SL2S6002

ICODE DNA

Rev. 3.0 — 16 June 2016
374730

Product short data sheet
COMPANY PUBLIC

1. General description

The ICODE DNA is a leading-edge HF tag IC targeting brand protection tagging applications which require HF long read range as well as cryptographic authentication check.The security is based in the first place on a 128-bit AES key which is securely stored on IC's and which is used to perform cryptographic authentication by an AES coprocessor. The current version of the ICODE DNA supports the following features:

- Tag and mutual authentication using AES128
- 3 user keys for tag authentication and/or mutual authentication
- Separate privileges to define different access rights per key
- Flexible user memory segmentation with corresponding access conditions
- 2016-bit available user memory
- NXP originality signature
- Counter feature

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 DNA 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.
- Tag/mutual authentication:

The ICODE DNA features three 128-bit keys for tag and mutual authentication.The tag authentication based on AES cryptography.

Tag authentication allows proving the authenticity of a tag based on a common secret.

Mutual authentication allows proving the authenticity of a tag based on a common secret and to prove the access rights of the reader to protected data or functionality of the tag.

- EAS and AFI functionality optionally protected by mutual authentication
- 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. The preset of the 16-bit counter is protected by mutual authentication.
- Privacy and Destroy functionality protected by mutual authentication

2. Features and benefits

2.1 ICODE DNA RF interface (ISO/IEC 15693)

- Contactless transmission of data and supply energy (no battery needed)
- Operating frequency: 13.56 MHz (ISM, world-wide license 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)
- Cryptographic tag/mutual authentication
- Additional fast anticollision read
- Persistent quiet mode to enable faster inventory speed

2.2 EEPROM

- 2048 bits user memory, organized in 64 blocks of 4 bytes each (last block reserved for counter feature)
- 50 years data retention
- Write endurance of 100,000 cycles

2.3 Security

- Unique identifier for each device (8 bytes)
- 32 byte originality signature
- Lock mechanism for each user memory block (write protection)
- Lock mechanism for DSFID, AFI, EAS
- AES Crypto-core for tag/mutual authentication with three 128-bit keys
- User memory segmentation with flexible access conditions with mutual authentication (privileges)
- Separate privileges for Read/Write access, EAS/AFI, Privacy and Destroy

- 16-bit counter

3. Applications

- Brand protection
- Counterfeit protection for consumer goods
- High value asset authentication
- Document tracking and authentication
- Ski ticketing

4. Ordering information

Table 1. Ordering information

Type number	Package		Version
	Name	Description	
SL2S6002FUD/BG	Wafer	sawn, bumped wafer, 120 μm with 7 μm Polyimide spacer, on film frame carrier, C_i between LA and LB = 23.5 pF (typical)	-

5. Block diagram

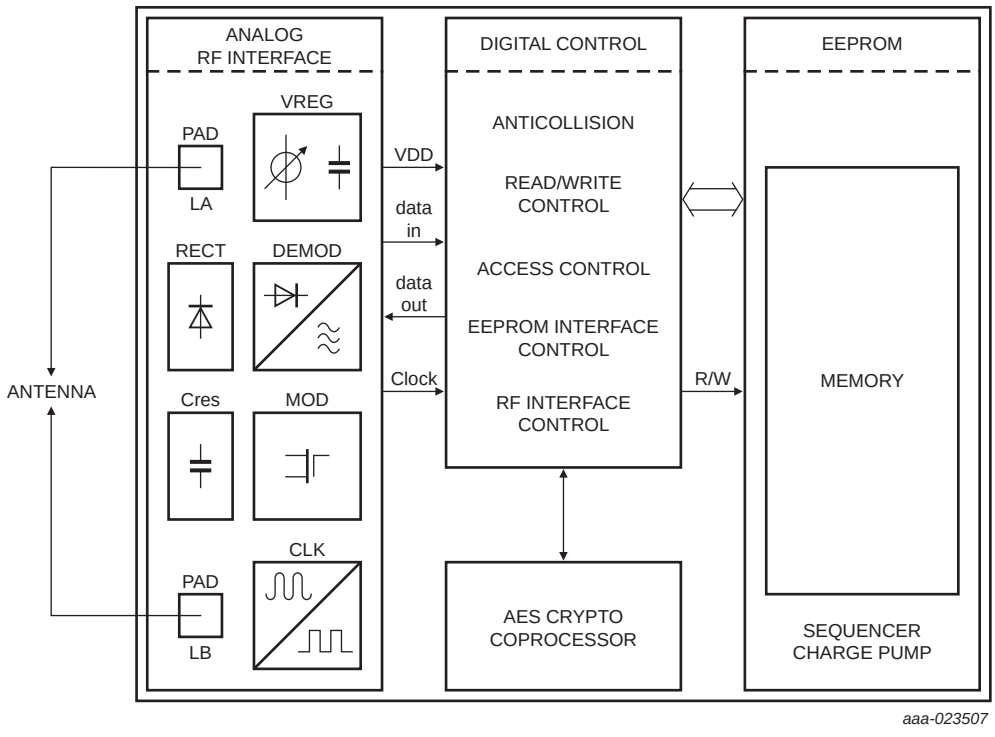

Fig 1. Block diagram of ICODE DNA

6. Functional description

For the detailed functional description, refer to Ref. 1.

6.1 Block description

The ICODE DNA IC consists of three major blocks:

- Analog RF interface
- Digital controller
- AES Crypto-Coprocessor
- 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).

6.2 Memory organization

The 2048-bit user accessible EEPROM memory is divided into 64 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 2 parts:

- User memory
  - Within the 2016-bit memory (63 blocks) area the user data are stored. Direct read/write access with the standard READ and WRITE commands 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 63) contains the 16-bit counter and the counter protection flag.
- Configuration area
  - Within this part of the memory all required security related information is stored, such as access keys with related privileges, headers, customer ID (CID) or originality signature. This memory area can only by accessed with the READ_CONFIG or WRITE_CONFIG commands depending on the configuration.

6.2.1 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 DNA IC is “01h”.

Bit 37 and bit 36 are used to differentiate between ICODE SLI, ICODE SLIX, ICODE SLIX2 and ICODE DNA (refer to Table 3).

Table 2. 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 3. Type indicator bits

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

6.2.2 User memory

Access to the user memory is possible with READ and WRITE commands depending on the settings of the access conditions.

Table 4. User memory organization

Block	Byte 0	Byte 1	Byte 2	Byte 3	Description
0					User memory: 63 blocks, 4 bytes each, 252 bytes in total.
1					
2					
3					
:	:	:	:	:	
60					
61					
62					
63	C0	C1	0x00	PROT	Counter

Only Blocks 0 to 63 can be addressed with standard READ and WRITE commands.

Remark: Block 63 contains the 16-bit counter and cannot be used to store user data. READ and WRITE commands to that block require special data considerations.

6.2.3 Configuration Memory

The configuration memory contains the security configuration information. Access to this memory area is only possible with READ_CONFIG and WRITE_CONFIG commands depending on the initialization status.

The configuration memory contains 48 blocks of 4 bytes.

6.2.3.1 Originality signature

The ICODE DNA offers a feature to verify the origin of a tag with a certain confidence with the UID towards an originality signature which is stored in the configuration memory bank. The originality signature can be read with the READ_SIGNATURE command or with the READ_CONFIG command.

The ICODE DNA provides the possibility to customize the originality signature to personalize the IC individually for specific application. At delivery the ICODE DNA is pre-programmed with the NXP originality signature described below. This signature is unlocked in the dedicated memory. If needed, the signature can be reprogrammed with a custom-specific signature using the WRITE_CONFIG command during the personalization process by the customer. The signature can be permanently locked afterwards by setting the Config Header to “locked “with the WRITE_CONFIG command to avoid further modifications.

Remark: If no customized originality signature is required, it is recommended to permanently lock the NXP signature during the initialization process by setting the Config Header to locked with the WRITE_CONFIG command.

6.2.3.2 Customer ID (CID)

The Customer ID is 0xC000 at delivery and can be reprogrammed and locked. In order to distinguish between NXP programmed and customized CIDs, the 2 most significant bits of CID_0 are automatically set to 1 when the CID is programmed with the WRITE_CONFIG command (input CID is bit wise OR with 0xC000).

CID = 0xC000 | <input CID>, e.g. 0xD053 = 0xC000 | 0x1053

The CID can be permanently locked afterwards by setting the Config Header to “locked” with the WRITE_CONFIG command to avoid further modifications.

Remark: If no customized originality signature is required, it is recommended to permanently lock the CID during the initialization process by setting the Config Header to “locked” with the WRITE_CONFIG command.

6.2.3.3 Authentication Limit

The Authentication Limit is a feature to limit the number of authentications (tag as well as mutual authentications) with the CHALLENGE or AUTHENTICATE command.

6.2.3.4 Key Privileges

The key privileges define the privileges for the related key used with mutual authentication. If the related privilege is enabled, the access for the depending feature is granted after mutual authentication with the related key.

Table 5. Definition of Key Privilege

Privilege	Description
Read	Read access to read protected user memory area
Write	Write access to write protected user memory area
Privacy	Enable/disable of the Privacy mode
Destroy	Access to the DESTROY functionality
EAS/AFI	Access for write alike command for EAS and AFI as following: PROTECT EAS/AFI SET EAS RESET EAS LOCK EAS WRITE EAS ID WRITE AFI LOCK AFI
Crypto Config	Preset of Authentication Limit Modification of transport keys

6.2.3.5 Keys

The keys are stored in the configuration memory. The usages of the individual keys depends on the related Key Privileges.

Key3 is pre-programed for NXP usage for tag authentication.

6.2.4 Configuration of delivered IC

ICODE DNA 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
- Custom ID is programmed to 0xC000 and is not locked
- Originality Signature is programmed with the NXP originality signature and is not locked
- Key0, Key1, Key2
  - The Key Headers are set to “Not active”
  - Keys are not defined
- Key3 contains the NXP key for tag authentication only (no privileges enabled)
- Key Privileges are not defined unlocked
- User data memory is **not** protected
- 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.

6.3 Communication principle

For detailed description of the protocol and timing, refer to ISO/IEC 15693-2 (modulation, bit-coding, framing, Ref. 3) and ISO/IEC 15693-3 (anticollision, timing, protocol, Ref. 4).

6.4 State diagram

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

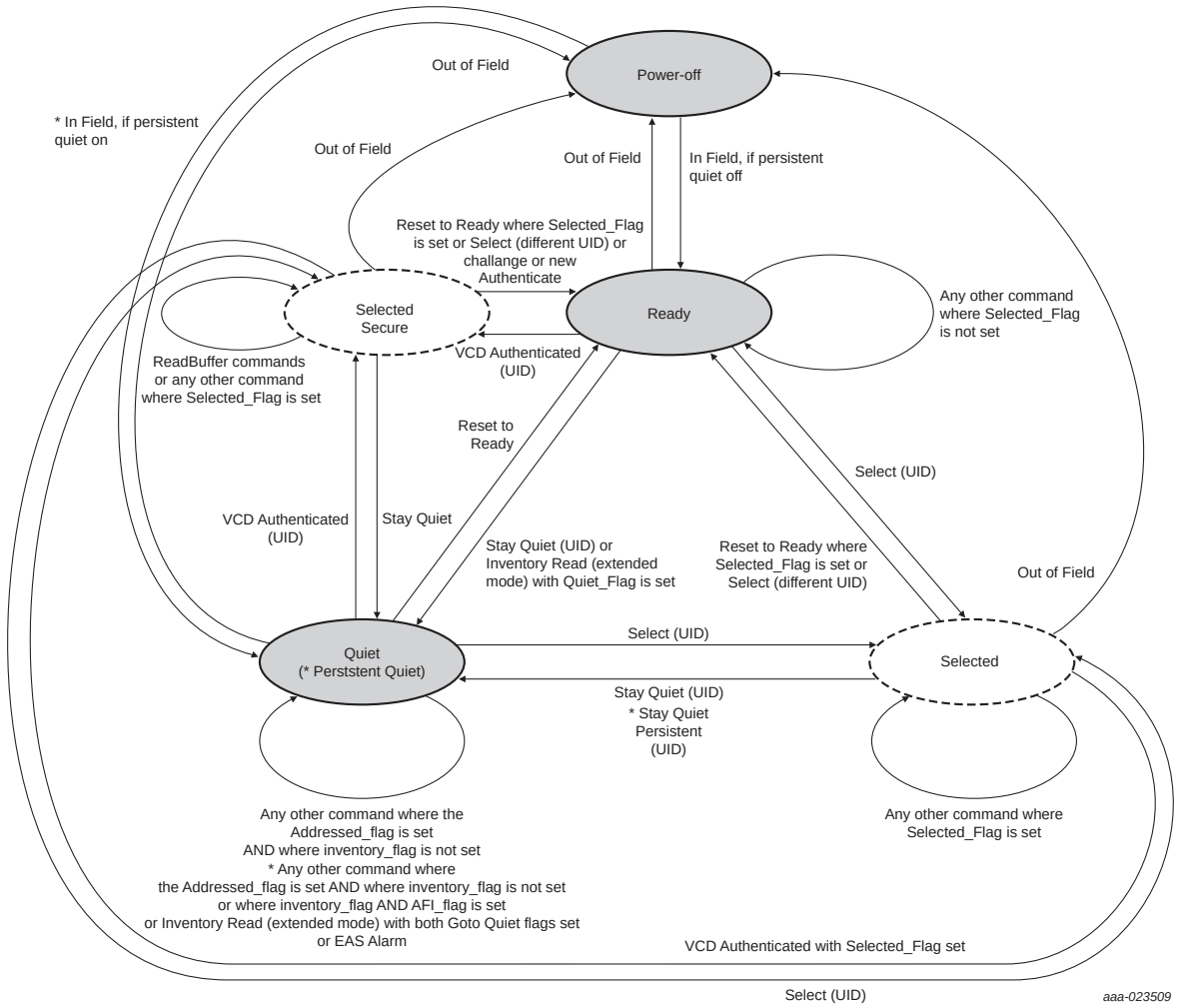

Fig 2. State diagram ICODE DNA

Remark: It is possible to set the ICODE DNA IC into the Quiet and Persistent Quiet 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.

6.5 RF interface

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

7. Limiting values

Table 6. 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.

8. Characteristics

8.1 Wafer memory characteristics

Table 7. 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

8.2 Interface characteristics

Table 8. Interface characteristics

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

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
f_i	input frequency	[1]	13.553	13.56	13.567	MHz
$V_{i(RMS)min}$	minimum RMS input voltage	operating read/write	1.1	-	1.3	V
$P_{i(min)}$	minimum input power	operating [2]	-	40	-	µW
C_i	input capacitance	between LA and LB [3]	22.3	23.5	24.7	pF
$t_{persist}$	persistent time	[4]	2	-	-	s

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

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

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

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

9. Abbreviations

Table 9. 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
IC	Integrated Circuit
LCR	Inductance, Capacitance, Resistance
LSB	Least Significant Byte/Bit
MSB	Most Significant Byte/Bit
RF	Radio Frequency
UID	Unique IDentifier

10. References

[1] **Product data sheet —** SL2S6002, ICODE DNA - Document number 3486**[1]

[2] **ISO Standard —** ISO/IEC 15693 - Identification cards - Contactless integrated circuit cards - Vicinity cards.

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

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

[5] **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.

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

1. ** ... document version number

11. Revision history

Table 10. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
SL2S6002 v. 3.0	20160616	Product short data sheet	-	SL2S6002 v. 2.0
Modifications:	• Initial version			

12. Legal information

12.1 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.

12.2 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.

12.3 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.

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

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

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.

12.4 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.

13. Contact information

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

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

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: 16 June 2016
374730