Chipsmall Limited consists of a professional team with an average of over 10 year of expertise in the distribution of electronic components. Based in Hongkong, we have already established firm and mutual-benefit business relationships with customers from,Europe,America and south Asia,supplying obsolete and hard-to-find components to meet their specific needs.

With the principle of “Quality Parts,Customers Priority,Honest Operation,and Considerate Service”,our business mainly focus on the distribution of electronic components. Line cards we deal with include Microchip,ALPS,ROHM,Xilinx,Pulse,ON,Everlight and Freescale. Main products comprise IC,Modules,Potentiometer,IC Socket,Relay,Connector.Our parts cover such applications as commercial,industrial, and automotives areas.

We are looking forward to setting up business relationship with you and hope to provide you with the best service and solution. Let us make a better world for our industry!

Contact us

Tel: +86-755-8981 8866 Fax: +86-755-8427 6832
Email & Skype: info@chipsmall.com Web: www.chipsmall.com
Address: A1208, Overseas Decoration Building, #122 Zhenhua RD., Futian, Shenzhen, China

SL2S2602

ICODE SLIX2

Rev. 4.1 — 25 July 2017
276341

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/BG	Wafer	sawn, bumped wafer, 120 µm with 7 µ Polyimide spacer, on film frame carrier, C_i between LA and LB = 23.5 pF (typical)	-
SL2S2602FA8	MOA8	plastic lead less module carrier package; 35 mm wide tape; C_i between LA and LB = 23.5 pF (typical)	SOT500-4

5 Block diagram

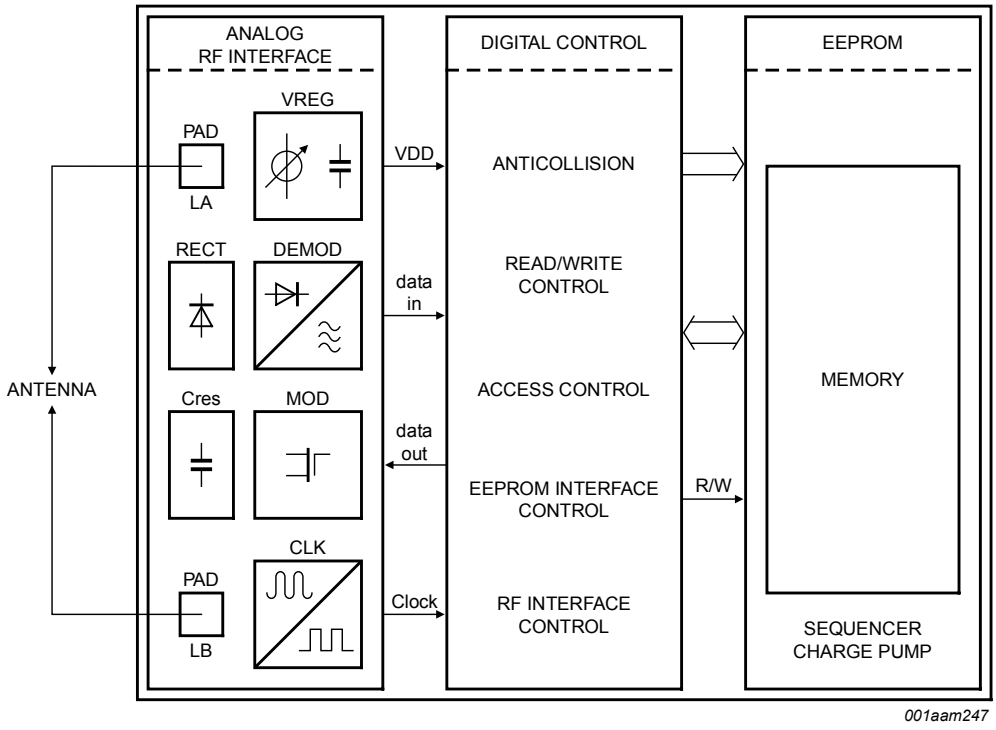
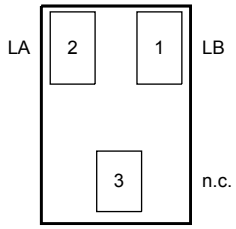


Figure 1. Block diagram of ICODE SLIX2

6 Pinning information



Transparent top view

Figure 2. Pin configuration for SOT1122

Table 2. Pin description SOT1122

Pin	Symbol	Description
1	LB	antenna RF input
2	LA	antenna RF input
3	n.c.	not connected

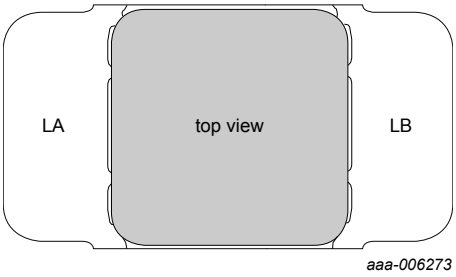


Figure 3. Pin configuration for SOT500-4 (MOA8)

Table 3. Pin description SOT500-4 (MOA8)

Pin	Symbol	Description
LA	LA	antenna RF input
LB	LB	antenna RF input

7 Wafer Layout

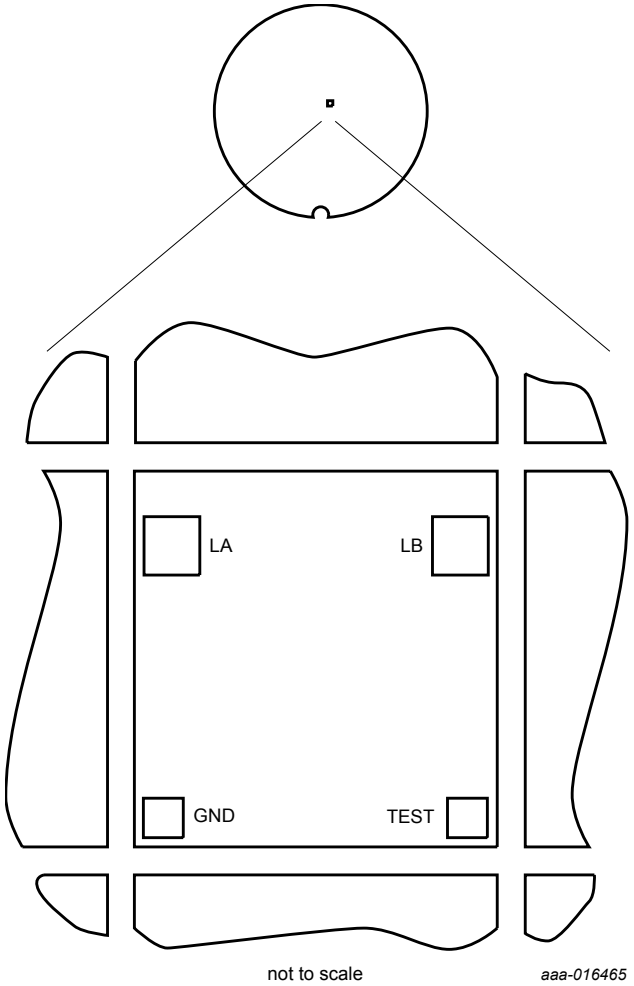


Figure 4. Wafer SL2S2602FUD/BG layout and pin configuration for the bare die

7.1 Pin Description

Table 4. Bonding pad description

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

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

8 Mechanical specification

The ICODE SLIX2 wafers are available in 120 µm thickness. The 120 µm thick wafer is enhanced with 7 µm Polyimide spacer providing better assembly tolerance (e.g. pressure).

8.1 Wafer specification

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

Table 5. 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 = 0.29322 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	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
Polyimide spacer	7 µm ± 1 µm
Au bump	
Material	>99.9 % pure Au
Hardness	35 HV to 80 HV 0.005

Shear strength	>70 MPa
Height	25 µm[1]
Height uniformity	
within a die	±2 µm
within a wafer	±3 µm
wafer to wafer	±4 µm
Bump flatness	±1.5 µm
Bump size	
LA, LB	80 µm × 80 µm
TEST, GND	60 µm × 60 µm
variation	±5 µm
Under bump metallization	sputtered TiW

1. Because of the 7 µm spacer, the bump will measure 18 µm relative height protruding the spacer.

8.1.1 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".

8.1.2 Map file distribution

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

9 Functional description

9.1 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).

9.2 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 6. 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").

9.2.1 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 8).

Table 7. 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 8. Type indicator bits

Bit 37	Bit 36	ICODE Type
0	0	ICODE SLI
1	0	ICODE SLIX

Bit 37	Bit 36	ICODE Type
0	1	ICODE SLIX2
1	1	RFU

9.2.2 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 9.5.3.20 "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).

9.2.3 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.

9.3 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).

For additional recommendations when using 100% ASK refer to Ref. 8.

9.4 State diagram

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

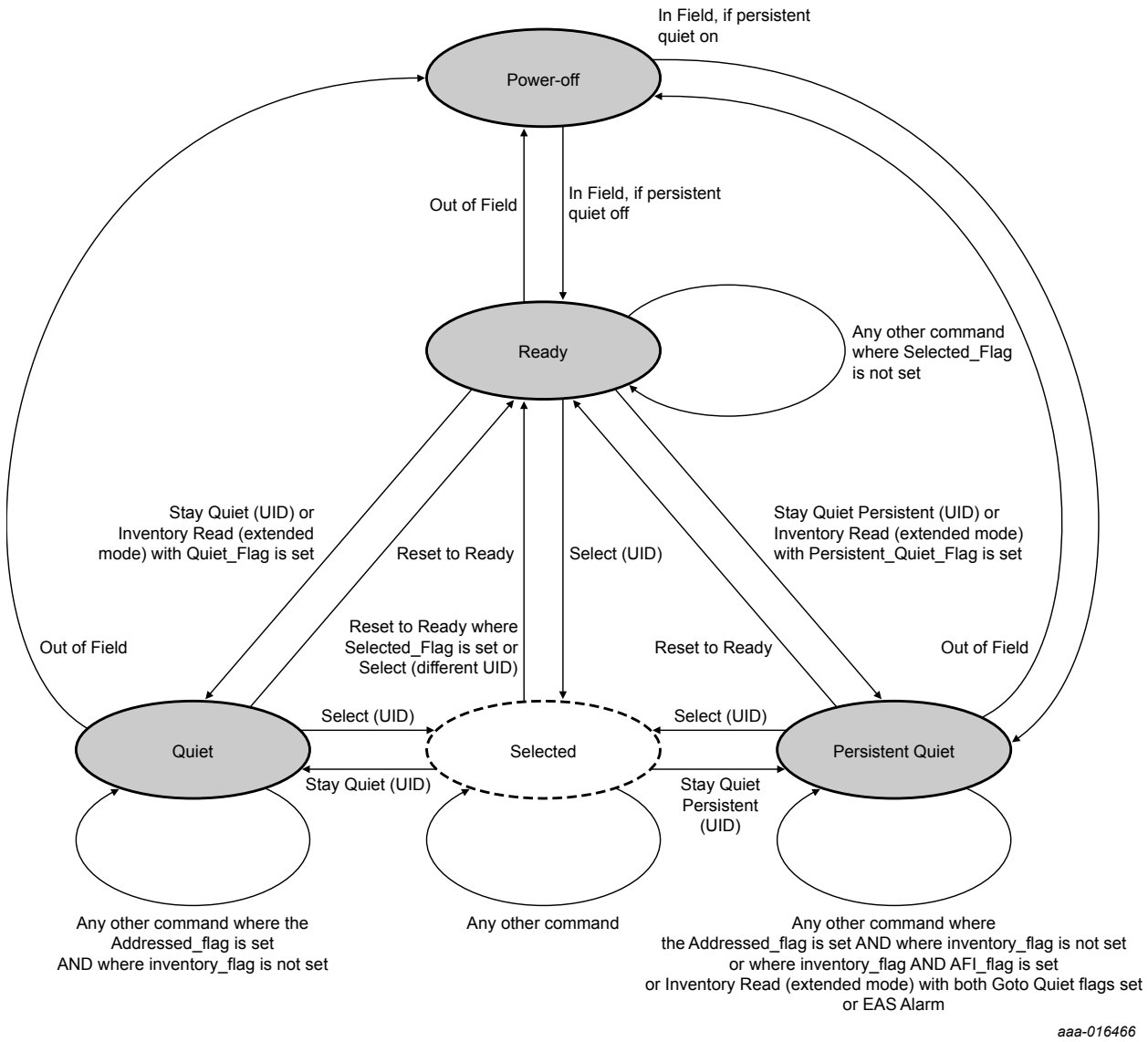


Figure 5. State diagram ICODE SLIX2

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.

9.5 Supported commands

9.5.1 Mandatory commands

9.5.1.1 INVENTORY

As defined in ISO/IEC 15693-3.

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

9.5.1.2 STAY QUIET

As defined in ISO/IEC 15693-3.

9.5.2 Optional commands

9.5.2.1 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 9.6 "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").

9.5.2.2 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 9.5.3.6 "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 9.6 "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").

9.5.2.3 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 9.5.3.6 "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 9.6 "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").

9.5.2.4 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 9.6 "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").

9.5.2.5 SELECT

As defined in ISO/IEC 15693-3.

9.5.2.6 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 9.5.3.10 "INVENTORY READ" and Section 9.5.3.19 "STAY QUIET PERSISTENT")into the READY state.

9.5.2.7 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 9.5.3.16 "PASSWORD PROTECT EAS/AFI".

9.5.2.8 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 9.5.3.16 "PASSWORD PROTECT EAS/AFI".

9.5.2.9 WRITE DSFID

As defined in ISO/IEC 15693-3.

Option 0 (Option flag not set) is supported.

Option 1 (Option flag set) is supported.

9.5.2.10 LOCK DSFID

As defined in ISO/IEC 15693-3.

Option 0 (Option flag not set) is supported.

Option 1 (Option flag set) is supported.

9.5.2.11 GET SYSTEM INFORMATION

As defined in ISO/IEC 15693-3.

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

9.5.2.12 GET MULTIPLE BLOCK SECURITY STATUS

As defined in ISO/IEC 15693-3.

9.5.3 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.

9.5.3.1 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 9.5.3.2 "SET PASSWORD").

The different passwords are addressed with the password identifier.

Table 9. 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 10. GET RANDOM NUMBER response when Error_flag set

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

Table 11. GET RANDOM NUMBER response format when Error_flag NOT set

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

9.5.3.2 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 9.5.3.9 "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 12. 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 13. Password Identifier

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

Table 14. SET PASSWORD response format when Error_flag set

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

Table 15. 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.

9.5.3.3 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 9.5.3.4 "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 16. 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 17. Password Identifier

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

Table 18. WRITE PASSWORD response format when Error_flag set

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

Table 19. WRITE PASSWORD response format when Error_flag NOT set

SOF	Flags	CRC16	EOF
-	8 bits	16 bits	-

9.5.3.4 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 20. 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 21. Password identifier

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

Table 22. LOCK PASSWORD response format when Error_flag set

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

Table 23. LOCK PASSWORD response format when Error_flag NOT set

SOF	Flags	CRC16	EOF
-	8 bits	16 bits	-

9.5.3.5 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 24. 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 25. 64 BIT PASSWORD PROTECTION response format when Error_flag set

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

Table 26. 64 BIT PASSWORD PROTECTION response format when Error_flag NOT set

SOF	Flags	CRC16	EOF
-	8 bits	16 bits	-

9.5.3.6 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 27 shows an example of the user memory segmentation with the protection pointer address 20 (0x14).

Table 27. 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 9.5.3.7 "LOCK PAGE PROTECTION CONDITION" on page 21

The timing of the command is write alike.

Table 28. 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 29. Extended Protection status byte

Bit	Name	Value	Description
b1 (LSB)	RL	0	Page L is not read protected

Bit	Name	Value	Description
		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 30. 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 31. POTECT PAGE response format when Error_flag set

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

Table 32. 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 9.5.3.18 "GET NXP SYSTEM INFOMATION")

9.5.3.7 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 33. 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 9.6 "Error handling").

Table 34. LOCK PAGE PROTECTION CONDITION response format when Error_flag set

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

Table 35. LOCK PAGE PROTECTION CONDITION response format when Error_flag NOT set

SOF	Flags	CRC16	EOF
-	8 bits	16 bits	-

9.5.3.8 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 36. 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 37. DESTROY response format when Error_flag set

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

Table 38. DESTROY response format when Error_flag NOT set

SOF	Flags	CRC16	EOF
-	8 bits	16 bits	-

9.5.3.9 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 39. 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 40. ENABLE PRIVACY response format when Error_flag set

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

Table 41. ENABLE PRIVACY response format when Error_flag NOT set

SOF	Flags	CRC16	EOF
-	8 bits	16 bits	-

9.5.3.10 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.