SL2S5302; SL2S5402

ICODE SLIX-S

Rev. 3.2 — 27 August 2012
192132

Product data sheet
COMPANY PUBLIC

1. General description

The ICODE SLIX-S IC is a dedicated chip for smart label applications with the need for a higher security level, larger memory and/or a product which takes care of the increasing demand for perfect customer privacy. This IC is the third generation of a product family of smart label ICs based on the ISO standards ISO/IEC 15693 (Ref. 1) and ISO/IEC 18000-3 (Ref. 4), prolonging a successful story of NXP in the field of vicinity identification systems.

The ICODE system offers the possibility of operating labels simultaneously in the field of the reader antenna (anticollision). It is designed for long range applications.

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 SLIX-S 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.
- Password protected memory management (Read/Write access):

  Pages (1 page = 4 blocks of 4 bytes each) can be protected with a password, which ensures that only authorized users get read/write access to the protected parts of the user memory (anti counterfeiting).
- Password protected Label Destroy:

  The 32-bit Destroy password enables an addressed label to be destroyed with the DESTROY SLIX-S 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 is transmitted to the label within the mentioned commands.

2. Features and benefits

2.1 ICODE SLIX-S 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 SLIX-S command with 32-bit Destroy password
- Additional fast anticollision read
- Write distance equal to read distance

2.2 EEPROM

- 2048 bits (2 KB), organized in 64 blocks of 4 bytes each, 4 blocks are summed up to 1 page
- 50 years data retention
- Write endurance of 100000 cycles

2.3 Security

- Unique identifier for each device
- 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

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

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	
SL2S5302FUD	wafer	sawn, bumped wafer, 120 μm, on film frame carrier, C_i between LA and LB = 23.5 pF (typical)	-
SL2S5402FUD	wafer	sawn, bumped wafer, 120 μm, on film frame carrier, C_i between LA and LB = 97 pF (typical)	-

5. Block diagram

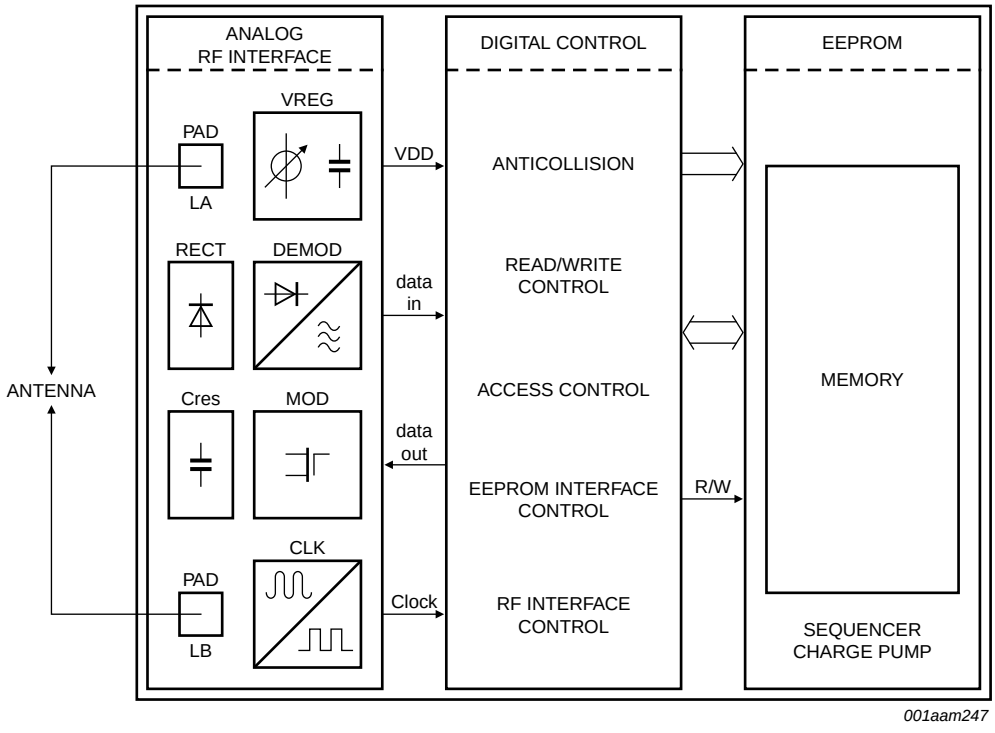


Fig 1. Block diagram of ICODE SLIX-S

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

6. Pinning information

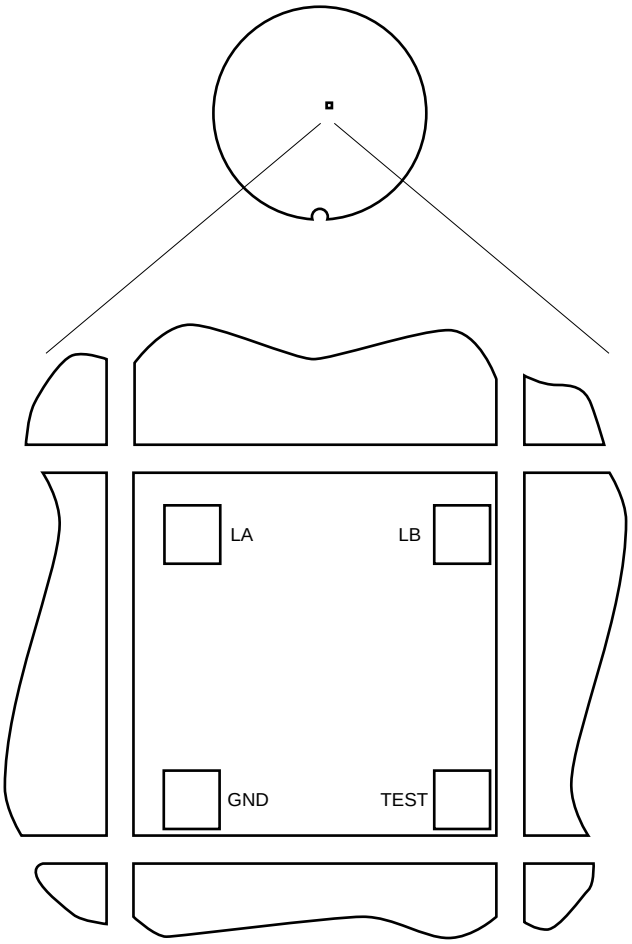


Fig 2. Wafer SL2S5302FUD layout and pin configuration for the bare die

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

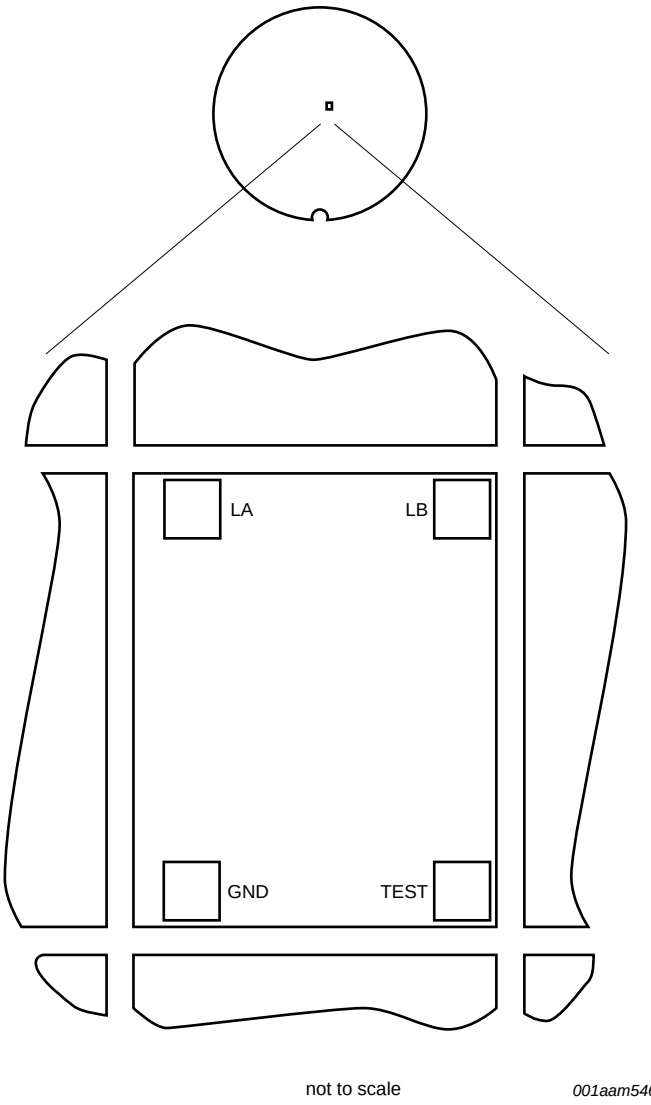


Fig 3. Wafer SL2S5402FUD layout and pin configuration for the bare die

6.1 Pin description

Table 2. Bonding pad description

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

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

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	
SL2S5302FUD	110050
SL2S5402FUD	88225
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	
SL2S5302FUD	520 μm × 484 μm = 251680 mm^2
SL2S5402FUD	520 μm × 607 μm = 315640 mm^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	400 μm
Distance pad to pad LB to TEST	
SL2S5302FUD	360 μm
SL2S5402FUD	517 μm
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

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

Table 3. Wafer specification

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	60 μm × 60 μm
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”.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

8. Functional description

8.1 Block description

The ICODE SLIX-S 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 2048 bit EEPROM memory is divided into 64 blocks. A block is the smallest access unit. Each block consists of 4 bytes (1 block = 32 bits). 4 blocks are summed up to 1 page for password protection. Bit 0 in each byte represents the least significant bit (LSB) and bit 7 the most significant bit (MSB), respectively.

The memory is divided into 2 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. This memory area cannot be directly accessed.
- User memory
  - Within the 1280 bit memory 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.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

Table 4. Memory organization

Page	Block	Byte 0	Byte 1	Byte 2	Byte 3	Description
						Configuration area for internal use
0	0					User memory:
	1					10 pages,
	2					4 blocks each,
	3					4 bytes each,
:	:	:	:	:	:	160 bytes in total.
9	36					
	37					
	38					
	39					

Blocks 0 to 39 can be addressed with read and write commands only.

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 SLIX-S IC is “02h”.

Bit 37 is set to logic 1 for the ICODE SLIX-S IC which indicates that this type supports the password protected AFI feature (not supported by ICODE SLI-S with bit 37 set to logic 0).

Table 5. Unique identifier

MSB							LSB
64:57	56:49	48:41	40:1				
“E0”	“04”	“02”	IC manufacturer serial number				
UID 7	UID 6	UID 5	UID 4	UID 3	UID 2	UID 1	UID 0

8.2.2 Configuration of delivered ICs

ICODE SLIX-S 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
- 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

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

- 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 Supported commands

8.4.1 Mandatory commands

8.4.1.1 INVENTORY

As defined in ISO/IEC 15693-3.

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

8.4.1.2 STAY QUIET

As defined in ISO/IEC 15693-3.

8.4.2 Optional commands

8.4.2.1 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 8.5 “Error handling”).

8.4.2.2 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.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

If the addressed block is part of a write protected page or only protected with the Read Password (see Section 8.4.3.6 “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 8.5 “Error handling”).

8.4.2.3 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 8.4.3.6 “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 8.5 “Error handling”).

8.4.2.4 SELECT

As defined in ISO/IEC 15693-3.

8.4.2.5 RESET TO READY

As defined in ISO/IEC 15693-3.

8.4.2.6 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 8.4.3.17 “PASSWORD PROTECT EAS/AFI”.

8.4.2.7 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 8.4.3.17 “PASSWORD PROTECT EAS/AFI”.

8.4.2.8 WRITE DSFID

As defined in ISO/IEC 15693-3.

Option 0 (Option flag not set) is supported.

Option 1 (Option flag set) is supported.

8.4.2.9 LOCK DSFID

As defined in ISO/IEC 15693-3.

Option 0 (Option flag not set) is supported.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

Option 1 (Option flag set) is supported.

8.4.2.10 GET SYSTEM INFORMATION

As defined in ISO/IEC 15693-3.

The TAG type of the ICODE SLIX-S IC is “02h”.

8.4.3 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.

8.4.3.1 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 command have to be calculated with the password and the random number (see Section 8.4.3.2 “SET PASSWORD”).

The different passwords are addressed with the password identifier.

Table 6. 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 7. Response format when Error_flag set

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

Table 8. Response format when Error_flag NOT set

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

8.4.3.2 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 8.4.3.10 “ENABLE PRIVACY”), the timing of the SET PASSWORD command is write alike.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

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 9. 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 10. Password Identifier

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

Table 11. Response format when Error_flag set

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

Table 12. 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.

8.4.3.3 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 8.4.3.4 “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.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

Option 1 (Option flag set) is supported.

Table 13. 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 14. Password Identifier

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

Table 15. Response format when Error_flag set

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

Table 16. Response format when Error_flag NOT set

SOF	Flags	CRC16	EOF
-	8 bits	16 bits	-

8.4.3.4 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 17. 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	-

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

Table 18. Password identifier

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

Table 19. Response format when Error_flag set

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

Table 20. Response format when Error_flag NOT set

SOF	Flags	CRC16	EOF
-	8 bits	16 bits	-

8.4.3.5 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 PROTECT EAS/AFI command.

The timing of the command is write alike.

Table 21. 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 22. Response format when Error_flag set

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

Table 23. Response format when Error_flag NOT set

SOF	Flags	CRC16	EOF
-	8 bits	16 bits	-

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

8.4.3.6 PROTECT PAGE

Command code = B6h

The PROTECT PAGE command enables the page protection condition to be changed under the following circumstances:

- The related passwords (Read and/or Write password) have been transmitted first with the SET PASSWORD command. If the 64-bit PASSWORD PROTECT EAS/AFI is enabled, the Read and Write passwords have to be transmitted first.
- The addressed page protection condition is not locked (see Section 8.4.3.7 “LOCK PAGE PROTECTION CONDITION” on page 16

The timing of the command is write alike.

Table 24. Request format

SOF	Flags	PROTECT PAGE	IC Mfg code	UID	Page number	Protection status	CRC16	EOF
-	8 bits	8 bits	8 bits	64 bits optional	8 bits	8 bits	16 bits	-

Table 25. Protection status

Protection status	32 bit password protection	64 bit password protection
00h	Public	Public
01h	Read and Write protected by the Read password	Read and Write protected by the Read plus Write password
10h	Write protected by the Write password	Write protected by the Read plus Write password
11h	Read protected by the Read password **and** Write protected by the Write password	Read and Write protected by the Read plus Write password

Table 26. Response format when Error_flag set

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

Table 27. Response format when Error_flag NOT set

SOF	Flags	CRC16	EOF
-	8 bits	16 bits	-

8.4.3.7 LOCK PAGE PROTECTION CONDITION

Command code = B7h

The LOCK PAGE PROTECTION CONDITION command enables the status of the page protection condition of the related page to be locked if the Read and Write passwords have been transmitted first with the SET PASSWORD command.

The timing of the command is write alike.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

Table 28. Request format

SOF	Flags	LOCK PAGE PROTECTION CONDITION	IC Mfg code	UID	Page number	CRC16	EOF
-	8 bits	8 bits	8 bits	64 bits optional	8 bits	16 bits	-

Table 29. Response format when Error_flag set

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

Table 30. Response format when Error_flag NOT set

SOF	Flags	CRC16	EOF
-	8 bits	16 bits	-

8.4.3.8 GET MULTIPLE BLOCK PROTECTION STATUS

Command code = B8h

The GET MULTIPLE BLOCK PROTECTION STATUS command requests the label to respond with the block protection status of the requested blocks.

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

Remark: 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 security status bytes is less than the requested number, which means that the last returned status byte is the one corresponding to the highest available user block, followed by the 16-bit CRC and the EOF.

Table 31. Request format

SOF	Flags	GET MULTIPLE BLOCK PROTECTION STATUS	IC Mfg code	UID	First block number	Number of blocks	CRC16	EOF
-	8 bits	8 bits	8 bits	64 bits optional	8 bits	8 bits	16 bits	-

Table 32. Response format when Error_flag set

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

Table 33. Response format when Error_flag NOT set

SOF	Flags	Block protection status	CRC16	EOF
-	8 bits	8 bits	16 bits	-
		Repeated as needed		

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

Table 34. Block protection status

Bit	Name	Value	Description
b1 (LSB)	Lock bit (WAC)[1]	0	Block is not locked
		1	Block is locked (LOCK BLOCK command)
b2	Read password protected	0	disabled
		1	enabled
b3	Write password protected	0	disabled
		1	enabled
b4	Page protection lock	0	not locked
		1	locked
b5 to b8 (MSB)	-	0	

[1] WAC: Write Access Condition.

8.4.3.9 DESTROY SLIX-S

Command code = B9h

The DESTROY SLIX-S command enables the ICODE SLIX-S Label IC to be destroyed if the Destroy SLIX-S password is correct. This command is irreversible and the ICODE SLIX-S will never respond to any command again.

The DESTROY SLIX-S 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 35. Request format

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

Table 36. Response format when Error_flag set

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

Table 37. Response format when Error_flag NOT set

SOF	Flags	CRC16	EOF
-	8 bits	16 bits	-

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

8.4.3.10 ENABLE PRIVACY

Command code = BAh

The ENABLE PRIVACY command enables the ICODE SLIX-S Label IC to be set to Privacy mode if the Privacy password is correct. The ICODE SLIX-S 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 38. 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 39. Response format when Error_flag set

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

Table 40. Response format when Error_flag NOT set

SOF	Flags	CRC16	EOF
-	8 bits	16 bits	-

8.4.3.11 INVENTORY PAGE READ

Command code = B0h

When receiving the INVENTORY PAGE READ request, the ICODE SLIX-S IC performs the same as the anticollision sequence, with the difference that instead of the UID and the DSFID, the requested memory content is re-transmitted from the ICODE SLIX-S IC.

If an error is detected, the ICODE SLIX-S IC remains silent.

If the Option flag is set to logic 0, n pages of data including page protection status (password protection condition) are re-transmitted. If the Option flag is set to logic 1, n pages (4 blocks = 16 byte) of data including page protection status (password protection condition) and the part of the UID which is not part of the mask are re-transmitted.

The request contains:

- Flags
- INVENTORY PAGE READ command code
- IC manufacturer code
- AFI (if AFI flag set)

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

- Mask length
- Mask value (if mask length > 0)
- First page number to be read
- Number of pages to be read
- CRC 16

Table 41. Request format

SOF	Flags	INVENTORY PAGE READ	IC Mfg code	Optional AFI	Mask length	Mask value	First page number	Number of pages	CRC16	EOF
-	8 bits	8 bits	8 bits	8 bits	8 bits	0 to 64 bits	8 bits	8 bits	16 bits	-

The Inventory_flag must be set to logic 1.

The meaning of flags 5 to 8 is in accordance with table 5 in ISO/IEC 15693-3.

The number of pages in the request is one less than the number of pages that the ICODE SLIX-S IC returns in its response.

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

Table 42. Response format: Option flag logic 0

SOF	Flags	Data	CRC16	EOF
-	8 bits	Page status & data	16 bits	-
		Repeated as needed		

The ICODE SLIX-S IC reads the requested page(s) including page protection status and sends back their value in the response. The mechanism and timing of the INVENTORY PAGE READ command performs the same as the INVENTORY command which is described in clause 8 of ISO/IEC 15693-3.

The requested page(s) is (are) transmitted in the following format and repeated as necessary (depending on number of pages):

Table 43. Page protection status byte

Page Protection Status byte		Page data
00h:	page is public (not protected with Read password) or the valid Read password has been transmitted before	16 byte page data content
0Fh:	page is protected with the Read password and the valid Read password has not been transmitted before	no data

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

Table 44. 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	Page status & data	16 bits	-
		Multiple of 8 bits	Repeated as needed		

The ICODE SLIX-S IC reads the requested page(s) including page protection status 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

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

with zeros up to the next byte boundary, the corresponding bits of the UID are returned. The mechanism and timing of the INVENTORY PAGE READ command perform the same as the INVENTORY command which is described in clause 8 of ISO/IEC 15693-3.

The requested page(s) is (are) transmitted in the following format and repeated as necessary (depending on number of pages):

Table 45. Page protection status byte

Page Protection Status Byte		Page data
00h:	page is public (not protected with Read password) or the valid Read password has been transmitted before	16 byte page data content
0Fh:	page is protected with the Read password and the valid Read password has not been transmitted before	no data

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

- 16 slots: 60 bits (bit 64 to bit 5) - 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 page number and number of pages exceeds the total available number of user pages, the number of transmitted pages is less than the requested number of pages, which means that the last returned page is the highest available user page, followed by the 16-bit CRC and the EOF.

- Example: mask length = 30 bits
- Returned: bit 64 to bit 5 (30 bits) = 30 bits gives 4 bytes

Table 46. 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 SLIX-S IC

8.4.3.12 FAST INVENTORY PAGE READ

Command code = B1h

When receiving the FAST INVENTORY PAGE READ command the ICODE SLIX-S IC behaves the same as the INVENTORY PAGE READ command with the following exceptions:

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

In the ICODE SLIX-S IC to the interrogator direction, only the single subcarrier mode is supported.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

8.4.3.13 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 47. Request format

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

Table 48. Response format when Error_flag set

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

Table 49. Response format when Error_flag NOT set

SOF	Flags	CRC16	EOF
-	8 bits	16 bits	-

8.4.3.14 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 50. Request format

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

Table 51. Response format when Error_flag set

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

Table 52. Response format when Error_flag NOT set

SOF	Flags	CRC16	EOF
-	8 bits	16 bits	-

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

8.4.3.15 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 53. Request format

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

Table 54. Response format when Error_flag set

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

Table 55. Response format when Error_flag NOT set

SOF	Flags	CRC16	EOF
-	8 bits	16 bits	-

8.4.3.16 EAS ALARM

Command code = A5h

The EAS ALARM command can be used in the following three 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 SLIX-S 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 SLIX-S 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 SLIX-S IC will answer with its EAS ID.

Table 56. 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	-

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

If an error is detected the ICODE SLIX-S 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 57. Response format

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 58. Response format

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 8.4.3.14 “RESET EAS”), the ICODE SLIX-S IC remains silent.

8.4.3.17 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 59. 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 60. Response format when Error_flag set

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

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

Table 61. Response format when Error_flag NOT set

SOF	Flags	CRC16	EOF
-	8 bits	16 bits	-

8.4.3.18 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 protectd (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.

Table 62. 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 63. Response format when Error_flag set

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

Table 64. Response format when Error_flag NOT set

SOF	Flags	CRC16	EOF
-	8 bits	16 bits	-

8.5 Error handling

8.5.1 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.

8.5.2 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.

8.5.2.1 Non Addressed Mode

The label IC remains silent.

8.5.2.2 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.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

8.5.3 Parameter out of range

8.5.3.1 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.

8.5.3.2 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 behaviour 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).

8.6 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)

8.7 RF interface

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

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

9. Limiting values

Table 65. 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 66. 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 67. 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		1.5	-	1.7	V
$P_{i(min)}$	minimum input power	operating	[2]	-	40	-	µW
C_i	input capacitance	between LA and LB	[3]				
		SL5302FUD		22.3	23.5	24.7	pF
		SL5402FUD		92	97	102	pF

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

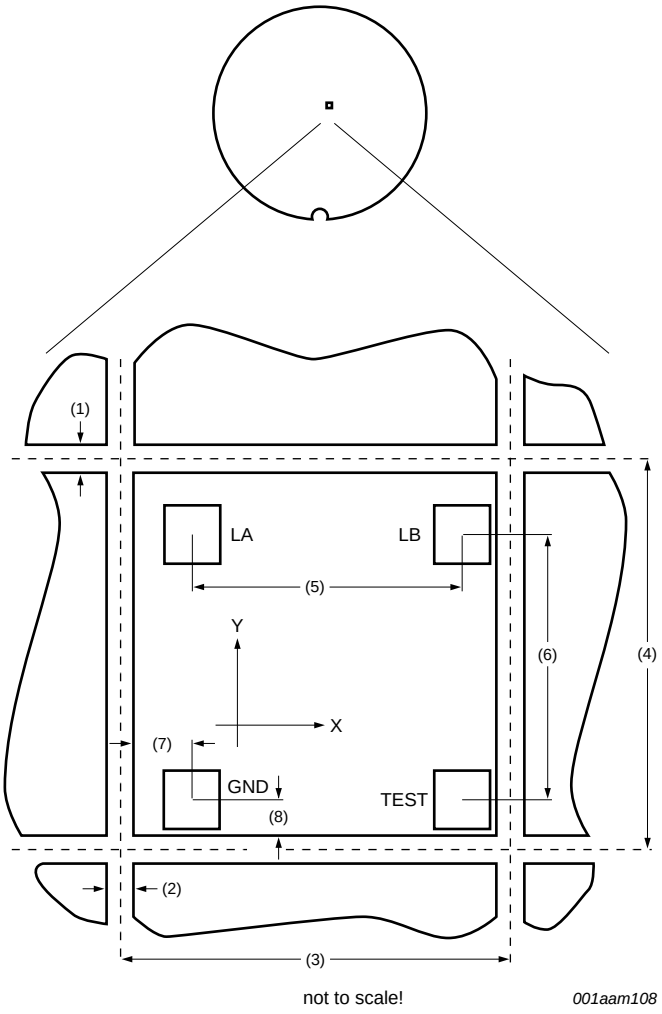
[2] Including losses in the resonant capacitor and rectifier.

[3] Measured with an HP4285A LCR meter at 13.56 MHz and 2 V RMS.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

11. Bare die outline



(1) X-scribe line width: 15 μm

(2) Y-scribe line width: 15 μm

(3) Chip step, X-length: 535 μm

(4) Chip step, Y-length: 499 μm

(5) Bump to bump distance X (LA - LB): 400 μm

(6) Bump to bump distance Y (LB - TEST): 360 μm

(7) Distance bump to nitride edge X: 75 μm

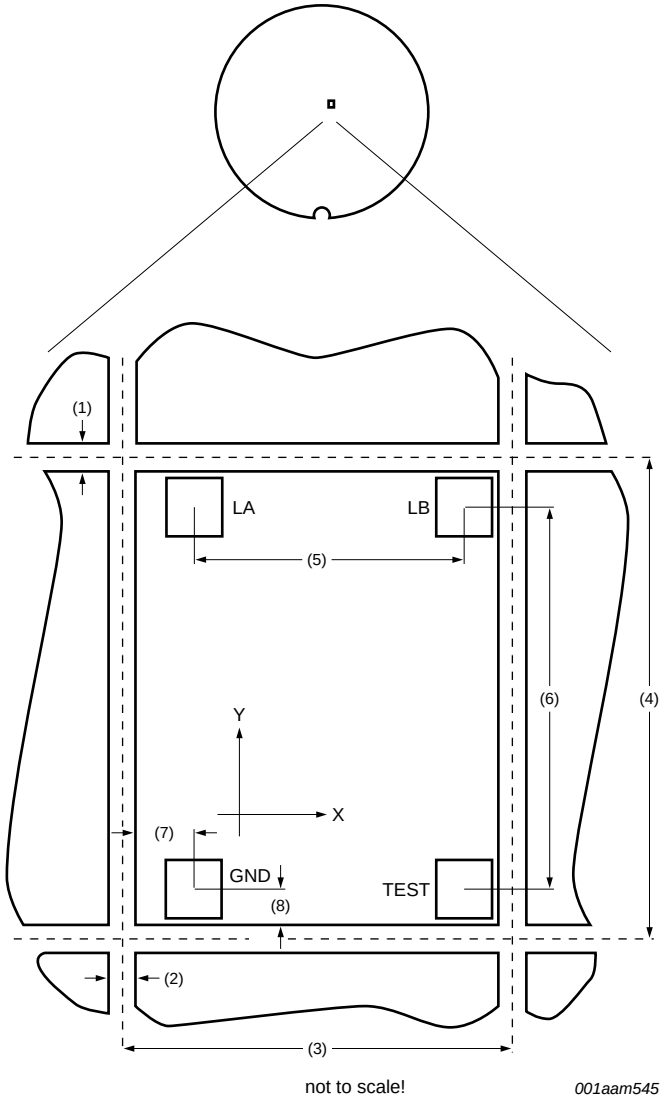
(8) Distance bump to nitride edge Y: 45 μm

Bump size X × Y: 60 μm × 60 μm

Fig 4. Wafer SL2S5302FUD bare die layout

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.



(1) X-scribe line width: 15 μm

(2) Y-scribe line width: 15 μm

(3) Chip step, X-length: 535 μm

(4) Chip step, Y-length: 622 μm

(5) Bump to bump distance X (LA - LB): 400 μm

(6) Bump to bump distance Y (LB - TEST): 517 μm

(7) Distance bump to nitride edge X: 75 μm

(8) Distance bump to nitride edge Y: 45 μm

Bump size X × Y: 60 μm × 60 μm

Fig 5. Wafer SL2S5402FUD bare die layout

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

12. Abbreviations

Table 68. 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 – BL-ID document number: 1093**[1].

1. ** ... document version number

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

14. Revision history

Table 69. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
SL2S5302_SL2S5402 v.3.2	20120827	Product data sheet	-	SL2S5302_SL2S5402 v.3.1
Modifications:	• Security status changed into “COMPANY PUBLIC”			
SL2S5302_SL2S5402 v.3.1	20100930	Product data sheet	-	SL2S5302 v.3.0
Modifications:	• Added type number SL2S5402 • Document layout updated • Table 67: symbols and parameter descriptions updated			
SL2S5302 v.3.0	20100527	Product data sheet	-	192120
192120	20100517	Preliminary data sheet	-	-

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

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.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

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 B.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**

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

17. Tables

Table 1. Ordering information 3
Table 2. Bonding pad description 5
Table 3. Wafer specification 6
Table 4. Memory organization 9
Table 5. Unique identifier 9
Table 6. Request format 12
Table 7. Response format when Error_flag set 12
Table 8. Response format when Error_flag NOT set . . . 12
Table 9. Request format 13
Table 10. Password Identifier 13
Table 11. Response format when Error_flag set 13
Table 12. Response format when Error_flag NOT set . . . 13
Table 13. Request format 14
Table 14. Password Identifier 14
Table 15. Response format when Error_flag set 14
Table 16. Response format when Error_flag NOT set . . . 14
Table 17. Request format 14
Table 18. Password identifier 15
Table 19. Response format when Error_flag set 15
Table 20. Response format when Error_flag NOT set . . . 15
Table 21. Request format 15
Table 22. Response format when Error_flag set 15
Table 23. Response format when Error_flag NOT set . . . 15
Table 24. Request format 16
Table 25. Protection status 16
Table 26. Response format when Error_flag set 16
Table 27. Response format when Error_flag NOT set . . . 16
Table 28. Request format 17
Table 29. Response format when Error_flag set 17
Table 30. Response format when Error_flag NOT set . . . 17
Table 31. Request format 17
Table 32. Response format when Error_flag set 17
Table 33. Response format when Error_flag NOT set . . . 17
Table 34. Block protection status 18
Table 35. Request format 18
Table 36. Response format when Error_flag set 18
Table 37. Response format when Error_flag NOT set . . 18
Table 38. Request format 19
Table 39. Response format when Error_flag set 19
Table 40. Response format when Error_flag NOT set . . 19
Table 41. Request format 20
Table 42. Response format: Option flag logic 0 20
Table 43. Page protection status byte 20
Table 44. Response format: Option flag logic 1 20
Table 45. Page protection status byte 21
Table 46. Example: mask length = 30 21
Table 47. Request format 22
Table 48. Response format when Error_flag set 22
Table 49. Response format when Error_flag NOT set . . 22
Table 50. Request format 22
Table 51. Response format when Error_flag set 22
Table 52. Response format when Error_flag NOT set . . 22
Table 53. Request format 23
Table 54. Response format when Error_flag set 23
Table 55. Response format when Error_flag NOT set . . 23
Table 56. Request format 23
Table 57. Response format 24
Table 58. Response format 24
Table 59. Request format 24
Table 60. Response format when Error_flag set 24
Table 61. Response format when Error_flag NOT set . . 25
Table 62. Request format 25
Table 63. Response format when Error_flag set 25
Table 64. Response format when Error_flag NOT set . . 25
Table 65. Limiting values (Wafer)[1][2] 27
Table 66. Wafer EEPROM characteristics 27
Table 67. Interface characteristics 27
Table 68. Abbreviations 30
Table 69. Revision history 31

18. Figures

Fig 1. Block diagram of ICODE SLIX-S 3
Fig 2. Wafer SL2S5302FUD layout and pin configuration for the bare die. 4
Fig 3. Wafer SL2S5402FUD layout and pin configuration for the bare die. 5
Fig 4. Wafer SL2S5302FUD bare die layout 28
Fig 5. Wafer SL2S5402FUD bare die layout 29

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2012. All rights reserved.

19. Contents

1 General description 1
1.1 Contactless energy and data transfer 1
1.2 Anticollision 1
1.3 Security and privacy aspects 1
2 Features and benefits 2
2.1 ICODE SLIX-S RF interface (ISO/IEC 15693) . 2
2.2 EEPROM 2
2.3 Security 2
3 Applications 3
4 Ordering information 3
5 Block diagram 3
6 Pinning information 4
6.1 Pin description 5
7 Mechanical specification 6
7.1 Wafer specification 6
7.1.1 Fail die identification 7
7.1.2 Map file distribution 7
8 Functional description 8
8.1 Block description 8
8.2 Memory organization 8
8.2.1 Unique identifier 9
8.2.2 Configuration of delivered ICs 9
8.3 Communication principle 10
8.4 Supported commands 10
8.4.1 Mandatory commands 10
8.4.1.1 INVENTORY 10
8.4.1.2 STAY QUIET 10
8.4.2 Optional commands 10
8.4.2.1 READ SINGLE BLOCK 10
8.4.2.2 WRITE SINGLE BLOCK 10
8.4.2.3 LOCK BLOCK 11
8.4.2.4 SELECT 11
8.4.2.5 RESET TO READY 11
8.4.2.6 WRITE AFI 11
8.4.2.7 LOCK AFI 11
8.4.2.8 WRITE DSFID 11
8.4.2.9 LOCK DSFID 11
8.4.2.10 GET SYSTEM INFORMATION 12
8.4.3 Custom commands 12
8.4.3.1 GET RANDOM NUMBER 12
8.4.3.2 SET PASSWORD 12
8.4.3.3 WRITE PASSWORD 13
8.4.3.4 LOCK PASSWORD 14
8.4.3.5 64 BIT PASSWORD PROTECTION 15
8.4.3.6 PROTECT PAGE 16
8.4.3.7 LOCK PAGE PROTECTION CONDITION . . . 16
8.4.3.8 GET MULTIPLE BLOCK PROTECTION STATUS 17
8.4.3.9 DESTROY SLIX-S 18
8.4.3.10 ENABLE PRIVACY 19
8.4.3.11 INVENTORY PAGE READ 19
8.4.3.12 FAST INVENTORY PAGE READ 21
8.4.3.13 SET EAS 22
8.4.3.14 RESET EAS 22
8.4.3.15 LOCK EAS 23
8.4.3.16 EAS ALARM 23
8.4.3.17 PASSWORD PROTECT EAS/AFI 24
8.4.3.18 WRITE EAS ID 25
8.5 Error handling 25
8.5.1 Transmission errors 25
8.5.2 Not supported commands or options 25
8.5.2.1 Non Addressed Mode 25
8.5.2.2 Addressed or Selected Mode 25
8.5.3 Parameter out of range 26
8.5.3.1 Read commands 26
8.5.3.2 Write and lock commands 26
Non Addressed Mode 26
Addressed or Selected Mode 26
8.6 Data integrity 26
8.7 RF interface 26
9 Limiting values 27
10 Characteristics 27
10.1 Wafer memory characteristics 27
10.2 Interface characteristics 27
11 Bare die outline 28
12 Abbreviations 30
13 References 30
14 Revision history 31
15 Legal information 32
15.1 Data sheet status 32
15.2 Definitions 32
15.3 Disclaimers 32
15.4 Trademarks 33
16 Contact information 33
17 Tables 34
18 Figures 34
19 Contents 35

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

© NXP B.V. 2012. All rights reserved.

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

Date of release: 27 August 2012
192132

X-ON Electronics

Largest Supplier of Electrical and Electronic Components

Click to view similar products for NFC/RFID Tags & Transponders ***category:***

Click to view products by NXP ***manufacturer:***

Other Similar products are found below :

PCF7941ATSM2AB120, NT2H0301F0DTL,125 PNEV512B,699 V680-D1KP54T V680S-A40 50M PN7120A0EV/C10801Y TRPGR30ATGA SPS1M003B SPS1M003A SPS1M002B SPS1M002A V680S-A40 10M V680-D1KP66T ATA5577M2330C-DBQ SL2S5302FTBX LXMSJZNCMD-217 60208 60170 P5DF081X0/T1AD2060 MF1S5030XDA8/V1J MF1S7030XDA4/V1J HT1MOA4S30/E/3J HT2MOA4S20/E/3/RJ MFRC52302HN1,157 TRPGR30ATGB NRF51822-QFAA-R 20926410601 CLRC66303HNE ART915X1620TX16-IC ART915X2117225TX21-IC 28448 ART923X1015YZ10-IC ART868X130903TX13 ART868X25275YZ25 ART915X050503OP-IC ART915X100202TO-IC ART915X100503JA-IC ART915X130930TX13-IC ART915X250903AM-IC ART915X2509EP60-IC ART915X252503MA-IC ART915X25275YZ25 ART915X25275YZ25-IC ART923X1015YZ10 AS3932-BTST AS3933-BTST 20926410802 LXMSJZNCMF-198 MIKROE-779 13356-0571