# AN11809

## Feature comparison between ICODE SLIX, ICODE SLIX2, ICODE DNA, and ICODE 3

Rev. 1.1 — 2 April 2024 Application note

**Document information**

| Information | Content |
|---|---|
| Keywords | ICODE SLIX, ICODE SLIX2, ICODE DNA, ICODE 3, features |
| Abstract | Feature comparison between ICODE family products |

# 1 Introduction

This application note provides an overview of the ICODE SLIX, ICODE SLIX2, ICODE DNA, and ICODE 3 features. The ICODE ICs are ISO18000-3M1 and ISO/IEC 15693 compliant, with extended features to make the read/write and anti-collision operations faster and more efficient. These extended features can be used with a mix of ICODE and other ISO/IEC 15693 compliant tags.

# 2 Feature comparison

## 2.1 Feature comparison matrix

**Table 1. ICODE feature comparison table**

| Product features | ICODE SLIX | ICODE SLIX2 | ICODE DNA | ICODE 3 | ICODE 3 TagTamper |
|---|---|---|---|---|---|
| User memory [bit] | 896 | 2528 | 2016 | 2400 | 2400 |
| UID size [bit] | 64 | 64 | 64 | 64 | 64 |
| Data Retention [years] | 50 | 50 | 50 | 50 | 50 |
| Write Endurance [cycles] | 100.000 | 100.000 | 100.000 | 100.000 (typ. 500k for counter) | 100.000 (typ. 500k for counter) |
| Anti-collision Speed | up to 60 units/s | 90 units/s[1] | 90 units/s[1] | 90 units/s[1] | 90 units/s[1] |
| Fast Inventory | ✓ | ✓ | ✓ | ✓ | ✓ |
| SELFAdjust | - | - | - | ✓ | ✓ |
| TagTamper | - | - | - | - | ✓ |
| NFC Mirror | - | - | - | UID / Counter | UID / Counter / TagTamper |
| **Security Functions** | | | | | |
| Tag Authentication | - | - | AES – 128-bit | - | - |
| EAS | ✓ | ✓ | ✓ | ✓ | ✓ |
| EAS Protection | 32-bit password | 32-bit password | AES – 128-bit | 32-bit password | 32-bit password |
| EAS Selective | - | ✓ | ✓ | ✓ | ✓ |
| AFI | ✓ | ✓ | ✓ | ✓ | ✓ |
| AFI Protection | 32-bit password | 32-bit password | AES – 128-bit | 32-bit password | 32-bit password |
| Persistent Quiet | - | ✓ | ✓ | ✓ | ✓ |
| Memory write lock | ✓ | ✓ | ✓ | ✓ | ✓ |
| Memory access protection | - | 32-bit password | AES – 128-bit | 32-bit password | 32-bit password |
| Privacy Protection | - | 32-bit password | AES – 128-bit | 32-bit password | 32-bit password |
| Destroy Protection | - | 32-bit password | AES – 128-bit | 32-bit password | 32-bit password |
| Counter / NFC Counter | - | ✓ | ✓ | ✓ / ✓ | ✓ / ✓ |
| Originality Signature | - | ✓ | reprogrammable | reprogrammable up to 384 bit | reprogrammable up to 384 bit |
| Cres Capacitance [pF] | no / 23.5 / 97 | 23.5 | 23.5 | 23.5 | 23.5 |

[1] With extended Fast Inventory Read

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

- Cryptographic Tag authentication:
  - As defined in ISO/IEC 15693-3 Amendment 4 ([1]) and ISO/IEC 29167-10 ([2]), ICODE DNA supports the authentication procedure. It allows tag or mutual authentication based on 128-bit AES password protection.
  - Three (3) user keys can be used. Each key has separate privileges to define different access rights. Optionally, an authentication limit – maximum number of authentications - may be set (and reset with valid mutual authentication).
- Authentication limit: the maximum number of authentications can be set. Reset is possible with valid mutual authentication.
- Reprogrammable customer ID (CID).

The **ICODE DNA** and/or **ICODE 3** support the following features:

- Programmable originality signature:
  - 32-byte ECC-based originality signature (ICODE DNA)
  - 32-byte or 48-byte ECC-based originality signature (ICODE 3)
- Counter feature (already introduced in SLIX2): enables the counting of WRITE commands, and the control of the counter values and access.
- Improved privacy mode.

## 2.2 Use cases of ICODE DNA special features

### 2.2.1 Product authentication

The cryptographic authentication of the tag increases the likelihood that the tag is authentic.

### 2.2.2 Mutual/reader authentication

Mutual authentication provides:

- Proof of the tag authenticity based on a common secret key.
- Proof of the reader access rights to the protected data or functionality of the tag.
- Protection against unauthorized data access or unauthorized manipulation.

Reader authentication has an increased level of security for:

- User memory
- EAS/AFI
- Privacy
- Destroy

### 2.2.3 Reprogrammable Customer ID

Examples of use of the Customer ID (CID) are: IC customization, application identification, product family, and more. The CID can be reprogrammed and permanently locked.

### 2.2.4 Authentication limit

The authentication limit feature is used to limit the number of authentications (tag and mutual authentications) with each CHALLENGE or AUTHENTICATE command. After reaching the limit number, no further authentications are possible – irreversible status. Prior to reaching the authentication limit, mutual authentication is necessary to reset the limit. This feature adds security value.

## 2.3 Use cases of ICODE DNA and ICODE 3 special features

### 2.3.1 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

### 2.3.2 Reprogrammable Originality Signature

Brand owners and consumers can validate the originality of goods using their own signature.

Customers have the ability to rewrite the factory programmed Originality Signature according to their own needs. They can use the WRITE_CONFIG command to overwrite the Originality Signature bytes. The Originality Signature is located in Configuration memory. As the WRITE_CONFIG command allows only 4 bytes to be written at once, eight (8) writes are needed for the 32-byte Originality Signature.

***Note:*** *ICODE 3 supports 32-byte or 48-byte ECC originality signature. Refer to [3].*

Customers can use any crypto system (for example RSA, AES, or ECC). The recommendation is to use an asymmetric system, which allows the public key (signature verification) to be shared.

# 3 References

[1] ISO/IEC 15693-3:2019 Cards and security devices for personal identification — Contactless vicinity objects — Part 3: Anticollision and transmission protocol

[2] ISO/IEC 29167-10:2017 Information technology — Automatic identification and data capture techniques — Part 10: Crypto suite AES-128 security services for air interface communications

[3] Data sheet - SL2S3003/SL2S3003TT ICODE 2 (TagTamper) (link)

# 4 Revision history

**Table 2. Revision history**

| Document ID | Release date | Description |
|---|---|---|
| AN11809 v.1.1 | 02 April 2024 | • Extended the applicability to ICODE 3. |
| AN11809 v.1.0 | 16 June 2016 | • Initial version |

# Legal information

## Definitions

**Draft** — A draft status on a document indicates that 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 in a draft version of a document and shall have no liability for the consequences of use of such information.

## 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.

**Terms and conditions of commercial sale** — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://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.

**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.

**Suitability for use in non-automotive qualified products** — Unless this document 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, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

**Security** — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

**NXP B.V.** — NXP B.V. is not an operating company and it does not distribute or sell products.

## Trademarks

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

**NXP** — wordmark and logo are trademarks of NXP B.V.

**ICODE and I-CODE** — are trademarks of NXP B.V.

# Tables

# Contents





**Date of release: 2 April 2024**
**Document identifier: AN11809**