NFC TYPE 2 AUTHENTICITY TAG IC

DESCRIPTION

em|linq is part of the latest generation of EM Microelectronic NFC devices and represents the most optimized hardware solution for product authentication applications in the market. **em|linq** is compliant with NFC Forum Type 2 and ISO 14443-A standards.

Target applications and market segments include consumer engagement and brand protection in retail, industrial, automotive and other B2C applications.

em|linq comes with 3 main security elements: a unique identifier (UID), a security token and a cryptographic signature, enabling the generation of a secure dynamic URL for web authentication with message substitution.

The **em|linq** supports the NFC Forum Tag Type-2 standard with data rate at 106kbps. The memory offers R/W user's memory structured by segments and memory pages. The memory contains the NFC capability container, the NDEF message and other proprietary data.

The NDEF message can be composed of preprogramed URL and IC automatically inserts UID value and token and secures it with the crypto signature generated using a 256-bit cryptographic key.

The **em|linq** offers two levels of security:

- In high level mode the Secure mode is protected by Authentication with a 256-bit key.

- In low level mode the Secure mode is protected by a 4-byte password.

Each **em|linq** chip is delivered with a unique 7-byte unique ID number programmed at wafer level.

NFC Forum and the NFC Forum logo are trademarks of the Near Field Communication Forum

FEATURES

- NFC Forum Type 2 compatible
- Communication baud rates at 106kbps
- 7-byte unique ID number
- Automatic append of UID, token and crypto signature into the NDEF URL.
- New and unique URL generated at each tap.

NFC INTERFACE

- NFC Forum Type 2 Tag compliant
- Communication baud rates at 106kbps
- 7-byte unique ID number
- 50pF resonance capacitor

MEMORY

- EEPROM size of 308 Bytes
- Minimum 100k write cycles endurance
- Minimum 10 years data retention
- Anti-tearing features
- RD/WR protection mechanism

SECURITY

- Crypto Signature / One Time Password (HOTP)
  - Keyed-hash Message Authentication Code SHA-1
  - Calculated from random forward value and UID
- 256-bit secret key
- Secure mode
  - Protecting defined part of memory against write
  - Login with password 32b
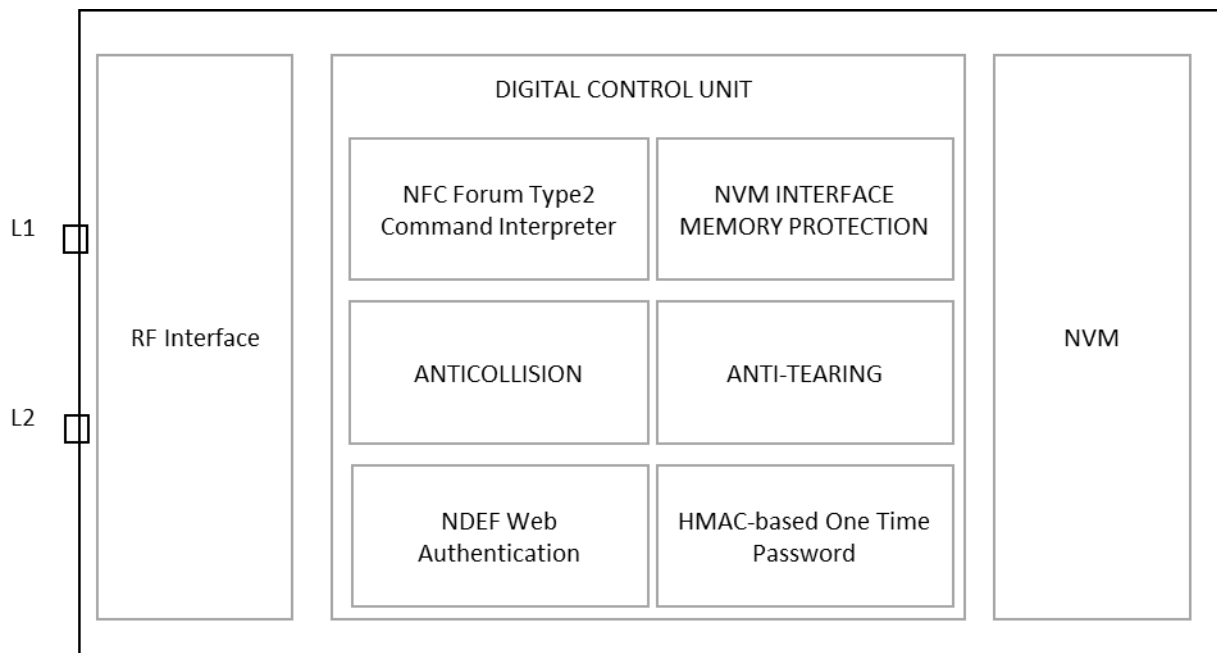 - Login with HMAC
- Secure product life cycle management.

APPLICATIONS

- Product authentication
- Customer engagement, coupon, loyalty programs
- Proof of presence

1. TYPICAL OPERATING CONDITIONS
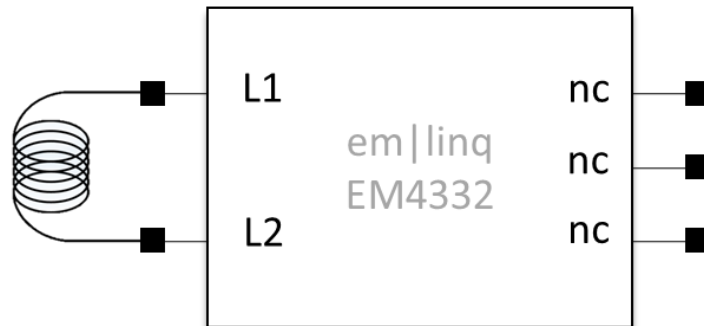
2. BLOCK DIAGRAM

3. ELECTRICAL SPECIFICATIONS

3.1. ABSOLUTE MAXIMUM RATINGS

Parameters	Symbol	Min	Max	Unit
Storage temperature	T_{STORE}	-50	125	°C
Maximum magnetic field strength with PICC 1 antenna (rms)	$H_{MAX\_MAG\_PICC1}$		12	A/m
Maximum magnetic field strength with PICC 6 antenna (rms)**Error! Bookmark not defined.**	$H_{MAX\_MAG\_PICC6}$		28.8	A/m
ESD hardness pad HF+ and HF -[1]	V_{ESD}	-2000	2000	V

Stresses above these listed maximum ratings may cause permanent damages to the device. Exposure beyond specified operating conditions may affect device reliability or cause malfunction.

---

[1] Human Body Model, between HF+, HF- pins and HF+ resp. HF- pins against VSS

3.2. HANDLING PROCEDURES

This device has built-in protection against high static voltages or electric fields; however, anti-static precautions must be taken as for any other CMOS component. Unless otherwise specified, proper operation can only occur when all terminal voltages are kept within the voltage range. Unused inputs must always be tied to a defined logic voltage level.

3.3. OPERATING CONDITIONS

Parameters	Symbol	Min	Max	Unit
Operating Temperature	T_{OP}	-40	+85	°C
Maximum operating field strength with PICC 1 antenna (rms)	H_{MAX_PICC1}		7.5	A/m
Maximum operating field strength with PICC 6 antenna (rms)	H_{MAX_PICC6}		18	A/m

Table 1 Operating Conditions

3.4. ELECTRICAL CHARACTERISTICS

CONDITIONS (UNLESS OTHERWISE SPECIFIED): TOP=25°C

Parameter	Symbol	Conditions	Min	Typ	Max	Unit
Resonance Capacitor	C_{RES}	fc = 13.56MHz U = 2Vrms	47.5	50	52.5	pF
Erase / write endurance	T_{CYC}		100k			Cycles
Retention	T_{RET}	T_{OP} = 55ºC	10			Years
Minimum Activation field		ISO10373-6 Class 6 antenna, Fres = 13.7MHz@100mV	0.3			A/m

Table 2 Electrical Specifications

3.5. TIMING CHARACTERISTICS

The time between the end of the last pause transmitted by reader and the first modulation edge within the start bit transmitted by IC is defined as follows for data rate fc/128:

Last reader bit = (1)b

$$(N \times 128 + 84) / fc \ [ms]$$

Last reader bit = (0)b

$$(N \times 128 + 20) / fc \ [ms]$$

Symbol	Minimum time [N]	Maximum time [N]	Maximum time [ms]
GT_A			5
T_{NACK}	9	9	
T_{READ}	9	≥ 9	4.75
T_{WRITE}	9	≥ 9	9.5
TSECTOR_SELECT	9	9	
$T_{READ\_MULTIPLE\_BLOCKS}$	9	≥ 9	4.75
$T_{READ\_INCREMENTAL}$	9	≥ 9	4.75
T_{LOGIN}	9	≥ 9	4.75
T_{AUTH}	9	≥ 9	4.75

Table 3 Timings

Note: The NFC memory write operation timing can differ depending on the current content and data being written, it means that IC can reply in different timeslots.

4. PRODUCT OVERVIEW

em|linq is used in passive transponder applications and provides support for use as an HF product or as a NFC product.

Main features :

- Crypto Signature (HMAC-SHA-1 based One-Time Password (HOTP) algorithm)
- Token: Increment token value with random step. Value is presetable and lockable.
- Security Level (Password or Mutual Authentication)

4.1. OVERVIEW (HF)

em|linq corresponds to ISO 14443 offering innovative and enriched features.

em|linq supports data rates at 106kps.

em|linq offers the maximum of flexibility in terms of security using password protection or mutual authentication based on SHA-1 cryptographic hash function.

Each em|linq chip is delivered with a unique 64-bit inalterable UID number programmed at wafer level to ensure full traceability.
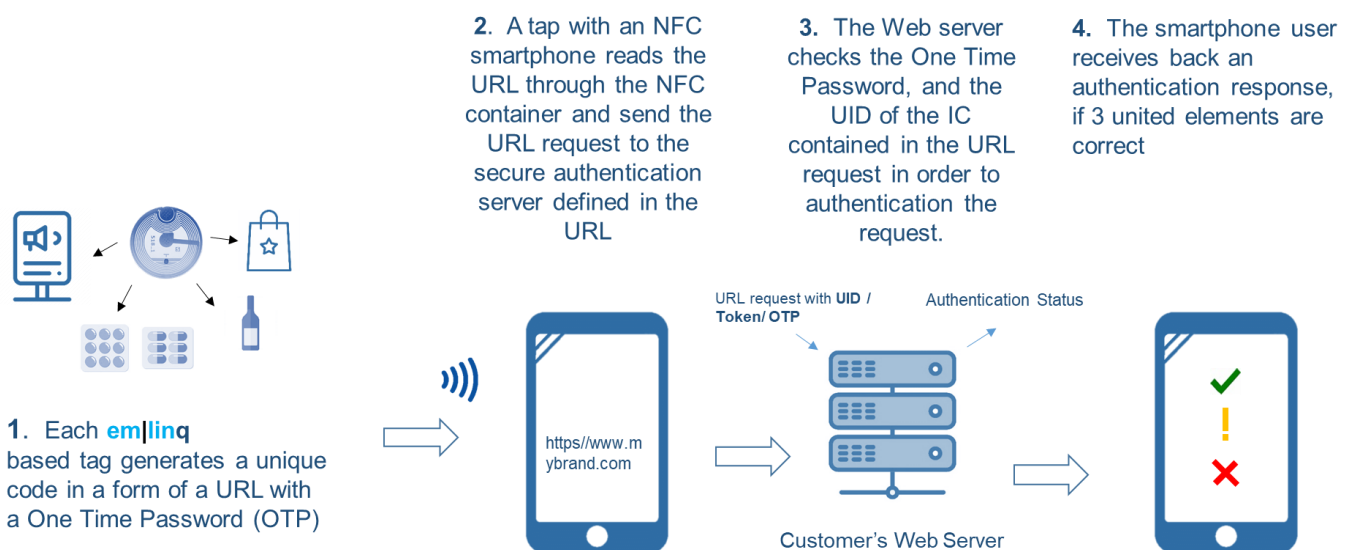
4.2. OVERVIEW (NFC)

em|linq corresponds to NFC Forum Type 2 devices offering innovative and enriched features.

em|linq supports data rates at 106kps.

em|linq memory contains the NFC Capability Container, the NDEF message, and other proprietary data.

The user has the option to enable the use of the token and web based OTP crypto authentication.
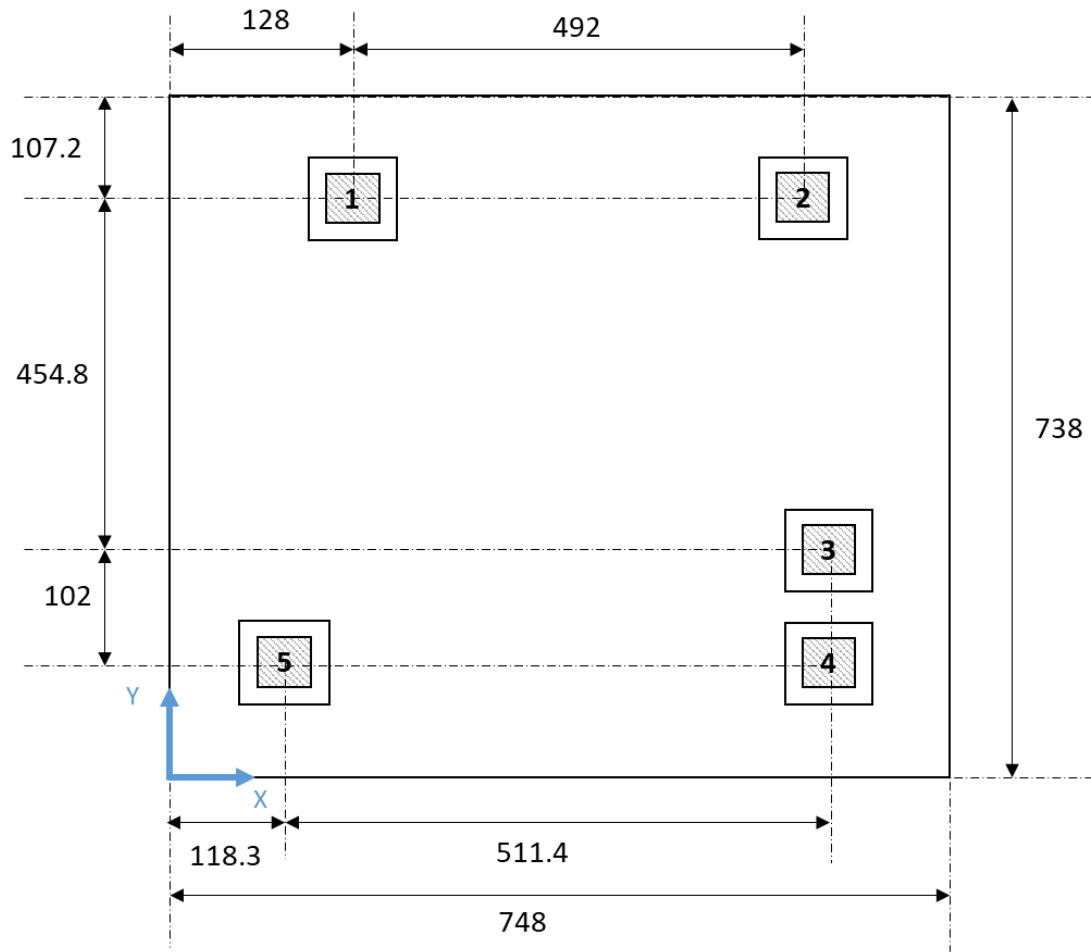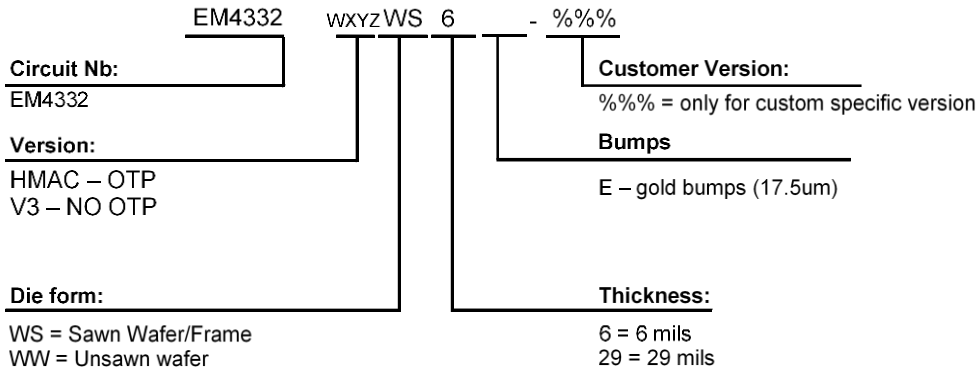
4.3. TYPICAL APPLICATION CASE

2. A tap with an NFC smartphone reads the URL through the NFC container and send the URL request to the secure authentication server defined in the URL

3. The Web server checks the One Time Password, and the UID of the IC contained in the URL request in order to authentication the request.

4. The smartphone user receives back an authentication response, if 3 united elements are correct

URL request with **UID / Token/ OTP**

Authentication Status

https//www.mybrand.com

Customer's Web Server

1. Each em|linq based tag generates a unique code in a form of a URL with a One Time Password (OTP)

5. PAD LOCATION DIAGRAM

Figure 1 Bump position

Pin number	Pin name	Description
1	L1	Coil antenna input
2	L2	Coil antenna input
3	T1	Test purpose pad – functionally disconnected during sawing. It can be connected to any pad including coils
4	T2	Test purpose pad – functionally disconnected during sawing. It can be connected to any pad including coils
5	T3	Test purpose pad – functionally disconnected during sawing. It can be connected to any pad including coils

Table 4 Bump list

6. ORDERING INFORMATION

```
        EM4332    WXYZ WS  6      -  %%%
```

Circuit Nb:
EM4332

Version:
HMAC – OTP
V3 – NO OTP

Die form:
WS = Sawn Wafer/Frame
WW = Unsawn wafer

Customer Version:
%%% = only for custom specific version

Bumps
E – gold bumps (17.5um)

Thickness:
6 = 6 mils
29 = 29 mils

Part Nb	Delivery Form
EM4332HMACWS6E	8 inch, 6 mils thickness, sawn wafer with gold bumps HOTP function activated.
EM4332V3WS6E	8 inch, 6 mils thickness, sawn wafer with gold bumps, no HOTP function.

Table 5 Ordering Information

For other delivery, formats please contact EM Microelectronics representative.

7. PRODUCT SUPPORT

Check our website at www.emmicroelectronic.com under Products/RF Identification section. Questions can be submitted to rfidsupport@emmicroelectronic.com .