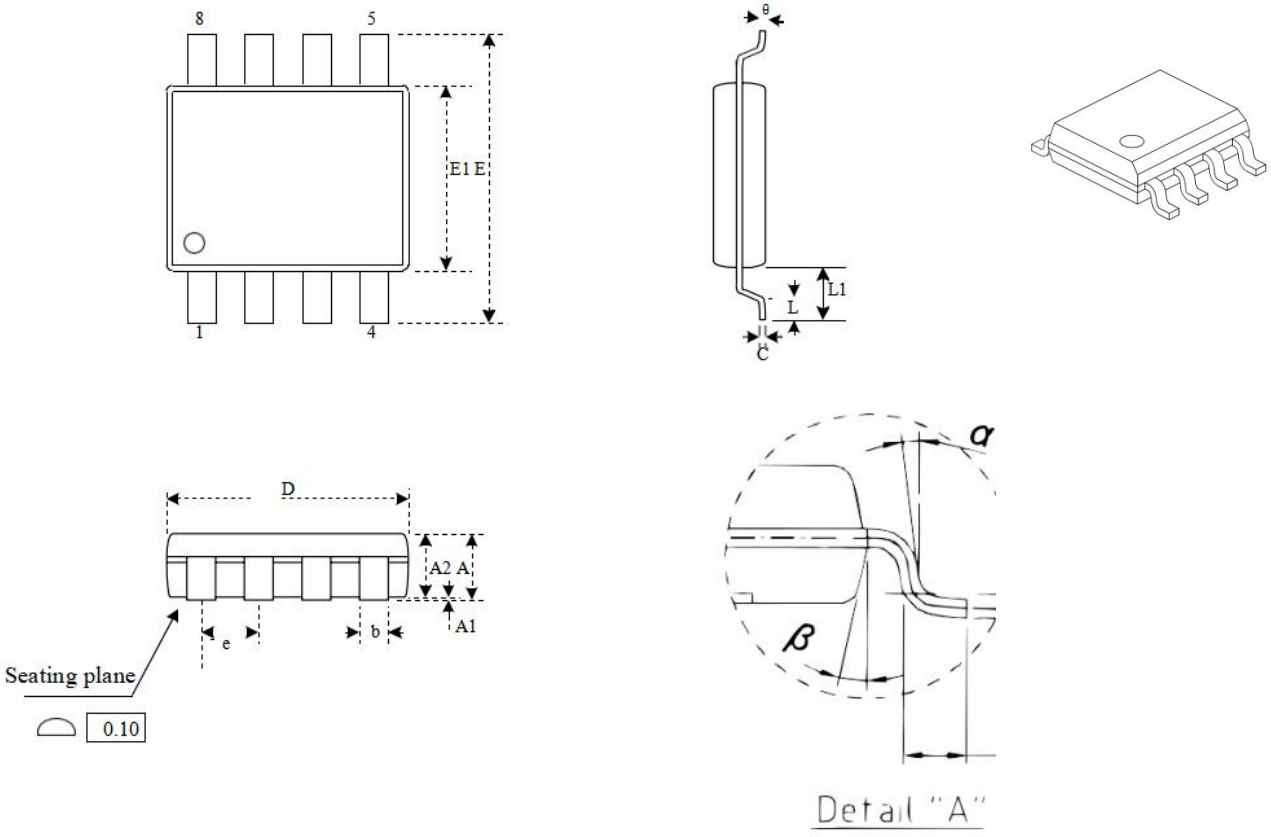
Table 3-2 DC Parameters on All I/O Interfaces

参数	条件	VCC	Min	Type	Max	单位
VIH	Input high voltage, all standard inputs and bidirectional ports	3.3V	2.0	-	-	V
		1.8V	1.2	-	-	V
VIL	Input low voltage, all standard inputs and bidirectional ports	3.3V	-	-	0.8	V
		1.8V	-	-	0.6	V
VOH	All standard inputs and bidirectional ports	3.3V	VCC-0.4	-	-	V
		1.8V	VCC-0.4	-	-	V
VOL	Output low voltage, all standard inputs and two-way ports	3.3V	-	-	0.4	V
		1.8V	-	-	0.4	V
IIL	IO pad force -0.2V @VDDIO=3.6V，IIL= -120~-70uA					
IIH	IO pad force 3.8V @VDDIO=3.6V， IIH = 8uA~16uA					
Icc	Waiting for I/O during I/O transfers or execution of non-ECC/SM2 commands. Independent of Clock Divider value.	3.3V	-	1.6	-	mA

4. Package Drawings

4.1 SOP8

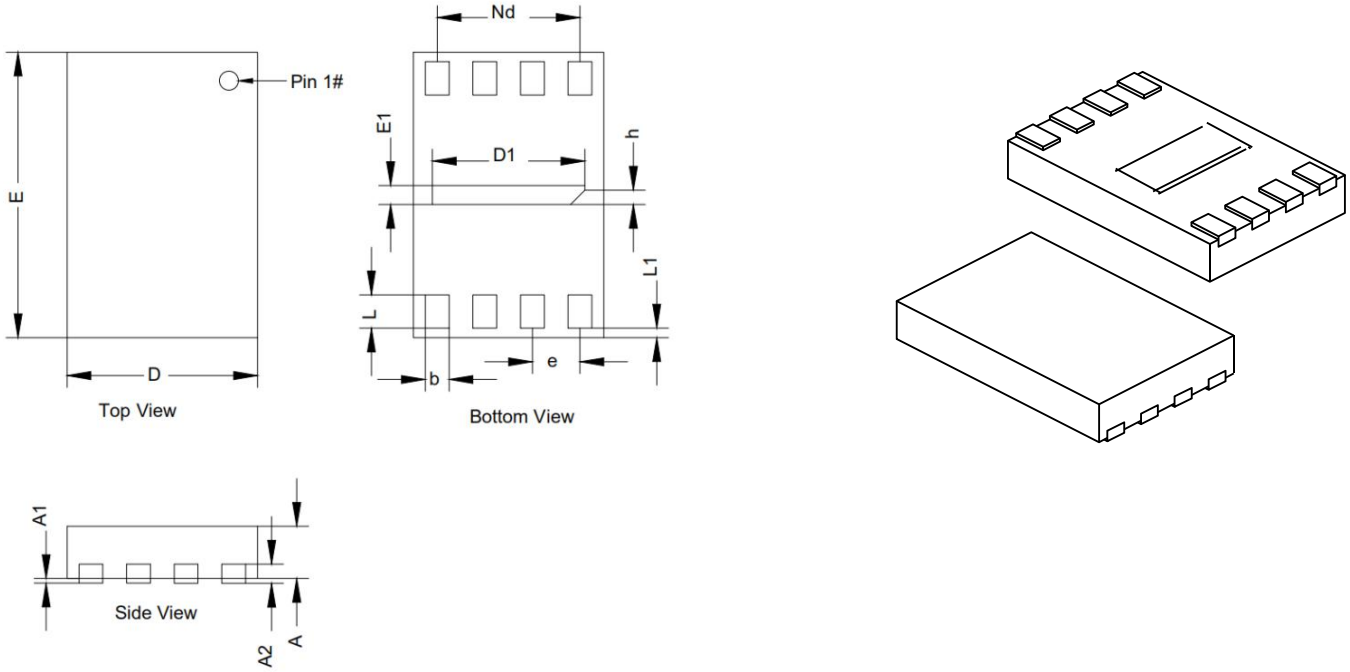
Narrow, 3.90 mm (.150 In.) Body [SOP8]



COMMON DIMENSIONS (UNITS OF MEASURE=MILLIMETERS)															
Symbol / **Unit**		**A**	**A1**	**A2**	**b**	**C**	**D**	**E**	**E1**	**e**	**L**	**L1**	**θ**	**α**	**β**
mm	**Min**	1.35	0.05	1.35	0.31	0.15	4.77	5.80	-	-	0.40	0.85	0°	6°	11°
	Nom	-	-	-	-	-	4.90	6.00	3.90	1.27	-	1.06	-	7°	12°
	Max	1.75	0.25	1.55	0.51	0.25	5.03	6.20	-	-	0.90	1.27	8°	8°	13°
Inch	**Min**	0.053	0.002	0.053	0.012	0.006	0.188	0.228	-	-	0.016	0.033	0°	6°	11°
	Nom	-	-	-	0.016	-	0.193	0.236	0.154	0.050	-	0.042	-	7°	12°
	Max	0.069	0.010	0.061	0.020	0.010	0.198	0.244	-	-	0.035	0.050	8°	8°	13°

4.2 DFN8

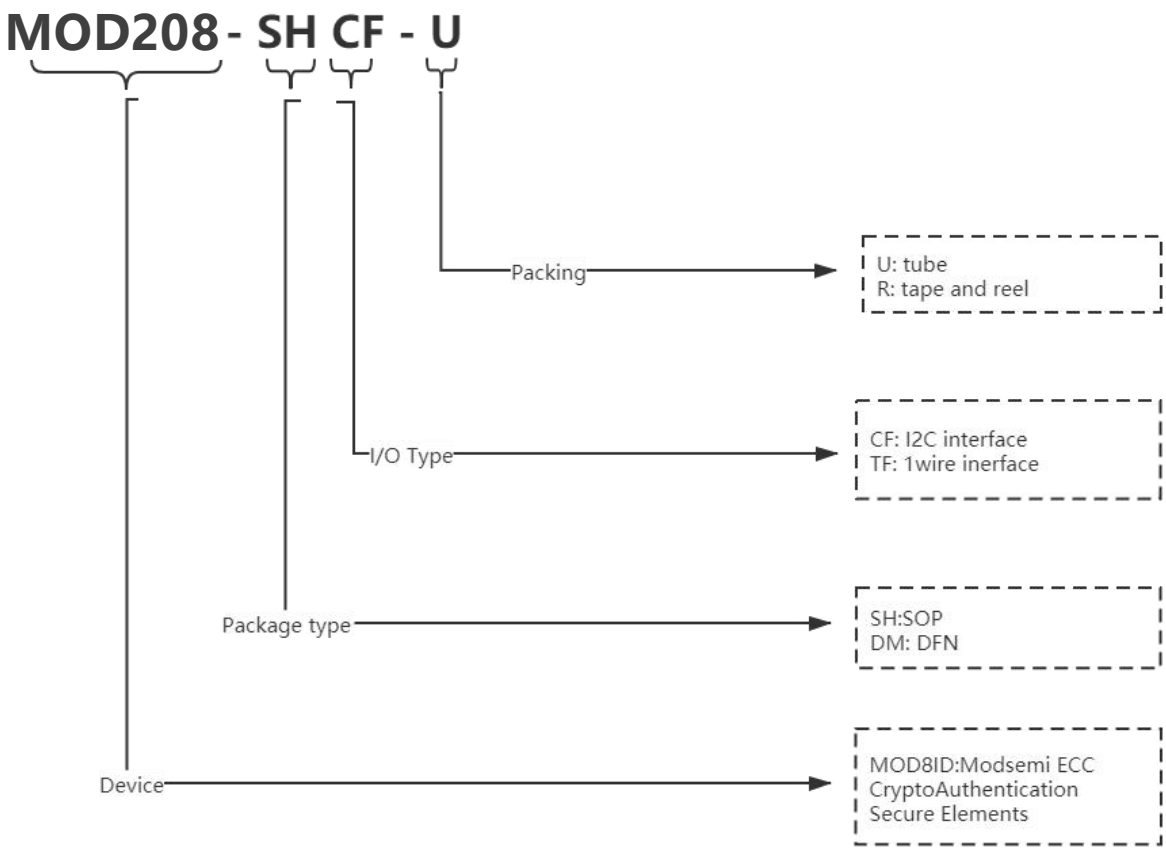
2x3mm body [DFN8]



COMMON DIMENSIONS (UNITS OF MEASURE=MILLIMETERS)			
SYMBOL	MILLMETERS		
	MIN	NOM	MAX
A	0.50	0.55	0.60
A1	0.00	0.02	0.05
A2	0.152REF		
b	0.20	0.25	0.30
D	1.95	2.00	2.05
E	2.95	3.00	3.05
D1	1.50	1.60	1.70
E1	0.10	0.20	0.30
e	0.50BSC		
Nd	1.50BSC		
L	0.30	0.35	0.40
L1	0.05	0.10	0.15
h	0.10	0.15	0.20

5. Part numbering

To order or obtain information, e.g., on pricing or delivery, refer to the factory or the listed sales office.



Examples:

- **MOD208-SHCF-U**: SOP8 (0.150” Wide Body), I^2C, Tube
- **MOD208-DMCF-R**: DFN(2 x 3 x 0.6 mm Body), I^2C, Type and Reel

Trademarks

All referenced product or service

names and trademarks are the property of their respective owners.

Edition 2020-07-24 Published by

Document reference IMPORTANT NOTICE

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics .With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Modsemi hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.In addition, any information given in this document is subject to customer's compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer’s products and any use of the product of Modsemi in customer's applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer’s technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application

For further information on the product, technology delivery terms and conditions and prices please contact your nearest Modsemi office (www.modsemi.com).

WARNINGS

Due to technical requirements products may contain dangerous substances. For information on the type in question please contact your nearest Modsemi office.

Except as otherwise explicitly approved by Modsemi in a written document signed b authorized representatives of Modsemi, Modsemi’s products may not be used in any applications where a failure of the product or any consequences of the use thereof can reareasonably be expected to result in personal injury.