SL2S2602

ICODE SLIX2

Rev. 3.2 — 26 January 2015
276332

Product data sheet
COMPANY PUBLIC

1. General description

The ICODE SLIX2 IC is the newest member of NXP's SLIX product family. The chip is fully backwards compatible to SLIX and offers an increased user memory size, along with new outstanding features and performance:

- NXP originality signature
- Increased speed for Inventory management
- Increased reading range
- Increased robustness against detuning effects
- 2.5 kbit user memory size
- Flexible user memory segmentation with separate access conditions
- Password protected on chip service cycle counter

1.1 Contactless energy and data transfer

Whenever connected to a very simple and easy-to-produce type of antenna (as a result of the 13.56 MHz carrier frequency) made out of a few windings printed, winded, etched or punched coil, the ICODE SLIX2 IC can be operated without line of sight up to a distance of 1.5 m (gate width). No battery is needed. When the smart label is positioned in the field of an interrogator antenna, the high speed RF communication interface enables data to be transmitted up to 53 kbit/s.

1.2 Anticollision

An intelligent anticollision function enables several tags to operate in the field simultaneously. The anticollision algorithm selects each tag individually and ensures that the execution of a transaction with a selected tag is performed correctly without data corruption resulting from other tags in the field.

1.3 Security and privacy aspects

- Unique IDentifier (UID):

  The UID cannot be altered and guarantees the uniqueness of each label.
- Originality signature:

  32 byte ECC based originality signature.
- Password protected memory management (Read/Write access):

The user memory can be segmented into two pages and the access rights for read/write access can be defined for each of them. This ensures that 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 SLI and ICODE SLIX.

- Password protected Label Destroy:

  The 32-bit Destroy password enables an addressed label to be destroyed with the DESTROY SLIX2 command. That status is irreversible and the label will never respond to any command again.

- Password protected Privacy Mode:

  The 32-bit Privacy password enables a label to be set to the Privacy mode with the ENABLE PRIVACY command. In this mode the label will not respond to any command except the command GET RANDOM NUMBER, until it next receives the correct Privacy password. This mode is especially designed to meet the increasing demand to take care of the customers 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 needs to be transmitted before with the SET PASSWORD command.

- 16 bit counter:

  The last block of the user memory provides a special feature - the 16 bit counter. The counter can be increased by one with a WRITE command (optionally password protected by the read password). The counter can be reset to an initial value with the write password.

2. Features and benefits

2.1 ICODE SLIX2 RF interface (ISO/IEC 15693)

- Contactless transmission of data and supply energy (no battery needed)
- Operating distance: up to 1.5 m (depending on antenna geometry)
- Operating frequency: 13.56 MHz (ISM, world-wide licence freely available)
- Fast data transfer: up to 53 kbit/s
- High data integrity: 16-bit CRC, framing
- True anticollision
- Electronic Article Surveillance (EAS)
- Application Family Identifier (AFI) supported
- Data Storage Format Identifier (DSFID)
- ENABLE PRIVACY command with 32-bit Privacy password
- DESTROY SLIX2 command with 32-bit Destroy password
- Additional fast anticollision read
- Persistent quiet mode to enable faster inventory speed
- Write distance equal to read distance

2.2 EEPROM

- 2560 bits user memory, organized in 80 blocks of 4 bytes each (last block reserved for counter feature)
- 50 years data retention
- Write endurance of 100000 cycles

2.3 Security

- Unique identifier for each device (8 byte)
- 32 byte originality signature
- Lock mechanism for each user memory block (write protection)
- 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
- 16 bit counter (optionally password protected with the read and write password)

3. Applications

- Libraries
- Item level tagging in pharmaceutical supply chains
- Counterfeit protection for consumer goods
- Industrial applications
- Asset and document tracking

4. Ordering information

Table 1. Ordering information

Type number	Package		Version
	Name	Description	
SL2S2602FUD	Wafer	sawn, bumped wafer, 120 μm, on film frame carrier, C_i between LA and LB = 23.5 pF (typical)	-

5. Block diagram

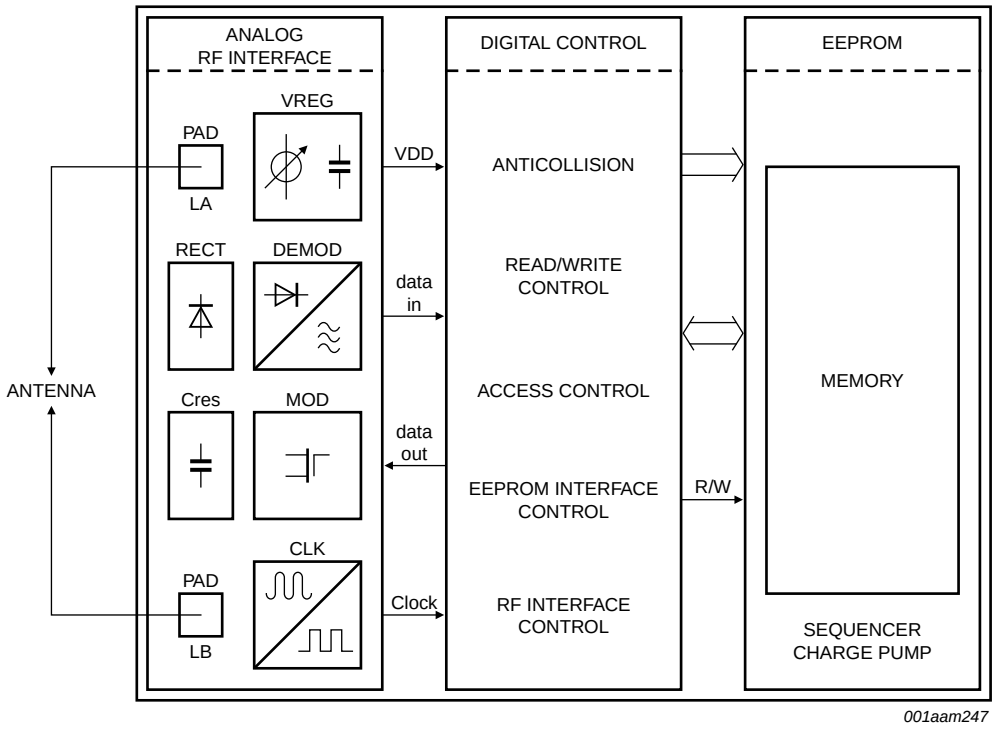


Fig 1. Block diagram of ICODE SLIX2

6. Pinning information

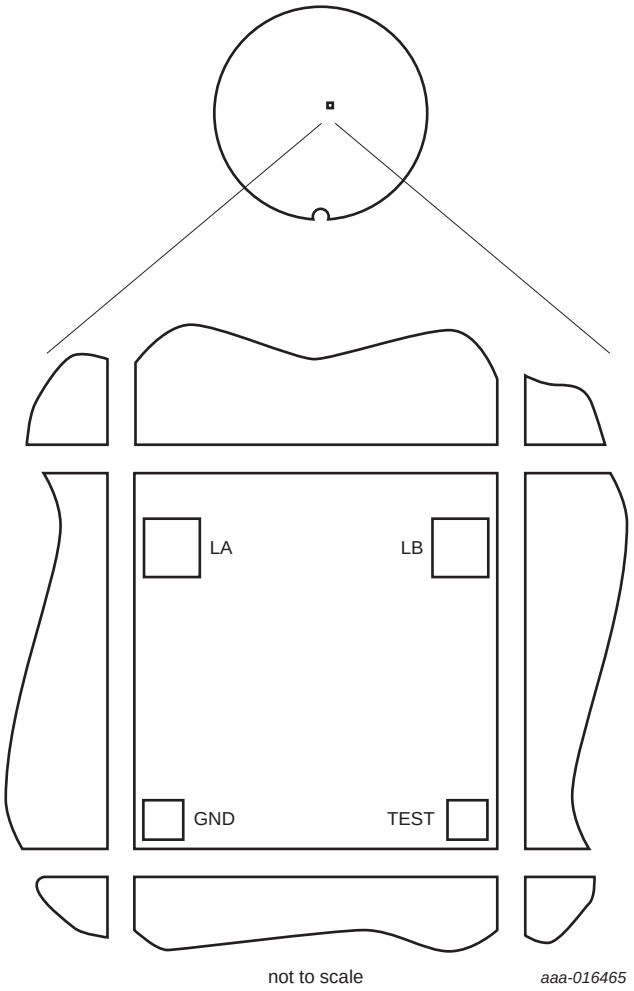


Fig 2. Wafer SL2S2602FUD layout and pin configuration for the bare die

6.1 Pin description

Table 2. Bonding pad description

Symbol	Description
LA	antenna RF input
LB	antenna RF input
GND	ground
TEST	test input

7. Mechanical specification

7.1 Wafer specification

See Ref. 6 “General specification for 8” wafer on UV-tape with electronic fail die marking”.

Table 3. Wafer specification

Wafer	
Designation	each wafer is enscribed with batch number and wafer number
Diameter	200 mm (8 inches)
Thickness	120 μm ± 15 μm
Process	CMOS 0.14 μm
Batch size	25 wafers
Dies per wafer	94823
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	540 μm × 543 μm = 0,29322mm^2
Scribe line width	
X-dimension	15 μm (scribe line width measured between nitride edges)
Y-dimension	15 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	430 μm (center to center)
Distance pad to pad LB to TEST	371.5 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
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

Table 3. Wafer specification *...continued*

TEST, GND	60 μm × 60 μm
variation	±5 μm
Under bump metallization	sputtered TiW

7.1.1 Fail die identification

No inkdots 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 Ref. 6 “General specification for 8” wafer on UV-tape with electronic fail die marking”.

7.1.2 Map file distribution

See Ref. 6 “General specification for 8” wafer on UV-tape with electronic fail die marking”.

8. Functional description

8.1 Block description

The ICODE SLIX2 IC consists of three major blocks:

- Analog RF interface
- Digital controller
- EEPROM

The analog section provides stable supply voltage and demodulates data received from the reader for processing by the digital section. The analog section's modulation transistor also transmits data back to the reader.

The digital section includes the state machines, processes the protocol and handles communication with the EEPROM.

The label requires no internal power supply. Its contactless interface generates the power supply and the system clock via the resonant circuitry by inductive coupling to the interrogator. The interface also demodulates data that are transmitted from the interrogator to the ICODE Label, and modulates the electromagnetic field for data transmission from the ICODE Label to the interrogator.

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

8.2 Memory organization

The 2560 bit user accessible EEPROM memory is divided into 80 blocks. A block is the smallest access unit. Each block consists of 4 bytes (1 block = 32 bits). Bit 0 in each byte represents the least significant bit (LSB) and bit 7 the most significant bit (MSB), respectively.

The entire memory is divided into 3 parts:

- Configuration area
  - Within this part of the memory all required information is stored, such as UID, write protection, access control information, passwords, AFI and EAS and originality signature. This memory area cannot be directly accessed.
- User memory
  - Within the 2528 bit memory (79 blocks) area the user data are stored. Direct read/write access to this part of the memory is possible depending on the related security and write protection conditions.
- 16 bit counter
  - The last block of the EEPROM memory (block 79) contains the 16 bit counter and the counter password protection flag.

Table 4. Memory organization

Block	Byte 0	Byte 1	Byte 2	Byte 3	Description
-					Configuration area for internal use
0					User memory: 79 blocks, 4 bytes each, 316 bytes in total.
1					
2					
3					
:	:	:	:	:	
76					
77					
78					
79	C0	C1	0x00	PROT	Counter

Only Blocks 0 to 79 can be addressed with read and write commands.

Remark: Block 79 contains the 16 bit counter and can not be used to store user data. READ and WRITE commands to that block require special data considerations (refer to section “16 bit counter feature”).

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 afterwards.

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 (bit 41 to 48, next to the manufacturer code which is “04h” for NXP Semiconductors).

The TAG type of the ICODE SLIX2 IC is “01h”.

Bit 37and bit 36 are used to differentiate between ICODE SLI, ICODE SLIX and ICODE SLIX2 (refer to Table 6).

Table 5. 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 6. Type indicator bits

Bit 37	Bit 36	ICODE Type
0	**0**	**ICODE SLI**
1	0	ICODE SLIX
0	1	ICODE SLIX2
1	1	RFU

8.2.2 Originality signature

ICODE SLIX2 features a cryptographically supported originality check. With this feature, it is possible to verify with a high confidence that the tag is using an IC manufactured by NXP Semiconductors. This check can be performed on personalized tags as well.

ICODE SLIX2 digital signature is based on standard Elliptic Curve Cryptography (curve name secp128r1), according to the ECDSA algorithm. The use of a standard algorithm and curve ensures easy software integration of the originality check procedure in NFC devices without specific hardware requirements.

Each ICODE SLIX2 UID is signed with a NXP private key and the resulting 32-byte signature is stored in a hidden part of the ICODE SLIX2 memory during IC production.

This signature can be retrieved using the READ_SIGNATURE command (refer to Section 8.5.3.20 “READ SIGNATURE”) and can be verified in the NFC device by using the corresponding ECC public key provided by NXP. In case 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) the tool domain parameters shall be set to secp128r1, defined within the standards for elliptic curve cryptography SEC (Ref. 7).

8.2.3 Configuration of delivered ICs

ICODE SLIX2 ICs are delivered with the following configuration by NXP Semiconductors:

- Unique identifier is unique and read only
- Write access conditions allow change to user blocks, AFI, DSFID, EAS and passwords (password protection disabled)
- All password bytes are 00h for the read and write protection password and the EAS/AFI password
- All password bytes are 0Fh for the Privacy and Destroy passwords
- User data memory is **not** password protected
- Password protected Privacy Mode is disabled
- EAS and AFI password protection is disabled
- Status of EAS mode is not defined
- AFI is supported and not defined
- DSFID is supported and not defined
- User data memory is not defined

Remark: Because the EAS mode is undefined at delivery, the EAS mode shall be set (enabled or disabled) according to your application requirements during the test or initialization phase.

Remark: If password protection is not required, depending on the targeted application, it is recommended to write random passwords during the label initialization.

8.3 Communication principle

For detailed description of the protocol and timing please refer to ISO/IEC 15693-2 (modulation, bit-coding, framing, Ref. 2) and ISO/IEC 15693-3 (anticollision, timing, protocol, Ref. 3).

8.4 State diagram

The state diagram illustrates the different states of the ICODE SLIX2.

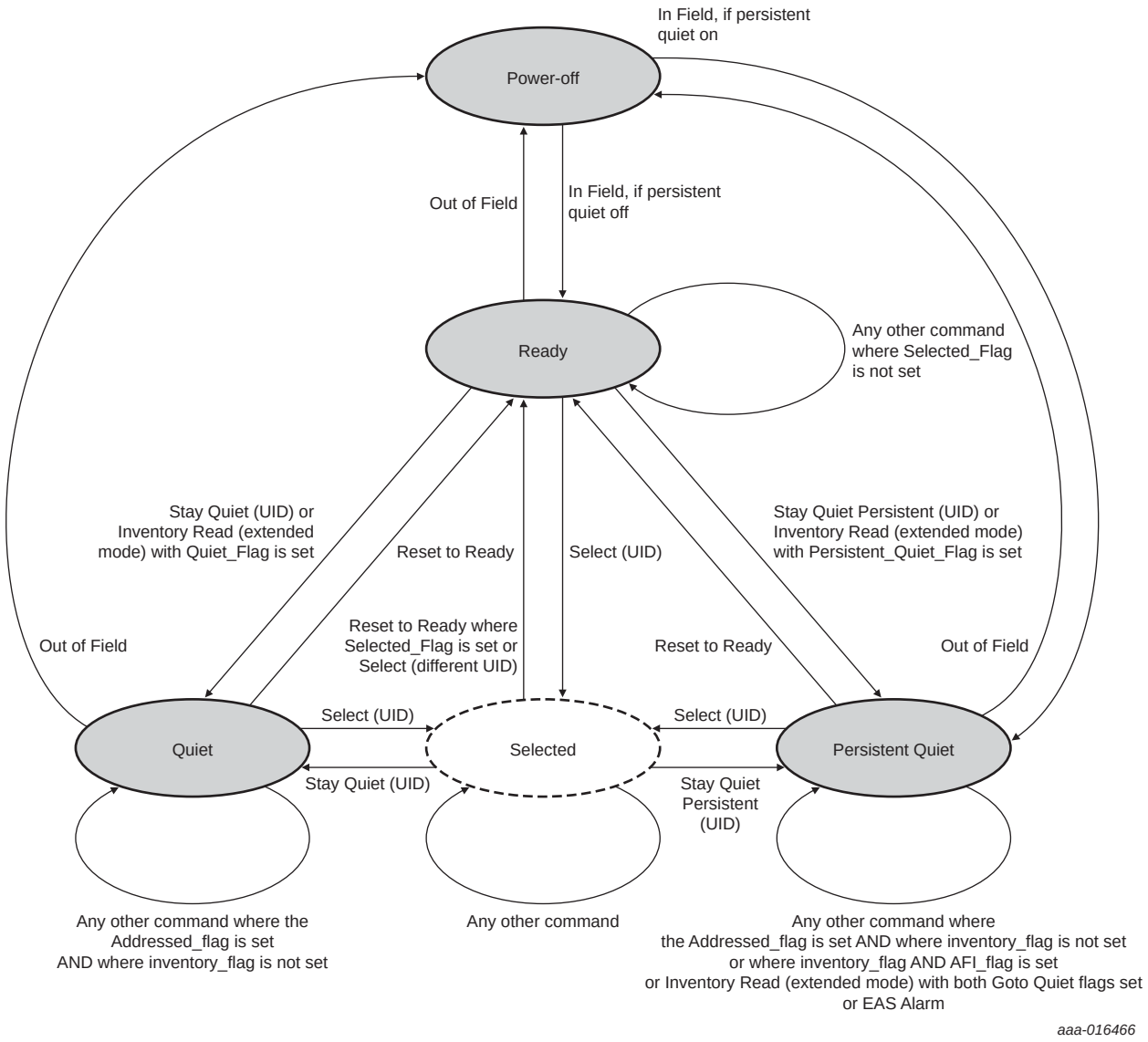


Fig 3. State diagram ICODE SLIX2

Remark: It is possible to set the ICODE SLIX2 IC into the Quiet and Persistent Qiet.mode 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. The IC enters to the Persistent Quiet mode at the next power-on if the persistent time has not been exceeded.

8.5 Supported commands

8.5.1 Mandatory commands

8.5.1.1 INVENTORY

As defined in ISO/IEC 15693-3.

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

8.5.1.2 STAY QUIET

As defined in ISO/IEC 15693-3.

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 the password has not been transmitted first with the SET PASSWORD command the label will respond according to the error handling (see Section 8.6 “Error handling”).

Remark: Block 79 of the user memory contains the 16 bit counter feature and needs to be treated differently (refer to section “16 bit counter feature”).

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 only protected with the Read Password (see Section 8.5.3.6 “PROTECT PAGE”) and the password has not been transmitted first with the SET PASSWORD command the label will respond according to the error handling (see Section 8.6 “Error handling”).

Remark: Block 79 of the user memory contains the 16 bit counter feature and needs to be treated differently (refer to section “16 bit counter feature”).

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 only protected with the read password (see Section 8.5.3.6 “PROTECT PAGE”) and the password has not been transmitted first with the SET PASSWORD command, the label will respond according to the error handling (see Section 8.6 “Error handling”).

Remark: Block 79 of the user memory contains the 16 bit counter feature and can not be locked (refer to section “16 bit counter feature”).

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 the password has not been transmitted first with the SET PASSWORD command the label will respond according to the error handling (see Section 8.6 “Error handling”).

Remark: Block 79 of the user memory contains the 16 bit counter feature and needs to be treated differently (refer to section “16 bit counter feature”).

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.

Remark: RESET TO READY also resets the label IC from the persistent quiet state (refer to Section 8.5.3.10 “INVENTORY READ” and Section 8.5.3.19 “STAY QUIET PERSISTENT”)into the READY state.

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.

Remark: This command maybe password protected, refer to Section 8.5.3.16 “PASSWORD PROTECT EAS/AFI”.

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.

Remark: This command maybe password protected, refer to Section 8.5.3.16 “PASSWORD PROTECT EAS/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.

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.

8.5.2.11 GET SYSTEM INFORMATION

As defined in ISO/IEC 15693-3.

The TAG type of the ICODE SLIX2 IC is “01h”.

8.5.2.12 GET MULTIPLE BLOCK SECURITY STATUS

As defined in ISO/IEC 15693-3.

8.5.3 Custom commands

The manufacturer code of NXP Semiconductors is defined in ISO/IEC 7816-6A1 (Ref. 5). It has the value “04h”.

For the structure of custom commands please refer to ISO/IEC 15693-3.

If not explicitly specified differently all 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 that will be transmitted with the SET PASSWORD,ENABLE PRIVACY and DESTROY commands have to 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 7. 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 8. GET RANDOM NUMBER response when Error_flag set

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

Table 9. 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 functionalities of the following commands. The SET PASSWORD command has to be executed just once for the related passwords if the label is powered.

Remark: The SET PASSWORD command can only be executed in Addressed or Selected mode except for the Privacy password. If the Privacy password is transmitted (see Section 8.5.3.9 “ENABLE PRIVACY”), the timing of the SET PASSWORD command is write alike.

The XOR password has to be calculated with the password and two times 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 10. 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 11. Password Identifier

Password identifier	Password
01h	Read
02h	Write
04h	Privacy
08h	Destroy
10h	EAS/AFI

Table 12. SET PASSWORD response format when Error_flag set

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

Table 13. SET PASSWORD response format when Error_flag NOT set

SOF	Flags	CRC16	EOF
-	8 bits	16 bits	-

Remark: If the IC receives an invalid password, it will not execute any following command until a Power-On Reset (POR) (RF reset) is executed.

8.5.3.3 WRITE PASSWORD

Command code = B4h

The WRITE PASSWORD command enables a new password to be written into the related memory if the related old password has already been transmitted with a SET PASSWORD command and the addressed password is not locked (see Section 8.5.3.4 “LOCK PASSWORD”).

Remark: The WRITE PASSWORD command can only be executed in addressed or selected mode. The new password takes effect immediately which means that the new password has to 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.

Table 14. 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 15. Password Identifier

Password identifier	Password
01h	Read
02h	Write
04h	Privacy
08h	Destroy
10h	EAS/AFI

Table 16. WRITE PASSWORD response format when Error_flag set

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

Table 17. 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 enables the addressed password to be locked if the related password has already been transmitted with a SET PASSWORD command. 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.

Table 18. 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 19. Password identifier

Password identifier	Password
01h	Read
02h	Write
04h	Privacy
08h	Destroy
10h	EAS/AFI

Table 20. LOCK PASSWORD response format when Error_flag set

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

Table 21. 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 enables the Label IC to be instructed that both of 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 & 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.

Remark: A retransmission of the passwords is not required after the execution of the 64-bit PASSWORD PROTECTION command.

Remark: The 64-bit PASSWORD PROTECTION does not include the 16 bit counter block.

The timing of the command is write alike.

Table 22. 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 23. 64 BIT PASSWORD PROTECTION response format when Error_flag set

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

Table 24. 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 to divide the user memory into two arbitrarily sized pages and defines 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 25 shows an example of the user memory segmentation with the protection pointer address 20 (0x14).

Table 25. 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

Remark: If the protection pointer address is set to block 0, the entire user memory (block 0 to block 78) 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” on page 20

The timing of the command is write alike.

Table 26. 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 0x4E (block 78). Block 79 (containing the 16 bit counter) is excluded from the standard user memory password protection scheme.

Table 27. 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

Table 28. 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 29. POTECT PAGE response format when Error_flag set

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

Table 30. 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 INFOMATION”)

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 if the Read and Write passwords have been transmitted first with the SET PASSWORD command.

The timing of the command is write alike.

Table 31. 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	-

Remark: If the transmitted protection pointer address does not match with the stored address the label will respond according to the error handling (see Section 8.6 “Error handling”).

Table 32. LOCK PAGE PROTECTION CONDITION response format when Error_flag set

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

Table 33. 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 SLIX2 command enables the ICODE SLIX2 Label IC to be destroyed if the Destroy password is correct. This command is irreversible and the ICODE SLIX2 will never respond to any command again.

The DESTROY SLIX2 command can only be executed in addressed or selected mode.

The XOR password has to be calculated with the password and two times 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 34. 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 35. DESTROY response format when Error_flag set

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

Table 36. 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 enables the ICODE SLIX2 Label IC to be set to Privacy mode if the Privacy password is correct. The ICODE SLIX2 will not respond to any command except GET RANDOM NUMBER and SET PASSWORD.

The XOR password has to be calculated with the password and two times 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 has to be transmitted to the IC with the SET PASSWORD command.

The timing of the command is write alike.

Table 37. 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 38. ENABLE PRIVACY response format when Error_flag set

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

Table 39. 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 SLIX2 IC performs the same as the anticollision sequence, with the difference that instead of the UID and the DSFID, the requested response is defined by additional options.

The INVENTORY READ command provides 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 (refer to Section “8.4.3.10.1. Standard mode”)
- Extended mode (MSB mask length byte equal 1)
  The extended mode offers additional features to optimize the inventory procedure for different requirements (refer to Section “8.4.3.10.2 Extended Mode”)

8.4.3.10.1 Standard mode

If MSB mask length byte equal 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 SLIX2 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 40. 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 tags in the READY or SELECTED state will 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.

The INVENTORY READ command can also be transmitted in the addressed or selected mode (refer to “Section 8.4.3.10.3 Addressed and selected mode).

The number of blocks in the request is one less than the number of blocks that the ICODE SLIX2 IC returns in its response.

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

Table 41. INVENTORY READ response format: Option flag logic 0

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

The ICODE SLIX2 IC reads the requested block(s) and sends back their value in the response. The mechanism and timing of the INVENTORY READ command performs the same as the INVENTORY command which is 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 42. 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 SLIX2 IC reads the requested block(s) and sends back their value in the response. Additionally 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 perform the same as the INVENTORY command which is described in clause 8 of ISO/IEC 15693-3.

Remark: The number of bits of the re-transmitted UID can be calculated as follows:

- 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

Remark: If the sum of first block number and number of blocks exceeds the total available number of user blocks, the number of transmitted blocks is less than the requested number of blocks, which means that 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 43. 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 SLIX2 IC

8.4.3.10.2 Extended Mode

If the most significant bit of the Mask Length byte is equal 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 44. Inventory Read (extended mode) response format

SOF	Flags	Inventory Read	IC Mfr. code	AFI	Mask Length	ext. Options	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	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 will 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.

The INVENTORY READ command can also be transmitted in the addressed or selected mode (refer to Section “8.4.3.10.3 Addressed and selected mode”).

Table 45. 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	-	0	**RFU**
4	-	0	**RFU**
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 46 “QUIET and PERSISTANT QUIET bit in Extended options”
7	PERSISTENT QUIET	0	refer to Table 46 “QUIET and PERSISTANT QUIET bit in Extended options”
8 (MSB)	-	**0**	**RFU**

Table 46. 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 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 47. Inventory Read (extended mode) response format: Option flag logic 1

SOF	Flags	Optional truncated UID OR complete UID	Optional data	CRC16	EOF
-	8 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 performs the same as at the INVENTORY command which is 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 48. 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 SLIX2 IC

8.4.3.10.3 Addressed and selected mode

The INVENTORY READ command can also be transmitted 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.

In the addressed or selected mode the INVENTORY READ command behaves similar to 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).

Remark: If the INVENTORY READ command is used in the addressed or selected mode, the AFI shall not be transmitted and the label IC will only respond in the first time slot.

8.5.3.11 FAST INVENTORY READ

Command code = A1h

When receiving the FAST INVENTORY READ command the ICODE SLIX2 IC behaves the same as the INVENTORY READ command with the following exceptions:

The data rate in the direction ICODE SLIX2 IC to the interrogator is twice that defined in ISO/IEC 15693-3 depending on the Datarate_flag 53 kbit (high data rate) or 13 kbit (low data rate).

The data rate from the interrogator to the ICODE SLIX2 IC and the time between the rising edge of the EOF from the interrogator to the ICODE SLIX2 IC remain unchanged (stay the same as defined in ISO/IEC 15693-3).

In the ICODE SLIX2 IC to the interrogator direction, 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 has to be first transmitted 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 49. 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 50. SET EAS response format when Error_flag set

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

Table 51. 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

The RESET EAS command disables the EAS mode if the EAS mode is not locked. If the EAS mode is password protected the EAS password has to be first transmitted 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 52. 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 53. RESET EAS response format when Error_flag set

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

Table 54. 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 has to be first transmitted 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 55. 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 56. LOCK EAS response format when Error_flag set

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

Table 57. 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 EAS ID value shall not be transmitted.

  If the EAS mode is enabled, the EAS response is returned from the ICODE SLIX2 IC. This configuration is compliant with the EAS command of the ICODE SLI IC.

- Option flag is set to 1:

  Within the command the EAS ID mask length has to be transmitted to identify how many bits of the following EAS ID value are valid (multiple of 8-bits). Only those ICODE SLIX2 ICs will respond with the EAS sequence which have stored the corresponding data in the EAS ID configuration (selective EAS) and if the EAS Mode is set.

  If the EAS ID mask length is set to 0, the ICODE SLIX2 IC will answer with its EAS ID.

Table 58. 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 SLIX2 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 59. 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 60. 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 (see RESET EAS command in Section 8.5.3.13 “RESET EAS”), the ICODE SLIX2 IC remains silent.

Remark: Labels in the QUIET state will not respond to an EAS ALARM command except of the addressed flag is set. Labels in the PERSISTANT QUIET mode will 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 if the EAS/AFI password is first transmitted with the SET PASSWORD command.

Option flag set to logic 0: EAS will be password protected.

Option flag set to logic 1: AFI will be password protected.

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

Remark: Independent of the Option flag, this write-alike command will be executed like a write command with Option flag 0 (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).

Table 61. 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 62. PASSWORD PROTECT EAS/AFI response format when Error_flag set

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

Table 63. 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 enables a new EAS Identifier to be stored in the corresponding configuration memory. If EAS is password protected (for Set and Reset EAS) the EAS password has to be first transmitted 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.

Table 64. 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 65. WRITE EAS ID response format when Error_flag set

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

Table 66. 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 INFOMATION

Command code = ABh

The command GET NXP SYSTEM INFORMATION command provides information about the IC access conditions and supported features.

Table 67. 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 68. GET NXP SYSTEM INFORMATION response format when Error_flag set

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

Table 69. 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 value of the bits in Table 70 define if the related feature is enabled or disabled:

- 0: feature disabled
- 1: feature enabled

Table 70. 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 71. 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 72. 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	-	RFU
9	ORIGINALITY SIG	READ SIGNATURE command supported (refer to Section 8.5.3.20 “READ SIGNATURE”)
10	ORIGINALITY SIG PP	Password protection for READ SIGNATURE command supported (refer to Section 8.5.3.20 “READ SIGNATURE”)
11	P QUIET	STAY QUIET PERSISTENT command supported (refer to Table note [8.5.3.19]
12	-	RFU
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”)
15-31	-	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 will not send back a response.

Remark: The STAY QUIET PERSISTENT command provides the same behavior as the mandatory STAY QUIET command with the only difference at a reset (power off). The label IC will turn to the ready state, if the power off time is exceeding the persistent time.

When in PERSISTENT QUIET state:

The label IC will not process any request where the Inventory_flag is set, except

- the AFI_flag is set or
- the QUIET and PERSTENT QUIET flags in the extended mode of the (Fast) Inventory command are both set.

The label IC will process any

- EAS ALARM request
- addressed or selected request

The label IC will exit the persistent quiet state when:

- reset (power off) exceeding the persistent time,
- receiving a SELECT request. It shall then go to the Selected state.
- receiving a RESET TO READY request. It shall then go to the Ready state.

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

Table 73. 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 ECC signature, to verify NXP Semiconductors as the silicon vendor. The signature is programmed at chip production and cannot be changed afterwards.

Table 74. READ SIGNATURE request format

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

Table 75. READ SIGNATURE response format when Error_flag set

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

Table 76. READ SIGNATURE response format when Error_flag NOT set

SOF	Flags	Originality Signature	CRC16	EOF
-	8 bits	256 bits	16 bits	-

Details on how to check the signature value will be provided in the Application note “ICODE SLIX2 Originality Signature Validation”. It is foreseen to offer an online and offline way to verify originality of ICODE SLIX2.

8.5.3.21 16 bit Counter

Block 79 of the user memory contains the 16 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 is not valid for block 79.

The 16 bit counter (block 79) can be

- read
- increased by one optionally protected with the read password
- preset to initial start value protected with the write password

The counter can be read with a READ SINGLE BLOCK command to block 79 or a READ MULTIPLE BLOCK command including block 79. The 4 byte data from block 79 provide the following information:

Table 77. COUNTER BLOCK data structure

Byte	Name	Value	Description
0	C0	0x00 - 0xFF	LSB of the counter value
1	C1	0x00 - 0xFF	MSB of the counter value
2	-	0x00	RFU
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 79. 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 if 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 78.

Remark: A Preset counter value of 0x0001 is not possible, a WRITE SINGLE BLOCK command with that value will only increment the counter.

Table 78. Preset counter data structure

Byte	Name	Value	Description
0	C0	0x00, 0x02 - 0xFF	LSB of the counter value
1	C1	0x00 - 0xFF	MSB of the counter value
2	-	0x00	RFU
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 79. 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 78.

Remark: The counter can only be incremented with the C0 and C1 values defined in Table 79. Other values than that preset the counter if the write password had been transmitted before with a SET PASSWORD command or leads to an error message.

Table 79. Increment counter data structure

Byte	Name	Value	Description
0	C0	0x01	LSB of the counter value
1	C1	0x00	MSB of the counter value
2	-	0x00	RFU
3	PROT	0x00	Incrementing of the counter value is not password protected

8.6 Error handling

8.6.1 Transmission errors

According to ISO/IEC 15693 the label IC will not respond if a transmission error (CRC, bit coding, bit count, wrong framing) is detected and will silently wait for the next correct received command.

8.6.2 Not supported commands 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

The addressed or selected 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 will 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 available number of user blocks, the number of transmitted blocks is less than the requested number of blocks, which means that 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 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 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

Following mechanisms are implemented in the contactless communication link between interrogator and label to ensure very reliable data transmission:

- 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 and ISO/IEC 15693-3.

9. Limiting values

Table 80. 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	+85	°C
$I_{i(max)}$	maximum input current	LA to LB; peak [3]	-	±60	mA
I_I	input current	LA to LB; RMS	-	30	mA
V_{ESD}	electrostatic discharge voltage	Human body model [4]	-	±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] The voltage between LA and LB is limited by the on-chip voltage limitation circuitry (corresponding to parameter I_I).

[4] For ESD measurement, the IC was mounted in a CDIP8 package.

10. Characteristics

10.1 Wafer memory characteristics

Table 81. 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 82. 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	input capacitance	between LA and LB [3]	22.3	23.5	24.7	pF
$t_{persist}$	persistent time	[4]	2	-	-	s

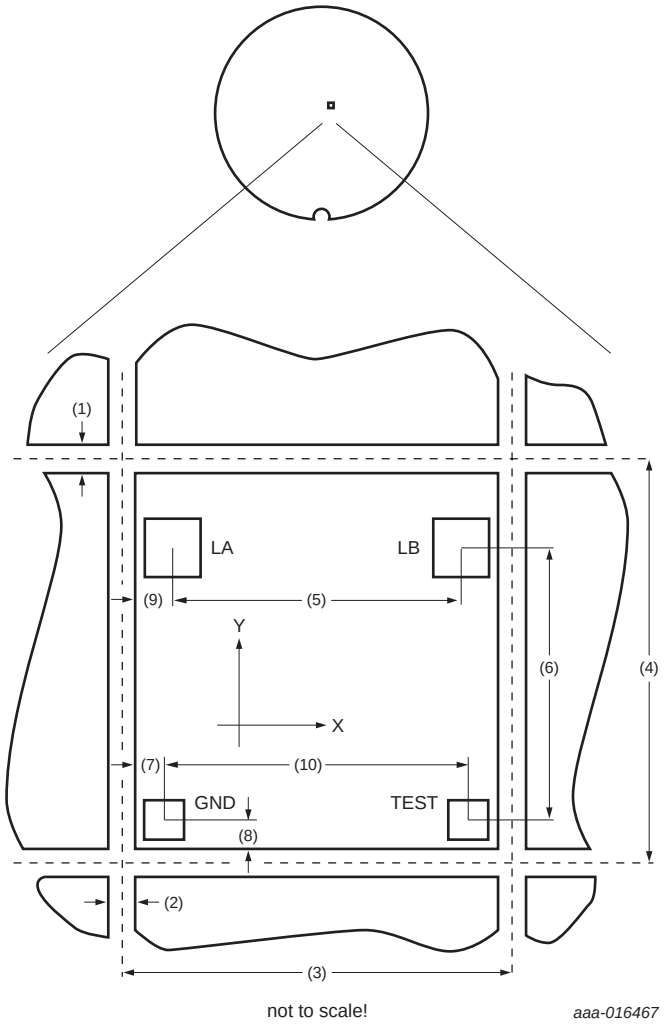
[1] Bandwidth limitation (± 7 kHz) according to ISM band regulations.

[2] Including losses in the resonant capacitor and rectifier.

[3] Measured with an HP4285A LCR meter at 13.56 MHz and 1.5 V RMS.

[4] The maximum persistent time strongly depends on the ambient temperature.

11. Bare die outline



(1) X-scribe line width: 15 μm
(2) Y-scribe line width: 15 μm
(3) Chip step, X-length: 555 μm
(4) Chip step, Y-length: 558 μm
(5) Bump to bump distance X (LA - LB): 430 μm
(6) Bump to bump distance Y (LB - TEST): 371.5 μm
(7) Distance GND bump to nitride edge X: 45 μm
(8) Distance GND bump to nitride edge Y: 45 μm
(9) Distance LA bump to nitride edge X: 55 μm
(10) Bump to bump distance X (GND - TEST): 450 μm
Bump size LA and LB (X × Y): 80 μm × 80 μm
Bump size TEST and GND (X × Y): 60 μm × 60 μm

Fig 4. Wafer SL2S2602FUD bare die layout

12. Abbreviations

Table 83. 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 18000-3 - Information technology - Radio frequency identification for item management - Part 3: Parameters for air interface communications at 13.56 MHz.

[5] **ISO Standard —** ISO/IEC 7816-6 - Identification cards - Integrated circuit cards - Part 6: Interindustry data elements for interchange.

[6] **General specification for 8” wafer on UV-tape with electronic fail die marking —** Delivery type description – BU-ID document number: 1093**[1].

[7] **Certicom Research. SEC 2 —** Recommended Elliptic Curve Domain Parameters, version 2.0, January 2010.

1. ** ... document version number

14. Revision history

Table 84. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
SL2S2602 v. 3.2	20150126	Product data sheet	-	SL2S2602_276331
Modifications:	• Editorial changes			
SL2S2602_276331	20141210	Product data sheet	-	276330
Modifications:	• Security status changed into COMPANY PUBLIC			
276330	20141118	Product data sheet	-	276311
Modifications:	• Data sheet status changed from objective to product			
276311	20140528	Objective data sheet	-	276310
Modifications:	• Section 8.4 “State diagram” added • Conditions added for STAY QUIETPERSITANT command in Section 8.5.3.19 • Modification of the QUIET and PERSISTANT QUIET bit in the extended mode of the INVENTORY READ command in Table 45 “Extended options” and Table 46 “QUIET and PERSISTANT QUIET bit in Extended options” • Added remark for QUIET and PERSISTANT QUIET state in Section 8.5.3.15 “EAS ALARM” • Update of die dimensions in Section 7.1 “Wafer specification” and Section 11 “Bare die outline” • Editorial changing			
276310	20131001	Objective data sheet	-	-
Modifications:	• Initial version			

15. Legal information

15.1 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 http://www.nxp.com.

15.2 Definitions

Draft — The document is a draft version only. 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 herein 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.

15.3 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 http://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.

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.

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.

Non-automotive qualified products — Unless this data sheet 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 is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

15.4 Trademarks

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

ICODE and I-CODE — are trademarks of NXP Semiconductors N.V.

16. Contact information

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

For sales office addresses, please send an email to: **salesaddresses@nxp.com**

17. Contents

continued >>

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 26 January 2015
276332