Modsemi ECC CryptoAuthentication Secure Elements

Revision history

Document version	Date of release	Description of changes
1.37	2023-08-05	Add instructions for providing VCC power supply through GPIO.
1.34	2022-06-05	
1.33	2022-05-05	
1.32	2022-03-05	Add Part numbering
1.31	2022-02-01	
1.30	2021-09-01	
1.00	2019-05-01	Initial Version
0.51	2017-03-19	Draft Version
0.50	2017-03-05	Initial Version (Internal release)

MOD8ID

Modsemi ECC CryptoAuthentication Secure Elements

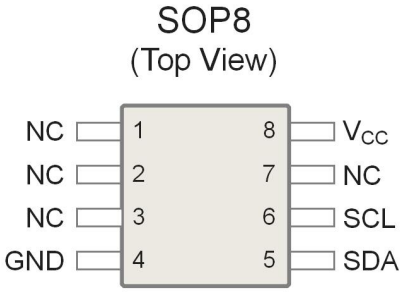
Key features

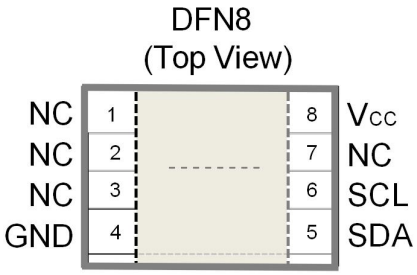
- Security co-processor with cryptographic algorithm and key storage
  - > High-end security controller
  - > Protected Storage for Keys, Certificates or Data
- Hardware Support for Asymmetric Sign,Verify,authentication,Key Agreement:
  - > Hardware cryptographic algorithm processor: SM2, ECC-P256, SHA-256, TRNG
  - > ECDSA: Elliptic Curve Digital Signature
  - > ECDH: Elliptic Curve Diffie-Hellman
  - > SM2: Diffie-Hellman Ephemeral (ECDHE) over the SM2 elliptic curve
- Hardware Support for Symmetric Algorithms:
  - > SHA-256 & HMAC
  - > SM4: Block-cipher symmetric algorithm Encrypt/Decrypt
  - > AES-128/256: Encrypt/Decrypt,AES-GCM/ECB/CBC
- Networking Key Management Support:
  - > security key generation and key agreement
  - > Communication data encryption with protected
  - > Turnkey PRF/HKDF calculation for TLS
- Security update and firmware Support:
  - > High security ECDSA firmware signature validation
  - > Full life cycle secure boot validation
  - > Firmware upgrade protection and data encryption protection
- Internal High-Quality NIST Standard Random Number Generator(RNG)
- Up to 5kB of user security storage to store extended security information
- Unique Serial Number
- High-Endurance Monotonic Counters
- Interface Options Available400k/1 MHz Standard I2C Interface
- Fast and easy integration
- DFN8 and SOP8 Packages

Benefits

- IoT network endpoint key management & exchange/IoT Node Crypto-Protection
- Encryption protection and key protection of IoT nodes
- Protect the authenticity, integrity and confidentiality of your products, data and intellectual property
- Secure communication and communication data encryption
- Data storage protection
- Lifecycle management
- Platform integrity protection
- Security update and firmware protection
- Electronic accessories protection

Description of PIN





Pin	Function
GND	Ground
SDA	Serial Data
SCL	Serial Clock Input
V_{CC}	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 MOD8ID is a high-security authenticator that provides a core set of cryptographic accelerators derived from integrated asymmetric (ECC-P256/SM2) and symmetric (SHA-256/AES/SM4) 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,a decrement-only counter,The MOD8ID combine key storage with advanced hardware cryptographic accelerators to implement various authentication applications.

1.2 Features

The MOD8ID based on an advanced security controller with built-in tamper proof NVM for secure storage and Symmetric/Asymmetric crypto engines to support SM2, SM4,ECC 256 and AES/SHA-256. The MOD8ID includes an security NVM which can be used for storage keys, certificates and private data，security read/write, read-only or secret data, consumption logging, and security configurations.This new security technology greatly enhances your overall system security.

MOD8ID has an I2C interface that supports secure communication, which can easily and fast integrate with host micro-controller software.

MOD8ID covers a broad range of use cases necessary for many types of security applications that include the following:：

- IoT node/edge computing node equipment
- Smart home
- Electronic Accessories
- Mobile devices
- Webcam
- smart Lock

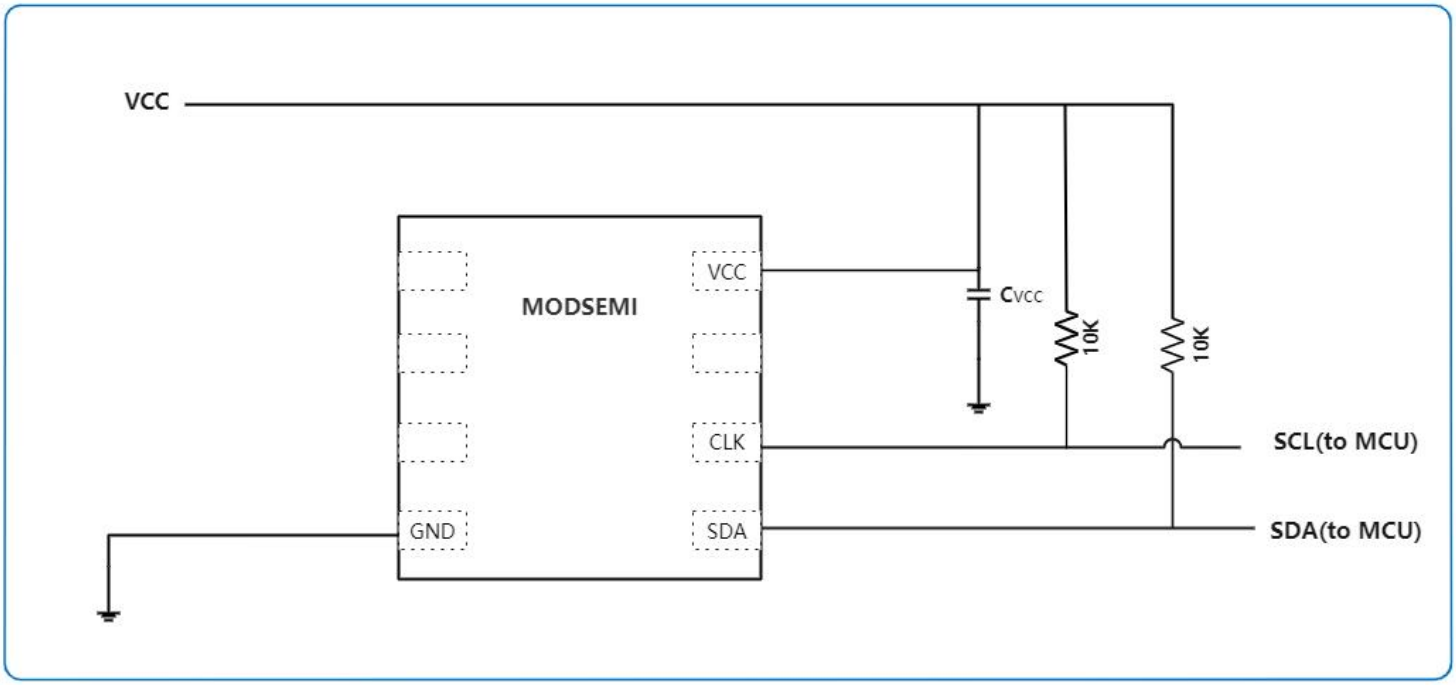
2. Interface and Schematics

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 MOD8ID with your local host.

Figure 2 -1 System Integration Schematic Diagram

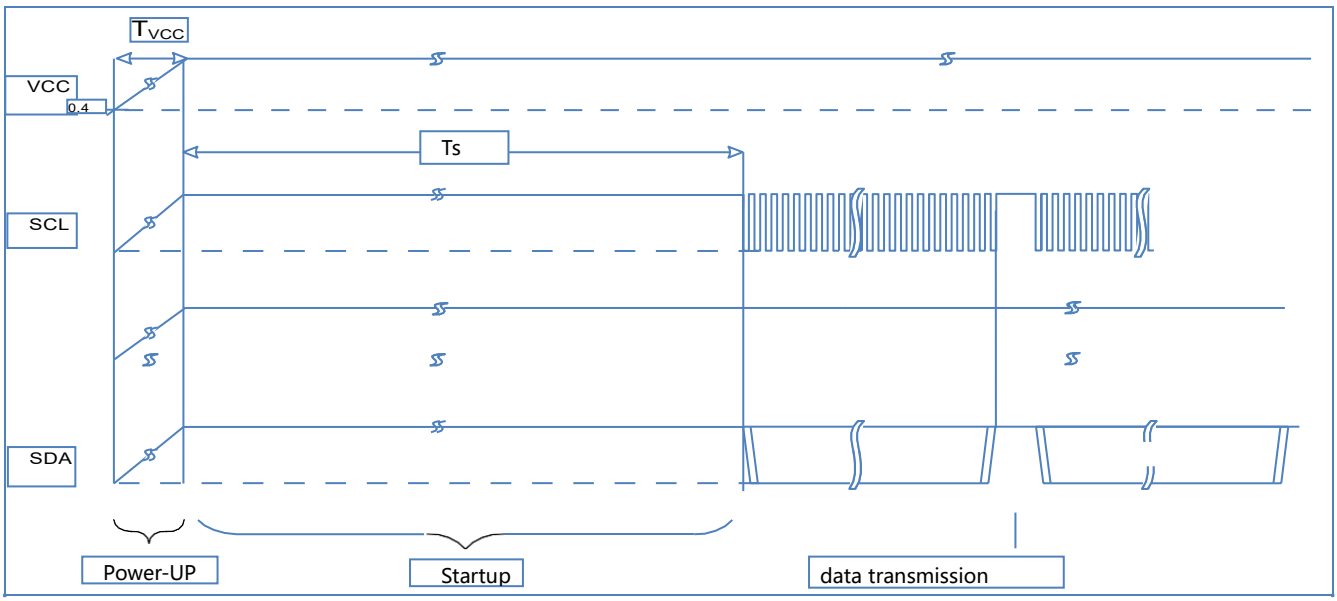


NOTE 1: Value of the pull up resistors and Cvcc depend on the target application circuit and the targeted I2C frequency.

NOTE 2 : As stated in the NOTE of Section 2.2 on interface timing in, it is recommended that the MOD8ID can be powered via VCC through the GPIO on the master control side.

2.2 interface timing

The following figure shows the startup timing of the I2C interface for this case



Interface timing

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min	TYPE	MAX		
Startup time	Ts	25			mS	Power up to the first command execution time
VCC power-up time	Tvcc	0.1		1	mS	power-up time

NOTE：If the VCC power-up time cannot meet this criterion during integration, please supply power to the MOD8ID's VCC via the GPIO on the MCU side, which allows for flexible control of the power supply timing and power on/off.

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	3.5	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 MOD8ID is fabricated with high reliability NVM manufacturing technology.

Table 3-1. NVM 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

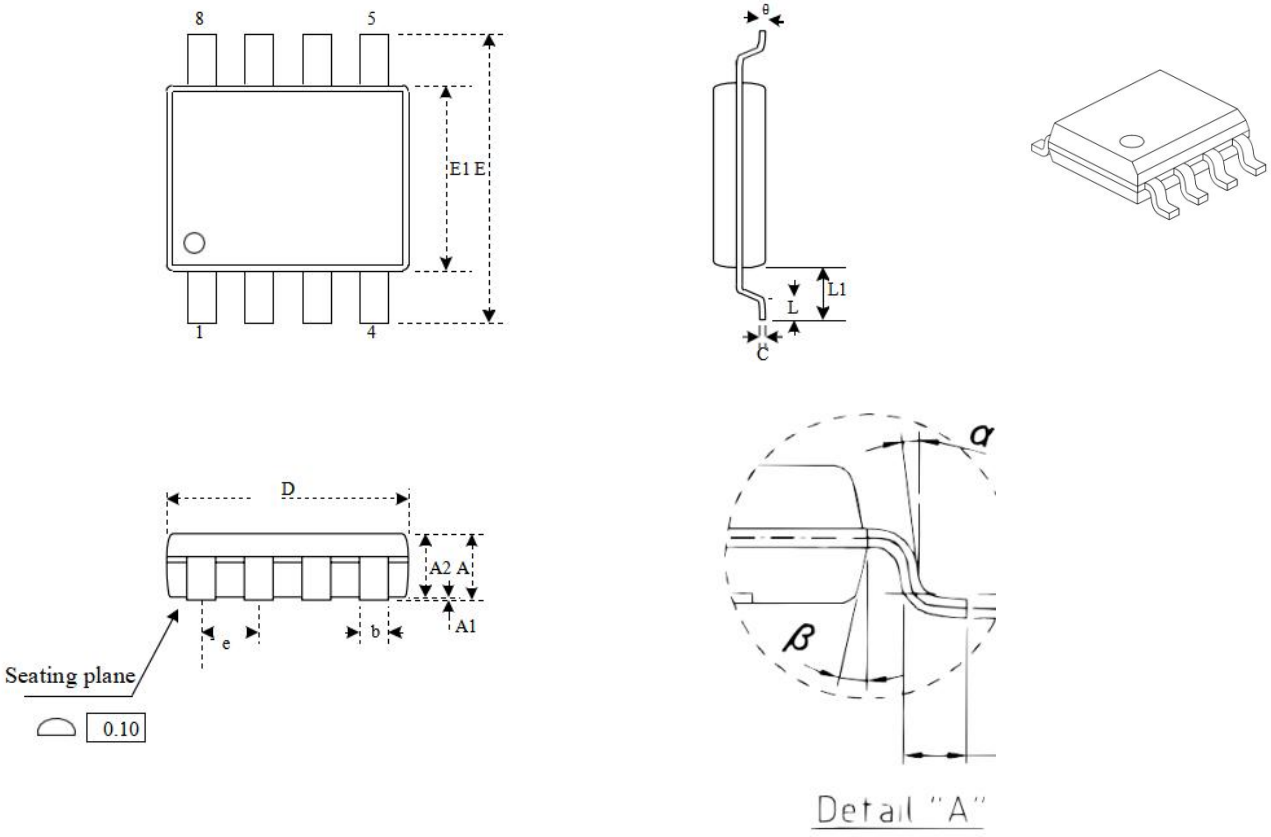
Parameter	Condition	VCC	Min	Type	Max	Units
VIH	Input high voltage, all standard inputs and bidirectional ports	3.3V	2.0	-	-	V
		1.8V	1.2	-	-	V
VIL	Input low voltage, all standard inputs and bidirectional ports	3.3V	-	-	0.8	V
		1.8V	-	-	0.6	V
VOH	All standard inputs and bidirectional ports	3.3V	VCC-0.4	-	-	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

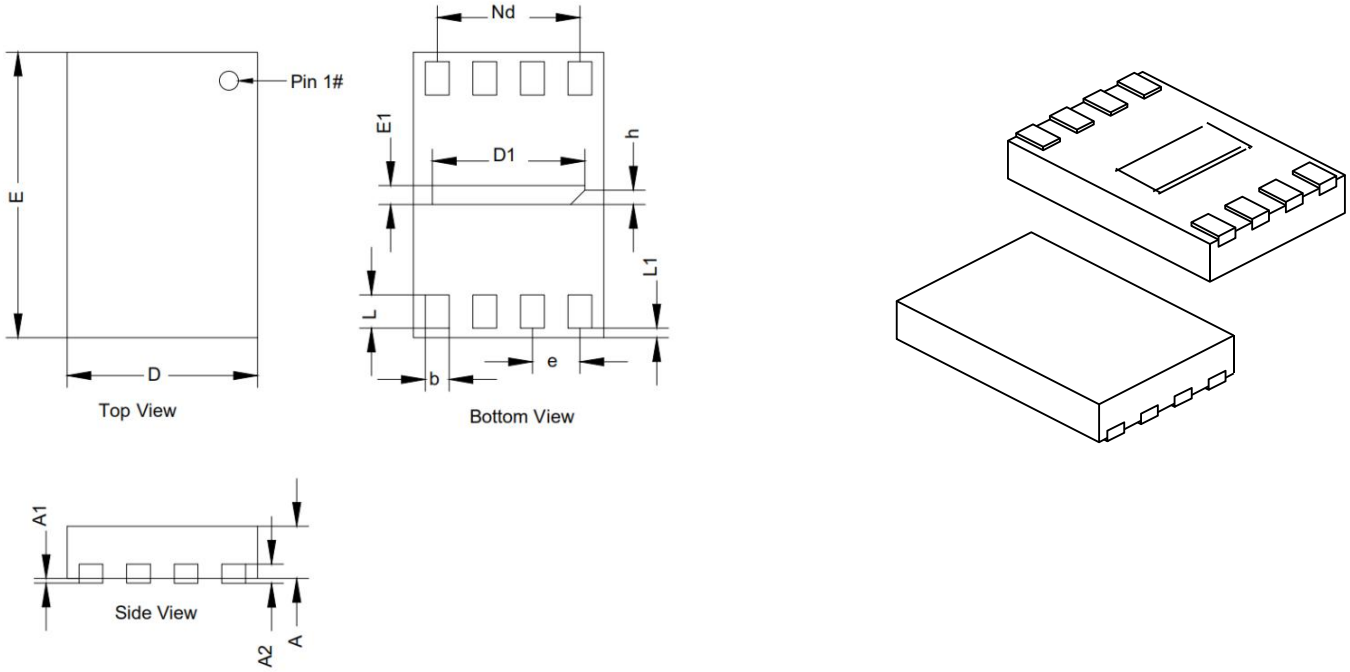
Narrow, 3.90 mm (.150 In.) Body [SOP8]



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

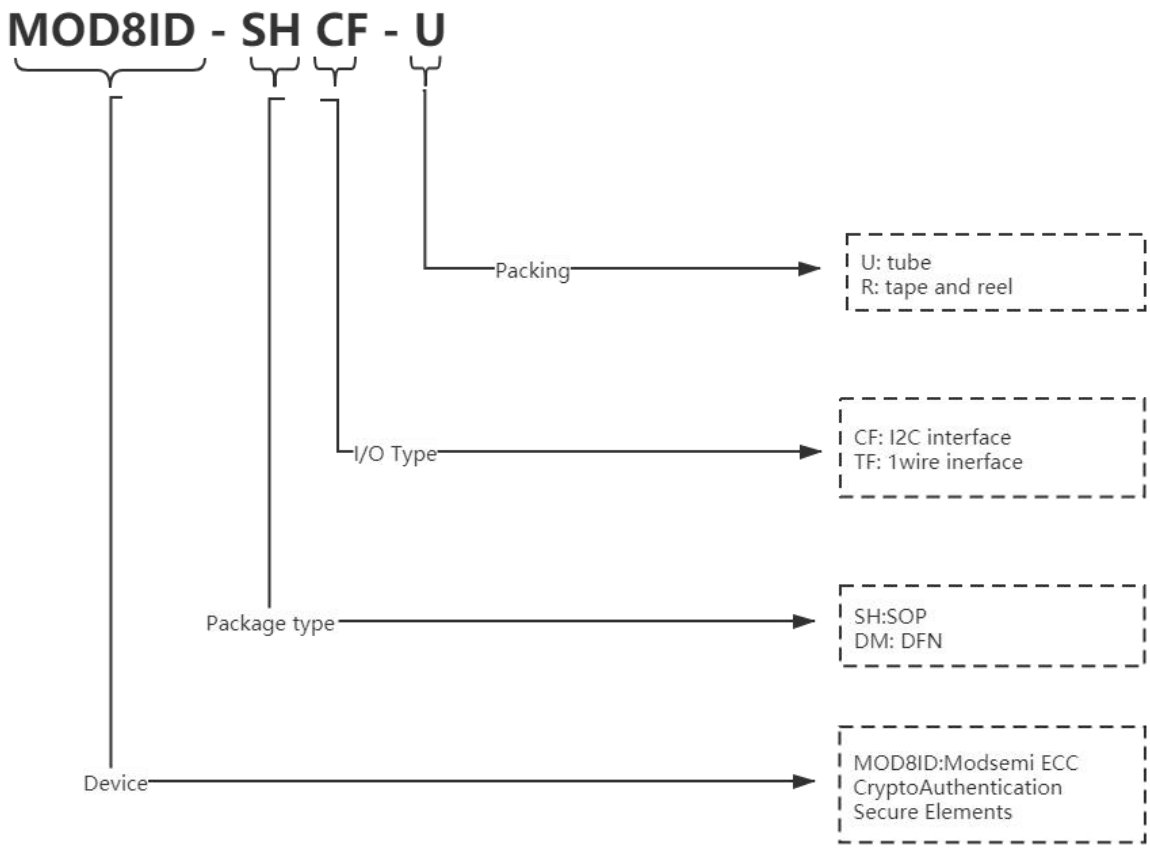
2x3mm body [DFN8]



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:

- **MOD8ID-SHCF-U**: SOP8 (0.150” Wide Body), I^2C, Tube
- **MOD8ID-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.