SL2 ICS53/SL2 ICS54

I•CODE SLI-S/I•CODE SLI-S HC

Rev. 3.0 — 14 March 2007
113730

Product data sheet
PUBLIC

1. General description

The I•CODE SLI-S/I•CODE SLI-S HC 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 second member of a product family of smart label ICs based on the ISO standard ISO/IEC 15693 as well as on EPC Global compliant commands.

The I•CODE system offers the possibility of operating more than one label simultaneously in the field of the reader antenna (Anticollision). It is designed for long range applications with a special command for the use under the European regulations.

1.1 Anticollision

An intelligent anticollision function allows to operate more than one tag 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.

1.2 Contactless energy and data transfer

Whenever connected to a very simple and cheap 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 I•CODE SLI-S/I•CODE SLI-S HC 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 allows to transmit data with up to 53 kbit/s.

1.3 Security and privacy aspects

1. Unique Identifier (UID)

   The UID can not be altered and guarantees the uniqueness of each label.

2. OTP Memory for EPC Code

   The memory for the EPC Code is an one time programmable memory, which ensures that the data can not be changed after user programming.

3. Password protected memory management (Read/Write access)

   Pages (1 page = 4 blocks of 4 byte 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).

4. Password protected Label Destroy

   With the 32-bit destroy password an addressed label can be destroyed with the Destroy command. That status is irreversible and the label will never respond to any command again.

5. Password protected Privacy Mode

   With the 32-bit Privacy password a label can be set to the Privacy mode with the Set to Privacy Mode command. In that mode the label will not respond to any command except of the command Get Random Number till it receives again the right Privacy password. That mode is especially designed to meet the increasing demand to take care of the customers privacy.

6. Password protected EAS Functionality

   With the 32-bit EAS password the addressed label can be set in a mode that the commands Set EAS and Reset EAS are only executed by the label if the right EAS password is transmitted to the label within the mentioned commands.

2. Features

2.1 I•CODE SLI-S RF interface

- 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 free available)
- I•CODE SLI-S Functionality (ISO/IEC 15693)
  - Fast data transfer: up to 53 kbit/s
  - High data integrity: 16-bit CRC, framing
  - True anti-collision
  - Additional fast anti-collision read
  - Password protected Electronic Article Surveillance (EAS) incl. application selection
  - Application Family Identifier (AFI) supported
  - Data Storage Format Identifier (DSFID)
  - Privacy command with 32-bit Privacy password
  - Destroy command with 32-bit Destroy password
- I•CODE EPC Functionality
  - Fast data transfer: up to 53 kbit/s
  - High data integrity: 16-bit CRC, framing
  - Anti-collision with high identification speed (approx. 200 I•CODE EPC smart labels per second)
  - Label DESTROY command with 24-bit Destroy Code protection for EPC functionality only
- Long Range Command
- Write distance equal to read distance

2.2 EEPROM

- 2048 bits (2 kbit), organized in 64 blocks of 4 byte each, 4 blocks are summed up to 1 page
- Data retention of 10 years
- Write endurance 100.000 cycles

2.3 Security features

- 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 Functionality

3. Applications

- Supply Chain Management
- Asset Management
- Container Identification
- Pallet & Case Tracking

4. Quick reference data

The data sheet describes the functionality of the smart label ICs I•CODE SLI-S and I•CODE SLI-S HC. These ICs distinguish between the built in resonance capacitance. The I•CODE SLI-S HC shows a higher capacitance value than the I•CODE SLI-S. Therefore with the I•CODE SLI-S HC smaller label designs can be realized.

Table 1: Quick reference data

	Description	Typ[1]	Unit
SL2 ICS53	I•CODE SLI-S	23.5	pF
SL2 ICS54	I•CODE SLI-S HC	97.0	pf

[1] Typical values are not guaranteed. These values listed are at room temperature.

5. Ordering information

Table 2: Ordering information

Type number	Package		
	Name	Description	Version
SL2 ICS5301EW/V7	FFC	sawn wafer 150 μm on film frame carrier	-
SL2 FCS5301EV/DH	FCP	Flip Chip Package	-
SL2 MOS5301EV	MOA2	Module for contactless chip card ICs PLMCC-05	SOT500AA1
SL2 ICS5401EW/V7	FFC	sawn wafer 150 μm on film frame carrier	-
SL2 FCS5401EV/DH	FCP	Flip Chip Package	-
SL2 MOS5401EV	MOA2	Module for contactless chip card ICs PLMCC-05	SOT500AA1

6. Block diagram

The SL2 ICS53/SL2 ICS54 IC consists of three major blocks:

Analog RF Interface

Digital Controller

EEPROM

The analog part provides stable supply voltage and demodulates data received from the reader for being processed by the digital part. Further, the modulation transistor of the analog part transmits data back to the reader.

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

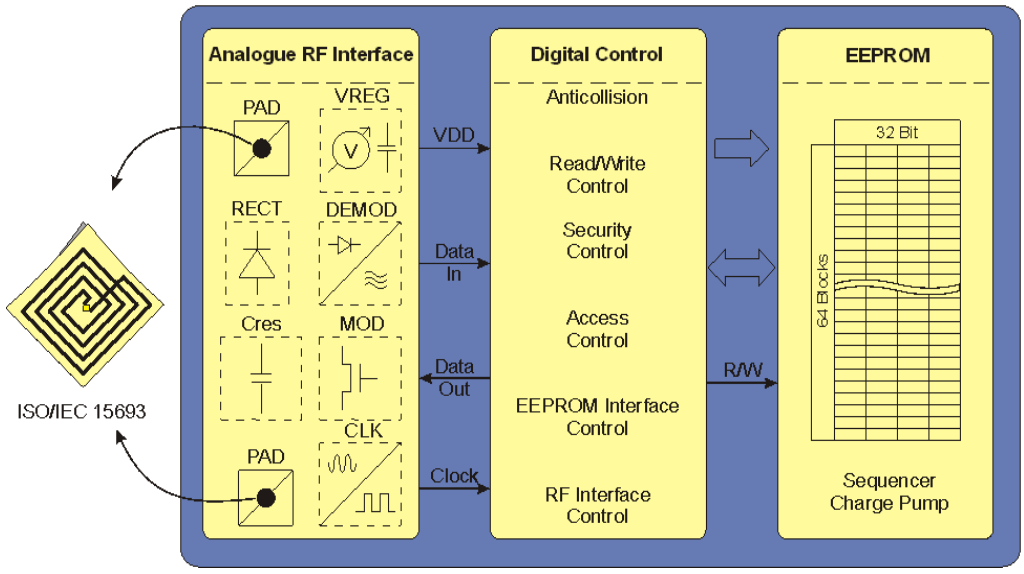

Fig 1. Block diagram of label IC

7. Functional description

7.1 Block description

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 I•CODE Label, and modulates the electromagnetic field for data transmission from the I•CODE Label to the interrogator.

Data are stored in a non-volatile memory (EEPROM). The EEPROM has a memory capacity of 2048 bit and is organized in 64 blocks consisting of 4 bytes each (1 block = 32 bits). The higher 40 blocks contain user data and the lowest 24 blocks contain the unique identifier, EPC Memory, security, the write access conditions and special data like AFI and DSFID.

7.2 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 are stored like UID, EPC Data, Write protection, Access control information, Passwords and so on. Direct access to this memory area is not possible.
- User Memory
  - Within this 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.

Table 3. Memory Organization

Page	Block	Byte 0	Byte 1	Byte 2	Byte 3	Description
-6	-24					Configuration Area for internal use
	-23					
	-22					
	-21					
:	:	:	:	:	:	
:	:	:	:	:	:	
:	:	:	:	:	:	
:	:	:	:	:	:	
-1	-4					
	-3					
	-2					
	-1					
0	0					User Memory • 10 pages • 4 blocks each • 4 bytes each • (total 160 bytes)
	1					
	2					
	3					
:	:	:	:	:	:	
:	:	:	:	:	:	
:	:	:	:	:	:	
:	:	:	:	:	:	
9	36					
	37					
	38					
	39					

7.2.1 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 numbering of the 64 bits is done according to ISO/IEC 15693-3 starting with the LSB 1 and ending with the MSB 64. This is in contrast to the general used bit numbering within a byte (starting with LSB 0).

The TAG type is a part of the UID (bit 41 to 48, after the manufacturer code which is “04h” for NXP Semiconductors).

The TAG type of the SL2 ICS53/SL2 ICS54 is “02h”

Table 4. Unique Identifier description

Byte	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
Name	UID 7	UID 6	UID 5	UID 4	UID 3	UID 2	UID 1	UID 0
Value	E0	04	02	IC manufacturer serial number				
Bit	64 to 57	56 to 49	48 to 41	40 to 1				
	MSB							LSB

7.2.2 Configuration of delivered ICs

I•CODE SLI-S/I•CODE SLI-S HC ICs are delivered with the following configuration by NXP Semiconductors:

- Unique Identifier is unique and read only
- Write Access Conditions allow to change user blocks, AFI, DSFID, EAS and Passwords
- All password bytes are 00h (Protection Password, Privacy Password, Destroy Password, EAS Password)
- User Data memory is **not** password protected
- Password protected Privacy Mode is disabled
- EAS password protection is disabled
- Status of EAS mode is **not** defined
- AFI is supported and **not** defined
- DSFID is supported and **not** defined
- EPC Memory is **not** defined and can be written once
- User Data memory is **not** defined

7.3 Communication principle

ISO/IEC 15693 command set

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

EPC command set

For detailed description of the protocol and timing please refer to EPC Specification “13.56 MHz ISM Band Class 1 Radio Frequency (RF) Identification Tag Interface Specification”.

8. Command set

8.1 ISO/IEC 15693 command set

8.1.1 Mandatory commands

8.1.1.1 Inventory

As defined in ISO/IEC 15693-3.

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

8.1.1.2 Stay Quiet

As defined in ISO/IEC 15693-3.

8.1.2 Optional Commands

8.1.2.1 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 Privacy or Destroy mode is enabled the label will not respond.

If the related page of the addressed block is protected with the Read-Password and the password has not been transmitted before with the Set Password command the label will respond according to the error handling (see Section 8.4 “Error handling”).

8.1.2.2 Write Single Block

Only Option 0 (Option flag is not set) is supported.

If the addressed block is part of a write protected page or only protected with the Read Password (see Section 8.1.3.6 “Protect page”) and the password has not been transmitted before with the Set Password command the label will respond according to the error handling (see Section 8.4 “Error handling”).

8.1.2.3 Lock Block

Only Option 0 (Option flag is not set) is supported.

If the addressed block is part of a write protected page or only protected with the Read Password (see Section 8.1.3.6 “Protect page”) and the password has not been transmitted before with the Set Password command the label will respond according to the error handling (see Section 8.4 “Error handling”).

8.1.2.4 Select

As defined in ISO/IEC 15693-3.

8.1.2.5 Reset to Ready

As defined in ISO/IEC 15693-3.

8.1.2.6 Write AFI

As defined in ISO/IEC 15693-3.

Only Option 0 (Option flag is not set) is supported.

8.1.2.7 Lock AFI

As defined in ISO/IEC 15693-3.

Only Option 0 (Option flag is not set) is supported.

8.1.2.8 Write DSFID

As defined in ISO/IEC 15693-3.

Only Option 0 (Option flag is not set) is supported.

8.1.2.9 Lock DSFID

As defined in ISO/IEC 15693-3.

Only Option 0 (Option flag is not set) is supported.

8.1.2.10 Get System Information

As defined in ISO/IEC 15693-3.

The TAG type of the SL2 ICS53/SL2 ICS54 is “02h”.

8.1.3 Custom Commands

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

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

8.1.3.1 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 8.1.3.2 “Set password”).

The different passwords are addressed with the Password Identifier.

Table 5. Request format

SOF	Flags	Get Random Number	IC Mfg code	UID	CRC16	EOF
	8 bits	8 bits	8 bits	64 bits	16 bits	

Table 6. Response format when Error_flag is set

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

Table 7. Response format when Error_flag is NOT set

SOF	Flags	Random Number	CRC16	EOF
	8 bits	16 bits	16 bits	

8.1.3.2 Set password

Command Code = B3h

With the Set Password command the different Passwords can be transmitted to the Label to get access to the different protected functionalities on 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 of the Privacy 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]}

The different passwords are addressed with the Password Identifier.

Table 8. Request format

SOF	Flags	Set Password	IC Mfg code	UID	Password Identifier	XOR Password	CRC16	EOF
	8 bits	8 bits	8 bits	64 bits	8 bits	32 bits	16 bits	

Table 9. Password Identifier

Password Identifier	Password
01h	Read
02h	Write
04h	Privacy
08h	Destroy SLI-S
10h	EAS

Table 10. Response format when Error_flag is set

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

Table 11. Response format when Error_flag is 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 (RF Reset) is executed.

8.1.3.3 Write password

Command Code = B4h

With the Write Password command a new password will be written into the related memory, if the related old password has already been transmitted with a Set Password command before and the addressed password is not locked (see Section 8.1.3.4 “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 get access to protected blocks/pages.

The different passwords are addressed with the Password Identifier.

Table 12. Request format

SOF	Flags	Write Password	IC Mfg code	UID	Password Identifier	Password	CRC16	EOF
	8 bits	8 bits	8 bits	64 bits	8 bits	32 bits	16 bits	

Table 13. Password Identifier

Password Identifier	Password
01h	Read
02h	Write
04h	Privacy
08h	Destroy SLI-S
10h	EAS

Table 14. Response format when Error_flag is set

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

Table 15. Response format when Error_flag is NOT set

SOF	Flags	CRC16	EOF
	8 bits	16 bits	

8.1.3.4 Lock password

Command Code = B5h

With the Lock Password command the addressed password will be locked if the related password has already been transmitted with a Set Password command before. A locked password can not be changed any longer.

The different passwords are addressed with the Password Identifier.

Table 16. Request format

SOF	Flags	Lock Password	IC Mfg code	UID	Password Identifier	CRC16	EOF
	8 bits	8 bits	8 bits	64 bits	8 bits	16 bits	

Table 17. Password identifier

Password Identifier	Password
01h	Read
02h	Write
04h	Privacy
08h	Destroy SLI-S
10h	EAS

Table 18. Response format when Error_flag is set

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

Table 19. Response format when Error_flag is NOT set

SOF	Flags	CRC16	EOF
	8 bits	16 bits	

8.1.3.5 64 bit password protection

Command Code = BBh

With the 64-bit Password Protection command the Label IC can 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 already been transmitted with a Set Password command before.

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

Table 20. Request format

SOF	Flags	64 bit PWD Parameter	IC Mfg code	UID	CRC16	EOF
	8 bits	8 bits	8 bits	64 bits	16 bits	

Table 21. Response format when Error_flag is set

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

Table 22. Response format when Error_flag is NOT set

SOF	Flags	CRC16	EOF
	8 bits	16 bits	

8.1.3.6 Protect page

Command Code = B6h

With the Page Protection command the page protection condition can be changed under the following circumstances:

- The related passwords (Read and/or Write password) have been transmitted before with the Set Password command. If the page is public no password is required.
- The addressed page Protection condition is not locked (see Page Protection Condition Lock)

Table 23. Request format

SOF	Flags	Protect Page	IC Mfg code	UID	Page number	Protection Status	CRC16	EOF
	8 bits	8 bits	8 bits	64 bits	8 bits	8 bits	16 bits	

Table 24. 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 25. Response format when Error_flag is set

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

Table 26. Response format when Error_flag is NOT set

SOF	Flags	CRC16	EOF
	8 bits	16 bits	

8.1.3.7 Lock page protection condition

Command Code = B7h

With the Lock Page Protection Condition command the status of the Page Protection Condition of the related page will be locked if the related passwords (Read and/or Write password) have been transmitted before with the Set Password command. If the page is public no password is required.

Table 27. Request format

SOF	Flags	Lock Page Protection Condition	IC Mfg code	UID	Page number	CRC16	EOF
	8 bits	8 bits	8 bits	64 bits	8 bits	16 bits	

Table 28. Response format when Error_flag is set

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

Table 29. Response format when Error_flag is NOT set

SOF	Flags	CRC16	EOF
	8 bits	16 bits	

8.1.3.8 Get multiple block protection status

Command Code = B8h

To the Get Multiple Block Protection Status command the label responds with the block protection status of the requested blocks.

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 30. 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	8 bits	8 bits	16 bits	

Table 31. Response format when Error_flag is set

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

Table 32. Response format when Error_flag is NOT set

SOF	Flags	Block Protection Status	CRC16	EOF
	8 bits	8 bits	16 bits	
		Repeated as needed		

Table 33. 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

8.1.3.9 Destroy SLI-S

Command Code = B9h

With the Destroy SLI-S command the I•CODE SLI-S/I•CODE SLI-S HC Label IC can be destroyed if the Destroy SLI-S password has been transmitted before. This command is irreversible and the I•CODE SLI-S/I•CODE SLI-S HC will never respond to any command again (ISO and EPC commands).

Remark: The Destroy SLI-S can only be executed in addressed or selected mode.

Table 34. Request format

SOF	Flags	Destroy SLI-S	IC Mfg code	UID	CRC16	EOF
	8 bits	8 bits	8 bits	64 bits	16 bits	

Table 35. Response format when Error_flag is set

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

Table 36. Response format when Error_flag is NOT set

SOF	Flags	CRC16	EOF
	8 bits	16 bits	

8.1.3.10 Enable privacy

Command Code = BAh

With the Enable Privacy command the I•CODE SLI-S/I•CODE SLI-S HC Label IC can be set into the Privacy mode. The I•CODE SLI-S/I•CODE SLI-S HC will not respond to any command except Get Random Number and Set Password.

To get out of the Privacy Status the valid Privacy password has to be transmitted to the IC with the Set Password command.

Table 37. Request format

SOF	Flags	Enable Privacy	IC Mfg code	UID	CRC16	EOF
	8 bits	8 bits	8 bits	64 bits optional	16 bits	

Table 38. Response format when Error_flag is set

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

Table 39. Response format when Error_flag is NOT set

SOF	Flags	CRC16	EOF
	8 bits	16 bits	

8.1.3.11 Inventory page read

Command Code = B0h

When receiving the Inventory Page Read request, the I•CODE SLI-S/I•CODE SLI-S HC IC performs the same as in the anti-collision sequence, with the difference that instead of the UID and the DSFID the requested memory content is re-transmitted from the I•CODE SLI-S/I•CODE SLI-S HC IC.

If an error is detected the I•CODE SLI-S/I•CODE SLI-S HC IC remains silent.

If the Option flag is set to 0 n pages of data including page protection status (password protection condition) are re-transmitted. If the option flag is set to 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 the AFI flag is set)
- Mask length
- Mask value (if mask length > 0)
- First page number to be read
- Number of pages to be read
- CRC 16

Table 40. Request format

SOF	Flags	Inventory 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 1.

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

The number of pages in the request is one less than the number of pages that the I•CODE SLI-S/I•CODE SLI-S HC IC returns in its response.

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

Table 41. Response format

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

The I•CODE SLI-S/I•CODE SLI-S HC IC reads the requested block(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 at 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 42. Page protection status byte

Page Protection Status byte		Block 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 1 the response contains:

Table 43. Response format

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 I•CODE SLI-S/I•CODE SLI-S HC 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 a padding 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 at 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 44. Page protection status byte

Page Protection Status Byte		Block 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 45. Example

Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	UID
mask value incl. padding with zeros								transmitted by Interrogator
				returned value				transmitted by I•CODE SLI-S/I•CODE SLI-S HC IC

8.1.3.12 Fast inventory page read

Command Code = B1h

When receiving the Fast Inventory Page Read command the I•CODE SLI-S/I•CODE SLI-S HC IC behaves the same as in the Inventory Page Read command with the following exceptions:

The data rate in the direction I•CODE SLI-S/I•CODE SLI-S HC IC to the interrogator is twice as 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 I•CODE SLI-S/I•CODE SLI-S HC IC and the time between the rising edge of the EOF from the interrogator to the I•CODE SLI-S/I•CODE SLI-S HC IC remain unchanged (stay the same as defined in ISO/IEC 15693-3).

In the direction I•CODE SLI-S/I•CODE SLI-S HC IC to the interrogator only the single subcarrier mode is supported.

8.1.3.13 Set EAS

Command Code = A2h

This 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 transmitted before with the Set Password command.

Table 46. Request format

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

Table 47. Response format when Error_flag is set

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

Table 48. Response format when Error_flag is NOT set

SOF	Flags	CRC16	EOF
	8 bits	16 bits	

8.1.3.14 Reset EAS

Command Code = A3h

This 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 transmitted before with the Set Password command.

Table 49. Request format

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

Table 50. Response format when Error_flag is set

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

Table 51. Response format when Error_flag is NOT set

SOF	Flags	CRC16	EOF
	8 bits	16 bits	

8.1.3.15 Lock EAS

Command Code = A4h

This 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 transmitted before with the Set Password command.

Table 52. Request format

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

Table 53. Response format when Error_flag is set

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

Table 54. Response format when Error_flag is NOT set

SOF	Flags	CRC16	EOF
	8 bits	16 bits	

8.1.3.16 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 set the EAS response is returned from the I•CODE SLI-S/I•CODE SLI-S HC IC. This configuration is compliant to 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 I•CODE SLI-S/I•CODE SLI-S HC ICs will respond with the EAS response 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 I•CODE SLI-S/I•CODE SLI-S HC IC will answer with its EAS ID.

Table 55. Request format

SOF	Flags	EAS Alarm	IC Mfg code	UID	EAS ID Mask Length	EAS ID Value	CRC16	EOF
	8 bits	8 bits	8 bits	64 bits optional	8 bits optional	0, 8 or 16 bits optional	16 bits	

If an error is detected the I•CODE SLI-S/I•CODE SLI-S HC IC remains silent.

Option flag is set to 0 or option flag is set to 1 and the EAS ID Mask Length is not equal 0:

Table 56. 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 1 and the EAS ID Mask Length is equal 0:

Table 57. 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 8.1.3.14 “Reset EAS”) the I•CODE SLI-S/I•CODE SLI-S HC IC remains silent.

8.1.3.17 Password protect EAS

Command Code = A6h

This command enables the password protection for EAS if the EAS password has to be transmitted before with the Set Password command.

Table 58. Request format

SOF	Flags	Password Protect EAS	IC Mfg code	UID	CRC16	EOF
	8 bits	8 bits	8 bits	64 bits optional	16 bits	

Table 59. Response format when Error_flag is set

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

Table 60. Response format when Error_flag is NOT set

SOF	Flags	CRC16	EOF
	8 bits	16 bits	

8.1.3.18 Write EAS ID

Command Code = A7h

With the command Write EAS ID a new EAS Identifier is stored in the corresponding configuration memory. If EAS is password protected (for Set and Reset EAS) the EAS password has to be transmitted before with the Set Password command.

Table 61. Request format

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

Table 62. Response format when Error_flag is set

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

Table 63. Response format when Error_flag is NOT set

SOF	Flags	CRC16	EOF
	8 bits	16 bits	

8.1.3.19 Read EPC

Command Code = A8h

On the command Read EPC the I•CODE SLI-S/I•CODE SLI-S HC ICs will respond with the EPC Data, if a Destroy EPC command had not been executed before.

Table 64. Request format

SOF	Flags	Read EPC	IC Mfg code	UID	CRC16	EOF
	8 bits	8 bits	8 bits	64 bits optional	16 bits	

Table 65. Response format when Error_flag is set

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

Table 66. Response format when Error_flag is NOT set

SOF	Flags	EPC	CRC16	EOF
	8 bits	96 bits, MSB first	16 bits	

8.2 EPC command set

8.2.1 Begin round

As defined in EPC Specification “13.56 MHz ISM Band Class 1 Radio Frequency (RF) Identification Tag Interface Specification”.

8.2.2 Write block

As defined in EPC Specification “13.56 MHz ISM Band Class 1 Radio Frequency (RF) Identification Tag Interface Specification”.

8.2.3 Destroy

As defined in EPC Specification “13.56 MHz ISM Band Class 1 Radio Frequency (RF) Identification Tag Interface Specification”.

Remark: With the Destroy command from the EPC command set only the EPC functionality will be destroyed.

8.3 Long range command

8.3.1 Long range CMD

Command Code = 40h

The Long Range CMD command is designed to allow the use of the higher limits defined in the ISO/TR 7003:1990. The bit and byte coding is the same as it is defined in EPC Specification “13.56 MHz ISM Band Class 1 Radio Frequency (RF) Identification Tag Interface Specification”.

To reduce the number of pulses the redundancy check is changed from a CRC8 calculation to an XOR of the transmitted parameters (Long Range CMD, Data Selector, Number of Slots)

- Number of slots:
  - If the *Data Selector* is transmitted for EAS the label will ignore the received Number of Slots parameter and will use always one Slot (like EAS Alarm command, see Section 8.1.3.16 “EAS alarm”) with EAS. For EAS typically 00h is used as the value for Number of Slots to reduce the number of transmitted pulses.
  - If the *Data Selector* is transmitted for UID or EPC the label will respond within one of the transmitted Number of Slots on a pseudo random basis and will calculate a new slot for a following command.

Labels, which have executed a Destroy EPC command before will not respond to this command if the Data Selector for EPC is transmitted.

Table 67. Request format

SSOF	Long Range CMD	Data Selector	Number of Slots	XOR	CEOF
	8 bits	8 bits	8 bits	8 bits	

Table 68. Number of Slots

Number of Slots	Value
1	10h
4	20h
8	40h
16	80h
32	00h
64	01h
128	02h
256	04h
512	08h

Table 69. Data selector

Data Selector	Value	Response
EAS	00h	LSB first
UID	01h	LSB first
EPC	02h	MSB first

Depending on Data Selector the Label ICs will respond with the requested data.

Table 70. Response format

RSOF	Requested Data	CRC16	REOF
	Depending on Data Selector	16 bits	

Table 71. Long range CMD

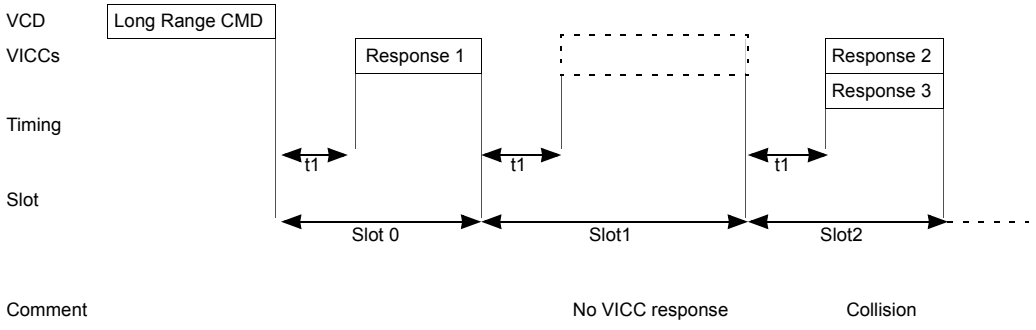

Table 72. Timing

Timing	Min.	Max.	Unit
t1	302.06 - 2.36	302.06 + 2.36	µs

8.4 Error handling

8.4.1 Transmission errors

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

8.4.2 Not supported commands or options

If the received command or option is not supported, the behaviour of the Label IC is depending on the addressing mechanism.

8.4.2.1 Non addressed mode

The label IC remains silent.

8.4.2.2 Addressed or selected mode

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

If the Inventory flag or the protocol extension flag is set the label IC will not respond if the command or option is not supported.

8.4.3 Parameter out of range

8.4.3.1 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.

8.4.3.2 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 is depending on the addressing mechanism.

8.4.3.3 Non addressed mode

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

8.4.3.4 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).

8.5 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 “1”, “0” and no information
- Channel monitoring (protocol sequence and bit stream analysis)

8.6 RF interface

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

9. Revision history

Table 73. Revision history

	Release date	Data sheet status	Change notice	Supersedes
113730	14 March 2007	Product data sheet		
Modifications:	• Initial version			

10. Legal information

10.1 Data sheet status

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.

10.2 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.

10.3 Disclaimers

General — 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.

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 medical, military, aircraft, space or life support equipment, nor in applications where failure or malfunction of a NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors accepts 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.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) may cause permanent damage to the device. Limiting values are stress ratings only and operation of the device at these or any other conditions above those given in the Characteristics sections of this document is not implied. Exposure to limiting values for extended periods may affect device reliability.

Terms and conditions of 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, including those pertaining to warranty, intellectual property rights infringement and limitation of liability, unless explicitly otherwise agreed to in writing by NXP Semiconductors. In case of any inconsistency or conflict between information in this document and such terms and conditions, the latter will prevail.

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.

10.4 Trademarks

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

11. Contact information

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

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

12. Tables

13. Figures

continued >>

14. Contents

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

Date of release: 14 March 2007
Document identifier: 113730