# SL2S3003/SL2S3003TT

## ICODE 3 (TagTamper)

**Rev. 3.0 — 28 March 2024** **Product data sheet**

## 1 General description

ICODE 3 is the next generation of the ICODE product family of 13.56 MHz based vicinity label ICs. ICODE 3 overcomes some known challenges in RFID solution design and industrialization process. ICODE 3 combines native NFC features with the increased read range of ISO/IEC 15693-based tags. SL2S3003TT is the ICODE 3 version with TagTamper feature, and SL2S3003 is the version without TagTamper.

Fully backward-compatible with SLIX 2, the ICODE 3 supports improved performance and new features:

- SELFAdjust
- Fast read with up to 212 kbit/s
- Configurable 24-bit counter
- ASCII mirror feature option
- One-shot read-only memory lock
- Extra configuration memory with optional password protection
- Programmable originality signature with 32 bytes or 48 bytes
- 2.4 kbit user memory size
- Flexible user memory segmentation with separate access conditions
- TagTamper feature with current and stored status (only SL2S3003TT)

## 1.1 Contactless energy and data transfer

The ICODE 3 can be operated at a distance of up to 1.5 m (gate width). No battery is needed.

The device is operated with easy-to-produce types of antennas[1] for the 13.56 MHz carrier frequency.

When the smart label is positioned in the field of an interrogator antenna, the high-speed RF communication interface enables data transmission at up to 212 kbit/s.

## 1.2 Anticollision

The anti-collision algorithm selects each tag individually. This ensures that the execution of a transaction with a selected tag is performed without data corruption from other tags in the field.

## 1.3 Data protection

- Unique IDentifier (UID):
  The UID guarantees the uniqueness of each label, and cannot be altered.
- Tag originality signature:
  32-byte or 48-byte ECC-based originality signature.
- Password protected memory management (Read/Write access):
  The user memory can be segmented into two pages. The read/write access rights can be defined for each page. Only authorized users get read/write access to the protected parts of the user memory (anti counterfeiting). READMULTIPLE BLOCK and (FAST) INVENTORY READ are compatible to ICODE SLIX 2.
- Password protected label Destroy:
  The 32-bit Destroy password enables an addressed label to be destroyed with the DESTROY command. The status is irreversible and the label never responds to any command again.
- Password-protected privacy modes:
  ICODE 3 supports two privacy modes to hide the original UID. A 32-bit password is used to enable or disable the privacy modes. This feature complies with the demand for data privacy.
- Password protected EAS and AFI functionality:
  The 32-bit EAS/AFI password enables the addressed label to be set in a mode where the EAS status, the EAS ID and/or the AFI value can only be changed if the correct EAS/AFI password is first transmitted with the SET PASSWORD command.
- 24-bit counter:
  The last block of the user memory is used for the 24-bit counter feature. The counter can be configured as a command-based counter or as a NFC counter. The NFC counter automatically increases by one when tapped with an NFC reader device.

1 For example, antennas made out of a few windings printed, winded, etched or punched coil.

# 2 Features and benefits

## 2.1 ICODE 3 RF interface (ISO/IEC 15693)

- SELFAdjust feature for optimal RF performance
  The ICODE 3 has an automatic mechanism implemented which adjusts the RF performance to the optimum in the operated environment. The adjustment is performed at start-up.
- Contactless transmission of data and power (no battery needed)
- Operating distance of up to 1.5 m (depending on the antenna geometry)
- Operating frequency of 13.56 MHz (ISM, worldwide license freely available)
- Fast data transfer of up to 212 kbit/s
- High data integrity: 16-bit CRC, framing
- True anticollision feature
- Persistent quiet mode to enable faster inventory speed
- Write distance equal to read distance

## 2.2 EEPROM

- 2432 bits of user memory organized in 76 blocks of 4 bytes each. The last block is reserved for the 24-bit counter feature.
- 50 years of data retention
- Write endurance of 100000 cycles

## 2.3 Data protection

- 8-byte unique identifier
- 32-byte or 48-byte programmable originality signature
- Lock mechanism for each user memory block (write protection), and lock protection pointer for fast locking
- Lock mechanism for DSFID, AFI, EAS
- Password (32-bit) protected memory management for Read access
- Password (32-bit) protected memory management for Write access
- Password (32-bit) protected label Destroy
- Password (32-bit) protected privacy mode
- Password (32-bit) protected EAS and AFI functionality
- Password (32-bit) protected memory configuration
- 24-bit counter (NFC counter, or command-based counter with optional password protection)
- Programmable open TagTamper message only visible after the detection of the first open event

# 3 Applications

- Product identification
- Product tracking and tracing
- Counterfeit and tamper protection
- Inventory management
- Smart-device consumable system communication
- Augmented mobile interaction

# 4 Ordering information

**Table 1. Ordering information**

| Part number | Package | | Version |
|---|---|---|---|
| | | Description | |
| SL2S3003FUD | Wafer | sawn, 12" bumped wafer, 120 µm, on film frame carrier, $C_i$ between LA and LB = 23.5 pF (typical) | - |
| SL2S3003TTFUD | Wafer | sawn, 12" bumped wafer, 120 µm, on film frame carrier, $C_i$ between LA and LB = 23.5 pF (typical), with TagTamper | - |

# 5 Block diagram

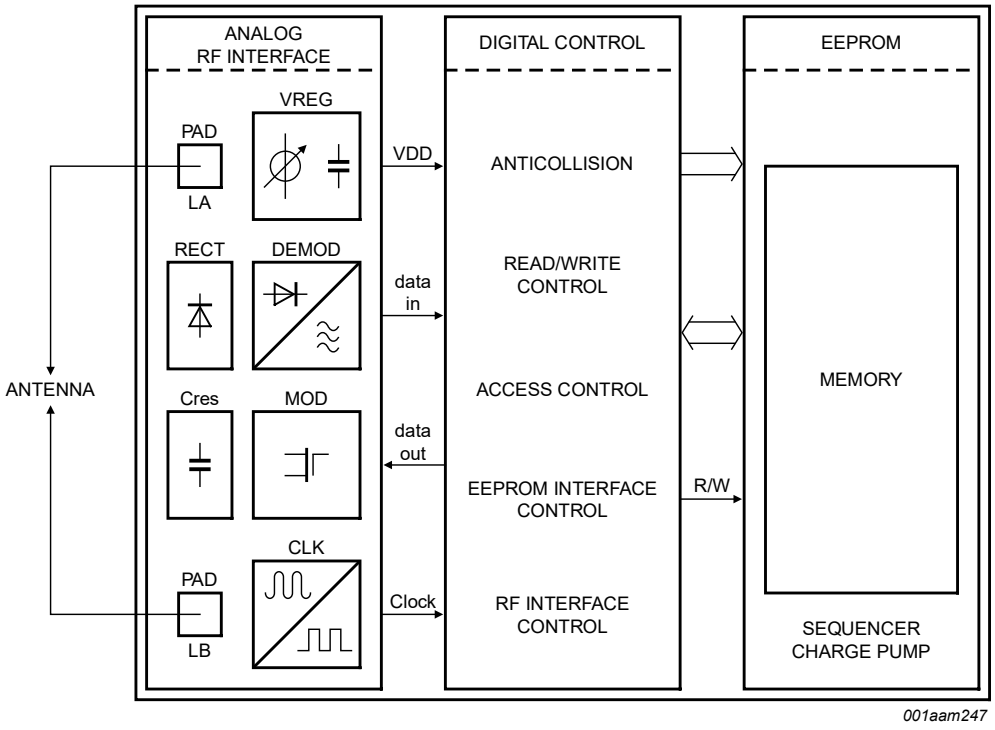



**Figure 1. Block diagram of ICODE 3 (SL2S3003)**

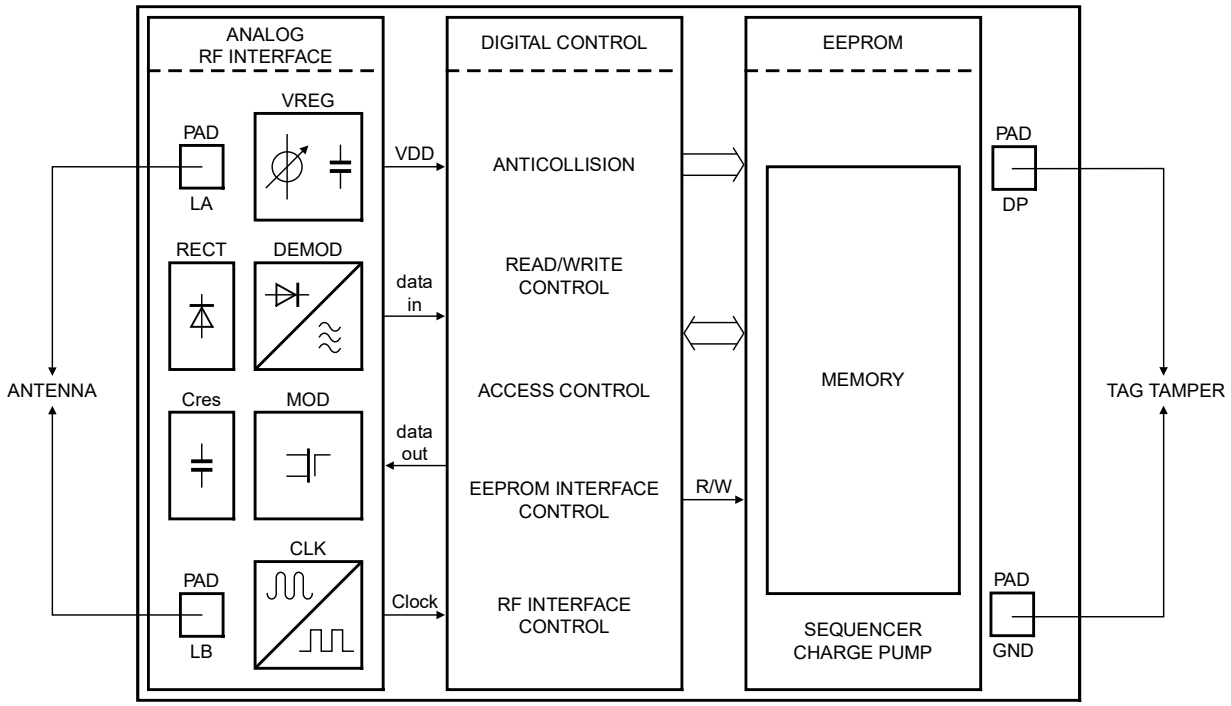
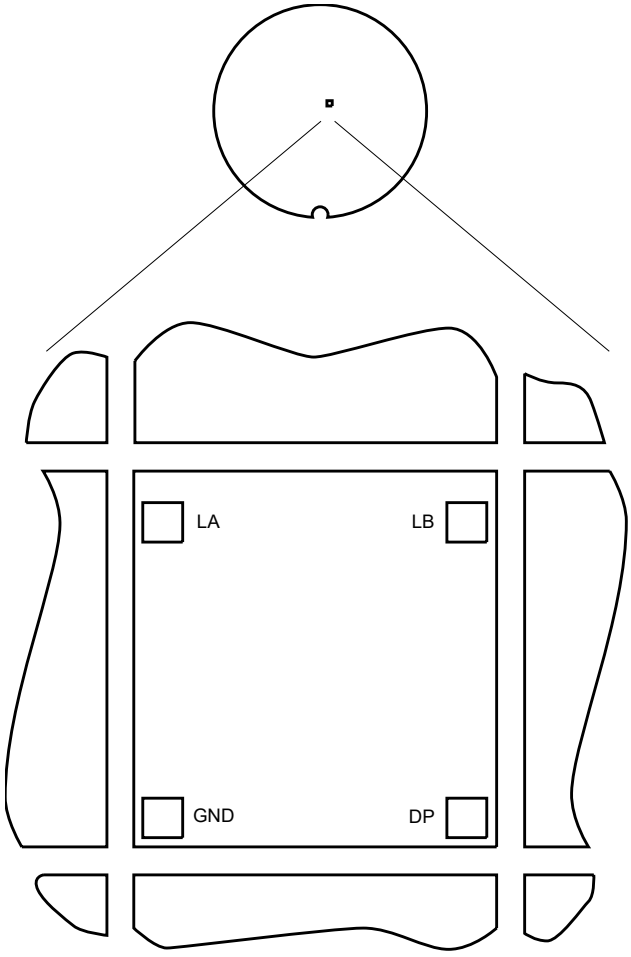



**Figure 2. Block diagram of ICODE 3 TagTamper (SL2S3003TT)**

# 6 Wafer layout




not to scale!

**Figure 3. SL2S3003TTFUD wafer layout and pin configuration for the bare die**

## 6.1 Pin description

**Table 2. Bonding pad description**

| Symbol | Description |
|---|---|
| LA | Antenna connection LA |
| LB | Antenna connection LB |
| GND | Ground (only connected to IC circuitry for SL2S3003TT) |
| DP | Detection pin (only connected to IC circuitry for SL2S3003TT) |

Refer to [5].

# 7 Mechanical specification

## 7.1 Wafer specification

Refer to [5].

**Table 3. Wafer specification**

| Parameter | Value |
|---|---|
| **Wafer** | |
| Designation | each wafer is enscribed with batch number and wafer number |
| Diameter | 300 mm (12 inches) |
| Thickness | 120 µm ± 15 µm |
| Process | CMOS 0.14 µm |
| Batch size | 25 wafers |
| Dies per wafer | 153333 |
| **Wafer backside** | |
| Material | Si |
| Treatment | ground and stress release |
| Roughness | $R_a$ minimum = 0.5 µm |
| | $R_t$ maximum = 5 µm |
| **Chip dimensions** | |
| Die size without scribe | 675 µm × 635 µm = 0.428625 $mm^2$ |
| **Scribe line width** | |
| X-dimension | 35 µm (scribe line width measured between nitride edges) |
| Y-dimension | 35 µm (scribe line width measured between nitride edges) |
| Number of pads | 4 |
| Pad location | non-diagonal/placed in chip corners |
| Distance pad to pad LA to LB | 530 µm (center to center) |
| Distance pad to pad LB to TEST | 452.2 µm (center to center) |
| **Passivation on front** | |
| Type | sandwich structure |
| Material | PE-nitride (on top) |
| Thickness | 1.75 µm total thickness of passivation |
| **Au bump** | |
| Material | >99.9 % pure Au |
| Hardness | 35 HV to 80 HV 0.005 |
| Shear strength | >70 MPa |
| Height | 18 µm |

**Table 3. Wafer specification***...continued*

| Parameter | Value |
|---|---|
| **Height uniformity** | |
| within a die | ±2 µm |
| within a wafer | ±3 µm |
| wafer to wafer | ±4 µm |
| Bump flatness | ±1.5 µm |
| **Bump size** | |
| LA, LB | 80 µm × 80 µm |
| TEST, GND | 80 µm × 80 µm |
| variation | ±5 µm |
| Under bump metallization | sputtered TiW |

### 7.1.1 Fail die identification

No ink dots are applied to the wafer.

Electronic wafer mapping (SECS II format) covers the electrical test results and additionally the results of mechanical/visual inspection.

See [5].

### 7.1.2 Map file distribution

See [5].

# 8 Functional description

## 8.1 Block description

The ICODE 3 includes three major blocks: the analog RF interface, the digital controller, and the EEPROM.

**Analog RF interface**

The interrogator generates an electromagnetic field. The analog RF interface generates the stable power supply and the system clock from the electromagnetic field via the antenna. The ICODE 3 requires no internal power supply.

The analog RF interface also includes:

- The demodulator: Demodulates the data transmitted from the interrogator to the ICODE label. The data is then processes in the digital control block.
- The modulator: Modulates the electromagnetic field for data transmission from the ICODE label to the interrogator.

**Digital control block**

The digital control block includes the state machines. The block is used to process the data and to handle the communication with the EEPROM.

**EEPROM**

Data are stored in a non-volatile memory (EEPROM).

## 8.2 Memory organization

The 2432-bit user-accessible EEPROM memory is divided into 76 blocks. The block is the smallest access unit. Each block consists of 4 bytes or 32 bits. Bit 0 in each byte represents the least significant bit (LSB) and bit 7 is the most significant bit (MSB).

The entire memory is divided into two parts:

- User memory
  - The blocks 0 to 74 (2400 bits) are used to store the user data. Direct read/write access to this part of the memory is possible depending on the security and write protection conditions. The user memory can be accessed with the READ and WRITE commands.
  - The last block of the user memory (block 75) contains the 24-bit counter and the password protection flag of the counter.
- Configuration memory
  - This part of the memory stores the information to configure the ICODE 3. The configuration memory can be accessed with the READ CONFIG and WRITE CONFIG commands.

**Table 4. User memory organization**

| Block | Byte 0 | Byte 1 | Byte 2 | Byte 3 | Description |
|---|---|---|---|---|---|
| 0 | | | | | User memory:<br>75 blocks,<br>4 bytes each,<br>300 bytes in total. |
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| : | : | : | : | : | |
| 72 | | | | | |
| 73 | | | | | |
| 74 | | | | | |
| 75 | C0 | C1 | C2 | PROT | Counter |

***Note:*** *Block 75 contains the 24-bit counter and cannot be used to store user data. READ and WRITE commands to that block require special data considerations (refer to Section 8.5.3.25).*

**Table 5. Configuration memory organization**

| Block | Byte 0 | Byte 1 | Byte 2 | Byte 3 | Description |
|---|---|---|---|---|---|
| 0 | | | | | Configuration memory:<br>48 blocks,<br>4 bytes each,<br>192 bytes in total. |
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| : | : | : | : | : | |
| 44 | | | | | |
| 45 | | | | | |
| 46 | | | | | |
| 47 | | | | | |
| 48 - 127 | RFU | RFU | RFU | RFU | Reserved configuration memory |

### 8.2.1 Unique identifier

The 64-bit unique identifier (UID) is programmed during the production process according to ISO/IEC 15693-3 and cannot be changed afterward. For more information on the ISO standard, refer to [3].

The 64 bits are numbered according to ISO/IEC 15693-3 starting with LSB 1 and ending with MSB 64. This is in contrast to the general used bit numbering within a byte.

The TAG type is a part of the UID (bits 41 to 48 next to the manufacturer code which is "04h" for NXP Semiconductors).

The TAG type of the ICODE 3 IC is "01h".

Bits 39 to 36 are used to identify the UID as ICODE 3.

**Table 6. Unique identifier**

| MSB | | | | | | | LSB |
|---|---|---|---|---|---|---|---|
| **64:57** | **56:49** | **48:41** | **40:1** | | | | |
| "E0" | "04" | "01" | IC manufacturer serial number | | | | |
| UID 7 | UID 6 | UID 5 | UID 4 | UID 3 | UID 2 | UID 1 | UID 0 |

**Table 7. Type indicator bits**

| Bit 39 | Bit 38 | Bit 37 | Bit 36 | ICODE Type |
|---|---|---|---|---|
| 0 | 1 | 0 | 0 | ICODE 3 |

### 8.2.2 Originality signature

The ICODE 3 can verify the origin of a tag. The device compares the UID compared with an originality signature stored in the configuration memory. The originality signature can be read either with the READ SIGNATURE command (refer to Section 8.5.3.20 "READ SIGNATURE"), or with the READ CONFIG command (refer to Section 8.5.3.21 "READ CONFIG"). The outcome of the command is verified on the reader side.

The originality signature can be customized for specific applications. At delivery, the ICODE 3 is preprogrammed with the 32-byte NXP originality signature. The signature is unlocked in the dedicated memory. If needed, the signature can be reprogrammed with a custom-specific signature using the WRITE CONFIG command (refer to Section 8.5.3.22 "WRITE CONFIG") during the customization process. Next, the signature can be permanently locked by setting the OTP_OS_LOCK bit to 1 with the WRITE CONFIG command to avoid further modifications.

The ICODE 3 can be configured with a 48-byte signature using the OS_CFG_MODE in the configuration memory (see Table 41). If the originality signature is set to 48 bytes, the customized signature must be programmed into blocks 0 to 11 in the configuration memory. Then the WRITE CONFIG command is used to set the configuration memory to "locked".

***Note:*** *If no customized originality signature is required, it is recommended to permanently lock the NXP signature during the initialization process by setting the configuration memory to "locked" with the WRITE CONFIG command.*

#### 8.2.2.1 Originality signature at delivery

At delivery, the ICODE 3 is programmed with a 32-byte NXP digital signature based on standard Elliptic Curve Cryptography (curve name secp128r1), according to the ECDSA algorithm [6]. The use of a standard algorithm and ECC curve ensures easy software integration. The originality check procedure in NFC devices does not require specific hardware. During production, each ICODE 3 UID is signed with an NXP private key. The resulting 32-byte signature is stored in the configuration memory blocks 0 to 7.

**Table 8. Originality Signature location in the configuration memory**

| Config Block | Byte 0 | Byte 1 | Byte 2 | Byte 3 |
|---|---|---|---|---|
| 0 | OS_0 (LSB) | OS_1 | OS_2 | OS_3 |
| 1 | OS_4 | OS_5 | OS_6 | OS_7 |
| : | : | : | : | : |
| 6 | OS_24 | OS_25 | OS_26 | OS_27 |
| 7 | OS_28 | OS_29 | OS_30 | OS_31 (MSB) |

Use the READ SIGNATURE command or the READ CONFIG command to retrieve the signature (refer to Section 8.5.3.20 "READ SIGNATURE"). Verify the signature in the NFC device by using the corresponding ECC public key provided by NXP [7].

If the NXP public key is stored in the reader device, the complete signature verification procedure can be performed offline.

To verify the signature (for example with the use of the public domain crypto library OpenSSL), set the tool domain parameters to secp128r1, defined within the standards for elliptic curve cryptography SEC [6].

### 8.2.3 Configuration memory

The configuration memory stores the IC configuration settings. Direct access to this memory area is only possible with READ_CONFIG and WRITE_CONFIG commands depending on the initialization status.

The configuration lock bit locks only the access with the WRITE CONFIG command. Commands (WRITE AFI, LOCK AFI, WRITE PASSWORD, and others) that modify specific data fields in the configuration memory can still be used, if the related data fields are not locked.

- Blocks 26 - 31 (OTP bits)
  OTP bits can be set to 1 with the WRITE CONFIG command, writing of 0 is ignored. Each OTP bit is set to 1 one time. Each block with OTP bits must not be written more than four times with the WRITE CONFIG command.
- Block 38 (status bits)
  The bits in block 38 can only be read with the READ CONFIG command. Programming with the WRITE CONFIG command returns a response with the ERROR_flag set to 1.
- Block 41 - 46 (passwords)
  If the password is not locked, the WRITE CONFIG or WRITE PASSWORD commands are used to program the password. See Section 8.5.3.3 "WRITE PASSWORD". The READ CONFIG command masks all the passwords bytes with 00h.

***Note:*** *Use diversified passwords. Use passwords diversified per application for the privacy passwords. Use the configuration password only in trusted environments.*

- Block 47 contains the open TagTamper message TT_OPEN_MSG for the SL2S3003TT. This block is RFU for the SL2S3003.
- RFU
  RFU marked fields are reserved for future use.

**Table 9. Configuration memory blocks**

| Block Address | Byte number | | | | |
|---|---|---|---|---|---|
| Dec | 0 | 1 | 2 | 3 | Access |
| 0 - 7 | OS 0 - 31 | | | | r/w |
| 8 - 11 | OS 32 - 47 | | | | r/w |
| 12 - 15 | RFU | | | | |
| 16 | DSFID | RFU | | | |
| 17 | AFI | RFU | | | r/w |
| 18 | EAS ID0 | EAS ID1 | RFU | | r/w |
| 19 | CID0 | CID1 | RFU | | r/w |
| 20 | PPC_PNTR | PPC_CTRL | RFU | | r/w |
| 21 | LP_PNTR | LP_CTRL | RFU | | r/w |
| 22 | NFC_MIRROR_CRT | NFC_MIRROR_BLK | RFU | | r/w |
| 23 | TT_SHOW_STATUS[1] | RFU | | | r/w |
| 24 - 25 | RFU | | | | r |
| 26 | OTP_LOCK0 | RFU | | | r/w |
| 27 | OPT_LOCK1 | RFU | | | r/w |
| 28 | OPT_LOCK2 | RFU | | | r/w |
| 29 | OPT_LOCK3 | RFU | | | r/w |
| 30 | OPT_LOCK4 | RFU | | | r/w |
| 31 | OPT_LOCK5 | RFU | | | r/w |

**Table 9. Configuration memory blocks***...continued*

| Block Address | Byte number | | | | |
|---|---|---|---|---|---|
| Dec | 0 | 1 | 2 | 3 | Access |
| 32 | PRIVACY_MODE | RFU | | | r/w |
| 33 | COUNTER_CFG0 | RFU | | | r/w |
| 34 | COUNTER_CFG1 | RFU | | | r/w |
| 35 | OS_CFG | RFU | | | r/w |
| 36 - 37 | RFU | | | | r |
| 38 | PRIVACY_STATUS | RFU | EAS_STATUS | RFU | r |
| 39 - 40 | RFU | | | | r |
| 41 | CFG_PWD0 (LSB) | CFG_PWD1 | CFG_PWD2 | CFG_PWD3 (MSB) | w |
| 42 | READ_PWD0 (LSB) | READ_PWD1 | READ_PWD2 | READ_PWD3 (MSB) | w |
| 43 | WRITE_PWD0 (LSB) | WRITE_PWD1 | WRITE_PWD2 | WRITE_PWD3 (MSB) | w |
| 44 | PRIVACY_PWD0 (LSB) | PRIVACY_PWD1 | PRIVACY_PWD2 | PRIVACY_PWD3 (MSB) | w |
| 45 | DESTROY_PWD0 (LSB) | DESTROY_PWD1 | DESTROY_PWD2 | DESTROY_PWD3 (MSB) | w |
| 46 | EASAFI_PWD0 | EASAFI_PWD1 | EASAFI_PWD2 | EASAFI_PWD3 (MSB) | w |
| 47[1] | TT_OPEN_MSG0 (LSB) | TT_OPEN_MSG1 | TT_OPEN_MSG2 | TT_OPEN_MSG3 (MSB) | r/w |
| 48 - 127 | RFU | | | | |

[1] RFU for SL2S3003

**Table 10. PPC_PNTR byte (Protect Page Pointer Address) configuration parameter descriptions**

| Field | Bit | Values at Delivery | Description |
|---|---|---|---|
| PPC_PTNR | 8 | 0b | The Protection Pointer Address defines the base address for the password protection of the higher user memory segment Page H. All block addresses smaller than the protection pointer address are in the user memory segment Page L. Section 8.5.3.6 |

**Table 11. PPC_CTRL byte (Protect Page Control)**

| Bit number | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| RL | WL | RFU | | RH | WH | RFU | |

**Table 12. PPC_CTRL byte configuration parameter descriptions**

| Field | Bit | Values at Delivery | Description |
|---|---|---|---|
| RL | 1 | 0b | Defines read password protection for Page L as defined with Section 8.5.3.6 |
| WL | 1 | 0b | Defines write password protection for Page L as defined with Section 8.5.3.6 |
| RH | 1 | 0b | Defines read password protection for Page H as defined with Section 8.5.3.6 |
| WH | 1 | 0b | Defines write password protection for Page H as defined with Section 8.5.3.6 |

**Table 13. LP_PNTR byte (Lock Protection Pointer Address) configuration parameter descriptions**

| Field | Bit | Values at Delivery | Description |
|---|---|---|---|
| LP_PTNR | 8 | 0b | The Lock Pointer Address defines the block from which the user memory is divided into two pages (Page L and Page H) for the write lock (see in Section 8.5.2.3). All block addresses smaller than the Lock Pointer Address are in the user memory segment Page L. The lock conditions for those two pages L and H are defined with the settings in the LP_CTR byte (see in Table 14). |

**Table 14. LP_CTRL byte (Lock Pointer Control)**

| Bit number | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| LP_CTRL_L | LP_CTRL_H | RFU | | | | | |

**Table 15. LP_CTRL byte configuration parameter descriptions**

| Field | Bit | Values at Delivery | Description |
|---|---|---|---|
| LP_CTRL_L | 1 | 0b | Defines the write lock for Page L defined with the lock protection pointer byte LP_PNTR. Individual blocks can be write locked with the LOCK BLOCK command (refer to Section 8.5.2.3)<br>0b ... Page L is not write locked<br>1b ... Page L is write locked |
| LP_CTRL_H | 1 | 0b | Defines the write lock for Page H defined with the lock protection pointer byte LP_PNTR. Individual blocks can be write locked with the LOCK BLOCK command (refer to Section 8.5.2.3)<br>0b ... Page H is not write locked<br>1b ... Page H is write locked |

**Table 16. NFC_MIRROR_CTR byte (NFC Mirror Control)**

| Bit number | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| NFC_MIRROR_SEL | | | NFC_MIRROR_BYTE | | RFU | | |

**Table 17. NFC_MIRROR_CTR byte configuration parameter descriptions**

| Field | Bit | Values at Delivery | Description |
|---|---|---|---|
| NFC_MIRROR_SEL | 3 | 000b | Defines the functionality for UID, NFC Counter and TagTamper message mirroring<br>000b ... NFC mirror is disabled<br>001b ... UID mirror is enabled<br>010b ... UID + NFC Counter mirror is enabled<br>For ICODE 3 TagTamper (SL2S3003TT) only:<br>011b … UID + NFC Counter + TagTamper Message mirror is enabled<br>1xxb … UID + NFC Counter + TagTamper Message + TagTamper Status mirror is enabled |
| NFC_MIRROR_BYTE | 2 | 00b | Defines the byte within the block defined in NFC_MIRROR_BLK where the NFC mirror shall start. |

**Table 18. NFC_MIRROR_BLK byte**

| Bit number | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| NFC_MIRROR_BLK | | | | | | | RFU |

**Table 19. NFC_MIRROR_BLK byte configuration parameter descriptions**

| Field | Bit | Values at Delivery | Description |
|---|---|---|---|
| NFC_MIRROR_BLK | 7 | 00h | Defines the first block within the user memory where the NFC mirror shall start. |

**Table 20. TT_SHOW_STATUS byte for SL2S3003TT (RFU for SL2S3003)**

| Bit number | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| TT_SHOW_STATUS | | RFU | | | | | |

**Table 21. TT_SHOW_STATUS byte configuration parameter descriptions**

| Field | Bit | Values at Delivery | Description |
|---|---|---|---|
| for SL2S3003TT (RFU for SL2S3003)<br>TT_SHOW_STATUS | 2 | 00h | Defines which TagTamper Status shall be shown by NFC mirror feature and READ TT command:<br>00b … No TagTamper status (actual status and stored TagTamper message are masked)<br>10b … Only actual TagTamper status is shown (stored TagTamper status is masked)<br>01b … Only stored TagTamper status is shown (actual TagTamper status is masked)<br>11b … actual and stored TagTamper status are shown |

**Table 22. OTP_LOCK0 byte**

| Bit number | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| OTP_CID_LOCK | OTP_LP_LOCK | OTP_PWD_R_LOCK | OTP_PWD_W_LOCK | RFU | | | |

**Table 23. OTP_LOCK0 byte configuration parameter descriptions**

| Field | Bit | Values at Delivery | Description |
|---|---|---|---|
| OTP_CID_LOCK | 1 | 0h | Defines the write access of the CID bytes in configuration memory block 19:<br>0b ... CID bytes are not write locked<br>1b ... CID bytes are locked<br>***Note:*** *Lock the CID at the end of the initialization of the IC. (Not required if the complete configuration memory is locked with the OTP_CONFIG_ LOCK (see Table 28)* |
| OTP_LP_LOCK | 1 | 0h | Defines the write access of the Lock Pointer bytes LP_PNTR and LP_CTR in configuration memory block 21:<br>0b ... Lock Pointer bytes are not write locked<br>1b ... Lock Pointer bytes are locked<br>***Note:*** *Lock the Lock Pointer at the end of the initialization of the IC.* |
| OTP_R_PWD_LOCK | 1 | 0h | Defines the write access of the Read Password in configuration memory block 42:<br>0b ... Read Password is not write locked<br>1b ... Read Password is locked. The Read password can also be locked with the LOCK PASSWORD command (see Section 8.5.3.4) |
| OTP_W_PWD_LOCK | 1 | 0h | Defines the write access of the Write Password in configuration memory block 43:<br>0b ... Write Password is not write locked<br>1b ... Write Password is locked. The Write password can also be locked with the LOCK PASSWORD command (see Section 8.5.3.4) |

**Table 24. OTP_LOCK1 byte**

| Bit number | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| OTP_PPC_LOCK | OTP_PRIVACY_PWD_LOCK | OTP_DESTROY_PWD_LOCK | OTP_OS_LOCK | RFU | | | |

**Table 25. OTP_LOCK1 byte configuration parameter descriptions**

| Field | Bit | Values at Delivery | Description |
|---|---|---|---|
| OTP_PPC_LOCK | 1 | 0h | Defines the write access of the Page Protection condition bytes PPC_PNTR and PPC_CTRL in configuration memory block 20:<br>0b ... Page Protection bytes are not write locked<br>1b ... Page Protection bytes are locked<br>***Note:*** *Lock the Page Protection condition at the end of the initialization of the IC.* |
| OTP_PRIVACY_PWD_LOCK | 1 | 0h | Defines the write access of the Privacy Password in configuration memory block 44:<br>0b ... Privacy Password is not write locked<br>1b ... Privacy Password is locked. The Privacy password can also be locked with the LOCK PASSWORD command (see Section 8.5.3.4). |
| OTP_DESTROY_PWD_LOCK | 1 | 0h | Defines the write access of the Destroy Password in configuration memory block 45:<br>0b ... Destroy Password is not write locked<br>1b ... Destroy Password is locked. The Destroy password can also be locked with the LOCK PASSWORD command (see Section 8.5.3.4). |
| OTP_OS_LOCK | 1 | 0h | Defines the write access of the Originality Signature in configuration memory blocks 0 - 11 as well as the length of the originality signature defined with the OS_CFG_MODE bit:<br>0b ... Originality Signature is not write locked<br>1b ... Originality Signature is locked<br>***Note:*** *Lock the Originality Signature at the end of the initialization of the IC. (Not required if the complete configuration memory is locked with the OTP_CONFIG_LOCK (see Table 28).* |

**Table 26. OTP_LOCK2 byte**

| Bit number | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| OTP_DSFID_LOCK | OTP_LOCKBITS_LOCK | OTP_AFI_PWD_EN | OTP_COUNTER_PRESET_DIS | RFU | | | |

**Table 27. OTP_LOCK2 byte configuration parameter descriptions**

| Field | Bit | Values at Delivery | Description |
|---|---|---|---|
| OTP_DSFID_LOCK | 1 | 0h | Defines the write access of the DSFID byte in configuration memory block 16:<br>0b ... DSFID byte is not write locked<br>1b ... DSFID byte is locked. The DSFID byte can also be locked with the LOCK DSFID command (see Section 8.5.2.10). |
| OTP_LOCKBITS_LOCK | 1 | 0h | Defines if internal block lock bits can be set with the LOCK BLOCK command:<br>0b ... LOCK BLOCK command is enabled<br>1b ... LOCK BLOCK command is disabled |
| OTP_AFI_PWD_EN | 1 | 0h | Defines if the AFI Password Protection is enabled:<br>0b ... AFI Password Protection is disabled<br>1b ... AFI Password Protection is enabled. The AFI password protection can also be enabled with the PASSWORD PROTECT EAS/AFI command (see Section 8.5.3.16).<br>***Note:*** *To avoid unauthorized change of the AFI, lock or password protect the AFI.* |
| OTP_COUNTER_PRESET_DIS | 1 | 0h | Defines if the Counter Preset is disabled:<br>0b ... Counter Preset is enabled<br>1b ... Counter Preset is disabled<br>***Note:*** *If this functionality is not needed, disable the counter preset (recommendation).* |

**Table 28. OTP_LOCK3 byte**

| Bit number | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| OTP_EAS_PWD_EN | OTP_EASAFI_PWD_LOCK | OTP_CONFIG_LOCK | OTP_CONFIG_PWD_LOCK | RFU | | | |

**Table 29. OTP_LOCK3 byte configuration parameter descriptions**

| Field | Bit | Values at Delivery | Description |
|---|---|---|---|
| OTP_EAS_PWD_EN | 1 | 0h | Defines if the EAS Password Protection is enabled:<br>0b ... EAS Password Protection is disabled<br>1b ... EAS Password Protection is enabled. The EAS password protection can also be enabled with the PASSWORD PROTECT EAS/AFI command (see Section 8.5.3.16).<br>***Note:*** *To avoid unauthorized change of EAS, lock or password protect the EAS functionality (recommendation).* |
| OTP_EASAFI_PWD_LOCK | 1 | 0h | Defines the write access of the EAS/AFI Password in configuration memory block 46:<br>0b ... EAS/AFI Password is not write locked<br>1b ... EAS/AFI Password is locked. The EAS/AFI password can also be locked with the LOCK PASSWORD command (see Section 8.5.3.4). |
| OTP_CONFIG_LOCK | 1 | 0h | Defines the write access to the configuration memory with the WRITE_CONFIG command:<br>0b ... Configuration memory access with WRITE_CONFIG command is enabled<br>1b ... Configuration memory access with WRITE_CONFIG command is disabled. Settings within the configuration memory can still be changed with other commands, depending on the related access conditions<br>***Note:*** *If no further changes need to be set with the WRITE CONFIG command, write lock the configuration memory at the end of the initialization of the IC. If the configuration memory cannot be locked because changes are needed in the application, program and activate the configuration memory password with the OTP_CONFIG_PWD _EN (see Table 30).* |
| OTP_CONFIG_PWD_LOCK | 1 | 0h | Defines the write access of the Config Password in configuration memory block 41:<br>0b ... CONFIG Password is not write locked<br>1b ... CONFIG Password is locked. The Config password can also be locked with the LOCK PASSWORD command (see Section 8.5.3.4). |

**Table 30. OTP_LOCK4 byte**

| Bit number | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| OTP_ CONFIG_ PWD_EN | RFU | OTP_AFI_ LOCK | OTP_EAS_ LOCK | RFU | | | |

**Table 31. OTP_LOCK4 byte configuration parameter descriptions**

| Field | Bit | Values at Delivery | Description |
|---|---|---|---|
| OTP_CONFIG_ PWD_EN | 1 | 0h | Defines if the write access with the WRITE CONFIG command is password protected with the CFG_PWD password. Access to the configuration memory always depends on related lock options:<br>0b ... Write access to the configuration memory is possible without password authentication<br>1b ... Write access to the configuration memory is only possible with a valid previous password authentication with the CF_PWD password<br>***Note:*** *If changes with the WRITE CONFIG command are required in the application, program and activate the configuration memory password with the OTP_CONFIG_PWD _EN after the IC initialization. In case no further changes are required, use WRITE_CONFIG command to lock the write access to the configuration memory with the OTP_CONFIG_ LOCK bit. See Table 28.* |
| OTP_AFI_LOCK | 1 | 0h | Defines if the AFI in block 17 is write locked:<br>0b ... AFI is not write locked<br>1b ... AFI is write locked. The AFI can also be locked with the LOCK AFI command (see Section 8.5.2.8)<br>***Note:*** *To avoid unauthorized change of the AFI, lock or password protect the AFI.* |
| OTP_EAS_ LOCK | 1 | 0h | Defines if the current state of the EAS mode and the EAS ID is locked:<br>0b ... EAS mode and EAS_ID are not locked<br>1b ... EAS mode and EAS_ID are locked. EAS mode and EAS_ID can also be locked with the LOCK EAS command (see Section 8.5.3.14).<br>***Note:*** *To avoid unauthorized change of EAS, password protect the EAS functionality.* |

**Table 32. OTP_LOCK5 byte**

| Bit number | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| OTP_PWD64_EN | OTP_TT_OPEN_MSG_LOCK (RFU) | OTP_TT_EN (RFU) | RFU | | | | |

**Table 33. OTP_LOCK5 byte configuration parameter descriptions**

| Field | Bit | Values at Delivery | Description |
|---|---|---|---|
| OTP_PWD64_EN | 1 | 0h | Defines if the 64-bit password protection is enabled:<br>0b ... 64 bit password protection is disabled<br>1b ... 64 bit password protection is enabled. The 64-bit password protection can also be enabled with the 64 BIT PASSWORD PROTECTION command (see Section 8.5.3.5). |
| for SL2S3003 TT (RFU for SL2 S3003)<br>OTP_TT_OPEN_MSG_LOCK | 1 | 0h | Defines if the TT_OPEN_MSG (TagTamper open message) in block 47 is write locked:<br>0b ... TT_OPEN_MSG is not write locked and TT_OPEN_MSG can be read with the READ CONFIG command<br>1b ... TT_OPEN_MSG is write locked and cannot be changed with the WRITE CONFIG command and on a READ CONFIG command the TT_OPEN_MSG is masked with 0x00 |
| for SL2S3003 TT (RFU for SL2 S3003)<br>OTP_TT_EN | 1 | 0h | Defines if the first TagTamper open event shall be stored permanently:<br>0b ... Store TagTamper status is disabled<br>1b ... Store TagTamper feature is enabled |

**Table 34. PRIVACY_MODE byte**

| Bit number | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| PRIVACY_ MODE_SEL | RFU | | | | | | |

**Table 35. PRIVACY_MODE byte configuration parameter descriptions**

| Field | Bit | Values at Delivery | Description |
|---|---|---|---|
| PRIVACY_ MODE_SEL | 1 | 0h | Defines the Privacy mode (see Section 8.5.3.9):<br>0b ... Privacy mode 1: In this mode, the IC only responds to the GET RANDOM NUMBER and SET PASSWORD commands<br>1b ... Privacy mode 2: All ICs in this mode are responding with the same UID to an INVENTORY command<br>***Note:*** *To avoid unauthorized changes to the privacy mode, lock or password protect the configuration memory .* |

**Table 36. COUNTER_CFG0 byte**

| Bit number | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| COUNTER_ MODE | RFU | | | | | | |

**Table 37. COUNTER_CFG0 byte configuration parameter descriptions**

| Field | Bit | Values at Delivery | Description |
|---|---|---|---|
| COUNTER_ MODE | 1 | 0h | Defines the mode of the counter (see Section 8.2.3.1):<br>0b ... Command-based counter is enabled<br>1b ... NFC Counter is enabled<br>***Note:*** *Lock or password protect the configuration memory to avoid unauthorized changes to the counter mode.* |

**Table 38. COUNTER_CFG1 byte**

| Bit number | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| NFC_ RETRY_ MODE | RFU | | | | | | |

**Table 39. COUNTER_CFG1 byte configuration parameter descriptions**

| Field | Bit | Values at Delivery | Description |
|---|---|---|---|
| NFC_RETRY_ MODE | 1 | 0h | Defines how often the IC retries to increase the NFC Counter (see Section 8.2.3.1):<br>0b ... 16 retries with a retry period of 4.8 ms<br>1b ... 64 retries with a retry period of 9.6 ms |

**Table 40. OS_CFG byte**

| Bit number | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| OS_CFG_ MODE | RFU | | | | | | |

**Table 41. OS_CFG byte configuration parameter descriptions**

| Field | Bit | Values at Delivery | Description |
|---|---|---|---|
| OS_CFG_MODE | 1 | 0h | Defines the length of the originality signature (see Section 8.2.2):<br>0b ... 32 byte originality signature (configuration memory blocks 0-7)<br>1b ... 48 byte originality signature (configuration memory blocks 0-11) |

**Table 42. STATUS_PRIVACY byte**

| Bit number | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| STATUS_ PRIVACY_ ACTIVE | RFU | | | | | | |

**Table 43. PRIVACY_STATUS byte configuration parameter descriptions**

| Field | Bit | Values at Delivery | Description |
|---|---|---|---|
| STATUS_ PRIVACY_ ACTIVE | 1 | 0h | Provides the information if the Privacy is enabled or disabled:<br>0b ... Privacy mode is not active<br>1b ... Privacy mode is active |

**Table 44. STATUS_EAS byte**

| Bit number | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| STATUS_ EAS_ACTIVE | RFU | | | | | | |

**Table 45. STATUS_EAS byte configuration parameter descriptions**

| Field | Bit | Values at Delivery | Description |
|---|---|---|---|
| STATUS_EAS_ ACTIVE | 1 | 0h | Provides the information if the EAS functionality is set or reset:<br>0b ... EAS functionality is reset<br>1b ... EAS functionality is set |

### 8.2.3.1 Counter feature

The ICODE 3 supports a 24-bit counter feature that is implemented in block 75 of the user memory.

The COUNTER_MODE bit in the configuration memory is used to set the mode of the counter mode:

- Command-based counter (see to Section 8.2.3.1.1) or
- NFC counter (see Section 8.2.3.1.2)

#### 8.2.3.1.1 Command-based counter

If the 24-bit counter is configured as a command-based counter:

- Use the WRITE SINGLE BLOCK command to increase and preset the counter.
- Use OTP_COUNTER_PRESET_DIS bit in the configuration memory to disable the option to preset the counter.COUNTER_MODE bit in the configuration memory.

Refer to Section 8.5.3.25 "24-bit counter".

#### 8.2.3.1.2 NFC counter

If the 24-bit counter is configured as an NFC counter, at each start of the IC, the label IC automatically increases the 24-bit counter value. In the NFC counter mode, the start-up time of the reader device must comply with the NFC Forum Tag 5 Type specification .

Once the NFC counter has reached the maximum value of FF FF FF hex, the NFC counter value does not change anymore.

The NFC counter is enabled or disabled with the COUNTER_MODE bit in the configuration memory bit. See Table 36 in Section 8.2.3.

To read the NFC counter value, use either a read command to block 75 or NFC counter mirror feature.

If the counter is configured as NFC counter, the counter is incremented every time the tag is tapped by an NFC device or other read point. Due to response time constraints in ISO/IEC 15693 [1], the increment is done at start-up and not at the first read access to the user memory. A circuit that preserves its state over HF resets prevents further increments of the NFC counter until a read of the user memory is executed.

To ensure that the NFC counter is also incremented in situations where the tag slowly enters the HF field (typically in long range systems), the label IC retries to increment the counter at start-up multiple times. To optimally adapt to the application, two options are available with the NFC_RETRY_MODE bit:

**Table 46. NFC_RETRY_MODE request format**

| NFC_RETRY_MODE | Number of retries | Time between retries | Total retry period | Recommended usage |
|---|---|---|---|---|
| 0 | 16 | 4.8 ms | > 77 ms | default (for most applications) |
| 1 | 64 | 9.6 ms | > 614 ms | Applications where the label enters the field very slow |

If all the retries fail, the counter returns 0x00 00 00 to indicate that the counter had not been increased. For the TagTamper version, the same retry mechanism is used for the stored TagTamper status. If all the retries fail, the stored TagTamper status is reported as “E”.

#### 8.2.3.2 TagTamper feature (SL2S3003TT)

The TagTamper feature in SL2S3003TT enables the label IC to detect if the TagTamper wire is open or closed at the start-up of the IC.

When detecting an open TagTamper wire after the label IC tag is powered by an RF field, the status is actual TagTamper. If the OTP_TT_EN bit (see Table 33) is set, the event is stored permanently in the IC.

During the tag initialization, the user programs the 4-byte TagTamper message into TT_OPEN_MSG configuration block 47h. If the TT_LOCK bit is set to 1:

- If the TagTamper open event has not been detected, the TT_OPEN_MSG bytes are masked with 00h at READ CONFIG command, or
- If the TagTamper open event has been detected and stored earlier, the programmed TT_OPEN_MSG bytes respond to a READ CONFIG command.

The TagTamper status can be read with:

- READ TT STATUS command, or
- TagTamper ASCII mirror feature.

If the TagTamper wire has never been detected as open at start-up:

- The READ TT command responds with actual and stored TagTamper status closed depending on the TT_SHOW_STATUS bits.
- If the TagTamper ASCII mirror is enabled, the original programmed user memory content is read at that position.

Once the TagTamper wire has been detected as open at start-up:

- The IC stores permanently the information about the open TagTamper wire if the OTP_TT_EN is enabled.
- On a READ TT command, the IC responds with the actual and stored TagTamper status as open.
- If the TagTamper ASCII mirror is enabled, the programmed TT_OPEN_MSG is mirrored in ASCII to the defined position in the user memory (see Section 8.2.3.3).

Parameters for the detection of open or closed TagTamper wire connected to DP and GND pad are specified in Section 10.2.

***Note:*** *To avoid interferences induced by the RF field during the measurement of the TagTamper, keep the area covered by the TagTamper wire connected to DP and GND as small as possible. The area must not be larger than 2.5 $cm^2$ depending on the RF field strength used in the application under the worst case conditions.*

#### 8.2.3.3 NFC ASCII mirror feature

The NFC ASCII mirror feature of ICODE 3 enables the label IC to virtually mirror:

- The 8-byte UID (see Section 8.2.1), and
- The 3-byte NFC counter value (see Section 8.2.3.1.2).

ICODE 3 TagTamper (SLS3003TT) virtually mirrors in addition:

- The 4-byte TagTamper message, and
- The 1-byte actual TagTamper status.

The feature depends on NFC mirror settings into the physical memory of the IC in ASCII code. On a READ or FAST READ command to the assigned user memory blocks, the label IC responds with the virtual memory content of the UID and/or NFC counter value (SL2S3003) and/or TagTamper message and/or current TagTamper status (SLS3003TT) in ASCII code depending on the settings in the NFC_MIRROR_CTR byte (see Table 16).

The required length of the reserved physical memory for the mirror functions and the order for the ASCII mirrors are specified in Table 47.

***Note:*** *The number of bytes (see Table 47) of the enabled ASCII mirrors must not exceed the boundary of the user memory. Use only valid values for NFC_MIRROR_BLK and NFC_MIRROR_BYTE. If the ASCII mirror exceeds the user memory area, the ASCII mirroring stops at the end of the user memory.*

**Table 47. Required memory space for ASCII mirror**

| ASCII mirror and order | Required number of bytes in the physical memory |
|---|---|
| UID mirror | 16 bytes |
| UID + NFC counter mirror | 23 bytes<br>(16 bytes for UID + 1 byte separation + 6 bytes NFC counter value) |
| ICODE 3 TagTamper (SL2S3003 TT) only:<br>UID + NFC counter mirror + Tag Tamper message mirror | 32 bytes<br>(16 bytes for UID + 1 byte separation + 6 bytes NFC counter value + 1 byte separation + 8 bytes TagTamper message) |
| ICODE 3 TagTamper (SL2S3003 TT) only:<br>UID + NFC counter mirror + Tag Tamper message mirror + Tag Tamper status | 34 bytes<br>(16 bytes for UID + 1 byte separation + 6 bytes NFC counter value + 1 byte separation + 8 bytes TagTamper message + 1 byte separation + 1 byte current TagTamper Status) |

The fields are mirrored into the defined user memory area in the following order:

- UID: MSB first
- NFC counter: MSB First
- TagTamper message: LSB fist

The NFC_MIRROR_BLK and NFC_MIRROR_BYTE values in the configuration define the position within the user memory where the mirroring of the ASCII mirror starts.

The NFC_MIRROR_BLK value defines the block where the ASCII mirror starts and the NFC_MIRROR_BYTE value defines the starting byte within the defined block.

The ASCII mirrors are enabled with the NFC_MIRROR_SEL bits (see Table 17.)

If more than one ASCII mirror is enabled, the ASCII mirrors are separated automatically with an "x" character (78h ASCII code).

### 8.2.4 Configuration of delivered ICs

NXP ICODE 3 ICs are delivered with the following configuration:

- The unique identifier is unique and read-only.
- The write access allows changes to user blocks, AFI, DSFID, EAS, and passwords (password protection disabled).
- All password bytes are 00h for the Read and Write protection password, for the EAS/AFI password, and for the Config password.
- All password bytes are 0Fh for the privacy mode and label Destroy passwords.
- User data memory is **not** password protected.
- Password protected privacy Mode is disabled.
- EAS and AFI password protection is disabled.
- The status of EAS mode is not defined.
- AFI is supported and not defined
- DSFID is supported and not defined.
- The user data memory is not defined.
- NFC mirror feature is disabled.

***Note:***

1. *As the EAS mode is undefined at delivery, enable or disable EAS mode according to your application requirements during the test or initialization phase.*
2. *If password protection is not required and depending on the targeted application, write random passwords during the label initialization (recommendation).*

## 8.3 Communication principle

For the detailed description of the protocol and timing refer to ISO/IEC 15693-2 [2] (modulation, bit-coding, framing), and ISO/IEC 15693-3 [3] (anti-collision, timing, protocol).

## 8.4 State diagram

The state diagram illustrates the different states of the ICODE 3.

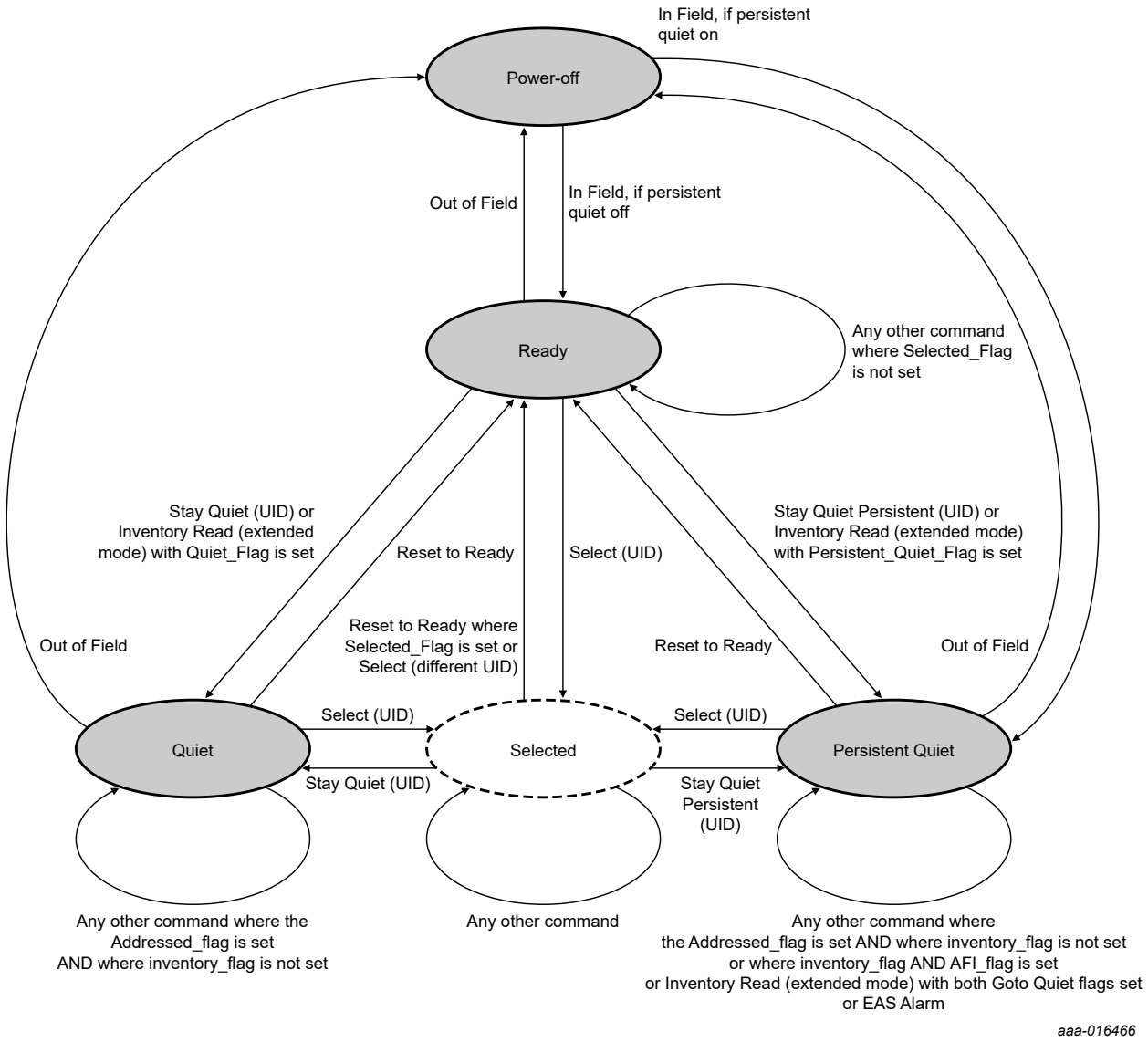



**Figure 4. State diagram ICODE 3**

***Note:*** *You can set the ICODE 3 IC in the Quiet state and Persistent Quiet state at the same time. In this case, the behavior is the same as for the Quiet state only until the IC enters the Power-off state. If the persistent time has not been exceeded, the IC enters to the Persistent Quiet mode at the next power-on.*

## 8.5 Supported commands

### 8.5.1 Mandatory commands

#### 8.5.1.1 INVENTORY

The command is as defined in ISO/IEC 15693-3 [3].

Exception: If the Privacy or Destroy mode is enabled, the label does not respond.

#### 8.5.1.2 STAY QUIET

The command is as defined in ISO/IEC 15693-3 [3].

### 8.5.2 Optional commands

#### 8.5.2.1 READ SINGLE BLOCK

As defined in ISO/IEC 15693-3.

Option 0 (Option flag not set) is supported.

Option 1 (Option flag set) is supported.

If the related page of the addressed block is protected with the Read-Password, and if the password has not been transmitted first with the SET PASSWORD command, the label responds according to the error handling (see Section 8.6 "Error handling").

***Note:*** *Block 75 of the user memory is used for the 24-bit counter feature and must be used differently. Refer to Section 8.5.3.25 "24-bit counter".*

#### 8.5.2.2 WRITE SINGLE BLOCK

As defined in ISO/IEC 15693-3.

Option 0 (Option flag not set) is supported.

Option 1 (Option flag set) is supported.

If the addressed block is part of a write protected page, or if the block is protected with the Read Password only (see Section 8.5.3.6 "PROTECT PAGE"), and the password has not been transmitted first with the SET PASSWORD command, the label responds according to the error handling (see Section 8.6 "Error handling").

***Note:*** *Block 75 of the user memory is used for the 24-bit counter feature and must be used differently. Refer to Section 8.5.3.25 "24-bit counter".*

#### 8.5.2.3 LOCK BLOCK

As defined in ISO/IEC 15693-3.

Option 0 (Option flag not set) is supported.

Option 1 (Option flag set) is supported.

If the addressed block is part of a write protected page, or if the block is protected with the read password only (see Section 8.5.3.6 "PROTECT PAGE"), and the password has not been transmitted first with the SET PASSWORD command, the label responds according to the error handling (see Section 8.6 "Error handling").

***Note:*** *Block 75 of the user memory is used for the 24-bit counter feature and must be used differently. Refer to Section 8.5.3.25 "24-bit counter".*

The ICODE 3 supports the option to lock larger sections of the user memory with the settings in the configuration memory block 21 (see Table 9). The Lock Pointer LP_PNTR defines the block from which the user memory is divided into two pages (Page L and Page H). The lock conditions for the two pages L and H are defined with the settings defined in the LP_CTR byte (see Table 14).

#### 8.5.2.4 READ MULTIPLE BLOCKS

As defined in ISO/IEC 15693-3.

Option 0 (Option flag not set) is supported.

Option 1 (Option flag set) is supported.

If one of the addressed blocks is part of a page protected with the Read-Password, and if the password has not been transmitted first with the SET PASSWORD command, the label responds according to the error handling (see Section 8.6 "Error handling").

***Note:*** *Block 75 of the user memory is used for the 24-bit counter feature and must be used differently. Refer to Section 8.5.3.25 "24-bit counter".*

#### 8.5.2.5 SELECT

As defined in ISO/IEC 15693-3.

#### 8.5.2.6 RESET TO READY

As defined in ISO/IEC 15693-3.

***Note:*** *RESET TO READY also resets the label IC from the persistent quiet state to the READY state. Refer to Section 8.5.3.10 "INVENTORY READ" and Section 8.5.3.19 "STAY QUIET PERSISTENT".*

#### 8.5.2.7 WRITE AFI

As defined in ISO/IEC 15693-3.

Option 0 (Option flag not set) is supported.

Option 1 (Option flag set) is supported.

***Note:*** *The command can be password protected. Refer to Section 8.5.3.16 "PASSWORD PROTECT EAS/AFI".*

***Note:*** *You can use also the WRITE CONFIG command to block 17 of the configuration memory to write the AFI. Refer to Table 9.*

#### 8.5.2.8 LOCK AFI

As defined in ISO/IEC 15693-3.

Option 0 (Option flag not set) is supported.

Option 1 (Option flag set) is supported.

***Note:***

1. *The command can be password protected. Refer to Section 8.5.3.16 "PASSWORD PROTECT EAS/AFI".*
2. *To lock the AFI, you can set the OTP_AFI_LOCK bit to 1 with the WRITE CONFIG command to block 30 of the configuration memory. Refer to Table 9.*
3. *To avoid unauthorized change of the AFI, lock or password protect the AFI.*

#### 8.5.2.9 WRITE DSFID

As defined in ISO/IEC 15693-3.

Option 0 (Option flag not set) is supported.

Option 1 (Option flag set) is supported.

The DSFID can also be written by a WRITE CONFIG command to block 16 of the configuration memory containing the DSFID. Refer to Table 9.

Also, the WRITE CONFIG command to block 16 of the configuration memory can write DSFID. Refer to Table 9.

#### 8.5.2.10 LOCK DSFID

As defined in ISO/IEC 15693-3.

Option 0 (Option flag not set) is supported.

Option 1 (Option flag set) is supported.

Also, setting the OTP_DSFID_LOCK bit to 1 with the WRITE CONFIG command to block 28 of the configuration memory can lock the DSFID. See Table 9 and Table 26.

#### 8.5.2.11 GET SYSTEM INFORMATION

As defined in ISO/IEC 15693-3.

The TAG type of the ICODE 3 IC is "01h".

#### 8.5.2.12 GET MULTIPLE BLOCK SECURITY STATUS

As defined in ISO/IEC 15693-3.

#### 8.5.2.13 FAST READ MULTIPLE BLOCK

As defined in ISO/IEC 15693-3 (2019).

Option 0 (Option flag not set) is supported.

Option 1 (Option flag set) is supported.

The supported data rates are as defined in ISO/IEC 15693-3 (2019):

- High data rate (26.48 kbits/s)
- X2 (52.97 kbits/s)
- X4 (105.94 kbits/s)
- X8 (211.88 kbits/s)

If one of the addressed blocks is part of a page protected with the Read-Password, and if the password has not been transmitted first with the SET PASSWORD command, the label responds according to the error handling (see Section 8.6 "Error handling").

***Note:*** *Block 75 of the user memory is used for the 24-bit counter feature and must be used differently. Refer to Section 8.5.3.25 "24-bit counter".*

### 8.5.3 Custom commands

The manufacturer code of NXP Semiconductors is defined in ISO/IEC 7816-6A1 [4]. The code has the value "04h".

For the structure of custom commands, refer to ISO/IEC 15693-3 [3].

Unless otherwise specified, all the address modes are supported.

#### 8.5.3.1 GET RANDOM NUMBER

**Command code = B2h**

The GET RANDOM NUMBER command is required to receive a random number from the label IC. The passwords transmitted with the SET PASSWORD, ENABLE PRIVACY and DESTROY commands must be calculated with the password and the random number (see Section 8.5.3.2 "SET PASSWORD").

The different passwords are addressed with the password identifier.

**Table 48. GET RANDOM NUMBER request format**

| SOF | Flags | GET RANDOM NUMBER | IC Mfg code | UID | CRC16 | EOF |
|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 16 bits | - |

**Table 49. GET RANDOM NUMBER response when Error_flag set**

| SOF | Flags | Error code | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 8 bits | 16 bits | - |

**Table 50. GET RANDOM NUMBER response format when Error_flag NOT set**

| SOF | Flags | Random number | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 16 bits | 16 bits | - |

### 8.5.3.2 SET PASSWORD

**Command code = B3h**

The SET PASSWORD command enables the different passwords to be transmitted to the label to access the different protected functions of the commands. If the label is powered, the SET PASSWORD command must be executed only once for the related passwords.

***Note:*** *The SET PASSWORD command can be executed only in Addressed or Selected mode except for the Privacy password. If the Privacy password is transmitted, the timing of the SET PASSWORD command is write alike. See Section 8.5.3.9 "ENABLE PRIVACY".*

The XOR password must be calculated with the password and with twice the received random number from the last GET RANDOM NUMBER command:

XOR_Password[31:0] = Password[31:0] XOR {Random_Number[15:0], Random_Number[15:0]}.

The different passwords are addressed with the password identifier.

**Table 51. SET PASSWORD request format**

| SOF | Flags | SET PASSWORD | IC Mfg code | UID | Password identifier | XOR password | CRC16 | EOF |
|---|---|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 8 bits | 32 bits | 16 bits | - |

**Table 52. Password Identifier**

| Password identifier | Password |
|---|---|
| 01h | Read |
| 02h | Write |
| 04h | Privacy |
| 08h | Destroy |
| 10h | EAS/AFI |
| 20h | Configuration memory |

**Table 53. SET PASSWORD response format when Error_flag set**

| SOF | Flags | Error code | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 8 bits | 16 bits | - |

**Table 54. SET PASSWORD response format when Error_flag NOT set**

| SOF | Flags | CRC16 | EOF |
|---|---|---|---|
| - | 8 bits | 16 bits | - |

***Note:*** *If the IC receives an invalid password, it does not execute commands like WRITE PASSWORD or LOCK PASSWORD until a Power-On Reset (POR) or RF reset.*

#### 8.5.3.3 WRITE PASSWORD

**Command code = B4h**

The WRITE PASSWORD command is used to write a new password into the related memory:

- If the related old password has already been transmitted with a SET PASSWORD command, and
- If the addressed password is not locked (see Section 8.5.3.4 "LOCK PASSWORD").

***Note:*** *The WRITE PASSWORD command can only be executed in addressed or selected mode. The new password takes effect immediately. That is, the new password must be transmitted with the SET PASSWORD command to access protected blocks/pages.*

The different passwords are addressed with the password identifier.

The timing of the command is write alike.

Option 0 (Option flag not set) is supported.

Option 1 (Option flag set) is supported.

Also, the WRITE CONFIG command to the related blocks 41-46 in the configuration memory can be used to write the passwords. See Table 9.

***Note:*** *Use diversified passwords. For the privacy passwords, use diversified passwords per application. Only use the configuration password in trusted environments.*

**Table 55. WRITE PASSWORD request format**

| SOF | Flags | WRITE PASSWORD | IC Mfg code | UID | Password identifier | Password | CRC16 | EOF |
|---|---|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 8 bits | 32 bits | 16 bits | - |

**Table 56. Password Identifier**

| Password identifier | Password |
|---|---|
| 01h | Read |
| 02h | Write |
| 04h | Privacy |
| 08h | Destroy |
| 10h | EAS/AFI |
| 20h | Configuration memory |

**Table 57. WRITE PASSWORD response format when Error_flag set**

| SOF | Flags | Error code | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 8 bits | 16 bits | - |

**Table 58. WRITE PASSWORD response format when Error_flag NOT set**

| SOF | Flags | CRC16 | EOF |
|---|---|---|---|
| - | 8 bits | 16 bits | - |

#### 8.5.3.4 LOCK PASSWORD

**Command code = B5h**

The LOCK PASSWORD command is used to lock the addressed password if the related password has been transmitted with a SET PASSWORD command already. A locked password cannot be changed.

The different passwords are addressed with the password identifier.

The timing of the command is write alike.

Option 0 (Option flag not set) is supported.

Option 1 (Option flag set) is supported.

***Note:*** *Setting the related OTP bit to 1 with the WRITE CONFIG command to blocks 26, 27 and 29 of the configuration memory also locks the passwords. See Table 9 and Table 26.*

**Table 59. LOCK PASSWORD request format**

| SOF | Flags | LOCK PASSWORD | IC Mfg code | UID | Password identifier | CRC16 | EOF |
|---|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 8 bits | 16 bits | - |

**Table 60. Password identifier**

| Password identifier | Password |
|---|---|
| 01h | Read |
| 02h | Write |
| 04h | Privacy |
| 08h | Destroy |
| 10h | EAS/AFI |
| 20h | Configuration memory |

**Table 61. LOCK PASSWORD response format when Error_flag set**

| SOF | Flags | Error code | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 8 bits | 16 bits | - |

**Table 62. LOCK PASSWORD response format when Error_flag NOT set**

| SOF | Flags | CRC16 | EOF |
|---|---|---|---|
| - | 8 bits | 16 bits | - |

#### 8.5.3.5 64-BIT PASSWORD PROTECTION

**Command code = BBh**

The 64-bit PASSWORD PROTECTION command instructs the Label IC that both the Read and Write passwords are required to get access to password-protected blocks (pages). This mode can be enabled if the Read and Write passwords have been transmitted first with a SET PASSWORD command.

If the 64-bit password protection is enabled, both passwords are required for read and write access to protected blocks (pages).

Once the 64-bit password protection is enabled, a change back to 32-bit password protection (read and write password) is not possible.

***Note:***

1. *The retransmission of the passwords is not required after the execution of the 64-bit PASSWORD PROTECTION command.*
2. *The 64-bit PASSWORD PROTECTION does not include the 16-bit counter block.*

The timing of the command is write alike.

Also, setting the OTP_PWD64_EN to 1 with a WRITE CONFIG command to block 31 in the configuration memory can enable the 64-bit PASSWORD PROTECTION. See Table 9 and Table 32.

**Table 63. 64-BIT PASSWORD PROTECTION request format**

| SOF | Flags | 64 BIT PASSWORD PROTECTION | IC Mfg code | UID | CRC16 | EOF |
|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 16 bits | - |

**Table 64. 64-BIT PASSWORD PROTECTION response format when Error_flag set**

| SOF | Flags | Error code | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 8 bits | 16 bits | - |

**Table 65. 64-BIT PASSWORD PROTECTION response format when Error_flag NOT set**

| SOF | Flags | CRC16 | EOF |
|---|---|---|---|
| - | 8 bits | 16 bits | - |

### 8.5.3.6 PROTECT PAGE

**Command code = B6h**

The PROTECT PAGE command defines the protection pointer address of the user memory. The user memory is divided into two arbitrarily sized pages. The command is used to define the access conditions for the two pages.

The protection pointer address defines the base address of the higher user memory segment Page H. All block addresses smaller than the protection pointer address are in the user memory segment Page L.

Table 66 shows an example of the user memory segmentation with the protection pointer address 20 (0x14).

**Table 66. Memory organization**

| Block | Byte 0 | Byte 1 | Byte 2 | Byte 3 | Description |
|---|---|---|---|---|---|
| 0 | | | | | Page L |
| 1 | | | | | |
| 2 | | | | | |
| : | : | : | : | : | |
| 18 | | | | | |
| 19 | | | | | |
| 20 | | | | | Page H |
| 21 | | | | | |
| : | : | : | : | : | |
| 77 | | | | | |
| 78 | | | | | |
| 79 | C0 | C1 | 0x00 | Protection | Counter |

***Note:*** *If the protection pointer address is set to block 0, the entire user memory (block 0 to block 74) is defined as Page H.*

The access conditions and the protection pointer address can be changed under the following circumstances:

- The related passwords (Read and Write password) have been transmitted first with the SET PASSWORD command.
- The page protection condition is not locked (see Section 8.5.3.7 "LOCK PAGE PROTECTION CONDITION").

The timing of the command is write alike.

**Table 67. POTECT PAGE request format**

| SOF | Flags | PROTECT PAGE | IC Mfg code | UID | Protection pointer address | Extended protection status | CRC16 | EOF |
|---|---|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 8 bits | 8 bits | 16 bits | - |

**Remark:** The label IC only accepts protection pointer address values from 0x00 (block 0) to 0x4A (block 74). Block 75 (containing the 24-bit counter) is excluded from the standard user memory password protection scheme.

***Note:*** *You can use the WRITE CONFIG command to block 20 in the configuration memory to write the protection pointer address PPC_PNTR. See Table 9).*

**Table 68. Extended Protection status byte**

| Bit | Name | Value | Description |
|---|---|---|---|
| b1 (LSB) | RL | 0 | Page L is not read protected |
| | | 1 | Page L is read protected |
| b2 | WL | 0 | Page L is not write protected |
| | | 1 | Page L is write protected |
| b3 | - | 0 | RFU |
| b4 | - | 0 | RFU |
| b5 | RH | 0 | Page H is not read protected |
| | | 1 | Page H is read protected |
| b6 | WH | 0 | Page H is not write protected |
| | | 1 | Page H is write protected |
| b7 | - | 0 | RFU |
| b8 (MSB) | - | 0 | RFU |

Also, the protection status bits can be set in the configuration memory with a WRITE CONFIG command to configure the related bits in the PPC_CTRL byte (Table 11).

**Table 69. Protection status bits definition**

| Wx | Rx | 32-bit password protection | 64-bit password protection |
|---|---|---|---|
| 0 | 0 | Public | Public |
| 0 | 1 | Read and Write protected by the Read password | Read and Write protected by the Read plus Write password |
| 1 | 0 | Write protected by the Write password | Write protected by the Read plus Write password |
| 1 | 1 | Read protected by the Read password **and** Write protected by the Read and Write password | Read and Write protected by the Read plus Write password |

**Table 70. POTECT PAGE response format when Error_flag set**

| SOF | Flags | Error code | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 8 bits | 16 bits | - |

**Table 71. POTECT PAGE response format when Error_flag NOT set**

| SOF | Flags | CRC16 | EOF |
|---|---|---|---|
| - | 8 bits | 16 bits | - |

The information about the stored settings of the protection pointer address and access conditions can be read with the GET NXP SYSTEM INFORMATION command (refer to Section 8.5.3.18 "GET NXP SYSTEM INFORMATION").

### 8.5.3.7 LOCK PAGE PROTECTION CONDITION

**Command code = B7h**

The LOCK PAGE PROTECTION CONDITION command locks the protection pointer address and the status of the page protection conditions. The Read and Write passwords must be transmitted first with the SET PASSWORD command.

The timing of the command is write alike.

Also, setting the OTP_PPC_LOCK bit to 1 with a WRITE CONFIG command to block 27 of the configuration memory can lock the protection pointer address and the status of the page protection conditions. See Table 9 and Table 24.

***Note:*** *Lock the Page Protection condition at the end of the initialization of the IC (recommendation).*

**Table 72. LOCK PAGE PROTECTION CONDITION request format**

| SOF | Flags | LOCK PAGE PROTECTION CONDITION | IC Mfg code | UID | Protection pointer address | CRC16 | EOF |
|---|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 8 bits | 16 bits | - |

***Note:*** *If the transmitted protection pointer address does not match the stored address, the label responds according to the error handling (see Section 8.6 "Error handling").*

**Table 73. LOCK PAGE PROTECTION CONDITION response format when Error_flag set**

| SOF | Flags | Error code | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 8 bits | 16 bits | - |

**Table 74. LOCK PAGE PROTECTION CONDITION response format when Error_flag NOT set**

| SOF | Flags | CRC16 | EOF |
|---|---|---|---|
| - | 8 bits | 16 bits | - |

#### 8.5.3.8 DESTROY

**Command code = B9h**

The DESTROY command is used to destroy ICODE 3 Label IC. The Destroy password must be correct. This command is irreversible and the ICODE 3 never responds to any command again.

The DESTROY command can only be executed in addressed or selected mode.

The XOR password must be calculated with the password and twice the received random number from the last GET RANDOM NUMBER command:

XOR_Password[31:0] = Password[31:0] XOR {Random_Number[15:0], Random_Number[15:0]}.

The timing of the command is write alike.

**Table 75. DESTROY request format**

| SOF | Flags | DESTROY | IC Mfg code | UID | XOR password | CRC16 | EOF |
|---|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 32 bits | 16 bits | - |

**Table 76. DESTROY response format when Error_flag set**

| SOF | Flags | Error code | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 8 bits | 16 bits | - |

**Table 77. DESTROY response format when Error_flag NOT set**

| SOF | Flags | CRC16 | EOF |
|---|---|---|---|
| - | 8 bits | 16 bits | - |

### 8.5.3.9 ENABLE PRIVACY

**Command code = BAh**

The ENABLE PRIVACY command sets the ICODE 3 Label IC to Privacy mode, if the Privacy password is correct. In the Privacy mode, the ICODE 3 is not traceable by its UID nor by the data stored in the user memory.

The two privacy modes of ICODE 3 are defined with the PRIVACY_MODE_SEL bit (see Table 34) in the configuration memory,and with the WRITE CONFIG command.

- Privacy mode 1
  In privacy mode 1, the ICODE 3 does not respond to any command except GET RANDOM NUMBER and SET PASSWORD.
- Privacy mode 2
  In privacy mode 2, the ICODE 3 responds to an Inventory command with the UID 0x E0 04 00 00 00 00 00 00.
  The IC reference in Get System Information command response is changed to 0x00.
  ICODE 3 labels in privacy mode 2 only support the following commands:
  - INVENTORY
  - SELECT
  - STAY QUIET
  - GET SYSTEM INFORMATION
  - PICK RANDOM ID
  - SET PASSWORD
  - GET RANDOM NUMBER
  - STAY QUIET PERSISTANT
  - RESET TO READY
  - READ SINGLE BLOCK
  - READ MULTIPLE BLOCKS

Read access to data from the user memory depends on the read password protection settings.

With the command PICK_RANDOM_ID (Section 8.5.3.24 "PICK RANDOM ID"), the ICODE 3 generates a random ID to respond to the inventory commands and to support the anti-collision feature. The random ID includes the CID to identify the group-key to disable the privacy mode.

The XOR password must be calculated with the password and twice the received random number from the last GET RANDOM NUMBER command:

XOR_Password[31:0] = Password[31:0] XOR {Random_Number[15:0], Random_Number[15:0]}.

To get out of the Privacy status, the valid Privacy password must be transmitted to the IC with the SET PASSWORD command.

The timing of the command is write alike.

**Table 78. ENABLE PRIVACY request format**

| SOF | Flags | ENABLE PRIVACY | IC Mfg code | UID | XOR password | CRC16 | EOF |
|---|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 32 bits | 16 bits | - |

**Table 79. ENABLE PRIVACY response format when Error_flag set**

| SOF | Flags | Error code | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 8 bits | 16 bits | - |

Table 80. ENABLE PRIVACY response format when Error_flag NOT set

| SOF | Flags | CRC16 | EOF |
|---|---|---|---|
| - | 8 bits | 16 bits | - |

### 8.5.3.10 INVENTORY READ

**Command code = A0h**

When receiving the INVENTORY READ request, the ICODE 3 IC performs the anti-collision sequence, but instead of the UID and the DSFID in the response, there are additional options.

The INVENTORY READ command generates two modes which are defined by the most significant bit of the mask length byte as follows:

- Standard mode (MSB mask length byte equal 0)
  The standard mode of the INVENTORY READ command is fully backward compatible to the ICODE SLI and ICODE SLIX ( Standard mode ).
- Extended mode (MSB mask length byte equal 1)
  The extended mode supports additional features to optimize the inventory procedure for different requirements ( Extended Mode ).

#### Standard mode

If MSB mask length byte equals 0, the INVENTORY READ command is used in the standard mode.

If the Inventory_flag is set to 1 and an error is detected, the ICODE 3 IC remains silent.

If the Option flag is set to logic 0, n blocks of data are re-transmitted. If the Option flag is set to 1, n blocks of data and the part of the UID which is not part of the mask are re-transmitted.

The request contains:

- Flags
- INVENTORY READ command code
- IC manufacturer code
- AFI (if AFI flag set)
- Mask length (most significant bit equal 0)
- Mask value (if mask length > 0)
- First block number to be read
- Number of blocks to be read
- CRC 16

Table 81. INVENTORY READ request format

| SOF | Flags | INVENTORY READ | IC Mfg code | AFI | Mask length | Mask value | First block number | Number of blocks | CRC16 | EOF |
|---|---|---|---|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 8 bits optional | 8 bits | 0 to 64 bits | 8 bits | 8 bits | 16 bits | - |

If the Inventory_flag is set to logic 1, only the tags in the READY or SELECTED state respond (same behavior as in the INVENTORY command). The meaning of flags 5 to 8 is in accordance with table 5 in ISO/IEC 15693-3 [3].

The INVENTORY READ command can be transmitted also in the addressed or selected mode ( Addressed and selected mode ).

The number of blocks in the request is one less than the number of blocks that the ICODE 3 IC returns in the response.

If the Option flag in the request is set to logic 0 the response contains:

**Table 82. INVENTORY READ response format: Option flag logic 0**

| SOF | Flags | Data | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | Block length | 16 bits | - |
| | | Repeated as needed | | |

The ICODE 3 IC reads the requested block(s) and sends back their value in the response. The mechanism and timing of the INVENTORY READ command are similar to the INVENTORY command described in clause 8 of ISO/IEC 15693-3.

If the Option flag in the request is set to logic 1, the response contains:

**Table 83. INVENTORY READ response format: Option flag logic 1**

| SOF | Flags | Rest of UID which is not part of the mask and slot number | Data | CRC16 | EOF |
|---|---|---|---|---|---|
| - | 8 bits | 0 to 64 bit | Block length | 16 bits | - |
| | | Multiple of 8 bits | Repeated as needed | | |

The ICODE 3 IC reads the requested block(s) and sends back their value in the response. The bytes of the UID, which are not parts of the mask, and the slot number in case of 16 slots, are returned. Instead of padding with zeros up to the next byte boundary, the corresponding bits of the UID are returned. The mechanism and timing of the INVENTORY READ command are similar to the INVENTORY command described in clause 8 of ISO/IEC 15693-3.

***Note:*** *The number of bits of the re-transmitted UID are calculated as:*

- *16 slots: 60 bits (bit 64 to bit 4) - mask length rounded up to the next byte boundary*
- *1 slot: 64 bits - mask length rounded up to the next byte boundary*

If the sum of the first block number and number of blocks exceeds the total number available user blocks, the number of transmitted blocks is less than the requested number of blocks. The last returned block is the highest available user block, followed by the 16-bit CRC and the EOF.

**Example**: mask length = 30 bits

Returned: bit 64 to bit 4 (30 bits) = 30 gives 4 bytes

**Table 84. Example: mask length = 30**

| Byte 0 | Byte 1 | Byte 2 | Byte 3 | Byte 4 | Byte 5 | Byte 6 | Byte 7 | UID |
|---|---|---|---|---|---|---|---|---|
| mask value including padding with zeros | | | | - | | | | transmitted by interrogator |
| | | | | returned value | | | | transmitted by ICODE 3 IC |

### Extended Mode

If the most significant bit of the Mask Length byte is equal to 1, the response format is defined by the extended option byte.

The request contains:

- Flags
- Inventory Read command code
- IC Manufacturer code
- AFI (if the AFI flag is set)
- Mask length (most significant bit equal 1)
- Extended Options
- Mask value (if mask length > 0)
- First Block Number, if specified in extended options byte
- Number of Blocks, if specified in extended options byte
- CRC 16

**Table 85. Inventory Read (extended mode) request format**

| SOF | Flags | Inventory Read | IC Mfr. code | AFI | Mask Length | ext. Options | opt. CID | Mask Value | First block number | Number of blocks | CRC 16 | EOF |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 8 bits | 8 bits | 8 bits | 8 bits optional | 8 bits MSB = 1 | 8 bits | 16 bits | 0 to 64 bits | 8 bits optional | 8 bits optional | 8 bits | |

If the Inventory_flag is set to logic 1, only tags in the READY or SELECTED state respond (similar behavior as INVENTORY command). The meaning of flags 5 to 8 is in accordance with table 5 in ISO/IEC 15693-3 [3].

The INVENTORY READ command can be transmitted in the addressed or selected mode also ( Addressed and selected mode ).

**Table 86. Extended options**

| Bit number | Bit name | Value | Feature |
|---|---|---|---|
| 1 (LSB) | EAS_MODE | 0 | Label responds independent from the EAS status |
| | | 1 | Only labels will respond which have the EAS enabled |
| 2 | UID_MODE | 0 | UID will be transmitted as in regular mode (truncated reply depending on least significant 7 bits value of mask length and the mask value) |
| | | 1 | Complete UID will be transmitted (independent from mask length) |
| 3 | CID_COMPARE | 0 | No CID is transmitted in the command |
| | | 1 | 16 bit CIDwill be transmitted in the command and only labels with the same CID will respond |
| 4 | CID_RESPONSE | 0 | CID will NOT be transmitted in the response from the label |
| | | 1 | CID will be transmitted in the response from the label |
| 5 | SKIP_DATA | 0 | Tag will add the user memory blocks in the response as requested with first block number byte and number of blocks byte in the command |
| | | 1 | No user memory data are requested from the tag, first block number byte and number of blocks byte shall not be transmitted in the command |
| 6 | QUIET | 0 | refer to Table 87 |

**Table 86. Extended options**...*continued*

| Bit number | Bit name | Value | Feature |
|---|---|---|---|
| 7 | PERSISTENT QUIET | 0 | refer to Table 87 |
| 8 (MSB) | - | **0** | **RFU** |

**Table 87. QUIET and PERSISTANT QUIET bit in Extended options**

| QUIET bit [6] | PERSISTENT QUIET bit [7] | Feature |
|---|---|---|
| 0 | 0 | remain in current state |
| 1 | 0 | go to Quiet State after response (refer to Section 8.5.1.2 "STAY QUIET") |
| 0 | 1 | go to Persistent Quiet State after Response (refer to Section 8.5.3.19 "STAY QUIET PERSISTENT") |
| 1 | 1 | only tags in the PERSISTENT QUIET state will respond to the command |

If the option flag in the request is set to 1, the response contains the truncated or the complete UID depending on the extended option flag 2.

If the option flag in the request is set to 0, the UID is not part of the response.

**Table 88. Inventory Read (extended mode) response format: Option flag logic 1**

| SOF | Flags | Optional CID | Optional truncated UID OR complete UID | Optional data | CRC16 | EOF |
|---|---|---|---|---|---|---|
| - | 8 bits | 16 bits | 0 to 64 bit | Block length | 16 bits | - |
| | | | Multiple of 8 bits | Repeated as needed | | |

The mechanism and timing of the INVENTORY READ command are similar to the INVENTORY command described in clause 8 of ISO/IEC 15693-3.

If the UID is requested in the truncated format, the re-transmitted UID can be calculated as follows:

16 slots: 64 - 4 - mask length rounded up to the next byte boundary

1 slot: 64 - mask length rounded up to the next byte boundary

**Example**: mask length = 30

Returned: 64 - 4 - 30 = 30 gives 4 bytes

**Table 89. Example**

| Byte 0 | Byte 1 | Byte 2 | Byte 3 | Byte 4 | Byte 5 | Byte 6 | Byte 7 | UID |
|---|---|---|---|---|---|---|---|---|
| mask value incl. padding with zeros | | | | | | | | transmitted by Interrogator |
| | | | | returned value | | | | transmitted by ICODE 3 IC |

### Addressed and selected mode

The INVENTORY READ command can be transmitted also in the addressed or selected mode. In this case, the Inventory_flag is set to 0, and the meaning of flags 5 to 8 is in accordance with table 4 in ISO/IEC 15693-3 [3].

In the addressed or selected mode, the INVENTORY READ command behaves like a READ or READ MULTIPLE BLOCK command.

In the addressed mode, it is recommended to address the label IC with a mask length of 64 and to transmit the complete UID in the mask value field.

In the selected mode (label IC has been selected with a valid SELECT command before), it is recommended to address the label IC with a mask length of 0 (and do not transmit the mask value field).

***Note:*** *If the INVENTORY READ command is used in the addressed mode or in the selected mode, the AFI is not transmitted. The label IC only responds in the first-time slot.*

### 8.5.3.11 FAST INVENTORY READ

**Command code = A1h**

When receiving the FAST INVENTORY READ command, the ICODE 3 IC response is the same as with the INVENTORY READ command. Exceptions are:

- The data rate from the ICODE 3 IC to the interrogator is twice the data rate defined in ISO/IEC 15693-3. The rate depends on the Datarate_flag 53 kbit (high data rate) or 13 kbit (low data rate).
- The data rate from the interrogator to the ICODE 3 IC, and the time between the rising edge of the EOF from the interrogator to the ICODE 3 IC remain unchanged. That is, same as defined in ISO/IEC 15693-3.
- In the direction of ICODE 3 IC to the interrogator, only the single subcarrier mode is supported.

### 8.5.3.12 SET EAS

**Command code = A2h**

The SET EAS command enables the EAS mode, if the EAS mode is not locked. If the EAS mode is password protected, the EAS password must be transmitted first with the SET PASSWORD command.

The timing of the command is write alike.

Option 0 (Option flag not set) is supported.

Option 1 (Option flag set) is supported.

**Table 90. SET EAS request format**

| SOF | Flags | SET EAS | IC Mfg code | UID | CRC16 | EOF |
|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 16 bits | - |

**Table 91. SET EAS response format when Error_flag set**

| SOF | Flags | Error code | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 8 bits | 16 bits | - |

**Table 92. SET EAS response format when Error_flag NOT set**

| SOF | Flags | CRC16 | EOF |
|---|---|---|---|
| - | 8 bits | 16 bits | - |

### 8.5.3.13 RESET EAS

**Command code = A3h**

If the EAS mode is not locked, the RESET EAS command disables the EAS mode. If the EAS mode is password protected, the EAS password must be transmitted first with the SET PASSWORD command.

The timing of the command is write alike.

Option 0 (Option flag not set) is supported.

Option 1 (Option flag set) is supported.

**Table 93. RESET EAS request format**

| SOF | Flags | RESET EAS | IC Mfg code | UID | CRC16 | EOF |
|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 16 bits | - |

**Table 94. RESET EAS response format when Error_flag set**

| SOF | Flags | Error code | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 8 bits | 16 bits | - |

**Table 95. RESET EAS response format when Error_flag NOT set**

| SOF | Flags | CRC16 | EOF |
|---|---|---|---|
| - | 8 bits | 16 bits | - |

### 8.5.3.14 LOCK EAS

**Command code = A4h**

The LOCK EAS command locks the current state of the EAS mode and the EAS ID. If the EAS mode is password protected, the EAS password must be transmitted first with the SET PASSWORD command.

The timing of the command is write alike.

Option 0 (Option flag not set) is supported.

Option 1 (Option flag set) is supported.

Setting the OTP_EAS_LOCK bit to 1 with a WRITE CONFIG command to block 30 of the configuration memory also locks the EAS mode and the EAS ID. See Table 9 and Table 30.

**Table 96. LOCK EAS request format**

| SOF | Flags | LOCK EAS | IC Mfg code | UID | CRC16 | EOF |
|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 16 bits | - |

**Table 97. LOCK EAS response format when Error_flag set**

| SOF | Flags | Error code | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 8 bits | 16 bits | - |

**Table 98. LOCK EAS response format when Error_flag NOT set**

| SOF | Flags | CRC16 | EOF |
|---|---|---|---|
| - | 8 bits | 16 bits | - |

### 8.5.3.15 EAS ALARM

**Command code = A5h**

The EAS ALARM command can be used in the following configurations:

- Option flag is set to 0:
  EAS ID mask length and the EAS ID value are not transmitted.
  If the EAS mode is enabled, the EAS response is returned from the ICODE 3 IC.
- Option flag is set to 1:
  Within the command, the EAS ID mask length must be transmitted to identify how many bits of the following EAS ID value are valid (multiple of 8 bits). If the EAS Mode is set, the ICODE 3 TagTamper ICs respond. The response includes the EAS sequence corresponding to the data in the EAS ID configuration (selective EAS). If the EAS ID mask length is set to 0, the ICODE 3 IC responds with its EAS ID.

**Table 99. EAS ALARM Request format**

| SOF | Flags | EAS ALARM | IC Mfg code | UID | EAS ID mask length | EAS ID value | CRC16 | EOF |
|---|---|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 8 bits optional | 0, 8 or 16 bits optional | 16 bits | - |

If an error is detected, the ICODE 3 IC remains silent.

Option flag is set to logic 0 or Option flag is set to logic 1 and the EAS ID mask length is not equal to 0:

**Table 100. EAS ALARM Response format (Option flag logic 0)**

| SOF | Flags | EAS sequence | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 256 bits | 16 bits | - |

EAS sequence (starting with the LSB, which is transmitted first; read from left to right):

```
11110100  11001101  01000110  00001110  10101011  11100101  00001001  11111110
00010111  10001101  00000001  00011100  01001011  10000001  10010010  01101110
01000001  01011011  01011001  01100001  11110110  11110101  11010001  00001101
10001111  00111001  10001011  01001000  10100101  01001110  11101100  11110111
```

Option flag is set to logic 1 and the EAS ID mask length is equal to 0:

**Table 101. EAS ALARM Response format (Option flag logic 1)**

| SOF | Flags | EAS ID value | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 16 bits | 16 bits | - |

If the EAS mode is disabled, the ICODE 3 IC remains silent. See RESET EAS command in Section 8.5.3.13 "RESET EAS".

***Note:*** *Labels in the QUIET state do not respond to an EAS ALARM command except if the addressed flag is set. Labels in the PERSISTANT QUIET mode respond even if the addressed flag is not set (refer to Section 8.4 "State diagram").*

### 8.5.3.16 PASSWORD PROTECT EAS/AFI

**Command code = A6h**

The PASSWORD PROTECT EAS/AFI command enables the password protection for EAS and/or AFI. The EAS/AFI password must be transmitted first with the SET PASSWORD command.

Option flag set to logic 0: EAS is password protected.

Option flag set to logic 1: AFI is password protected.

Both password protections (AFI and EAS) can be enabled separately.

***Note:*** *Independent of the Option flag, the write-alike command is executed like a write command with Option flag 0. That is, option flag not set.*

Once the EAS/AFI password protection is enabled, it is not possible to change back to unprotected EAS and/or AFI.

The timing of the command is write alike (as write command with Option flag 0).

The password protection for EAS and/or AFI can be enabled also with a WRITE CONFIG command to set the following bits set to 1 in the configuration memory:

OTP_EAS_PWD_EN bit in block 29: EAS is password protected.

OTP_AFI_PWD_EN bit in block 28: AFI is password protected.

***Note:*** *To avoid the unauthorized change of the EAS and AFI settings, password protect the EAS and AFI functionality.*

**Table 102. PASSWORD PROTECT EAS/AFI request format**

| SOF | Flags | PASSWORD PROTECT EAS/AFI | IC Mfg code | UID | CRC16 | EOF |
|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 16 bits | - |

**Table 103. PASSWORD PROTECT EAS/AFI response format when Error_flag set**

| SOF | Flags | Error code | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 8 bits | 16 bits | - |

**Table 104. PASSWORD PROTECT EAS/AFI response format when Error_flag NOT set**

| SOF | Flags | CRC16 | EOF |
|---|---|---|---|
| - | 8 bits | 16 bits | - |

### 8.5.3.17 WRITE EAS ID

**Command code = A7h**

The command WRITE EAS ID stores a new EAS Identifier in the corresponding configuration memory. If EAS is password protected (for Set and Reset EAS) the EAS password must be transmitted first with the SET PASSWORD command.

The timing of the command is write alike.

Option 1 (Option flag set) is supported.

Option 0 (Option flag not set) is supported.

Also, a WRITE CONFIG command to block 18 of the configuration memory can write the EAS ID. See Table 9.

**Table 105. WRITE EAS ID request format**

| SOF | Flags | WRITE EAS ID | IC Mfg code | UID | EAS ID value | CRC16 | EOF |
|---|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 16 bits | 16 bits | - |

**Table 106. WRITE EAS ID response format when Error_flag set**

| SOF | Flags | Error code | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 8 bits | 16 bits | - |

**Table 107. WRITE EAS ID response format when Error_flag NOT set**

| SOF | Flags | CRC16 | EOF |
|---|---|---|---|
| - | 8 bits | 16 bits | - |

### 8.5.3.18 GET NXP SYSTEM INFORMATION

**Command code = ABh**

The command GET NXP SYSTEM INFORMATION command is used to get information about the IC access conditions and supported features.

**Table 108. GET NXP SYSTEM INFORMATION request format**

| SOF | Flags | Get NXP System Info | IC Mfg code | UID | CRC16 | EOF |
|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 16 bits | - |

**Table 109. GET NXP SYSTEM INFORMATION response format when Error_flag set**

| SOF | Flags | Error code | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 8 bits | 16 bits | - |

**Table 110. GET NXP SYSTEM INFORMATION response format when Error_flag NOT set**

| SOF | Flags | PP pointer | PP conditions | Lock bits | Feature flags | CRC16 | EOF |
|---|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 8 bits | 32 bits | 16 bits | - |

On a valid received command, the label IC responds with the following information:

- Actual protection pointer address (PP pointer)
- Actual protection conditions for the password protection (PP conditions)
- Actual lock bits settings (Lock bits)
- Supported commands and features (Feature flags)

The bit values value in Table 113 indicate if the related feature is enabled or disabled:

- 0: feature disabled
- 1: feature enabled

**Table 111. PP conditions bits**

| Bit | Name | Feature |
|---|---|---|
| 1 (LSB) | RL | Page L read password protection status |
| 2 | WL | Page L write password protection status |
| 3-4 | - | RFU |
| 5 | RH | Page H read password protection status |
| 6 | WH | Page H write password protection status |
| 7-8 (MSB) | - | RFU |

**Table 112. Lock bits**

| Bit | Name | Feature |
|---|---|---|
| 1 (LSB) | AFI | AFI lock bit |
| 2 | EAS | EAS lock bit |
| 3 | DSFID | DSFID lock bit |
| 4 | PPL | Password protection pointer address and access conditions lock bit |
| 5-8 (MSB) | - | RFU |

**Table 113. Feature flags bits**

| Bit | Name | Feature |
|---|---|---|
| 1 (LSB) | UM PP | User memory password protection supported (refer to Section 8.5.3.6 "PROTECT PAGE") |
| 2 | COUNTER | Counter feature supported |
| 3 | EAS ID | EAS ID supported by EAS ALARM command (refer to Section 8.5.3.17 "WRITE EAS ID") |
| 4 | EAS PP | EAS password protection supported (refer to Section 8.5.3.16 "PASSWORD PROTECT EAS/AFI") |
| 5 | AFI PP | AFI password protection supported (refer to Section 8.5.3.16 "PASSWORD PROTECT EAS/AFI") |
| 6 | INVENTORY READ EXT | Extended mode supported by INVENTORY READ command (refer to Section 8.5.3.10 "INVENTORY READ") |
| 7 | EAS IR | EAS selection supported by extended mode in INVENTORY READ command (refer to Section 8.5.3.10 "INVENTORY READ") |
| 8 | CID | Customer ID (CID) supported |
| 9 | ORIGINALITY SIG | READ SIGNATURE command supported (refer to Section 8.5.3.20 "READ SIGNATURE") |
| 10 | TAGTAMPER | TagTamper feature supported (refer to Section 8.2.3.2 "TagTamper feature (SL2S3003TT)") |
| 11 | P QUIET | STAY QUIET PERSISTENT command supported (refer to Section 8.5.3.19) |
| 12 | NFC MIRROR | NFC mirror feature supported (refer to Section 8.2.3.3 "NFC ASCII mirror feature") |
| 13 | PRIVACY | ENABLE PRIVACY command supported (refer to Section 8.5.3.9 "ENABLE PRIVACY") |
| 14 | DESTROY | DESTROY command supported (refer to Section 8.5.3.8 "DESTROY") |
| 15 | WRITE CID | Programming of the Customer ID (CID) supported |
| 16 | HIGH DATA RATES | High data rates are supported (refer to Section 8.5.2.13 "FAST READ MULTIPLE BLOCK" |
| 17 - 31 | - | RFU |
| 32 (MSB) | EXT | Additional 32 bits feature flags are transmitted |

### 8.5.3.19 STAY QUIET PERSISTENT

**Command code = BCh**

When receiving the STAY QUIET PERSISTENT command, the label IC enters the persistent quiet state and does not send back a response.

***Note:*** *The STAY QUIET PERSISTENT command has the same behavior as the mandatory STAY QUIET command. The only difference is at reset (power off). If the power off time exceeds the persistent time, the label IC switches to the ready state,.*

When in PERSISTENT QUIET state:

- The label IC does not process any request where the Inventory_flag is set, except:
  - If the AFI_flag is set, or
  - If the QUIET and PERSTENT QUIET flags in the extended mode of the (Fast) Inventory command are both set.
- The label IC processes any EAS ALARM request, and any addressed or selected request.

The label IC exits the persistent quiet state when:

- Reset (power off) exceeds the persistent time.
- Receiving a SELECT request. The IC goes to the Selected state.
- Receiving a RESET TO READY request. The IC goes to the Ready state.

The STAY QUIET PERSISTENT command must be executed in addressed mode (Select_flag is set to 0 and Address_flag is set to 1).

**Table 114. STAY PERSISTENT QUIET request format**

| SOF | Flags | STAY QUIET PERSISTENT | IC Mfg code | UID | CRC16 | EOF |
|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 16 bits | |

### 8.5.3.20 READ SIGNATURE

**Command code = BDh**

The READ SIGNATURE command returns an IC specific 32-byte or 48-byte ECC signature, to verify NXP Semiconductors as the silicon vendor. The signature length is defined with the OS_CFG_MODE bit (Table 40).

The originality signature can also be read with a READ CONFIG command to

- blocks 0-7 if the 32 byte signature length is enabled or
- block 0-11 if the 48 byte signature length is enabled.

**Table 115. READ SIGNATURE request format**

| SOF | Flags | READ SIG NATURE | IC Mfg code | UID | CRC16 | EOF |
|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 16 bits | |

**Table 116. READ SIGNATURE response format when Error_flag set**

| SOF | Flags | Error code | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 8 bits | 16 bits | - |

**Table 117. READ SIGNATURE response format when Error_flag NOT set**

| SOF | Flags | Originality Signature | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 256 or 384 bits | 16 bits | - |

Details on how to check the signature value will be provided in the application note *ICODE 3 Originality Signature Validation*. Thew document will describe how to verify the originality of ICODE 3.

### 8.5.3.21 READ CONFIG

**Command code = C0h**

The READ CONFIG command reads the requested number of blocks (n-1). The reading starts with the first block defined by the block address of the configuration memory.

Access to the configuration blocks depends on the status and definition of the related block within the configuration memory (see Section 8.2.3 "Configuration memory").

If one of the requested configuration blocks is not accessible due to the actual status, the ICODE 3 responds with Error_flag set (see Table 119).

Within one command execution, a READ_CONFIG command can read one or multiple blocks of the following areas of the configuration memory:

- Block 0 to block 127
- Passwords cannot be read and are masked with 0x00 in the response
  Block 41: CFG_PWD (Configuration password)
  Block 42: READ_PWD (Read password
  Block 43: WRITE_PWD (Write password)
  Block 44: PRIVACY_PWD (Privacy password)
  Block 45: DESTROY_PWD (Destroy password
  Block 46: EASAFI_PWD (EAS/AFI password)

Block 47 (TT_OPEN_MSG) can only be read if it is not write-locked with the OTP_TT_OPEN_MSG_LOCK bit (see Table 32) otherwise it is locked with all bytes 0x00.

Option 0 (Option flag not set) is supported.

Option 1 (Option flag set) is not supported.

**Table 118. READ CONFIG request format**

| SOF | Flags | READ_CONFIG | IC Mfg code | UID | Block Address | Number of Blocks | CRC16 | EOF |
|---|---|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 8 bits | 8 bits | 16 bits | - |

**Table 119. READ CONFIG response format when Error_flag set**

| SOF | Flags | Error code | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 8 bits | 16 bits | - |

**Table 120. READ_CONFIG response format when Error_flag NOT set**

| SOF | Flags | Data | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 32 bits repeated as needed | 16 bits | - |

### 8.5.3.22 WRITE CONFIG

**Command code = C1h**

The WRITE_CONFIG command writes the 4-byte data to the requested block address of the configuration memory.

Access to the configuration blocks depends on the status and definition of the related block within the configuration memory (see Section 8.2.3 "Configuration memory").

If the configuration memory is password protected, write access is only possible after the valid authentication with the SET PASSWORD command with the Configuration password.

If the requested configuration block is not write accessible due to the actual status, the ICODE 3 responds with Error_flag set (Table 122).

If the Configuration memory is write-locked with the OTP_CFG_LOCK bit (see Table 29), ICODE 3 responds with Error_flag set.

The timing of the command is write alike.

Option 1 (Option flag set) is supported.

Option 0 (Option flag not set) is supported.

**Table 121. WRITE_CONFIG request format**

| SOF | Flags | WRITE_CONFIG | IC Mfg code | UID | Block Address | Data | CRC16 | EOF |
|---|---|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 8 bits | 32 bits | 16 bits | - |

**Table 122. WRITE_CONFIG response format when Error_flag set**

| SOF | Flags | Error code | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 8 bits | 16 bits | - |

**Table 123. WRITE_CONFIG response format when Error_flag NOT set**

| SOF | Flags | CRC16 | EOF |
|---|---|---|---|
| - | 8 bits | 16 bits | - |

### 8.5.3.23 READ TT

**Command code = C4h**

The READ TT command is only supported by the ICODE 3 TagTamper (SL2S3003TT).

The READ TT command provides the information about the TagTamper status. The status is detected when the label IC is powered by an RF field. The response on The READ TT includes:

- One byte about the actual status of the TagTamper wire detected at start-up, and
- One byte with the stored TagTamper Status depending whether the OTP_TT_EN bit has been set or not, and if a previous TagTamper event has been detected.

Option 0 (Option flag not set) is supported.

**Table 124. READ TT request format**

| SOF | Flags | READ TT | IC Mfg code | UID | CRC16 | EOF |
|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 16 bits | - |

**Table 125. READ TT response format when Error_flag set**

| SOF | Flags | Error code | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 8 bits | 16 bits | - |

**Table 126. READ TT response format when Error_flag NOT set**

| SOF | Flags | Actual TT Status | Stored TT Status | CRC16 | EOF |
|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bit | 16 bits | - |

For the the details on the Actual and Stored TT Status byte refer to Table 127.

**Table 127. Actual and Stored TagTamper Status response status bytes**

| Byte | ASCII | Actual TT Status | Stored TT STAUS |
|---|---|---|---|
| 0x4F | 'O' | Open | Open |
| 0x43 | 'C' | Closed | Closed |
| 0x49 | 'I' | Invalid | - |
| 0x45 | 'E' | - | Storing of the internal Stored TagTamper Status failed during startup (at the first detected open TagTamper event at startup) |
| 0x30 | '0' | Show Actual TagTamper Status is not enabled by the TT_SHOW_STATUS bits | Store TagTamper Status is not enabled with the OTP_TT_EN or show Stored Tag Tamper Status is not enabled by the TT_ SHOW_STATUS bits |

### 8.5.3.24 PICK RANDOM ID

**Command code = C2h**

The PICK RANDOM ID instructs an ICODE 3 in privacy mode to generate a random ID. After a valid PICK RANDOM ID command, the ICODE 3 responds with the random ID to INVENTORY commands or to Get System Information command, until a power-on reset.

Option 0 (Option flag not set) is supported.

Option 1 (Option flag set) not is supported.

**Table 128. PICK_RANDOM_ID request format**

| SOF | Flags | PICK_RANDOM_ID | IC Mfg code | UID | CRC16 | EOF |
|---|---|---|---|---|---|---|
| - | 8 bits | 8 bits | 8 bits | 64 bits optional | 16 bits | - |

**Table 129. PICK_RANDOM_ID response format when Error_flag set**

| SOF | Flags | Error code | CRC16 | EOF |
|---|---|---|---|---|
| - | 8 bits | 8 bits | 16 bits | - |

**Table 130. PICK_RANDOM_ID response format when Error_flag NOT set**

| SOF | Flags | CRC16 | EOF |
|---|---|---|---|
| - | 8 bits | 16 bits | - |

After a successful PICK_RANDOM_ID, the ICODE 3 responds to an INVENTORY command with a random ID defined in Table 131.

**Table 131. Random ID**

| MSB | | | | | | | LSB |
|---|---|---|---|---|---|---|---|
| **64:57** | **56:49** | **48:41** | **40:33** | **32:25** | **24:17** | **16:1** | |
| "E0" | "04" | "00" | "00" | CID_1 | CID_0 | 16-bit random ID | |
| RID 7 | RID 6 | RID 5 | RID 4 | RID 3 | RID 2 | RID 1 | RID 0 |

### 8.5.3.25 24-bit counter

Block 75 of the user memory contains the 24-bit counter. The block can be accessed with the standard READ and WRITE commands but special data considerations are required.

The standard password protection mechanisms for the user memory are not valid for block 75.

The 24-bit counter (block 75) can be:

- Read.
- Increased by one with the option of read password protection.
- Preset to the initial start value with the write password protection.

The counter can be read with any read command including block 75. The 4-byte data from block 75 provide the following information:

**Table 132. COUNTER BLOCK data structure**

| Byte | Name | Value | Description |
|---|---|---|---|
| 0 | C0 | 0x00 - 0xFF | LSB of the counter value |
| 1 | C1 | 0x00 - 0xFF | — |
| 2 | C2 | 0x00 - 0xFF | MSB of the counter value |
| 3 | PROT | 0x00 | Incrementing of the counter value is not password protected |
| | | 0x01 | Incrementing of the counter value is protect with the read password |

The counter can be preset to a start value with a WRITE SINGLE BLOCK command to block 75. As the counter preset is password protected with the write password, a SET PASSWORD command with the write password is required before executing the Preset (refer to Section 8.5.3.2 "SET PASSWORD").

The PROT byte (data byte 3) value defines whether the password protection to increment the counter is enabled or disabled. If the password protection is enabled, the read password is required to increment the counter value.

The data for the WRITE SINGLE BLOCK command to preset the counter are defined in Table 133.

***Note:*** *The Preset counter value of 0x0001 is not possible. A WRITE SINGLE BLOCK command with 0x0001 value only increments the counter.*

**Table 133. Preset counter data structure**

| Byte | Name | Value | Description |
|---|---|---|---|
| 0 | C0 | 0x00, 0x02 - 0xFF | LSB of the counter value |
| 1 | C1 | 0x00 - 0xFF | — |
| 2 | C2 | 0x00 - 0xFF | MSB of the counter value |
| 3 | PROT | 0x00 | Disable the password protection to increment the counter |
| | | 0x01 | Enable the password protection to increment the counter with read password |

To increment the counter by one with a WRITE SINGLE BLOCK command to block 75. If the password protection to increment the counter is enabled, the read password needs to be transmitted to the label IC with the SET PASSWORD command before (refer to Section 8.5.3.2 "SET PASSWORD").

The data for the WRITE SINGLE BLOCK command to increment the counter are defined in Table 133.

***Note:*** *The counter can be incremented only with the C0, C1 and C2 values defined in Table 134. If the write password has been transmitted earlier with a SET PASSWORD command, the other values preset the counter or lead to an error message.*

**Table 134. Increment counter by 1 data structure**

| Byte | Name | Value | Description |
|---|---|---|---|
| 0 | C0 | 0x01 | LSB of the counter value |
| 1 | C1 | 0x00 | — |
| 2 | C2 | 0x00 | MSB of the counter value |
| 3 | PROT | 0x00 | PROT value of 0x00 only accepts incrementing by 1 |

To increment the counter by up to 255 (0xFF), issue a WRITE SINGLE BLOCK command to block 75. If the password protection to increment the counter is enabled, the read password must be transmitted to the label IC with the SET PASSWORD command first (refer to Section 8.5.3.2 "SET PASSWORD").

The data for the WRITE SINGLE BLOCK command to increment the counter are defined in Table 133.

***Note:*** *The counter can be incremented only with the C0, C1 and C2 values defined in Table 134. If the write password has been transmitted earlier with a SET PASSWORD command, the other values preset the counter or lead to an error message.*

**Table 135. Increment counter by up to 0xFF data structure**

| Byte | Name | Value | Description |
|---|---|---|---|
| 0 | C0 | 0x01 - 0xFF | LSB of the counter value |
| 1 | C1 | 0x00 | |
| 2 | C2 | 0x00 | MSB of the counter value |
| 3 | PROT | 0x80 | PROT value of 0x80 allows incrementing from 0x01 up to 0xFF |

## 8.6 Error handling

### 8.6.1 Transmission errors

In compliance with ISO/IEC 15693[1], the label IC does not respond if a transmission error is detected. Examples of transmission errors are CRC, bit coding, bit count, or wrong framing. The device waits for the next correct received command.

### 8.6.2 Commands not supported or options

If the received command or option is not supported, the behavior of the label IC depends on the addressing mechanism.

#### 8.6.2.1 Non-addressed Mode

The label IC remains silent.

#### 8.6.2.2 Addressed or Selected Mode

In addressed mode or in selected mode, the label IC responds with the error code "0Fh" (error with no information given or error code is not supported).

If the Inventory flag or the Protocol Extension flag is set, the label IC does not respond if the command or option is not supported.

### 8.6.3 Parameter out of range

#### 8.6.3.1 Read commands

If the sum of the first block number and the number of blocks exceeds the total number of available user blocks, the number of transmitted blocks is less than the requested number of blocks. The last returned block is the highest available user block, followed by the 16-bit CRC and the EOF.

#### 8.6.3.2 Write and lock commands

If the address of a block to be written does not exist, or if a block to be written is locked, the behavior of the label IC depends on the addressing mechanism.

**Non-addressed Mode**

- The label IC remains silent and aborts the command without writing anything.

**Addressed Mode or Selected Mode**

- The addressed or selected label IC responds with the error code "0Fh" (error with no information given or error code is not supported).

## 8.7 Data integrity

The following mechanisms ensure the reliable transmission of data between the interrogator and label IC:

- 16-bit CRC per block
- Bit count checking
- Bit coding to distinguish between logic 1, logic 0, and no information
- Channel monitoring (protocol sequence and bit stream analysis)

## 8.8 RF interface

The definition of the RF interface is according to the standard ISO/IEC 15693-2 [2] and ISO/IEC 15693-3 [3].

# 9 Limiting values

**Table 136. Limiting values (Wafer)[1][2]**

*In accordance with the Absolute Maximum Rating System (IEC 60134).*

| Symbol | Parameter | Conditions | | Min | Max | Unit |
|---|---|---|---|---|---|---|
| $T_{stg}$ | storage temperature | | | -55 | +125 | °C |
| $P_{tot}$ | total power dissipation | | | - | 125 | mW |
| $T_j$ | junction temperature | | | -40 [3] | +105 | °C |
| $I_{i(max)}$ | maximum input current | LA to LB; peak | [4] | - | ±60 | mA |
| $I_I$ | input current | LA to LB; RMS | | - | 30 | mA |
| $V_{ind}$ | maximum induced voltage (for SL2S3003TT only) | DP | | - | 0.5 | V |
| $V_{ESD}$ | electrostatic discharge voltage | human body model (HBM) [5] | [6] | - | ±2 | kV |

1. Stresses above 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 conditions other than those described in the operating conditions and electrical characteristics sections of this specification is not implied.
2. This product includes circuitry specifically designed for the protection of its internal devices from the damaging effects of excessive static charge. Nonetheless, it is suggested that conventional precautions be taken to avoid applying greater than the rated maxima.
3. Under extreme conditions (negative temperatures and tag stays a long time at the maximum operating range) the use of HF Resets is recommended.
4. The voltage between LA and LB is limited by the on-chip voltage limitation circuitry (corresponding to parameter $I_I$).
5. According to ANSI/ESDA/JEDEC JS-001.
6. For ESD measurement, the IC was mounted in a SO28 package.

**CAUTION**

This device is sensitive to ElectroStatic Discharge (ESD). Observe precautions for handling electrostatic sensitive devices.

Such precautions are described in the *ANSI/ESD S20.20, IEC/ST 61340-5, JESD625-A* or equivalent standards.

# 10 Characteristics

## 10.1 Wafer memory characteristics

**Table 137. Wafer EEPROM characteristics**

| Symbol | Parameter | Conditions | Min | Typ | Max | Unit |
|---|---|---|---|---|---|---|
| $t_{ret}$ | retention time | $T_{amb} \leq 55$ °C | 50 | - | - | year |
| $N_{endu(W)}$ | write endurance | — | 100000 | - | - | cycle |

## 10.2 Interface characteristics

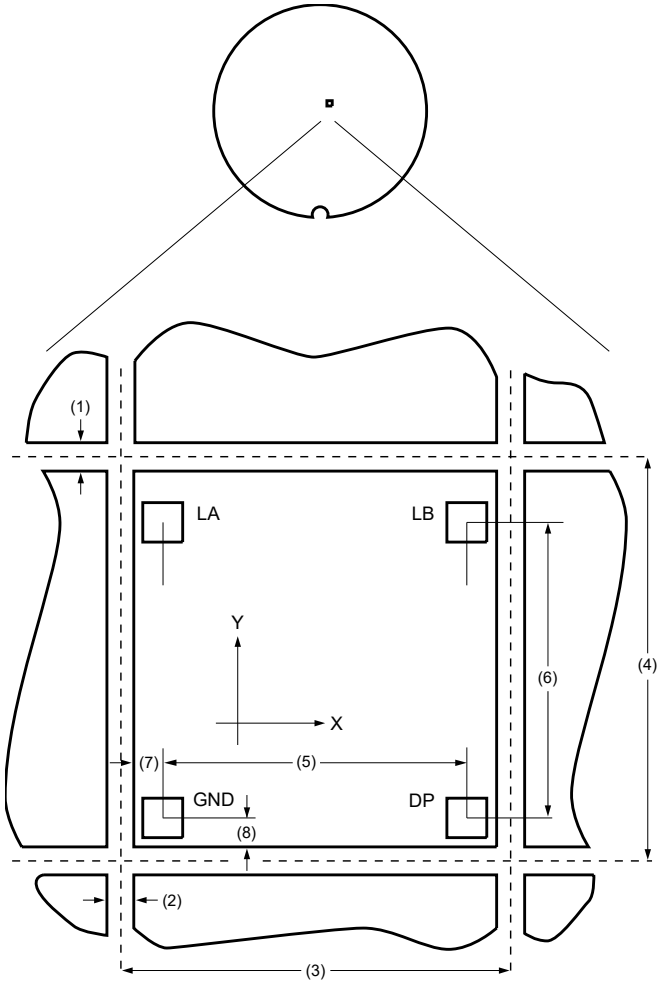
**Table 138. Interface characteristics**

*Typical ratings are not guaranteed. The values listed are at room temperature.*

| Symbol | Parameter | Conditions | | Min | Typ | Max | Unit |
|---|---|---|---|---|---|---|---|
| $f_i$ | input frequency | | [1] | 13.553 | 13.56 | 13.567 | MHz |
| $V_{i(RMS)min}$ | minimum RMS input voltage | operating read/ write | | 1.1 | - | 1.3 | V |
| $P_{i(min)}$ | minimum input power | operating | [2] | - | 40 | - | µW |
| $C_i$ | center input capacitance | between LA and LB | [3] | 22.3 | 23.5 | 24.7 | pF |
| $C_{adjust}$ | adjust input capacitance | between LA and LB | [3] | - | ± 1.5 | - | pF |
| $t_{persist}$ | persistent time | $T_{amb} \leq 55$ ° C | [4] | 2 | - | - | s |
| $R_{on}$ | resistance tag taper closed (for SL2S3003TT only) | between DP and GND | | - | - | 50 | Ω |
| $R_{off}$ | resistance tag taper open (for SL2S3003TT only) | between DP and GND | | 1 M | - | - | Ω |

1. Bandwidth limitation (± 7 kHz) according to ISM band regulations.
2. Including losses in the resonant capacitor and rectifier.
3. Measured with an HP4285A LCR meter at 13.56 MHz and 1.1 V RMS.
4. The maximum persistent time strongly depends on the ambient temperature.

## 11 Bare die outline




not to scale!

(1) X-scribe line width: 35 µm
(2) Y-scribe line width: 35 µm
(3) Chip step, X-length: 675 µm
(4) Chip step, Y-length: 635 µm
(5) Bump to bump distance X (LA - LB): 530 µm
(6) Bump to bump distance Y (LB - GND): 452.2 µm
(7) Distance GND bump to nitride edge X: 55 µm
(8) Distance GND bump to nitride edge Y: 55 µm
Bump size LA and LB (X × Y): 80 µm × 80 µm
Bump size DP and GND (X × Y): 80 µm × 80 µm

**Figure 5. Wafer SL2S3003/SL2S3003TT bare die layout**

# 12 Abbreviations

**Table 139. Abbreviations**

| Acronym | Description |
|---|---|
| AFI | Application Family Identifier |
| CRC | Cyclic Redundancy Check |
| DSFID | Data Storage Format Identifier |
| EAS | Electronic Article Surveillance |
| EEPROM | Electrically Erasable Programmable Read Only Memory |
| EOF | End Of Frame |
| IC | Integrated Circuit |
| LCR | Inductance, Capacitance, Resistance |
| LSB | Least Significant Byte/Bit |
| MSB | Most Significant Byte/Bit |
| RF | Radio Frequency |
| SOF | Start Of Frame |
| UID | Unique IDentifier |

## 13 References

[1] ISO Standard – ISO/IEC 15693 - Identification cards - Contactless integrated circuit cards - Vicinity cards.

[2] ISO Standard – ISO/IEC 15693-2 -Identification cards - Contactless integrated circuit cards - Vicinity cards - Part 2: Air interface and initialization.

[3] ISO Standard – ISO/IEC 15693-3 -Identification cards - Contactless integrated circuit cards - Vicinity cards - Part 3: Anticollision and transmission protocol.

[4] ISO Standard – ISO/IEC 7816-6 - Identification cards - Integrated circuit cards - Part 6: Inter-industry data elements for interchange.

[5] Specification – General specification for 12" wafer on UV-tape with electronic fail die marking
Delivery type description – BU-ID document number: 1862**[2].

[6] Publication – Certicom Research. SEC 2
Recommended Elliptic Curve Domain Parameters, version 2.0, January 2010.

[7] Application note – AN11600 - ICODE Originality Signature Verification

2 ** ... document version number

# 14 Revision history

**Table 140. Revision history**

| Document ID | Release date | Description |
|---|---|---|
| SL2S3003/SL2S3003TT v.3.0 | 28 March 2024 | Product data sheet<br>• Editorial changes<br>• Section 8.5.3.9 "ENABLE PRIVACY": corrected Privacy mode 2 of ENABLE PRIVACY command. |
| SL2S3003/SL2S3003TT v.1.0 | 16 August 2022 | Objective data sheet<br>• Initial version |

# Legal information

## Data sheet status

| Document status[1][2] | Product status[3] | Definition |
|---|---|---|
| Objective [short] data sheet | Development | This document contains data from the objective specification for product development. |
| Preliminary [short] data sheet | Qualification | This document contains data from the preliminary specification. |
| Product [short] data sheet | Production | This document contains the product specification. |

[1] Please consult the most recently issued document before initiating or completing a design.
[2] The term 'short data sheet' is explained in section "Definitions".
[3] The product status of device(s) described in this document may have changed since this document was published and may differ in case of multiple devices. The latest product status information is available on the Internet at URL https://www.nxp.com.

## Definitions

**Draft** — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

**Short data sheet** — A short data sheet is an extract from a full data sheet with the same product type number(s) and title. A short data sheet is intended for quick reference only and should not be relied upon to contain detailed and full information. For detailed and full information see the relevant full data sheet, which is available on request via the local NXP Semiconductors sales office. In case of any inconsistency or conflict with the short data sheet, the full data sheet shall prevail.

**Product specification** — The information and data provided in a Product data sheet shall define the specification of the product as agreed between NXP Semiconductors and its customer, unless NXP Semiconductors and customer have explicitly agreed otherwise in writing. In no event however, shall an agreement be valid in which the NXP Semiconductors product is deemed to offer functions and qualities beyond those described in the Product data sheet.

## Disclaimers

**Limited warranty and liability** — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

**Right to make changes** — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

**Suitability for use** — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

**Applications** — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

**Limiting values** — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

**Terms and conditions of commercial sale** — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

**No offer to sell or license** — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

**Quick reference data** — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

**Export control** — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

**Suitability for use in non-automotive qualified products** — Unless this document expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

**Translations** — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

**Security** — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

**NXP B.V.** — NXP B.V. is not an operating company and it does not distribute or sell products.

## Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

**NXP** — wordmark and logo are trademarks of NXP B.V.

**ICODE and I-CODE** — are trademarks of NXP B.V.

# Tables

# Figures

# Contents





For more information, please visit: https://www.nxp.com

**Date of release: 28 March 2024**
**Document identifier: SL2S3003/SL2S3003TT**