



2k bit Memory Secure ISO/IEC 15693 Standard Compliant Device

General Description

The EM4237 is a long range passive contactless tag IC intended for applications requiring strong levels of security and data privacy.

The EM4237 provides a 2k bit EEPROM memory offering high levels of flexibility in terms of memory management and secure access conditions.

The memory access conditions can be protected either by a 32-bit password or by a three pass mutual authentication. The level of security is selectable and can be tailored to the requirements of the end-user application.

The 4-bytes password can be used to personalize the tag IC in a secure environment and then the same tag can be secured in the application field with the Grain 128A crypto.

The Mutual authentication process is based on Grain 128A, a low power and fast stream cipher full fitting the existing and coming NFC and RFID application trends.

In order to enforce the chip security, the EM4237 offers a mechanism called secure messaging. In that operating mode, all the communication exchanges between the EM4237 and the RFID reader are encrypted.

Optional 4-bytes Message Authentication Code (MAC) can be added to all the communication transfers in order to protect the data integrity between the tag and the reader.

All these strong security mechanisms are commonly used today in a multitude of secure applications using ISO/IEC14443 technology.

The enhanced on-chip security features allow a flexible administration of the memory access rights enabling the device as a right solution for advanced theft protection.

One or several memory blocks can be separately read/write protected and/or even locked.

The IC customer privacy is guaranteed by all the chip security mechanisms. In a privacy operating mode, the EM4237 either remains silent to the reader requests or returns a random serial ID number which is then used for all the transactions between the EM4237 and the RFID interrogator.

Each EM4237 chip has a 64-bit unique serial number programmed at wafer level.

An optional 32-bytes signature based on standard Elliptic Curve Cryptography is generated using the device ID number, a public and private set of keys. The signature attests, with a good level of confidence, the authenticity of the EM4237 device.

This ECC based signature can be retrieved by sending a read_Sig ISO/IEC15693-3 custom command.

The verification can be done by using the corresponding ECC public key provided by EM Microelectronic Marin SA.

Features

- | ISO/IEC 15693 & ISO/IEC18000-3 standard compliant
- | Long range, low power vicinity transponder IC
- | 64-bit ISO/IEC 15693 Unique Identifier (UID)
- | 2112 bit user's data Memory - 66 blocks of 32 bit
- | Optional 32-byte ECC based signature
- | Chip Security based on Grain128A crypto algorithm
- | Security features used for:
 - Mutual Authentication based on challenge/response
 - Secure Messaging – encryption of the RF communication channel
 - Message Authentication Code (MAC)
- | Possibility to select security level based on a 32-bit password
- | Optional Random ID for enhanced security and privacy
- | Secure Customer Privacy feature
- | 60 years memory data retention
- | Data Storage Format Identifier (DSFID)
- | Application Field Identifier (AFI) supported
- | EEPROM blocks/pages Locking mechanisms
- | Destroy function to deactivate the chip forever
- | Support all mandatory and most of optional ISO/IEC 15693-3 commands and a complete set of custom commands
- | Fast double speed read multiple block command to speed up reader to tag transactions
- | On-chip resonant capacitor: 23.5pF
- | -40 °C to +85 °C temperature range
- | Bonding pads optimized for flip-chip assembly
- | Wafer delivery: 8 inch wafer, 75um thickness
- | Package delivery: 2 leads thinner DFN403

Applications

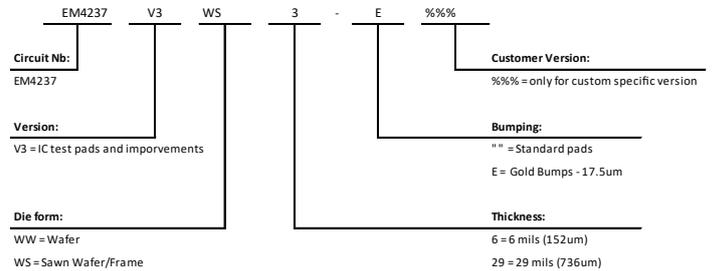
- | Product Authentication
- | Pharmaceuticals
- | Jewellery and luxury goods
- | Cards and secure documents
- | Healthcare
- | Bluetooth or WIFI Pairing
- | Ticketing
- | Asset tagging
- | Tax stamps
- | Supply Chain Management



Ordering Information

For wafer from delivery, please refer to EM4237 wafer specification document.

DIE FORM:

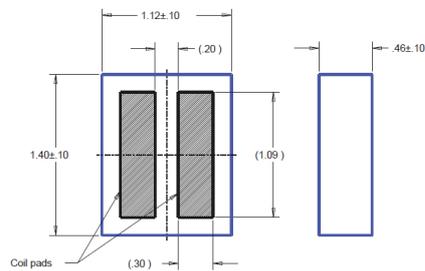


EMDFN403 PACKAGE:

2 leads Plastic extremely thin small outline package; body 1.1 x 1.4 x 0.46 mm: EMDFN403

All dimensions in inches [mm].

Packing method : Loose form (Aluminum canisters)

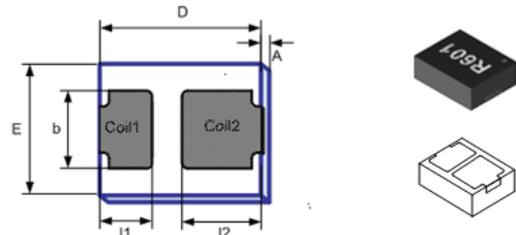


EMDFN-02 PACKAGE:

	A	D	E	B	I1	I2
Size	0.76	2.20	1.78	1.07	0.71	1.08
Tolerance	0.10	0.15	0.15	0.05	0.05	0.05

All dimensions in mm.

Packing method : Loose form (Aluminum canisters)



Standard Versions

The versions below are considered standards and should be readily available. For the other delivery form, please contact EM Microelectronic-Marín S.A. Please make sure to give the complete part number when ordering.

Part Number	Package / Die Form	Delivery form / Bumping	Comments
EM4237V3WS6E	Sawn wafer, 6 mils thickness	Gold bump	---
EM4237V3WW29	Un-Sawn wafer, 29 mils thickness	Standard aluminium pads	---