

AN11809

Feature comparison between ICODE SLI, SLIX, SLIX2, DNA

Rev. 1.0 — 16 June 2016
368210

Application note
COMPANY PUBLIC

Document information

Info	Content
Keywords	ICODE SLIX2, SLI, SLIX, DNA features
Abstract	Feature comparison between ICODE family products



Revision history

Rev	Date	Description
1.0	20160616	Initial revision

Contact information

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

1. Introduction

Products ICODE SLI/SLIX/SLIX2/DNA are ISO18000-3M1 and ISO15693 compliant tags with extended features to make the read/write and anti-collision faster and more efficient. This features can also be used in mixed populations together with other ISO15693 tags.

1.1 Feature comparison matrix

Table 1. ICODE feature comparison table

Product features	ICODE SLI	ICODE SLIX	ICODE SLIX2	ICODE DNA
User Memory [bit]	896	896	2528	2016
EPC Code Size [bit]	-	-	-	-
UID (TID1) size[bit]	64	64	64	64
Data Retention [Years]	10	50	50	50
Write Endurance [cycles]	100.000	100.000	100.000	100.000
Anti-collision Speed	up to 60 units/s	up to 60 units/s	90 units/s ¹	90 units/s ¹
Fast Inventory	✓	✓	✓	✓
Security Functions				
Tag Authentication	-	-	-	AES – 128bit
EAS	✓	✓	✓	✓
EAS Protection	-	32bit password	32bit password	AES – 128bit
EAS Selective	-	-	✓	✓
AFI	✓	✓	✓	✓
AFI Protection	-	32bit password	32bit password	AES – 128bit
Persistent Quiet	-	-	✓	✓
Memory write Lock	✓	✓	✓	✓
Memory access Protection	-	-	32bit password	AES – 128bit
Privacy Protection	-	-	32bit password	AES – 128bit
Destroy Protection	-	-	32bit password	AES – 128bit
Counter	-	-	✓	✓
Originality Signature	-	-	✓	re-programmable
Cres Capacitance [pF]	23.5	no / 23.5 / 97	23.5	23.5

[1] With extended Fast Inventory Read

The **ICODE DNA** in contrast to other family products provides the following features:

- Cryptographic Tag authentication:

As defined in ISO/IEC 15693-3 Amendment 4 (Ref. 5) and ISO/IEC 29167-10 (Ref. 6) ICODE DNA supports authentication procedure. It allows tag or mutual authentication based on 128bit AES password protection.

Three (3) user keys with separate privileges to define different access rights per key can be used. Optionally authentication limit – maximum number of authentications - may be set (and reset with valid mutual authentication).

- Re-programmable Originality Signature:
32 byte ECC based originality signature can be re-programmed and arranged regarding requirements
- Counter feature (already introduced in SLIX2):
enables counting WRITE commands and control over counter values and access
- Authentication limit:
limit of maximum number of authentications can be set. Reset is possible with valid mutual authentication
- Re-programmable Customer ID (CID)
- Improved Privacy Mode

1.2 Use cases of ICODE DNA special features

1.2.1 Improved Privacy

- tags in privacy mode show up in standard anti-collision
- anti-collision possible with several tags in privacy mode
- easy identification of group key based on CID

1.2.2 Product Authentication

Consumers can get prove - the originality of the tagged product with cryptographic authentication. Protection against unauthorized data access can be controlled.

1.2.3 Mutual/Reader Authentication

Mutual authentication allows to prove the authenticity of a tag based on a common secret (key) and to prove the access rights of the reader to protected data or functionality of the tag. Protection against unauthorized data access or unauthorized manipulation.

Reader Authentication has increased level of security for:

- User Memory
- EAS/AFI
- Privacy
- Destroy

1.2.4 Re-programmable Originality Signature

Brand owners and consumers can validate originality of goods by their own signature. Customers have ability to re-write factory programmed Originality Signature regarding their own needs. Customers can simply overwrite Originality Signature bytes with WRITE_CONFIG command. Originality Signature is located in Configuration memory. As this command allows only 4 bytes to be written at once, 8 writes are needed (Originality

Signature is 32 byte). Customers can use any cryptosystem they want (RSA, AES, ECC etc.) and it is recommended that it is asymmetric. This allows public key (for signature verification) to be publically available – shared.

1.2.5 Re-programmable Customer ID

CID can be used for e.g. customizing IC, identifying application, product family etc. Customer ID can be re-programmed and permanently locked.

1.2.6 Authentication Limit

The Authentication Limit is the feature to limit the number of authentications (tag and mutual authentications) with the each CHALLENGE or AUTHENTICATE command. After reaching limit number, no further authentications are possible – irreversible status. Before this happens mutual authentication is necessary to re-set the limit. This feature adds security value.

2. Legal information

2.1 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.

2.2 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.

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 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.

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.

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.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer.

In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out of the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages.

Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US\$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

2.3 Trademarks

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

ICODE — is a trademark of NXP B.V.

3. Contents

1.	Introduction	3
1.1	Feature comparison matrix.....	3
1.2	Use cases of ICODE DNA special features.....	4
1.2.1	Improved Privacy	4
1.2.2	Product Authentication	4
1.2.3	Mutual/Reader Authentication	4
1.2.4	Re-programmable Originality Signature	4
1.2.5	Re-programmable Customer ID	5
1.2.6	Authentication Limit.....	5
2.	Legal information	6
2.1	Definitions	6
2.2	Disclaimers.....	6
2.3	Trademarks.....	6
3.	Contents.....	7

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

© NXP B.V. 2016.

All rights reserved.

For more information, visit: <http://www.nxp.com>

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

Date of release: 16 June 2016

368210

Document identifier: AN11809