SGS Brightsight B.V.

Brassersplein 2
2612 CT Delft
The Netherlands

t (+31) 15 269 2500
brs.info@sgs.com

www.brightsight.com

coc 30105045

EUCC-3100-2026-7001701

Certification Report

NXP MF0AES(H)x0, NT2H2xy1G and NT2H2xy1S, release B0

26-CB-026

Version and Approval

Version	Date	Author	Reviewed
1.0	2026-04-10	Miquel Hernandez	Rob Kemper

Approved by:	Rob Kemper

Table Of Contents

Contents

1 Executive Summary

1.1 Required information

Name of the evaluated ICT product	MF0AES(H)x0, NT2H2xy1G and NT2H2xy1S, release B0

ICT product components that are part of the evaluation	• Hardware for all variants
	• Guidance
	  ○ [DS-MFU-20]
	  ○ [DS-MFU-30]
	  ○ [UG-MFU]
	  ○ [DS-NTAG-223]
	  ○ [DS-NTAG-224]
	  ○ [UG-NTAG]
	  ○ [DS-NTAG-223- SD]
	  ○ [DS-NTAG-224- SD]
	  ○ [UG-NTAG-SD]

ICT product version	B0
Name of the ITSEF that performed the evaluation	SGS Brightsight B.V. (referred to as Brightsight ITSEF)
List of subcontractors for the evaluation	N/A
Completion date of evaluation	2026-04-07
Reference to the evaluation technical report established by the ITSEF	[ETR]
CC Version	CC:2022 Revision 1
CC assurance package and security assurance components	EAL3, augmented with ALC_FLR.2
Assurance level as per Regulation (EU) 2019/881	Substantial
Presence of an approved patch management procedure	No

1.2 Security functionality of the evaluated ICT product

The ICT product has the following features:

TSF portion	Title	Description
TSF.Service	Service functionality	This portion of the TSF comprises internal services like random number generation and provides mechanisms to store initialization, prepersonalization, and/or other data on the TOE.
TSF.Protection	General security measures to protect the TSF	This portion of the TSF comprises physical and logical protection to avoid information leakage and detect fault injection.
TSF.Control	Operating conditions, memory and hardware access control	This portion of the TSF controls the operating conditions.
TSF.Authentication	Mutual Authentication	This portion of the TSF provides a mutual authentication mechanism to separate authorized subjects from unauthorized subjects.
TSF.Access-Control	Access Control	This portion of the TSF provides an access control mechanism to the subjects, objects, operations and attributes defined by the TOE Access Control Policy.
TSF.MAC	Message Authentication Code	This portion of the TSF allows both the TOE and the terminal to detect integrity violations, replay or man-in-the-middle attacks.
TSF.Monotonic-Count	Monotonic Counters	This portion of the TSF ensures that certain counter objects can only be incremented, but never decremented.
TSF.OTP	One-Time Programmable Memory	This portion of the TSF ensures that certain memory areas can only be written once, i.e. once a bit is set it cannot be unset anymore.
TSF.No-Trace	Preventing Traceability	This portion of the TSF prevents tracing of the TOE by e.g. simply retrieving its UID.
TSF.Tag-Tamper	Tag Tamper Detection	This portion of the TSF provides a mechanism for detection and permanent storage of the status of the tag tamper wire.

1.3 Summary of threats and organisational security policies addressed by the evaluated ICT product

Threats described in [ST] §3.2 have been considered in the evaluation, mostly defined in [PP].

Name	Title
T.Leak-Inherent	Inherent Information Leakage
T.Phys-Probing	Physical Probing
T.Malfunction	Malfunction due to Environmental Stress
T.Phys-Manipulation	Physical Manipulation
T.Leak-Forced	Forced Information Leakage
T.Abuse-Func	Abuse of Functionality
T.RND	Deficiency of Random Numbers

In addition to those, the developer has defined the following threats:

Name	Title
T.Data-Modification	Unauthorised Data Modification
T.Impersonate	Impersonating authorised users during authentication
T.Cloning	Cloning

T.Data-Modification **Unauthorised Data Modification**

User data stored by the TOE may be modified by unauthorised subjects. This threat applies to the processing of modification commands received by the TOE, it is not concerned with verification of authenticity.

T.Impersonate **Impersonating authorised users during authentication**

An unauthorised subject may try to impersonate an authorised subject during the authentication sequence, e.g. by a man-in-the-middle or replay attack.

T.Cloning **Cloning**

User and TSF data stored on the TOE (including keys) may be read out by an unauthorised subject in order to create a duplicate.

OSPs described in [ST] §3.3 have been considered in the evaluation, the one defined in the [PP].

Name	Title
P.Process-TOE	Identification during TOE Development and Production

In addition to those, the developer has defined the following OSP:

Name	Title
P.MAC	Integrity during communication
P.No-Trace	Untraceability of end-users
P.Tag-Tamper	Tag tamper detection

P.MAC	**Integrity during communication** The TOE shall provide the possibility to protect the contactless communication from modification or injections. This includes especially the possibility to detect replay or man-in-the-middle attacks within a session.
P.No-Trace	**Untraceability of end-users** The TOE shall provide the ability that authorised subjects can prevent that end-user of TOE may be traced by unauthorised subjects without consent. Tracing of end-users may happen by performing a contactless communication with the TOE when the end-user is not aware of it. Typically this involves retrieving the UID or any freely accessible data element.
P.Tag-Tamper	**Tag tamper detection** The TOE shall provide the possibility to detect and permanently record tampering status on the tag tamper wire.

1.4 Special configuration requirements

N/A

1.5 Assumptions about the operating environment

Assumptions about the operating environment are described in [ST] §3.4. One assumption from [PP] has been included in the ST:

Name	Title
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation

In addition to those, the developer has defined the following assumptions:

Name	Title
A.Secure-Values	Usage of secure values
A.Terminal-Support	Terminal Support

A.Secure-Values **Usage of secure values**

Only confidential and secure cryptographically strong keys shall be used to set up the authentication. These values are generated outside the TOE and they are downloaded to the TOE.

A.Terminal-Support **Terminal Support**

The terminal verifies information sent by the TOE in order to ensure integrity and confidentiality of the communication. Furthermore the terminal shall provide random numbers according to AIS20/31 [1] for the authentication.

1.6 Objectives in the environment for compliant operation

As described in the [ST] section 4.2 in order to ensure compliant operation, the product's environment must ensure the following objectives for the environment. OE.Process-Sec-IC is taken from [PP], whereas others have been defined in the ST:

Name	Title
OE.Process-Sec-IC	Protection during composite product manufacturing

Name	Title
OE.Secure-Values	Generation of secure values
OE.Terminal-Support	Terminal support to ensure integrity, confidentiality and use of random numbers

The TOE provides specific functionality that requires the TOE Manufacturer to implement measures for the unique identification of the TOE. Therefore, OE.Secure-Values is defined to allow a TOE specific implementation (refer also to A.Secure-Values).

OE.Secure-Values **Generation of Secure Values**

The environment shall generate confidential and cryptographically strong keys for authentication purpose. These values are generated outside the TOE and are

	downloaded to the TOE during the personalisation or usage in phase 5 to 7.

The TOE provides specific functionality to protect the transaction with the terminal. Therefore, OE.Terminal-Support is defined to indicate that this also requires certain actions from the terminal.

OE.Terminal-Support	**Terminal support to ensure integrity, confidentiality and use of random numbers** The terminal shall verify information sent by the TOE in order to ensure integrity of the communication. This involves checking of MAC values, verification of redundancy information according to the cryptographic protocol and secure closing of the communication session. Furthermore the terminal shall provide random numbers according to AIS20/31 [1] for the authentication.

1.7 Brief description of the certification report results

This Certification Report presents the results of the Common Criteria security evaluation of NXP MF0AES(H)x0, NT2H2xy1G and NT2H2xy1S. The TOE was developed by NXP Semiconductors Germany GmbH, who also sponsored the evaluation and certification.

The purpose is also to inform potential buyers about the conditions required for the product's proper use, so they can ensure it complies with the requirements under which it was evaluated and certified. Therefore, users should review the certification report alongside the relevant usage and administration guides, as well as the [ST], which outlines assumed threats, environmental factors, and usage conditions. This helps users decide if the product aligns with their security goals.

The TOE is primarily designed for secure applications such as public transportation, access, event ticketing, loyalty, smart packaging, and brand protection. TOE functionality is defined by the requirements in the [ST]. Additional information on TOE features is provided in chapter 2.

Brightsight ITSEF performed the evaluation. The evaluation was completed on April 7, 2026, resulting in the evaluation technical report [ETR]. The certification procedure was conducted in accordance with the EUCC, as set out in Commission Implementing Regulation (EU) 2024/482 of 31 January 2024, and its amendments.

The scope of the evaluation is defined in the security target [ST]. The [ST] sets out the evaluation assumptions, the intended operating environment for the TOE, the security requirements, and evaluation assurance level at which the product is intended to meet those requirements. A subset of terms and definitions from [PP] have been included in the certification scope, but it should be noted that no claims to the PP are made due to the claim to the assurance package EAL3, below the minimum required by the PP.

Consumers are advised to confirm that their own environment is consistent with the [ST] and to take into account the comments, observations, and recommendations in this Certification Report.

The evaluation concluded that the TOE has no special configuration requirements beyond those specified in the user guidance. Users shall review these requirements and install the TOE in the operational environment accordingly.

The results documented in the evaluation technical report [ETR] provide sufficient evidence that the TOE meets the EAL3 augmented assurance requirements for the evaluated security functionality. The assurance level is augmented with ALC_FLR.2 and is recognised by Article 52 of [CSA] as “Substantial”.

The evaluation was performed using the Common Methodology for Information Technology Security Evaluation, CC:2022, R1 [CEM] and assessed conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 R1 [CC] (Parts 1–5).

This certificate applies only to the specific version and release of the product in its evaluated configuration.

1.8 Disclaimer(s)

Certification does not ensure a product is completely free of exploitable vulnerabilities.

2 Identification of the ICT product or the ICT product category for protection profiles

2.1 Product Name

This certification considers the following product:

NXP MF0AES(H)x0, NT2H2xy1G and NT2H2xy1S, release B0

2.2 Product components

The TOE comprises the following hardware and software:

	Name	Version
Hardware	TOE Hardware for all variants	B0

The TOE consists of the following three configurations:

- MF0AES(H)x0 – **MIFARE Ultralight AES**
- NT2H2xy1G – **NTAG 22x DNA**
- NT2H2xy1S – **NTAG 22x DNA StatusDetect**

The list of guidance documents to use with the product in its certified configuration is as follows and is unique for each listed-above configuration.

For the **MIFARE Ultralight AES**, the following guidance components are delivered.

Reference	Name	Version	Date
[DS-MFU-20]	MF0AES(H)20, MIFARE Ultralight AES contactless limited-use IC, Product data sheet	3.2	28 March 2023
[DS-MFU-30]	MF0AES(H)30, MIFARE Ultralight AES contactless limited-use IC, Objective data sheet	2.0	4 February 2022
[UG-MFU]	MIFARE Ultralight AES, Information on Guidance and Operation, Guidance and operation manual	2.0	12 December 2025

Table 2. Guidance components delivered to the customer (MIFARE Ultralight AES)

For the **NTAG 22x DNA**, the following guidance components are delivered.

Reference	Name	Version	Date
[DS-NTAG-223]	NT2H2331G0, NTAG 223 DNA - NFC T2T compliant IC, Product data sheet	3.2	16 December 2025
[DS-NTAG-224]	NT2H2421G0, NTAG 224 DNA - NFC T2T compliant IC, Product data sheet	3.3	16 December 2025
[UG-NTAG]	NTAG 22x DNA, Guidance and operation manual	2.0	12 December 2025

For the **NTAG 22x DNA**, the following guidance components are delivered.

Reference	Name	Version	Date
[DS-NTAG-223]	NT2H2331G0, NTAG 223 DNA - NFC T2T compliant IC, Product data sheet	3.2	16 December 2025
[DS-NTAG-224]	NT2H2421G0, NTAG 224 DNA - NFC T2T compliant IC, Product data sheet	3.3	16 December 2025
[UG-NTAG]	NTAG 22x DNA, Guidance and operation manual	2.0	12 December 2025

Table 3 Guidance components delivered to the customer (NTAG 22x DNA).

For the **NTAG 22x DNA StatusDetect**, the following guidance components are delivered.

Reference	Name	Version	Date
[DS-NTAG-223-SD]	NT2H2331S0, NTAG 223 DNA StatusDetect - NFC T2T compliant IC with StatusDetect feature, Product data sheet	3.2	16 December 2025
[DS-NTAG-224-SD]	NT2H2421S0, NTAG 224 DNA StatusDetect - NFC T2T compliant IC with StatusDetect feature, Product data sheet	3.3	16 December 2025
[UG-NTAG-SD]	NTAG 22x DNA StatusDetect, Guidance and operation manual	2.0	12 December 2025

2.3 Identification of additional requirements to the operating environment

Please refer to section1.6 .

2.4 Holder of the EUCC certificate

Sponsor Name: NXP Semiconductors Germany GmbH
Address: Beiersdorfstraße 12, 22529 Hamburg, Germany
PoC: Holger Matz

2.5 Patch management procedure included into the certificate

N/A

2.6 Additional information

Supplementary cybersecurity information for the certified ICT product in accordance with Article 55 of Regulation (EU) 2019/881 is provided at the following websites: www.nxp.com/products/nxp-product-information/eucc-certified-products and www.nxp.com/psirt.

3 Security services

The ICT product implements the security services described in chapter 7 of this report.

4 Vulnerability handling policy

4.1 Reference

[Incident-Resp] Product Security Incident Response Process, NXPOMS-1719007347-4179, 14 Mar 2024, NXP Semiconductors

4.2 Description

The vulnerability management process mandated by (EU) 2024/482 Chapter VI and the supplemented information required by (EU) 2024/482 Article 11 paragraph 4 bullet (c) has been provided in [Incident-Resp], and ALC_FLR.2 aspects have been assessed by the evaluator. The result was reported in [ALC PRES].

The ITSEF has established that [Incident-Resp] has been provided to the Certification Body in order to meet (EU) 2024/482 regulation and has also verified that email-address psirt@nxp.com and NXP website www.nxp.com/psirt exist. All evaluator analysis with respect to vulnerability handling has been made within the ITSEF accreditations, such as ISO17025, leaving the developer responsibilities with NXP. The developer is explicitly made aware of these (EU) 2024/482 responsibilities for a certificate holder.

5 Assurance continuity policy

N/A

6 Assumptions and clarification of scope

6.1 Assumptions on usage and deployment

Refer to section 1.5

6.2 Assumptions on the environment for compliant operation

Refer to section 1.6

7 Architectural information

The TOE is a Security IC comprising a dedicated hardware platform and a set of data elements stored in EEPROM. For each variant of the product, the documentation consists of:

- The Product Data Sheet providing the functional specification as well as the delivery formats and interface variants, and
- The Guidance and Operational Manual providing guidelines for secure usage and operation of the security functionality of the variant of the TOE.

The logical architecture, originating from the Security Target [ST] of the TOE can be depicted as follows:

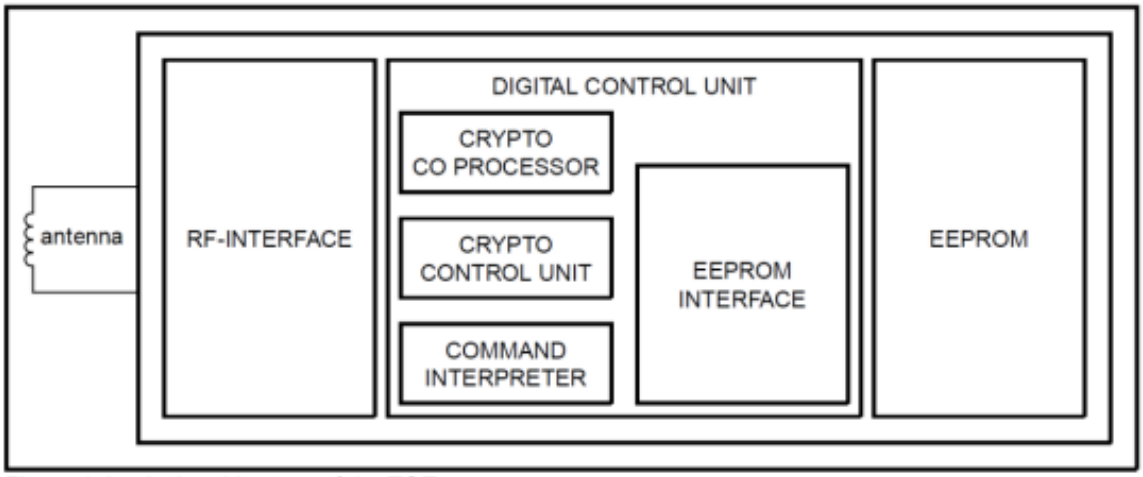


Figure 1. Logical architecture of the TOE.

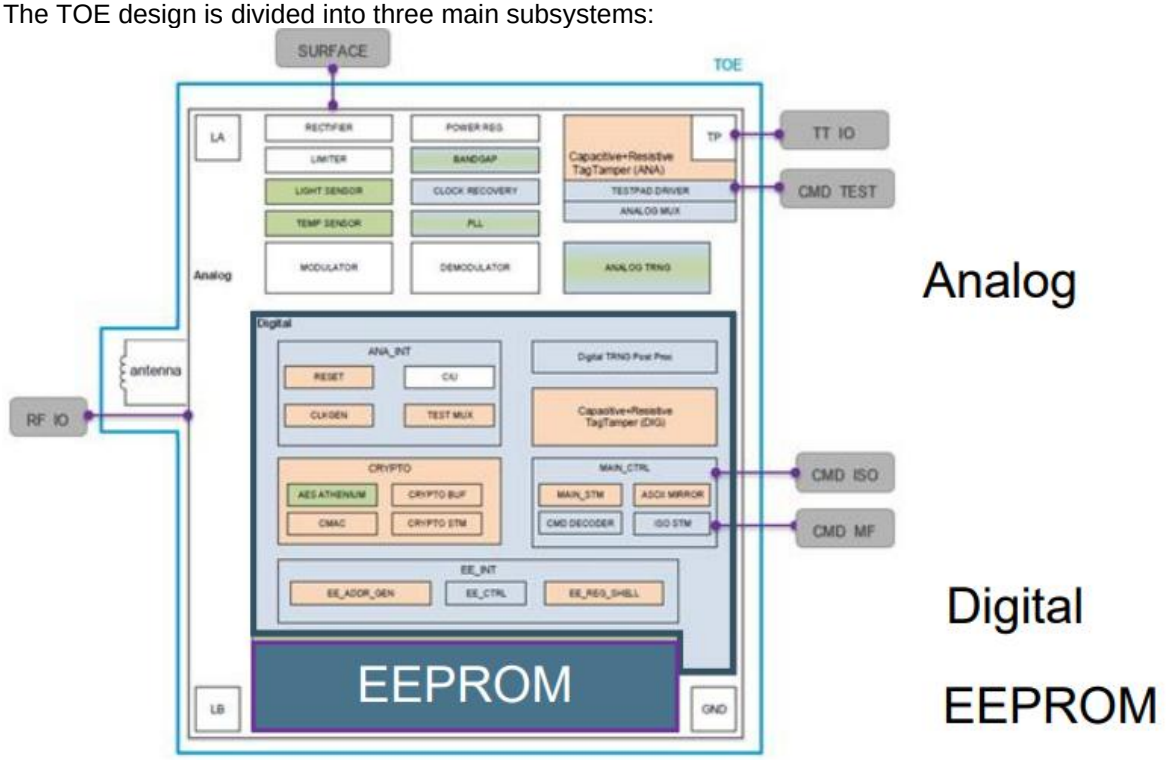
The TOE has the following features:

- Secure mutual authentication to support authentication of authorized users and the TOE.
- Secure channel establishment and secure messaging to support integrity protected data transfer on the MIFARE Ultralight AES variant of the TOE.
- Secure user one-time programmable memory area.
- Secure read-only locking of the user memory.
- One or more secure monotonic counters.
- Secure dynamic messaging to allow secure export of data in unauthenticated state on NTAG 22x (StatusDetect) variants of the TOE.
- Supporting non-traceability of the TOE by providing the option to use random IDs during contactless protocol establishment on the MIFARE Ultralight AES variant of the TOE.
- Additional functionality to detect the status of tamper evidence provided by the NTAG 22x StatusDetect variant of the TOE.

These security functionalities aim at enabling card issuers to use the product for various use-cases as outlined in the following.

- **MIFARE Ultralight AES**: the MF0AES(H)x0 variants of the TOE is intended for limited use transport tickets, event ticketing (e.g. cinema, game or concert) or access control badges, the hospitality industry (e.g. hotels) and also loyalty cards with limited value.
- **NTAG 22x DNA**: the NT2H2xy1G variants of the TOE are intended as NFC Forum Type 2 Tag. It might generate Secure Unique NFC Message in each tap for direct access to web services. The main use cases are brand protection and smart packaging. A subset of the supported card reader command set is to be compatible with the NFC Forum Type 2 Tag standard.
- **NTAG 22x DNA StatusDetect**: the NT2H2xy1S variants of the TOE are identical to NTAG 22x DNA, but support additionally the "StatusDetect" feature, which allows the user to control and detect when a tamper evidence mechanism has been triggered. This feature supports use cases, where product integrity needs to be verified e.g. seals for high-value liquids.

The TOE design is divided into three main subsystems:



8 Supplementary cybersecurity information

In relation with information to be made available by the certificate holder according to (EU) 2024/482 Chapter VII, www.nxp.com/products/nxp-product-information/eucc-certified-products and www.nxp.com/psirt is stated to contain guidance and information needed by the user, provide information up to five years after the certificate validity, and to describe the process of responsible disclosure of vulnerabilities.

9 ICT product testing

9.1 Required information

Certificate issuer contact	SGS Brightsight B.V. (referred to as Brightsight CB) Contact: Rob Kemper rob.kemper@sgs.com +31 15 269 25 44
	Dutch Authority for Digital Infrastructure – Ministry of Economic Affairs Contact: eucc@dutchncca.nl
ITSEF which performed the evaluation	SGS Brightsight B.V. (referred to as Brightsight ITSEF)
Assurance Components used	• EAL3 augmented by ALC_FLR.2
State of the Art documents and other criteria used	• "Minimum Site Security Requirements", version 2, February 2025 • "Application of CC to Integrated Circuits", version 2, December 2024 • "Security Architecture Requirements for Smart Cards and Similar Devices", version 1.1, 31 January 2024 • "Application of Attack Potential to Smartcards", version 2, 19 December 2025 • "STAR methodology", version 1, 25 March 2025 • "ISO/IEC 14443-1:2016- Identification cards — Contactless integrated circuit cards — Proximity cards Part 1: Physical characteristics", March 2016 • "ISO/IEC 14443-2:2016 - Identification cards — Contactless integrated circuit cards — Proximity cards Part 2: Radio frequency power and signal interface", July 2016 • "ISO/IEC 14443-3:2016 - dentification cards — Contactless integrated circuit cards — Proximity cards Part 3: Initialization and anticollision", September 2016 • Methodology used for vulnerability analysis: ITSEF proprietary method
Protection profile details:	N/A

9.2 Product settings and configuration

As stated in the [ST] section 1.4.1.1 the product has the following possible configurations:

Configuration	Description
MIFARE Ultralight AES	The MIFARE Ultralight AES (MF0AES(H)x0) variant of the TOE has a commercial type naming convention with the format MF0AES(H)xyffDpp.
NTAG 22x DNA (with or without StatusDetect)	The NTAG 22x DNA and NTAG 22x DNA StatusDetect variants of the TOE share the same commercial type naming convention which has the following format: NT2H2xy1vwDzz.

The TOE was tested in the following configurations:

☐ MF0AES(H)x0 – MIFARE Ultralight AES

- NT2H2xy1S – NTAG 223 DNA StatusDetect
- NT2H2xy1G – NTAG 224 DNA

Testing is performed on sample format that does not have the antenna built in, which is acceptable since none of the security functionality is implemented by the antenna. An adapter board with antenna is provided by developer to allow for testing in penetration test setup.

9.3 Testing approach and depth

The developer performed extensive testing on interface and subsystem level. The evaluators examined developer's testing activities documentation and verified that the developer has met their testing responsibilities.
All parameter choices were addressed at least once. All boundary cases identified were tested explicitly.
The evaluators reproduced a sample of the developer tests by means of a remote witnessing session, due to the complexity to setup the testing environment.
For the testing performed by the evaluators, the developer provided samples that were used for penetration testing.

9.4 Penetration testing

The vulnerability analysis was performed according to the AVA_VAN.2 requirements in line with the methodologies mandated by the technical domain, resulting in a test plan reported in the [ETR].

9.5 Test results

The testing activities, including configurations, test cases and results are summarised in the [ETR], with references to the documents containing the full details.
The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in it [ST] and functional specification.
No exploitable vulnerabilities were found with the penetration test plan devised by the evaluator.
The test results reveal that the TOE is resistant to a basic attack potential associated to the attack rating in the scope of AVA_VAN.2

10 Identification of the certificate holder's lifecycle management processes and production facilities

[ST] section 1.4.3 describes the life cycle model based on [PP] up to phase 6:
For the usage phase the TOE will be embedded in a credit card (meaning ID-1 sized) plastic card (micro-module embedded into the plastic card) or another supported package. The module and card embedding of the TOE provide external security mechanisms because they make it harder for an attacker to access parts of the TOE for physical manipulation.
NXP will deliver the TOE at the end of Phase 6. Therefore the TOE evaluation perimeter comprising the development and production environment of the TOE, consists of lifecycle phases 1 - 6. The TOE is a fully integrated composite product comprised of the underlying security IC hardware developed by NXP. Therefore, Phase 5 is fully under control of NXP and does not involve data exchange with other parties. NXP also provides a commercial option to configure the TOE on behalf of the customer in order to personalize before the usage. Alternatively, the customer can also finalize the partially personalized TOE after delivery. In case that all required security anchors (key material) are already installed during personalization by NXP, the customer can finalize the personalization of the non-volatile memory content relying on the operational security features of the TOE. The TOE is being locked to the user operating mode before TOE delivery at the end of Phase 6. The TOE is able to control two different logical phases. After production of the chip every start-up will lead to the initial operating mode. In the initial operating mode the production test shall be performed and the TOE is trimmed and initialized. The selection of the required variant is part of the initialization. At the end of the production test, the access to the test and initialization functionality is physically disabled. Subsequent start-ups of the chip will always enter the user operating mode. The TOE will stay in the user operating mode until the end of its life-time. In exceptional cases, which impact the integrity of the TOE in a non-recoverable way (typically if the TOE configuration is corrupted or TOE faces physical damage) the TOE switches into the mute or freeze operating mode. In those modes the TOE is effectively unusable.

10.1 Development and Production Facilities

Development and production facilities and its certificates are based on the re-use of the site audit results. The STARs are valid at the date of this report, meaning that such inputs can effectively be reused at the date of issuance of this certificate.

11 Results of the evaluation and information regarding the certificate

11.1 Required information

Certificate identifier	EUCC-3100-2026-7001701
Certificate date of issuance	2026-04-10
Certificate period of validity	5 years
Assurance level	Substantial
Assurance requirements that are met	EAL3, augmented with ALC_FLR.2
AVA_VAN level	AVA_VAN.2

11.2 Assurance requirements

The chosen assurance level is EAL 3 augmented with ALC_FLR.2. The evaluation results and the corresponding verdicts are detailed in the subsections below.

11.2.1 ASE

ASE has no **OPEN** comments.

Evaluator action	**Content (CEM ID)**	**Report reference, including slide# or section #**	**ITSEF verdict**	**CB TR verdict**
ST introduction ASE_INT				
1.1E	1.1C (CEM:1-1)	[IR-ASE] §2.1	Pass	Pass
	1.2C (1-2)	[IR-ASE] §2.1	Pass	Pass
	1.3C (1-3/4)	[IR-ASE] §2.1	Pass	Pass
	1.4C (1-5)	[IR-ASE] §2.1	Pass	Pass
	1.5C (1-6/7)	[IR-ASE] §2.1	Pass	Pass
	1.6C (1-8)	[IR-ASE] §2.1	Pass	Pass
	1.7C (1-9)	[IR-ASE] §2.1	Pass	Pass
	1.8C (1-10)	[IR-ASE] §2.1	Pass	Pass
	1.9C (1-11)	[IR-ASE] §2.1	Pass	Pass
1.2E	- (1-12)	[IR-ASE] §2.1	Pass	Pass
Conformance claims ASE_CCL				
1.1E	1.1C (1-1)	[IR-ASE] §2.2	Pass	Pass
	1.2C (1-2)	[IR-ASE] §2.2	Pass	Pass
	1.3C (1-3)	[IR-ASE] §2.2	Pass	Pass
	1.4C (1-4/5)	[IR-ASE] §2.2	Pass	Pass

Evaluator action	Content (CEM ID)	Report reference, including slide# or section #	ITSEF verdict	CB TR verdict
	1.5C (1-6/7/8/9/10/11/12)	[IR-ASE] §2.2	Pass	Pass
	1.6C (1-13, 1-14)	[IR-ASE] §2.2	Pass	Pass
	1.7C (1-15)	[IR-ASE] §2.2	Pass	Pass
	1.8C (1-16)	[IR-ASE] §2.2	Pass	Pass
	1.9C (1-17)	[IR-ASE] §2.2	Pass	Pass
	1.10C (1-18)	[IR-ASE] §2.2	Pass	Pass
	1.11C (1-19)	[IR-ASE] §2.2	Pass	Pass
	1.12C (1-20)	[IR-ASE] §2.2	Pass	Pass
	1.13C (1-21)	[IR-ASE] §2.2	Pass	Pass
Security problem definition ASE_SPD				
1.1E	1.1C (1-1)	[IR-ASE] §2.3	Pass	Pass
	1.2C (1-2)	[IR-ASE] §2.3	Pass	Pass
	1.3C (1-3)	[IR-ASE] §2.3	Pass	Pass
	1.4C (1-4)	[IR-ASE] §2.3	Pass	Pass
Security objectives ASE_OBJ				
2.1E	2.1C (2-1)	[IR-ASE] §2.4	Pass	Pass
	2.2C (2-2)	[IR-ASE] §2.4	Pass	Pass
	2.3C (2-3)	[IR-ASE] §2.4	Pass	Pass
	2.4C (2-4)	[IR-ASE] §2.4	Pass	Pass
	2.5C (2-5)	[IR-ASE] §2.4	Pass	Pass
	2.6C (2-6)	[IR-ASE] §2.4	Pass	Pass
Extended components definition (ASE_ECD)				
1.1E	1.1C (1-1)	[IR-ASE] §2.5	Pass	Pass
	1.2C (1-2)	[IR-ASE] §2.5	Pass	Pass
	1.3C (1-3/4)	[IR-ASE] §2.5	Pass	Pass
	1.4C (1-5/6/7/8/9/10/11)	[IR-ASE] §2.5	Pass	Pass
	1.5C (1-12)	[IR-ASE] §2.5	Pass	Pass
1.2E	- (1-13)	[IR-ASE] §2.5	Pass	Pass

Evaluator action	Content (CEM ID)	Report reference, including slide# or section #	ITSEF verdict	CB TR verdict
Security requirements (ASE_REQ)				
2.1E	2.1C (2-1/2)	[IR-ASE] §2.6	Pass	Pass
	2.2C (2-3/4)	[IR-ASE] §2.6	Pass	Pass
	2.3C (2-5/6/7/8)	[IR-ASE] §2.6	Pass	Pass
	2.4C (2-9)	[IR-ASE] §2.6	Pass	Pass
	2.5C (2-10)	[IR-ASE] §2.6	Pass	Pass
	2.6C (2-11/12/13/14)	[IR-ASE] §2.6	Pass	Pass
	2.7C (2-15)	[IR-ASE] §2.6	Pass	Pass
	2.8C (2-16)	[IR-ASE] §2.6	Pass	Pass
	2.9C (2-17)	[IR-ASE] §2.6	Pass	Pass
	2.10C (2-18)	[IR-ASE] §2.6	Pass	Pass
	2.11C (2-19)	[IR-ASE] §2.6	Pass	Pass
TOE summary specification (ASE_TSS)				
1.1E	1.1C (1-1)	[IR-ASE] §2.7	Pass	Pass
1.2E	- (1-2)	[IR-ASE] §2.7	Pass	Pass

11.2.2 ADV

ADV has no **OPEN** comments.

		Report reference, including slide# or section #	ITSEF verdict	CB TR verdict
Security architecture (ADV_ARC)				
1.1E	1.1C	[ADV PRES] Part 4	Pass	Pass
	1.2C	[ADV PRES] Part 4	Pass	Pass
	1.3C	[ADV PRES] Part 4	Pass	Pass
	1.4C	[ADV PRES] Part 4	Pass	Pass
	1.5C	[ADV PRES] Part 4	Pass	Pass
Functional specification ADV_FSP				
ADV_FSP.3.1E	3.1C	[ADV PRES] Part 1	Pass	Pass
	3.2C	[ADV PRES] Part 1	Pass	Pass

		Report reference, including slide# or section #	**ITSEF verdict**	**CB TR verdict**
	3.3C	[ADV_AGD_MFU] and [ADV_AGD_NTAG] section 3.1	Pass	Pass
	3.4C	[ADV_AGD_MFU] and [ADV_AGD_NTAG] section 3.1	Pass	Pass
	3.5C	[ADV_AGD_MFU] and [ADV_AGD_NTAG] section 3.1	Pass	Pass
	3.6C	[ADV_AGD_MFU] and [ADV_AGD_NTAG] section 3.1	Pass	Pass
	5.7C	[ADV PRES] Part 3	Pass	Pass
ADV_FSP.3.2E	-	[ADV PRES] Part 3	Pass	Pass
TOE design ADV_TDS				
ADV_TDS.2.1E	2.1C	[ADV PRES] Part 2	Pass	Pass
	2.2C	[ADV PRES] Part 2	Pass	Pass
	2.3C	[ADV PRES] Part 2	Pass	Pass
	2.4C	[ADV PRES] Part 2	Pass	Pass
	2.5C	[ADV PRES] Part 2	Pass	Pass
	2.6C	[ADV PRES] Part 2	Pass	Pass
	2.7C	[ADV PRES] Part 2	Pass	Pass
	2.8C	[ADV PRES] Part 2	Pass	Pass
ADV_TDS.2.2E	-	[ADV PRES] Part 3	Pass	Pass

11.2.3 AGD

AGD has no **OPEN** comments.

		Report reference, including slide# or section #	**ITSEF verdict**	**CB TR verdict**
Operational user guidance AGD_OPE				
AGD_OPE.1.1E	1.1C	[ADV_AGD_MFU] and [ADV_AGD_NTAG] chapter 4	Pass	Pass
	1.2C	[ADV_AGD_MFU] and [ADV_AGD_NTAG] chapter 4	Pass	Pass
	1.3C	[ADV_AGD_MFU] and [ADV_AGD_NTAG] chapter 4	Pass	Pass
	1.4C	[ADV_AGD_MFU] and [ADV_AGD_NTAG] chapter 4	Pass	Pass
	1.5C	[ADV_AGD_MFU] and [ADV_AGD_NTAG] chapter 5	Pass	Pass

		Report reference, including slide# or section #	**ITSEF verdict**	**CB TR verdict**
	1.6C	[ADV_AGD_MFU] and [ADV_AGD_NTAG] chapter 6	Pass	Pass
	1.7C	[ADV_AGD_MFU] and [ADV_AGD_NTAG] chapter 4-8	Pass	Pass
Preparative procedures AGD_PRE.				
AGD_PRE.1.1E	1.1C	[ADV_AGD_MFU] and [ADV_AGD_NTAG] chapter 7	Pass	Pass
	1.2C	[ADV_AGD_MFU] and [ADV_AGD_NTAG] chapter 6 and 8	Pass	Pass
AGD_PRE.1.2E		[ATE PRES] Part 5	Pass	Pass

11.2.4 ALC

ALC has no **OPEN** comments.

		Report reference, including slide# or section #	**ITSEF verdict**	**CB TR verdict**
CM capabilities ALC_CMC				
ALC_CMC.3.1E	3.1C	[ALC PRES] 2nd meeting. ALC_CMC	Pass	Pass
	3.2C	[ALC PRES] 1st meeting.	Pass	Pass
	3.3C	[ALC PRES] 2nd meeting. ALC_CMC	Pass	Pass
	3.4C	[ALC PRES] 2nd meeting. ALC_CMC	Pass	Pass
	3.5C	[ALC PRES] 2nd meeting. ALC_CMC	Pass	Pass
	3.6C	[ALC PRES] 2nd meeting. ALC_CMC	Pass	Pass
	3.7C	[ALC PRES] 2nd meeting. ALC_CMC	Pass	Pass
	3.8C	[ALC PRES] 2nd meeting. ALC_CMC	Pass	Pass
CM Scope ALC_CMS				
ALC_CMS.3.1E	3.1C	[ALC PRES] 1st meeting.	Pass	Pass
	3.2C	[ALC PRES] 2nd meeting. ALC_CMS	Pass	Pass
	3.3C	[ALC PRES] 2nd meeting. ALC_CMS	Pass	Pass
Delivery ALC_DEL				
ALC_DEL.1.1E	1.1C	[ALC PRES] 2nd meeting. ALC_DEL	Pass	Pass
Development security ALC_DVS				
ALC_DVS.1.1E	1.1C	[ALC PRES] 2nd meeting. ALC_DVS	Pass	Pass

		Report reference, including slide# or section #	**ITSEF verdict**	**CB TR verdict**
ALC_DVS.1.2E		[ALC PRES] 2nd meeting. ALC_DVS	Pass	Pass
Life cycle definition ALC_LCD				
ALC_LCD.1.1E	1.1C	[ALC PRES] 2nd meeting. ALC_LCD	Pass	Pass
	1.2C	[ALC PRES] 2nd meeting. ALC_LCD	Pass	Pass
Flaw remediation ALC_FLR				
ALC_FLR.2.1E	2.1C	[ALC PRES] 2nd meeting. ALC_FLR	Pass	Pass
	2.2C	[ALC PRES] 2nd meeting. ALC_FLR	Pass	Pass
	2.3C	[ALC PRES] 2nd meeting. ALC_FLR	Pass	Pass
	2.4C	[ALC PRES] 2nd meeting. ALC_FLR	Pass	Pass
	2.5C	[ALC PRES] 2nd meeting. ALC_FLR	Pass	Pass
	2.6C	[ALC PRES] 2nd meeting. ALC_FLR	Pass	Pass
	2.7C	[ALC PRES] 2nd meeting. ALC_FLR	Pass	Pass
	2.8C	[ALC PRES] 2nd meeting. ALC_FLR	Pass	Pass

11.2.5 ATE

ATE has no **OPEN** comments.

		Report reference, including slide# or section #	**ITSEF verdict**	**CB TR verdict**
Coverage ATE_COV				
ATE_COV.2.1E	2.1C	[ATE PRES] Part 2	Pass	Pass
	2.2C	[ATE PRES] Part 2	Pass	Pass
Depth ATE_DPT				
ATE_DPT.1.1E	1.1C	[ATE PRES] Part 2	Pass	Pass
Functional tests ATE_FUN				
ATE_FUN.1	1.1C	[ATE PRES] Part 1	Pass	Pass
	1.2C	[ATE PRES] Part 1	Pass	Pass
	1.3C	[ATE PRES] Part 1	Pass	Pass
	1.4C	[ATE PRES] Part 1	Pass	Pass
Independent testing ATE_IND				
ATE_IND.2.1E	2.1C	[ATE PRES] Part 4	Pass	Pass

		Report reference, including slide# or section #	**ITSEF verdict**	**CB TR verdict**
	2.2C	[ATE PRES] Part 3 and 4	Pass	Pass
ATE_IND.2.2E		[ATE PRES] Part 3 and 4	Pass	Pass
ATE_IND.2-3E		[ATE PRES] Part 3 and 4	Pass	Pass

11.2.6 AVA

AVA has no **OPEN** comments.

		Report reference, including slide# or section #	**ITSEF verdict**	**CB TR verdict**
Vulnerability analysis AVA_VAN				
AVA_VAN.2.1E	2.1C	[AVA PRES] Part 2	Pass	Pass
	2.2C	[AVA PRES] Part 2	Pass	Pass
AVA_VAN.2.2E		[AVA PRES] Part 1	Pass	Pass
AVA_VAN.2.3E		[AVA PRES] Part 1	Pass	Pass
AVA_VAN.2.4E		[AVA PRES] Part 2	Pass	Pass

12 Summary of the Security Target

12.1 Required information

ST reference	MF0AES(H)x0, NT2H2xy1G and NT2H2xy1S Security Target Lite, Version 2.4, NXP Semiconductors, 07 April 2026.

12.2 ST summary

NXP has developed the TOE to be used with Proximity Coupling Devices (PCDs, also called "terminal") according to ISO 14443 Type A [ISO 14443-1][ISO 14443-2][ISO 14443-3]. The communication protocol complies to ISO 14443 part 3 [ISO 14443-3]. The TOE is primarily designed for secure applications such as public transportation, access, event ticketing, loyalty, smart packaging and brand protection. It fully complies with the requirements for fast and secure data transmission and interoperability with existing infrastructure.
The TOE provides resistance against attack by an attacker with a basic attack potential. This is achieved by a combination of different security features that provide a baseline functional security protection complemented with implementation security protection against information leakage via side-channels, fault injections and physical attacks relevant for the targeted attack potential. Furthermore, the TOE protects the different operating modes of the Security IC to avoid abuse by an attacker. Protected by these security features the TOE implements the following main security services:

- secure mutual authentication to support authentication of authorized users and the TOE.
- secure channel establishment and secure messaging to support integrity protected data transfer on the MIFARE Ultralight AES variant of the TOE.
- secure user one-time programmable memory area.
- secure read-only locking of the user memory.
- one or more secure monotonic counters.
- secure dynamic messaging to allow secure export of data in unauthenticated state on NTAG 22x (StatusDetect) variants of the TOE.
- supporting non-traceability of the TOE by providing the option to use random IDs during contactless protocol establishment on the MIFARE Ultralight AES variant of the TOE.
- additional functionality to detect the status of tamper evidence provided by the NTAG 22x StatusDetect variant of the TOE.

These security functionalities aim at enabling card issuers to use the product for various use-cases as outlined in the following.

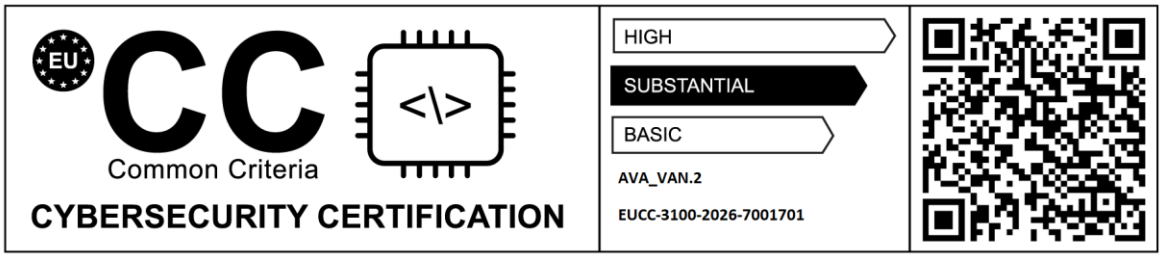
- **MIFARE Ultralight AES**: the MF0AES(H)x0 variants of the TOE is intended for limited-use transport tickets, event ticketing (e.g. cinema, game or concert) or access control badges, the hospitality industry (e.g. hotels) and also loyalty cards with limited value.
- **NTAG 22x DNA**: the NT2H2xy1G variants of the TOE are intended as NFC Forum Type 2 Tag. It might generate Secure Unique NFC Message in each tap for direct access to web services. The main use cases are brand protection and smart packaging. A subset of the supported card reader command set is to be compatible with the NFC Forum Type 2 Tag standard.

- **NTAG 22x DNA StatusDetect**: the NT2H2xy1S variants of the TOE are identical to NTAG 22x DNA, but support additionally the "StatusDetect" feature, which allows the user to control and detect when a tamper evidence mechanism has been triggered. This feature supports use cases, where product integrity needs to be verified e.g. seals for high-value liquids.

The concrete product variant is instantiated by NXP during production by properly configuring the platform and the provisioning of the correct memory layout. The security features of the platform enforce that once configured to one of above listed products the product variant cannot be further changed.

As a consequence, each variant of the TOE is identified precisely by the configuration during production. The TOE does not provide any functionality loading after production.

13 Mark or label associated to the scheme



14 Bibliography

14.1.1 Evaluation criteria

[CC] Common Criteria for Information Technology Security Evaluation, Part 1, 2, 3, 4 and 5, CC:2022 Revision 1

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, CC:2022 Revision 1

[CCMB-2024-002] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2

[NI002] Content and presentation of evaluation review meeting version 1

[MSSR] ENISA, Minimum Site Security Requirements, v1.1, October 2023

[CC_IC] ENISA, Application of Common Criteria to Integrated Circuits v2 (draft), March 2025

[SC_ARC] ENISA, Security Architecture Requirements for Smart Cards and Similar Devices, v1.1, April 2024

[SC_OPEN] ENISA, Certification of “open” Smart Card products, v1.1, October 2023

[AT_POT] ENISA, Application of Attack Potential to Smartcards, v2 (draft), February 2025

[JIL-AM] JIL, Attack Methods for Smartcards and Similar Devices (controlled distribution), Version 2.5 (Release 5), May 2022

14.1.2 Evaluation technical report

[ETR] Evaluation Technical Report “MF0AES(H)x0, NT2H2xy1G and NT2H2xy1S” – EAL3 augmented with ALC_FLR.2, v4.0

14.1.3 Technical reference documentation

[PP] Security IC Platform Protection Profile with Augmentation Packages, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014, Version 1.0, 13 January 2014

[ISO 14443-1] ISO/IEC 14443-1:2016- Identification cards — Contactless integrated circuit cards — Proximity cards Part 1: Physical characteristics”, March 2016

[ISO 14443-2] ISO/IEC 14443-2:2016 - Identification cards — Contactless integrated circuit cards — Proximity cards Part 2: Radio frequency power and signal interface”, July 2016

[ISO 14443-3] ISO/IEC 14443-3:2016 - dentification cards — Contactless integrated circuit cards — Proximity cards Part 3: Initialization and anticollision”, September 2016

14.1.4 Developer documentation

[ST] Security Target, MF0AES(H)x0, NT2H2xy1G and NT2H2xy1S, Rev. 2.4, 07 April 2026, NXP Semiconductors

[ST-lite] Security Target Lite, MF0AES(H)x0, NT2H2xy1G and NT2H2xy1S, Rev. 2.4, 07 April 2026, NXP Semiconductors

[UG-MFU]	MIFARE Ultralight AES, Information on Guidance and Operation, Rev. 2.0, 12 December 2025, NXP Semiconductors
[UG-NTAG]	NTAG 22x DNA, Information on Guidance and Operation, Rev. 2.0, 12 December 2025, NXP Semiconductors
[UG-NTAG-SD]	NTAG 22x DNA StatusDetect, Information on Guidance and Operation, Rev. 2.0, 12 December 2025, NXP Semiconductors
[DS-MFU-20]	MF0AES(H)20, Objective data sheet, Rev. 1.1, 20 December 2021, NXP
[DS-MFU-30]	MF0AES(H)30, Objective data sheet, Rev. 1.1, 20 December 2021, NXP
[DS-NTAG-223]	NT2H2331G0, NTAG 223 DNA – NFC T2T compliant IC, Product data sheet, Rev. 3.2, 16 December 2025, NXP Semiconductors
[DS-NTAG-223-SD]	NT2H2331S0, NTAG 223 DNA StatusDetect – NFC T2T compliant IC with StatusDetect feature, Product data sheet Rev. 3.2, 16 December 2025, NXP Semiconductors
[DS-NTAG-224]	NT2H2421G0, NTAG 224 DNA – NFC T2T compliant IC, Product data sheet, Rev. 3.3, 16 December 2025, NXP Semiconductors
[DS-NTAG-224-SD]	NT2H2421S0, NTAG 224 DNA StatusDetect – NFC T2T compliant IC with StatusDetect Feature, Product data sheet, Rev. 3.3, 16 December 2025, NXP Semiconductors

14.1.5 ITSEF documentation

[IR-ASE]	IR-ASE for MF0AES(H)x0, NT2H2xy1G and NT2H2xy1S, v5.0
[ADV PRES]	NTAG22x – ADV Presentation, v3.0
[ADV_AGD_MFU]	NTAG22x- AGD-ADV Reference Document -MFU, v2.0
[ADV_AGD_NTAG]	NTAG22x- AGD-ADV Reference Document -NTAG, v2.0
[ALC PRES]	NTAG22x – ALC Presentation, v5.0
[AVA PRES]	NTAG22x – AVA Presentation, v4.0
[ATE PRES]	NTAG22x – ATE Presentation v3.0
[TR]	NTAG22x – AVA Test Report v2.0