SGS Brightsight B.V.

Brassersplein 2
2612 CT Delft
The Netherlands

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

www.brightsightcb.com

coc 30105045

EUCC-3100-2026-7001701-1
Enisa Website Certificate ID: EUCC-3100-2026-000001-R-01

Certification Report – Reassessment

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

26-CB-050

Version and Approval

Version	Date	Author	Reviewed
1.0	2026-07-01	Miquel Hernandez	Thomas Ribbrock
2.0	2026-08-06	Miquel Hernandez	
3.0	2026-08-24	Rob Kemper	
4.0	2026-08-25	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
Name of the ITSEF which performed the evaluation	SGS Brightsight B.V. (referred to as Brightsight ITSEF)
Completion date of evaluation	2026-06-26
Date of issuance of the certificate	2026-08-06
Date of issuance of the initial certificate	2026-04-10
Validity period	5 years
Unique identification of the certificate	EUCC-3100-2026-7001701-1 Enisa Website Certificate ID: EUCC-3100-2026-000001-R-01
CC Version	ISO/IEC 15408, Common Criteria for Information Technology Security Evaluation (CC), 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, at AVA_VAN.2
Protection Profile(s)	N/A
Security Policy of the evaluated ICT product	Refer to chapter 4 of this report

1.1.1 Assurance continuity and certificate review

Assurance continuity Scope	Re-assessment
Impact of changes	• Unchanged ICT product that still meets its security requirements; • Minor editorial changes due to additional review; • Validity of site audit results was reviewed, resulting in a reference to updated STARs
Source certification	EUCC-3100-2026-7001701
Source Certification Report	26-CB-026 - EUCC-3100-2026-7001701 - Certification Report, version 1.0
Updated ETR	[ETR]
Certified ETR	[ETR-non-CCRA]
Status of initial certificate	To be withdrawn, as per Articles 13[1] & 14[2] of 2024/482
Completion date of certification	2026-08-06

[1] Following the results of the review, and where applicable of the re-evaluation, the certification body shall: withdraw the EUCC certificate in accordance with Article 14 and issue a new EUCC certificate with an identical scope and an extended validity period;

[2] Without prejudice to Article 58(8), point (e), of Regulation (EU) 2019/881, an EUCC certificate shall be withdrawn by the certification body that issued that certificate. The certification body referred to in paragraph 1 shall notify the national cybersecurity certification authority of the withdrawal of the certificate. It shall also notify ENISA of such withdrawal in view of facilitating the performance of its task under Article 50 of Regulation (EU) 2019/881. The national cybersecurity certification authority shall notify other relevant market surveillance authorities.

CC Version	ISO/IEC 15408, Common Criteria for Information Technology Security Evaluation (CC), 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

Please note that the contents of this section together with the remaining contents of the report serve as re-assessment report as per Annex IV of (EU) 2024/482.

The intent of this re-assessment is to certify the ICT product under CCRA compliance.

1.2 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 security target [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 June 26, 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 [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 according to 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.

1.3 International recognition of the certificate

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of published certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.
For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

1.4 Disclaimer(s)

The certification does not guarantee a product is completely free of exploitable vulnerabilities.

2 Identification of the ICT product

2.1 Unique identification

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	3.3	6 February 2026
[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

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 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 Additional requirements to the operating environment of the ICT product

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.

3 Contact information related to the evaluation of the ICT product

Developer Name	NXP Semiconductors Germany GmbH
EUCC certificate holder name and contact information	NXP Semiconductors Germany GmbH Beiersdorfstraße 12, 22529 Hamburg, Germany Contact: Holger Matz www.nxp.com holger.matz@nxp.com +49 (0) 40 5613 – 5103
Certification Body	SGS Brightsight B.V. (referred to as Brightsight CB) Brassersplein 2 2612 CT Delft The Netherlands Contact: Rob Kemper www.brightsightcb.com rob.kemper@sgs.com +31 15 269 25 44
National Cybersecurity Certification Authority	Dutch Authority for Digital Infrastructure – Ministry of Economic Affairs Contact: eucc@dutchncca.nl
ITSEF	SGS Brightsight B.V. (referred to as Brightsight ITSEF) Brassersplein 2 2612 CT Delft The Netherlands Contact: Magdalena Siwko www.brightsight.com/security-evaluations magdalena.siwko@sgs.com +31 15 203 09 13
Subcontractors	N/A

4 Security Policies

4.1 Security services

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.

4.2 Vulnerability handling policy

4.2.1 Reference

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

4.2.2 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 has explicitly been made aware of these (EU) 2024/482 responsibilities for a certificate holder.

4.3 Assurance continuity policy

Due to the nature of the re-assessment, where the certified ICT product is unchanged, an assurance continuity policy was not provided.

4.4 Patch management procedure

N/A

5 Assumptions and clarification of scope

5.1 Assumptions on usage and deployment

Assumptions about the operating environment are described in the [ST] section 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.

5.2 Assumptions on 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.

5.3 Threats to the ICT product not countered by its security functions

Threats described in the [ST] section 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.

All threats are countered by its security functions. However, the threat T.Data-Modification is also countered by the environment through OE.Terminal-Support, as outlined in the [ST] section 4.3: *This objective requires that the terminal must support this by checking the TOE responses.*

6 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:

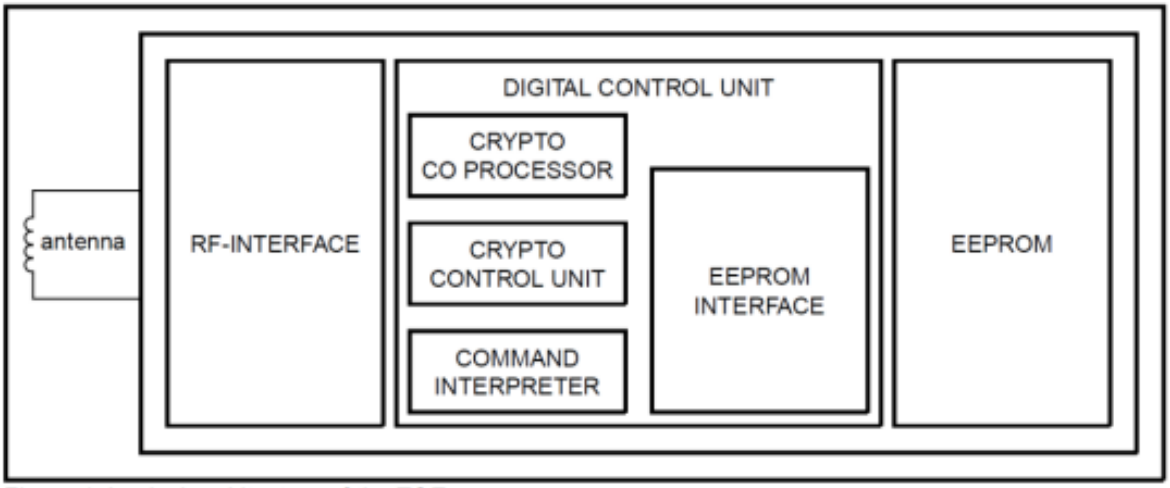


Figure 1. Logical architecture of the TOE.

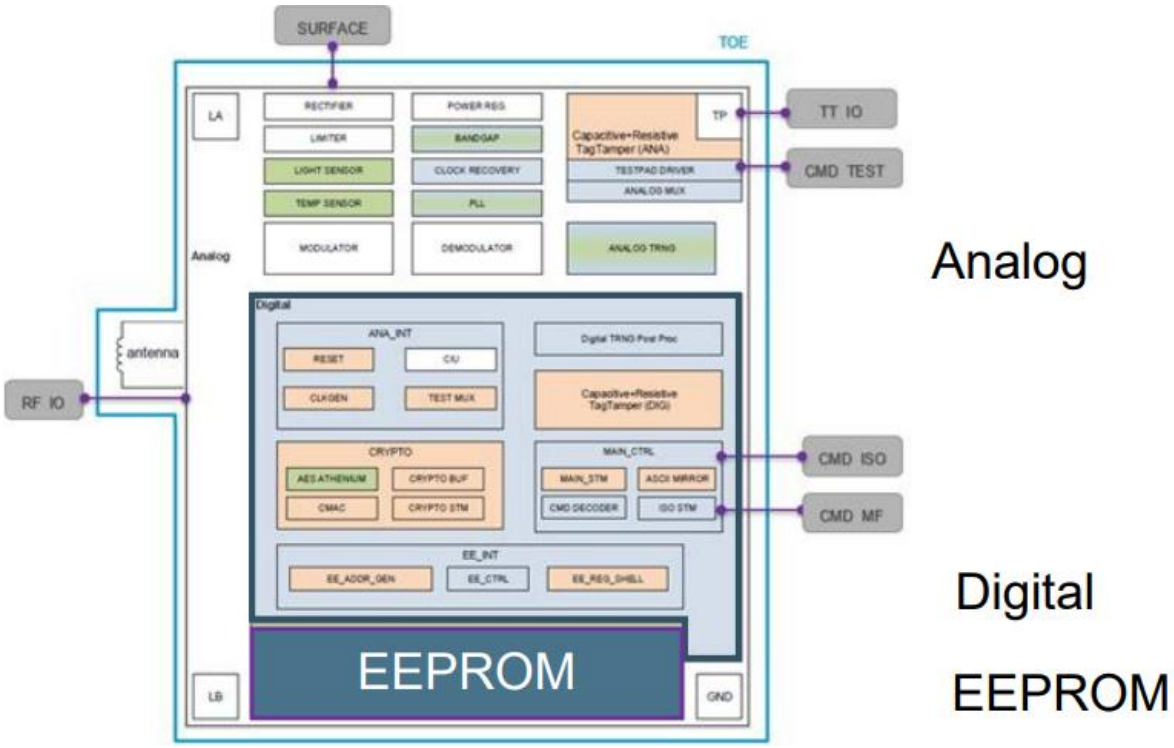
The TOE has the following features:

- 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:



7 Supplementary cybersecurity information

In relation with information to be made available by the certificate holder according to (EU) 2024/482 Chapter VII, https://www.nxp.com/products/nxp-product-information/eucc-certified-products:EUCC-CERTIFIED and www.nxp.com/psirt is stated to contain guidance and information needed by the user, provide information up to 5 years after the certificate validity, and to describe the process of responsible disclosure of vulnerabilities.

8 ICT product evaluation summary and evaluated configuration

8.1 Required information

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

8.2 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 Results of the evaluation and information regarding the certificate

9.1 Required information

Certificate identifier	EUCC-3100-2026-7001701-1
Certificate date of issuance	2026-08-06
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

9.2 Assurance requirements

The chosen assurance level is EAL 3 augmented with ALC_FLR.2. A detailed decomposition of the evaluation results can be found in Appendix A.

9.3 Testing approach and results

9.3.1 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 of setting up the testing environment.

For the testing performed by the evaluators, the developer provided samples that were used for penetration testing.

9.3.2 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].

9.3.3 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 [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.

The 2026 test results from EUCC-3100-2026-7001701 are considered still valid, as the test plan did not change (only additional referencing was added) and testing is sufficiently fresh.

10 Comments and recommendations

10.1 Comments

None.

10.2 Recommendations

None.

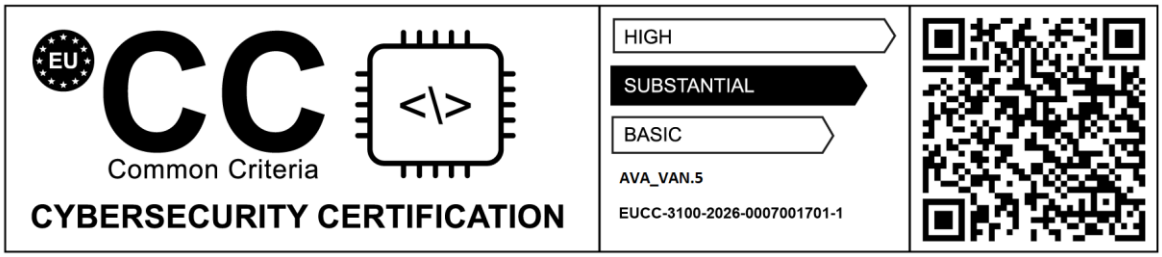
11 Security Target

The certification refers to the following security target:

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

Please note that the version published together with this certification report has been sanitized in line with [CCDB-2006-04-004], resulting in [ST-lite].

12 Mark or label associated to the scheme



13 Glossary

No terms have been used that are not already defined by the CC or CEM.

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
[CCDB-2006-04-004]	ST sanitizing for publication, April 2006

14.1.2 Evaluation technical report

[ETR]	26-RPT-457 – Evaluation Technical Report “MF0AES(H)x0, NT2H2xy1G and NT2H2xy1S” – EAL3 augmented with ALC_FLR.2, v4.0
[ETR-non-CCRA]	25-RPT-1567 – 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. 3.3, 6 February 2026, NXP
[DS-MFU-30]	MF0AES(H)30, Objective data sheet, Rev. 2.0, 4 February 2022, 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]	26-RPT-447 - IR-ASE for MF0AES(H)x0, NT2H2xy1G and NT2H2xy1S, v3.0
[ADV PRES]	26-RPT-448 - NTAG22x – ADV Presentation, v2.0
[ADV_AGD_MFU]	26-RPT-450 - NTAG22x – AGD-ADV Reference Document -MFU, v1.0
[ADV_AGD_NTAG]	26-RPT-451 - NTAG22x – AGD-ADV Reference Document -NTAG, v2.0
[ALC PRES]	26-RPT-452 - NTAG22x – ALC Presentation, v2.0
[AVA PRES]	26-RPT-453 - NTAG22x – AVA Presentation, v2.0
[ATE PRES]	26-RPT-454 - NTAG22x – ATE Presentation v2.0
[TP]	26-RPT-455 - NTAG22x – Test Plan, v3.0
[TR]	26-RPT-456 - NTAG22x – AVA Test Report v2.0

A Mapping of evaluator actions and verdicts

A.1 ASE

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] section 2.1	Pass	Pass
	1.2C (1-2)	[IR-ASE] section 2.1	Pass	Pass
	1.3C (1-3/4)	[IR-ASE] section 2.1	Pass	Pass
	1.4C (1-5)	[IR-ASE] section 2.1	Pass	Pass
	1.5C (1-6/7)	[IR-ASE] section 2.1	Pass	Pass
	1.6C (1-8)	[IR-ASE] section 2.1	Pass	Pass
	1.7C (1-9)	[IR-ASE] section 2.1	Pass	Pass
	1.8C (1-10)	[IR-ASE] section 2.1	Pass	Pass
	1.9C (1-11)	[IR-ASE] section 2.1	Pass	Pass
1.2E	- (1-12)	[IR-ASE] section 2.1	Pass	Pass
Conformance claims ASE_CCL				
1.1E	1.1C (1-1)	[IR-ASE] section 2.2	Pass	Pass
	1.2C (1-2)	[IR-ASE] section 2.2	Pass	Pass
	1.3C (1-3)	[IR-ASE] section 2.2	Pass	Pass
	1.4C (1-4/5)	[IR-ASE] section 2.2	Pass	Pass
	1.5C (1-6/7/8/9 /10/11/12)	[IR-ASE] section 2.2	Pass	Pass
	1.6C (1-13, 1-14)	[IR-ASE] section 2.2	Pass	Pass
	1.7C (1-15)	[IR-ASE] section 2.2	Pass	Pass
	1.8C (1-16)	[IR-ASE] section 2.2	Pass	Pass
	1.9C (1-17)	[IR-ASE] section 2.2	Pass	Pass
	1.10C (1-18)	[IR-ASE] section 2.2	Pass	Pass
	1.11C (1-19)	[IR-ASE] section 2.2	Pass	Pass
	1.12C (1-20)	[IR-ASE] section 2.2	Pass	Pass
	1.13C (1-21)	[IR-ASE] section 2.2	Pass	Pass

Evaluator action	Content (CEM ID)	Report reference, including slide# or section #	ITSEF verdict	CB TR verdict
Security problem definition ASE_SPD				
1.1E	1.1C (1-1)	[IR-ASE] section 2.3	Pass	Pass
	1.2C (1-2)	[IR-ASE] section 2.3	Pass	Pass
	1.3C (1-3)	[IR-ASE] section 2.3	Pass	Pass
	1.4C (1-4)	[IR-ASE] section 2.3	Pass	Pass
Security objectives ASE_OBJ				
2.1E	2.1C (2-1)	[IR-ASE] section 2.4	Pass	Pass
	2.2C (2-2)	[IR-ASE] section 2.4	Pass	Pass
	2.3C (2-3)	[IR-ASE] section 2.4	Pass	Pass
	2.4C (2-4)	[IR-ASE] section 2.4	Pass	Pass
	2.5C (2-5)	[IR-ASE] section 2.4	Pass	Pass
	2.6C (2-6)	[IR-ASE] section 2.4	Pass	Pass
Extended components definition (ASE_ECD)				
1.1E	1.1C (1-1)	[IR-ASE] section 2.5	Pass	Pass
	1.2C (1-2)	[IR-ASE] section 2.5	Pass	Pass
	1.3C (1-3/4)	[IR-ASE] section 2.5	Pass	Pass
	1.4C (1-5/6/7/8/9/10/11)	[IR-ASE] section 2.5	Pass	Pass
	1.5C (1-12)	[IR-ASE] section 2.5	Pass	Pass
1.2E	- (1-13)	[IR-ASE] section 2.5	Pass	Pass
Security requirements (ASE_REQ)				
2.1E	2.1C (2-1/2)	[IR-ASE] section 2.6	Pass	Pass
	2.2C (2-3/4)	[IR-ASE] section 2.6	Pass	Pass
	2.3C (2-5/6/7/8)	[IR-ASE] section 2.6	Pass	Pass
	2.4C (2-9)	[IR-ASE] section 2.6	Pass	Pass
	2.5C (2-10)	[IR-ASE] section 2.6	Pass	Pass
	2.6C (2-11/12/13/14)	[IR-ASE] section 2.6	Pass	Pass
	2.7C (2-15)	[IR-ASE] section 2.6	Pass	Pass
	2.8C (2-16)	[IR-ASE] section 2.6	Pass	Pass
	2.9C (2-17)	[IR-ASE] section 2.6	Pass	Pass

Evaluator action	Content (CEM ID)	Report reference, including slide# or section #	ITSEF verdict	CB TR verdict
	2.10C (2-18)	[IR-ASE] section 2.6	Pass	Pass
	2.11C (2-19)	[IR-ASE] section 2.6	Pass	Pass
TOE summary specification (ASE_TSS)				
1.1E	1.1C (1-1)	[IR-ASE] section 2.7	Pass	Pass
1.2E	- (1-2)	[IR-ASE] section 2.7	Pass	Pass

A.2 ADV

		Report reference, including slide# or section #	ITSEF verdict	CB TR verdict
Security architecture (ADV_ARC)				
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
	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
	3.7C	[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

		Report reference, including slide# or section #	**ITSEF verdict**	**CB TR verdict**
	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

A.3 AGD

		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
	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

A.4 ALC

		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
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

		Report reference, including slide# or section #	**ITSEF verdict**	**CB TR verdict**
	2.7C	[ALC PRES] 2nd meeting. ALC_FLR	Pass	Pass
	2.8C	[ALC PRES] 2nd meeting. ALC_FLR	Pass	Pass

A.5 ATE

		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
	1.2C	[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
	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

A.6 AVA

		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