MF0AES(H)x0, NT2H2xy1G and NT2H2xy1S

Security Target Lite

Rev. 1.1 — 18 January 2022
NSCIB-CC-0138361

Evaluation document
PUBLIC

Document information

Information	Content
Keywords	Common Criteria, Security Target Lite, MF0AES(H)x0, NT2H2xy1G and NT2H2xy1S
Abstract	Evaluation of the MF0AES(H)x0, NT2H2xy1G and NT2H2xy1S product, developed and provided by NXP Semiconductors, Business Unit Security and Connectivity, according to the Common Criteria for Information Technology Evaluation Version 3.1 at EAL3 augmented.

Revision History

Rev.	Date	Description
1.1	2022-01-18	Derived from full Security Target, Rev. 1.2

1 Introduction

1.1 ST Reference

MF0AES(H)x0, NT2H2xy1G and NT2H2xy1S Security Target Lite, Version 1.1, NXP Semiconductors, 18 January 2022.

1.2 TOE Reference

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

1.3 TOE Overview

1.3.1 Introduction

NXP has developed the TOE to be used with Proximity Coupling Devices (PCDs, also called "terminal") according to ISO 14443 Type A [20][21][22]. The communication protocol complies to ISO 14443 part 3 [22]. 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.

1.3.2 TOE Type

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.

All relevant documents are listed in Table 1, thus being components of the TOE.

1.3.3 Required non-TOE Hardware/Software/Firmware

The TOE requires an ISO 14443 [20][22][21] compliant card terminal to be provided with power and to receive adequate commands.

1.4 TOE Description

1.4.1 Physical Scope of the TOE

The Target of Evaluation (TOE) is an integrated circuit, which is used for all variants as described in Section 1.3.1. A block diagram of the IC hardware is depicted in Figure 1. The configuration data stored in the EEPROM of the device determines the actual variant and can only be set by NXP.

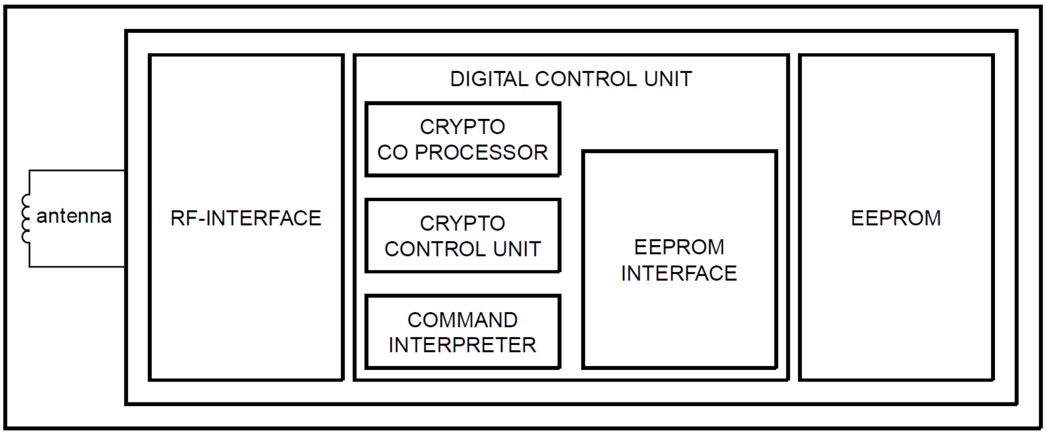

Figure 1. TOE hardware IC block diagram

The TOE deliverables for all variants are:

Table 1. TOE deliverables

Type	Description	Release	Form of delivery
IC Hardware	TOE Hardware for all variants	B0	Sawn wafer (FFC), modules.
Documentation	according to Table 2, Table 3, and Table 4, depending on ordered variant.	N/A	Electronic documents (PDF via NXP DocStore)

The following TOE components are relevant for the MIFARE Ultralight AES variant of the TOE only:

Table 2. MIFARE Ultralight AES components

Type	Name	Release	Form of delivery
Document	MF0AES(H)20, MIFARE Ultralight AES - Contactless ticket IC, Objective data sheet [7]	1.1	Electronic document (PDF via NXP DocStore)
Document	MF0AES(H)30, MIFARE Ultralight AES - Contactless ticket IC, Objective data sheet [8]	1.1	Electronic document (PDF via NXP DocStore)
Document	MIFARE Ultralight AES, Guidance and operation manual [9]	1.2	Electronic document (PDF via NXP DocStore)

The following TOE components are relevant for the NTAG 22x DNA variant of the TOE only:

Table 3. NTAG 22x DNA components

Type	Name	Release	Form of delivery
Document	NT2H2331G0, NTAG 223 DNA - NFC T2T compliant IC, Objective data sheet [10]	1.1	Electronic document (PDF via NXP DocStore)
Document	NT2H2421G0, NTAG 224 DNA - NFC T2T compliant IC, Objective data sheet [12]	1.1	Electronic document (PDF via NXP DocStore)

Table 3. NTAG 22x DNA components*...continued*

Type	Name	Release	Form of delivery
Document	NTAG 22x DNA, Guidance and operation manual [14]	1.2	Electronic document (PDF via NXP DocStore)

The following TOE components are relevant for the NTAG 22x DNA StatusDetect variant of the TOE only:

Table 4. NTAG 22x DNA StatusDetect components

Type	Name	Release	Form of delivery
Document	NT2H2331S0, NTAG 223 DNA StatusDetect - NFC T2T compliant IC with StatusDetect feature, Objective data sheet [11]	1.1	Electronic document (PDF via NXP DocStore)
Document	NT2H2421S0, NTAG 224 DNA StatusDetect - NFC T2T compliant IC with StatusDetect feature, Objective data sheet [13]	1.1	Electronic document (PDF via NXP DocStore)
Document	NTAG 22x DNA StatusDetect, Guidance and operation manual [15]	1.2	Electronic document (PDF via NXP DocStore)

The TOE (hardware) is shipped to the customer by NXP. The available documentation can be downloaded by customers in PDF format directly from the NXP DocStore.

1.4.1.1 Evaluated configurations

1.4.1.1.1 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. The naming convention is explained in the table below.

Table 5. Naming convention MIFARE Ultralight AES

Identifier	Description	Assignment	Meaning
MF0	product family (fixed value)	MF0	MIFARE Ultralight family
AES	product (fixed value)	AES	Advanced Encryption Standard
(H)	input capacitance	<omitted> H	17 pF 50 pF
x	user memory size	2 3	144 byte 208 byte
y	evolution (fixed value)	0	EV0
f	UID type	0 1	7 byte UID 10 byte UID
f	source	0 1	multi source single source

Table 5. Naming convention MIFARE Ultralight AES...*continued*

Identifier	Description	Assignment	Meaning
D	fixed value	D	
pp	package type	A8 UD UF	MOA8 contactless module bare die on FFC, 120µm thickness bare die on FFC, 75µm thickness

1.4.1.1.2 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 naming convention is explained in the table below.

Table 6. Naming convention NTAG 22x DNA (with or without StatusDetect)

Identifier	Description	Assignment	Meaning
NT2	Product (fixed value)	NT2	Fixed identifier for NTAG Type 2 Tag
H	input capacitance (fixed value)	H	Fixed identifier for input capacitance (50 pF)
2	evolution (fixed value)	2	EV2
x	user memory size	3 4	144 byte 208 byte
y	authentication method	2 3	Mutual authentication / SUN Password / SUN
1	process (fixed value)	1	C140 technology
v	IC type	G S	no StatusDetect with StatusDetect
w	UID type	0 1 S	7B UID 10B UID Service types (pre-programmed by NXP)
D	fixed value	D	
zz	delivery type	UD UF	bare die on FFC, 120µm thickness bare die on FFC, 75µm thickness

1.4.2 Logical Scope of the TOE

1.4.2.1 Hardware Description

The TOE is a hardware IC and implements a state-machine responsible for performing the claimed security functionality. It therefore does not contain a CPU. Communication with the TOE can be performed through the contactless interface. The AES co-processor supports AES operations with a key length of 128 bit. A hardware Random Number Generator provides true random numbers which are used internally for security purposes.

The hardware provides selected countermeasures to increase protection against physical manipulation and side-channel analysis. Sensors included in the hardware control the operating conditions (temperature, supply voltage, light). Security mechanisms are in place that prevent test functionality from being reactivated after TOE delivery.

1.4.2.2 Software Description

The TOE is a hardware IC implementing a state-machine and does not contain any software. The high-level functionality that the state-machine implements can be summarized as the following:

- **Authentication** The TOE provides an authentication mechanism to separate authorized users from unauthorized users. The authentication is performed by a cryptographic challenge response.The TOE product variants that only support password-based authentication are outside of the certification scope.
- **Access control** The TOE implements an access control policy, which manages the access to the data stored on the TOE, as well as authorized access to security attributes and keys.
- **Message authentication** CMAC-based secure messaging adds data to the communication stream that enables the terminal to detect integrity violations, replay attacks or man-in-the-middle attacks.
- **Monotonic Counter** The TOE provides one or more (depending on variant) monotonic counters that ensure that during the lifetime of the TOE, these can only be incremented.
- **One-time programmable memory** The TOE ensures that certain parts of the memory can only be written once.
- **No Traceability** The TOE provides an option to use a random UID, which prevents the card from being traced by simply retrieving its UID.
- **Tag Tamper detection** The TOE provides a mechanism for detection and permanent storage of the status of the tag tamper wire.

1.4.2.3 Documentation

All documentation available for the TOE and its variants is listed in Section 1.4.1.

1.4.3 Life Cycle and Delivery of the TOE

The life-cycle phases are organized according to the Security IC Platform Protection Profile with Augmentation Packages [6], Section 1.2.4:

- Phase 1: IC Embedded Software Development
- Phase 2: IC Development
- Phase 3: IC Manufacturing
- Phase 4: IC Packaging
- Phase 5: Composite Product Integration
- Phase 6: Personalisation
- Phase 7: Operational Usage

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 life-cycle 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.

1.4.4 TOE Intended Usage

The TOE user environment is the environment from TOE Delivery to Phase 7. At the phases up to 6, the TOE user environment must be a controlled environment. The only exception is that customer specific keys can be installed using trust provisioning services in Phase 6. In this case the customer can finalize the personalization at the end of Phase 6, already relying on the TOE provided operational security services. Regarding to Phase 7, the TOE is used by the end-user. The method of use of the product in this phase depends on the application. The TOE is intended to be used in an unsecured environment that does not avoid a threat.

In the end-user environment (Phase 7) smart card ICs are used in a wide range of applications to assure authorized conditional access. Examples of such are transportation or access management. The end-user environment therefore covers a wide spectrum of very different functions, thus making it difficult to avoid and monitor any abuse of the TOE.

The system integrators such as the terminal software developer may use samples of the TOE during the development phases for their testing purposes. These samples do not differ from the TOE, they do not have any additional functionality used for testing.

1.4.5 Interface of the TOE

The electrical interface of the TOE are the pads to connect the RF antenna, which allows communication according to ISO 14443 Type A. The communication protocol complies to part ISO 14443-3. The functional interface is defined by the commands implemented by the TOE and described in the product data sheet.

2 Conformance Claims

2.1 CC Conformance Claim

This Security Target claims to be conformant to the Common Criteria version 3.1:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, CCMB-2017-04-001, April 2017 [2].
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, CCMB-2017-04-002, April 2017 [3].
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, CCMB-2017-04-003, April 2017 [4].

For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 5, CCMB-2017-04-004, April 2017 [5].

This Security Target claims to be CC Part 2 extended and CC Part 3 conformant. The extended Security Functional Requirements are defined in Section 5.

2.2 Package Claim

This Security Target claims conformance to the assurance package EAL3 augmented, which in particular includes resistance against a **basic attack potential** (as implied by the inclusion of AVA_VAN.2). The augmentation to EAL3 is ASE_TSS.2.

2.3 PP Claim

This Security target does not claim conformance to any Protection Profile.

2.4 Conformance Claim Rationale

Even though this Security Target does not claim conformance to any Protection Profile, the general modelling approach of the security problem definition and the structure of the security functional requirements have been taken from the Security IC Platform Protection Profile with Augmentation Packages [6]. Whenever this Security Target is referring to 'Protection Profile', the reader of this Security Target must be aware about Section 2.3 and the current section.

The TOE is a similar product-type (security IC) as described in the Protection Profile. The primary difference is in the claimed attack resistance level, which is justified by the value of the assets protected by the TOE. A second difference is that the Protection Profile formulates the security objectives for the security IC from the perspective of a generic platform protecting arbitrary kinds of embedded software implementations, which this TOE does not support.

Therefore, the following modifications and precisions for the TOE use-case have been made: The assumption A.Resp-Appl and the related objective for the TOE environment OE.Resp-Appl have not been taken from the Protection Profile because they formulate assumptions on the behaviour of the embedded software, which is not relevant for this TOE.

3 Security Problem Definition

Although this Security Target does not claim conformance to any Protection Profile, the general modelling approach of the security problem definition and the structure of the security functional requirements have been taken over from the Security IC Platform Protection Profile with Augmentation Packages [6]. The only deviation is explained in Section 2.4. In the following paragraphs only the extensions of the different sections are detailed. The elements of the Security Problem Definition that are not extended in the Security Target are not repeated in this Security Target, they are cited here for completeness only.

3.1 Description of Assets

The assets to be protected by the TOE are based on on the assets described in Section 3.1 of the Protection Profile [6]. Assets related to the high-level security concerns are:

- Integrity and confidentiality of user data stored and in operation. More concretely, the user data comprises the data and key material contained in the data elements, customer configurable configuration options, as well as NXP configuration data and other administrative information that ensures proper operation of the TOE.
- Integrity and confidentiality of UID depending on configuration.
- Correct operation of the security services provided by the TOE.
- Deficiency of random numbers.

To be able to protect these assets the TOE shall self-protect its security functionality. Critical information about the security functionality shall be protected by the development environment and the operational environment. Critical information may include:

- Logical design data, physical design data, and configuration data.
- Initialisation Data and Pre-personalisation Data, specific development aids, test and characterisation related data, and photomasks.

Observe that the protection requirements for the assets are defined by the assumed basic attack potential and as such can be often lower than for products aiming at resisting against an attacker with a high attack potential. Also note that all assets valid for this TOE are considered when specifying the threats defined in the subsequent section.

3.2 Threats

All threats for the TOE which are defined in section 3.2 of the Protection Profile are applied to this Security Target and are listed in Table 7.

Table 7. Threats defined in the Protection Profile (PP-0084)

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

For details see Section 3.2 of the Protection Profile [6].

The following additional threats are defined in this Security Target:

Table 8. Additional threats defined in this Security Target

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.

3.3 Organisational Security Policies

All organisational security policies defined in the Protection Profile are valid for this Security Target and are listed in Table 9. For details see Section 3.3 of the Protection Profile [6].

Table 9. Organisational security policies defined in the Protection Profile (PP-0084)

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

This Security Target defines additional organisational security policies as specified below:

Table 10. Additional organisational security policies defined in this Security Target

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.

3.4 Assumptions

One of the assumptions defined in Section 3.4 of the Protection Profile [6] is valid for this Security Target and is listed in Table 11. Section 2.4 clarifies the ommited assumption with its reasoning.

Table 11. Assumption taken from Protection Profile (PP-0084)

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

This Security Target defines two additional assumptions as follows:

Table 12. Additional assumptions defined in this Security Target

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.

4 Security Objectives

4.1 Security Objectives for the TOE

All security ojectives for the TOE which are defined in section 4.1 of the Protection Profile are applied to this Security Target and are listed in Table 13.

Table 13. Security Objectives of the TOE (PP-0084)

Name	Title
O.Leak-Inherent	Protection against Inherent Information Leakage
O.Phys-Probing	Protection against Physical Probing
O.Malfunction	Protection against Malfunctions
O.Phys-Manipulation	Protection against Physical Manipulation
O.Leak-Forced	Protection against Forced Information Leakage
O.Abuse-Func	Protection against Abuse of Functionality
O.Identification	TOE Identification
O.RND	Random Numbers

This Security Target defines additional security objectives that are based on additional functionality provided by the TOE as follows:

Table 14. Additional security objectives defined in this Security Target

Name	Title
O.Access-Control	Access Control
O.Authentication	Authentication
O.MAC	Integrity-Protected Communication
O.No-Trace	Preventing Traceability
O.Type-Consistency	Data Type Consistency
O.Tag-Tamper	Tag tamper detection

O.Access-Control **Access Control**
The TOE must provide an access control mechanism for data stored by it. The access control mechanism shall apply to read, modify, create and delete operations for data elements and to reading and modifying security attributes as well as authentication data. It shall be possible to limit the right to perform a specific operation to a specific user. The security attributes (keys) used for authentication shall never be output.

O.Authentication **Authentication**
The TOE must provide an authentication mechanism in order to be able to authenticate authorised users. The authentication mechanism shall be resistant against replay and man-in-the-middle attacks.

O.MAC **Integrity-Protected Communication**

The TOE must be able to protect the communication by adding a MAC. This shall be implemented by security attributes that enforce integrity protected communication for the respective data elements. Usage of the protected communication shall also support the detection of injected and bogus commands within the communication session before the protected data transfer.

O.No-Trace **Preventing Traceability**

The TOE must be able to prevent that the TOE end-user can be traced. This shall be done by providing an option that disables the transfer of privacy-related information that is suitable for tracing an end-user by an unauthorised subject.

O.Type-Consistency **Data Type Consistency**

The TOE must provide a consistent handling of the different supported data types. This comprises regular data, one-time programmable data and monotonic counters.

O.Tag-Tamper **Tag tamper detection**

The TOE must be able to detect and permanently record tampering status on the tag tamper wire.

4.2 Security Objectives for the Operational Environment

All security objectives for the operational environment which are defined in section 4.3 of the Protection Profile are applied to this Security Target and are listed in Table 15.

Table 15. Security Objectives for the Operational Environment (PP-0084)

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

The following additional security objectives for the operational environment are defined in this Security Target:

Table 16. Additional security objectives for the operational environment defined in this Security Target

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.

.

4.3 Security Objectives Rationale

Section 4.4 in the Protection Profile [6] provides a rationale how the threats, organisational security policies and assumptions are addressed by the security objectives defined in the Protection Profile. This rationale is not repeated here.

The following table summarizes how threats, organisational security policies and assumptions are addressed by the security objectives with respect to those items defined in the Security Target.

Table 17. Security Problem Definition mapping to Security Objective

Security Problem Definition	Security Objective
T.Data-Modification	O.Access-Control O.Type-Consistency OE.Terminal-Support
T.Impersonate	O.Authentication
T.Cloning	O.Access-Control O.Authentication
P.MAC	O.MAC
P.No-Trace	O.Access-Control O.Authentication O.No-Trace
P.Tag-Tamper	O.Tag-Tamper
A.Secure-Values	OE.Secure-Values
A.Terminal-Support	OE.Terminal-Support

The rationale for the mapping is given below:

Justification related to T.Data-Modification:

Security Objective	Rationale
O.Access-Control	This objective requires an access control mechanism that limits the ability to modify data and code elements stored by the TOE.
O.Type-Consistency	This objective ensures that data types are adhered, so that TOE data can not be modified by abusing type-specific operations.
OE.Terminal-Support	This objective requires that the terminal must support this by checking the TOE responses.

Justification related to T.Impersonate:

Security Objective	Rationale
O.Authentication	This objective requires that the authentication mechanism provided by the TOE shall be resistant against attack scenarios targeting the impersonation of authorized users.

Justification related to T.Cloning:

Security Objective	Rationale
O.Access-Control	This objective requires that unauthorized users can not read any information that is restricted to the authorized subjects. The cryptographic keys used for the authentication are stored inside the TOE and are protected by this objective. This objective states that no keys used for authentication shall ever be output.
O.Authentication	This objective requires that users are authenticated before they can read any information that is restricted to authorized users.

Justification related to A.Secure-Values:

Security Objective	Rationale
OE.Secure-Values	This objective is an immediate transformation of the assumption, therefore it covers the assumption.

Justification related to A.Terminal-Support:

Security Objective	Rationale
OE.Terminal-Support	This objective is an immediate transformation of the assumption, therefore it covers the assumption. The TOE can only check the integrity of data received from the terminal. For data transferred to the terminal the receiver must verify the integrity of the received data. Furthermore the TOE cannot verify the entropy of the random number sent by the terminal. The terminal itself must ensure that random numbers are generated with appropriate entropy for the authentication. This is assumed by the related assumption, therefore the assumption is covered.

Justification related to P.MAC:

Security Objective	Rationale
O.MAC	This objective is an immediate transformation of the security policy, therefore it covers the security policy.

Justification related to P.No-Trace:

Security Objective	Rationale
O.Access-Control	This objective provides means to implement access control to data elements on the TOE in order to prevent tracing based on freely accessible data elements.
O.Authentication	This objective provides means to implement authentication on the TOE in order to prevent tracing based on freely accessible data elements.
O.No-Trace	This objective requires that the TOE shall provide an option to prevent the transfer of any information that is suitable for tracing an end-user by an unauthorized subject. This objective includes the UID.

Justification related to P.Tag-Tamper:

Security Objective	Rationale
O.Tag-Tamper	This objective is an immediate transformation of the security policy, therefore it covers the security policy.

5 Extended Components Definition

To define the Secure Dynamic Messaging functionality of the TOE, an additional component FDP_ETC.3 of the family FDP_ETC (export from the TOE) of the class FDP (user data protection) is defined.

As defined in CC Part 2 [3], the FDP class addresses user data protection. The FDP_ETC family defines functions for TSF-mediated exporting of user data from the TOE such that its security attributes and protection either can be explicitly preserved or can be ignored once it has been exported. The extended component FDP_ETC.3 (Export of user data in unauthenticated state) addresses a similar concern but does not require a TOE enforcement of an access control SFP(s) and/or information flow control SFP(s) as the already defined components of the FDP_ETC family.

5.1 Export of user data in unauthenticated state (FDP_ETC.3)

The class and family behaviour of FDP_ETC are already defined in CC Part 2 [3].

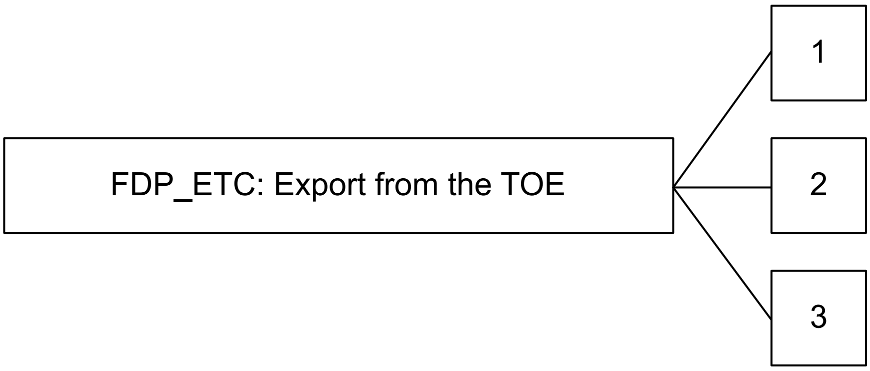

Figure 2. Component levelling of Extended Component FDP_ETC

FDP_ETC	Export from the TOE
Management:	FDP_ETC.3 There are no management activities foreseen.
Audit:	FDP_ETC.3 There are no actions defined to be auditable.
FDP_ETC.3	**Export of user data in unauthenticated state**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_ETC.3.1	**The TSF shall export the following pieces of user data: [assignment: *pieces of user data*] with the following user**

data's associated security attributes: [assignment: *list of security attributes*].

FDP_ETC.3.2 **The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.**

FDP_ETC.3.3 **The TSF shall enforce the following rules when user data is exported from the TOE: [assignment: *additional exportation control rules*]**

The extended component is defined to capture the Secure Unique NFC Message feature provided by the TOE, which allows for the authenticated extraction of user data without the need of establishing a trusted channel beforehand. Due to this specific property, the existing data export SFRs FDP_ETC.1 and FDP_ETC.2 did not apply well.

6 Security Requirements

This chapter defines the security requirements that shall be met by the TOE. These security requirements are composed of the security functional requirements and the security assurance requirements that the TOE must meet in order to achieve its security objectives.

CC allows several operations to be performed on security requirements (on the component level); refinement, selection, assignment, and iteration are defined in section 8.1 of CC Part 1 [2]. These operations are used in this Security Target.

The refinement operation is used to add details to requirements, and thus, further intensifies a requirement.

The selection operation is used to select one or more options provided by the Protection Profile or CC in stating a requirement. Selections having been made are denoted as italic text.

The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made are denoted as italic text.

The iteration operation is used when a component is repeated with varying operations. For the sake of a better readability, the iteration operation may also be applied to some single components (being not repeated) in order to indicate belonging of such SFRs to same functional cluster. In such a case, the iteration operation is applied to only one single component.

6.1 Security Functional Requirements

6.1.1 SFRs taken from the Protection Profile

Table 18 shows the SFRs taken from the Security IC Protection Profile [6] and which are also claimed for the TOE in this Security Target.

Table 18. SFRs taken from the Security IC Protection Profile

Name	Title
FAU_SAS.1	Audit Storage
FDP_ITT.1	Basic Internal Transfer Protection
FDP_IFC.1	Subset Information Flow Control
FDP_SDC.1	Stored data confidentiality
FDP_SDI.2	Stored data integrity monitoring and action
FMT_LIM.1	Limited Capabilities
FMT_LIM.2	Limited Availability
FPT_FLS.1	Failure with Preservation of Secure State
FPT_ITT.1	Basic Internal TSF Data Transfer Protection
FPT_PHP.3	Resistance to Physical Attack
FRU_FLT.2	Limited Fault Tolerance

Of the SFRs listed above, the SFRs FAU_SAS.1, FDP_SDC.1 and FDP_SDI.2 require an assignment or selection operation to be performed. The following subsections describe the operations for these SFRS. The SFRs that are taken directly from the Protection Profile and do not require an operation are not repeated in this Security Target.

6.1.1.1 FAU_SAS.1

The TOE shall meet the requirement "Audit storage" as defined in the PP [6], and as specified below.

FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide *the test process before TOE Delivery* with the capability to store *the Initialisation Data, Pre-personalisation Data, Customer-specific Data*[1] in the *non-volatile memory*[2].

6.1.1.2 FDP_SDC.1

The TOE shall meet the requirement "Stored data confidentiality" as defined in the PP [6], and as specified below.

FDP_SDC.1	**Stored data confidentiality**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_SDC.1.1	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the *volatile and non-volatile memory*[3].

6.1.1.3 FDP_SDI.2

The TOE shall meet the requirement "Stored data integrity monitoring and action" as defined in the PP [6], and as specified below.

FDP_SDI.2	**Stored data integrity monitoring and action**
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies.

[1] [selection: *the Initialisation Data, Pre-personalisation Data, [assignment: other data]*]
[2] [assignment: *type of persistent memory*]
[3] [assignment: *memory area*]

FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for *modification, deletion, repetition or loss of data*[4] on all objects, based on the following attributes: *integrity check information associated with the data storied in memories*[5].
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall *trigger a Security Reset* [6].

6.1.2 Security Functional Requirement regarding Random Numbers

The Security IC Protection Profile [6] defines the threat T.RND and security objective O.RND, which are also claimed for this Security Target (as explained in Section 3). The protection profile makes use of the SFR FCS_RNG.1 to fulfill this requirement. However, this TOE does not offer random numbers as a service to its users but only uses the random number generator internally in order to support a limited set of TSF (AES authentication and Random ID). The use of FCS_RNG.1 is therefore considered not appropiate for this TOE and the SFR FIA_SOS.2 as defined in CC Part 2 [3] is used. The benefit of using FIA_SOS.2 is that it makes it possible to exactly define for which TSF the random numbers are used for, besides defining a quality metric for the generated random numbers. FIA_SOS.2 for this TOE is defined as below.

6.1.2.1 FIA_SOS.2

The TOE shall meet the requirement "TSF Generation of secrets" as specified below.

FIA_SOS.2	**TSF Generation of secrets**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_SOS.2.1	The TSF shall provide a mechanism to generate secrets that meet: *Test procedure A as defined in [1] does not distinguish the generated secrets from output sequences of an ideal RNG*[7].
FIA_SOS.2.2	The TSF shall be able to enforce the use of TSF generated secrets for *AES authentication (generation of random RndB challenge) and Random ID*[8].

[4] [assignment: *integrity errors*]
[5] [assignment: *user data attributes*]
[6] [assignment: *action to be taken*]
[7] [assignment: *a defined quality metric*]
[8] [assignment: *list of TSF functions*]

6.1.3 Security Functional Requirements regarding Access Control

6.1.3.1 Access Control Policy

The Security Function Policy (SFP) *TOE Access Control Policy* uses the definitions listed in this paragraph. The defined subjects are:

Subject	AuthUser	Authenticated User
Info	The authenticated user is the subject that owns or has access to the AES authentication key for Data protection.	

Subject	UIDRetriever	UID Retriever
Info	The UID retriever is the subject that owns or has access to the AES authentication key for UID retrieval.	

Subject	OrigKeyUser	Originality Key User
Info	The OrigKeyUser is the subject that owns or has acces to the AES authentication key for Originality checking. The OrigKeyUser can authenticate with the TOE to prove the authenticity of the Security IC.	

Subject	Anybody	Anybody
Info	Any subject that does not belong to one of the roles AuthUser, UIDRetreiver or OrigKeyUser belongs to the role Anybody. This role includes the card holder (also referred to as end-user), and any other subject like an attacker for instance. The subjects belonging to Anybody do not possess any key and therefore are not able to perform any operation that is restricted to one of the roles which are explicitely excluded from the role Anybody.	

Subject	Nobody	Nobody
Info	Any subject that does not belong to one of the roles AuthUser, UIDRetreiver, OrigKeyUser or Anybody, belongs to the role Nobody. Due to the definition of Anybody, the set of all subjects belonging to the role Nobody is the empty set	

The objects defined for the *TOE Access Control Policy* are:

Object	DataProtKey	AES authentication key for Data protection
Info	This key protects the access to user data.	
Operation	Change	Change the DataProtKey.

Object	UIDRetrKey	AES authentication key for UID retrieval
Info	This key protects the access to the UID..	

Object	UIDRetrKey	AES authentication key for UID retrieval
Operation	Change	Change the UIDRetrKey.

Object	SUNCMACKey	AES key for SUN CMAC calculation
Info	This key is used to compute the CMAC of the Secure Unique NFC Message (SUN).	
Operation	Change	Change the SUNCMACKey.

Object	OrigKey	AES authentication key for Originality Checking
Info	This key can be used to check the originality of the card. It cannot be changed.	

Object	UID	Unique Identifier
Info	Either a 7-byte or 10-byte value that uniquely identifies the IC.	
Operation	Read	Read the UID.

Object	OrigSignature	Originality Signature
Info	ECC 192-bit curve signature	
Operation	Read	Read the OrigSignature.
Operation	Write	Write the OrigSignature.
Operation	Lock	Lock the OrigSignature (either temporary or permanently).
Operation	Unlock	Unlock the OrigSignature.

Object	LockBits	Locking Bits
Info	Locking bits allow for permanently locking of other data objects.	
Operation	Read	Read the LockBits.
Operation	WriteOnce	Write the LockBits irreversibly.

Object	BlockBits	Block locking Bits
Info	Block locking bits allow for permanently locking LockBits.	
Operation	Read	Read the BlockBits.
Operation	WriteOnce	Write the BlockBits irreversibly

Object	OTPBits	One-Time Programmable Bits
Info	One-Time Programmable Bits can be irreversibly written.	
Operation	Read	Read the OTPBits.
Operation	WriteOnce	Write the OTPBits irreversibly.

Object	UserConf	User Configuration
Info	User configuration elements define the behavior of the IC.	
Operation	Read	Read the UserConf.
Operation	Write	Write the UserConf.

Object	UserData	User Data
Info	User data.	
Operation	Read	Read the UserData.
Operation	Write	Write the UserData.

Object	NFCCounter	NFC Counter
Info	Monotonic 24-bit counter registrating the amount of times the IC was read.	
Operation	Read	Read the NFCCounter.
Operation	Increment	Increment the NFCCounter.

Object	AFCCounterX	AFC Counters
Info	Three monotonic 24-bit counters (with X being 0, 1, or 2)	
Operation	Read	Read AFCCounterX.
Operation	Increment	Increment AFCCounterX.

Remark

The *AuthUser* role and the *DataProtKey* object are only supported by the TOE product variants MF0AES(H)x0 and NT2H2x21G, NT2H2x21S i.e. variants supporting AES authentication instead of password-based authentication.

The *UIDRetriever* role, the *UIDRetrKey* and *AFCCounterX* objects are only supported by the TOE product variant MF0AES(H)x0.

The *SUNCMACKey* and *NFCCounter* objects are only supported by the TOE product variants NT2H2xy1G, NT2H2xy1S.

6.1.3.1.1 FMT_SMR.1

The TOE shall meet the requirement "Security roles" as specified below.

FMT_SMR.1	**Security roles**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles *AuthUser, UIDRetriever, OrigKeyUser and Anybody*[9].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.1.3.1.2 FDP_ACC.1

The TOE shall meet the requirement "Subset access control" as specified below.

FDP_ACC.1	**Subset access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	The TSF shall enforce the *TOE Access Control Policy*[10] on *all subjects, objects, operations and attributes defined by the TOE Access Control Policy*[11].

6.1.3.1.3 FDP_ACF.1

The TOE shall meet the requirement "Security attribute based access control" as specified below.

FDP_ACF.1	**Security attribute based access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1	The TSF shall enforce the *TOE Access Control Policy*[12] to objects based on the following: *all subjects, objects and attributes*[13].

[9] [assignment: the authorised identified roles]
[10] [assignment: *access control SFP*]
[11] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[12] [assignment: *access control SFP*]
[13] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:[14]

1. *The AuthUser is allowed to perform UserData.Read,NFCCounter.Read, AFCCounter2.Read, AFCCounter2.Increment, UserConf.Read, OTPBits.Read, LockBits.Read, BlockBits.Read and BlockBits.WriteOnce.*
2. *The AuthUser and UIDRetriever are allowed to perform UID.Read, OrigSignature.Read.*
3. *Anybody, AuthUser and UIDRetriever are allowed to perform AFCCounter0.Read, AFCCounter1.Read, AFCCounter0.Increment and AFCCounter1.Increment.*

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:[15]

1. *The AuthUser is allowed to perform UserData.Write, AFCCounterX.Increment, UserConf.Write, OTPBits.WriteOnce, LockBits.WriteOnce if the target is not locked.*
2. *Anybody and UIDRetriever are allowed to perform UserData.Read, NFCCounter.Read, AFCCounter2.Read, AFCCounter2.Increment, UserConf.Read, OTPBits.Read, LockBits.Read and BlockBits.Read and BlockBits.WriteOnce if allowed by the UserConf.*
3. *Anybody and UIDRetriever are allowed to perform UserData.Write, UserConf.Write, OTPBits.WriteOnce, LockBits.WriteOnce if allowed by the UserConf and the target is not locked.*
4. *Anybody is allowed to perform UID.Read, OrigSignature.Read if Random ID is not enabled.*
5. *Anybody, UIDRetriever and AuthUser are allowed to perform OrigSignature.Write if OrigSignature is not locked or permanently locked.*
6. *Anybody, UIDRetriever and AuthUser are allowed to perform OrigSignature.Lock and OrigSignature.Unlock if OrigSignature is not permanently locked.*
7. *Any one that is allowed to perform UserData.Read, UserConf.Read, OTPBits.Read, LockBits.Read, BlockBits.Read or UID.Read, is allowed to perform NFCCounter.Increment, if enabled by the UserConf, by executing one of those read operations.*

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:[16]

[14] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

[15] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

[16] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

1. *No one but the AuthUser and UIDRetriever is allowed to perform UID.Read if Random ID is enabled.*
2. *OrigKeyUser is not allowed to perform any operation on objects.*
3. *No one but Nobody is allowed to perform any operation on OrigKey.*

6.1.3.1.4 FMT_MSA.3

The TOE shall meet the requirement "Static attribute initialization" as specified below.

FMT_MSA.3	**Static attribute initialization**
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the *TOE Access Control Policy*[17] to provide *permissive*[18] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the *no one but Nobody*[19] to specify alternative initial values to override the default values when an object or information is created.
Application Note:	The memory system is fully instantiated (partially upon customer requests) during the initialization of the product. Therefore, the TOE Access Control Policy does not allow the creation and consequently the manipulation of the default values in operational mode.

6.1.3.1.5 FMT_MSA.1

The TOE shall meet the requirement "Management of security attributes" as specified below.

FMT_MSA.1	**Management of security attributes**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions

[17] [assignment: *access control SFP, information flow control SFP*]

[18] [selection, choose one of: *restrictive, permissive, [assignment: other property]*]

[19] [assignment: *the authorised identified roles*]

FMT_MSA.1.1 The TSF shall enforce the *TOE Access Control Policy*[20] to restrict the ability to *modify*[21] the security attributes *UserConf, LockBits and BlockBits*[22] to *any role*[23].

Application Note: Whether security attributes modification and change is restricted to only the AuthUser, or also allowed by the UIDRetriever and Anybody roles, depends on the current configuration of the security attributes.

6.1.3.1.6 FMT_MTD.1

The TOE shall meet the requirement "Management of TSF data" as specified below.

FMT_MTD.1 **Management of TSF data**

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to *modify and lock*[24] the *DataProtKey, UIDRetrKey and SUNCMACKey*[25] to *specific roles*[26].

Refinement: The detailed management abilities are:

1. *The AuthUser is allowed to perform DataProtKey.Change, UIDRetrKey.Change and SUNCMACKey.Change, if the targeted key is not locked.*
2. *Anybody and UIDRetriever are allowed to perform DataProtKey.Change, UIDRetrKey.Change and SUNCMACKey.Change, if allowed by the UserConf and the targeted key is not locked.*

6.1.3.1.7 FMT_SMF.1

The TOE shall meet the requirement "Specification of Management Functions" as specified below.

FMT_SMF.1 **Specification of Management Functions**

Hierarchical to: No other components.

[20] [assignment: *access control SFP(s), information flow control SFP(s)*]
[21] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[22] [assignment: *list of security attributes*]
[23] [assignment: *the authorised identified roles*]
[24] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[25] [assignment: *list of TSF data*]
[26] [assignment: *the authorised identified roles*]

Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions:[27] • Authenticate a user • Invalidating the current authentication state based on the functions: occurrence of any error during the execution of a command, starting a new authentication, and Reset/Halt of the card, • Changing a security attribute, • Changing a key.

6.1.3.1.8 FDP_ITC.2

The TOE shall meet the requirement "Import of user data with security attributes" as specified below.

FDP_ITC.2	**Import of user data with security attributes**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], FPT_TDC.1 Inter-TSF basic TSF data consistency
FDP_ITC.2.1	The TSF shall enforce the *TOE Access Control Policy*[28] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: *no additional rules*[29].

[27] [assignment: *list of management functions to be provided by the TSF*]
[28] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[29] [assignment: *additional importation control rules*]

6.1.3.2 Implications of the TOE Access Control Policy

The TOE Access Control Policy has some implications, that can be drawn from the policy and that are essential parts of the TOE security functions.

The TOE end-user does normally not belong to the group of authorised users (AuthUser and UIDRetriever), but regarded as Anybody by the TOE. This means that the TOE cannot determine if it is used by its intended end-user (in other words: it cannot determine if the current card holder is the owner of the card).

6.1.4 Additional SFRs regarding confidentiality, authentication and integrity

6.1.4.1 FCS_COP.1/AES

The TOE shall meet the requirement "Cryptographic Operation (AES)" as specified below.

FCS_COP.1/AES	**Cryptographic Operation (AES)**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/AES	The TSF shall perform *encryption and decryption for authentication and cipher based MAC for secure messaging communication*[30] in accordance with the specified cryptographic algorithm *Advanced Encryption Standard AES in one of the following modes of operation: CBC, CMAC*[31] and cryptographic key sizes *128 bits*[32] that meet the following:[33] • *FIPS PUB 197* [16] *(AES)* • *NIST SP 800-38A* [17] *(CBC mode)* • *NIST SP 800-38B* [18] *(CMAC mode)*

6.1.4.2 FIA_UID.2

The TOE shall meet the requirement "User identification before any action" as specified below.

FIA_UID.2	**User identification before any action**
Hierarchical to:	FIA_UID.1 Timing of identification

[30] [assignment: *list of cryptographic operations*]
[31] [assignment: *cryptographic algorithm*]
[32] [assignment: *cryptographic key sizes*]
[33] [assignment: *list of standards*]

Dependencies:	No dependencies.
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Application Note:	Identification of a user is performed upon an authentication request based on the key number. For example, if an authentication request for key number 00h is issued, the user is identified as the *AuthUser*. Before any authentication request is issued, the user is identified as *Anybody*.

6.1.4.3 FIA_UAU.2

The TOE shall meet the requirement "User authentication before any action" as specified below.

FIA_UAU.2	**User authentication before any action**
Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.4 FIA_UAU.3

The TOE shall meet the requirement "Unforgeable authentication" as specified below.

FIA_UAU.3	**Unforgeable authentication**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.3.1	The TSF shall *detect and prevent*[34] use of authentication data that has been forged by any user of the TSF.
FIA_UAU.3.2	The TSF shall *detect and prevent*[35] use of authentication data that has been copied from any other user of the TSF.

6.1.4.5 FIA_UAU.5

The TOE shall meet the requirement "Multiple authentication mechanisms" as specified below.

[34] [selection: *detect, prevent*]
[35] [selection: *detect, prevent*]

FIA_UAU.5	**Multiple authentication mechanisms**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1	The TSF shall provide *'none' and cryptographic authentication*[36] to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the *following rules:*[37] • *The 'none' authentication is performed with anyone who communicates with the TOE without issuing an explicit authentication request. The 'none' authentication implicitly and solely authorizes the 'Anybody' role.* • *The cryptographic authentication is used to authorise the AuthUser and UIDRetriever roles.*

6.1.4.6 FCS_CKM.1

The TOE shall meet the requirement "Cryptographic key generation" as specified below.

FCS_CKM.1	**Cryptographic key generation**
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *session key generation*[38]and specified cryptographic key sizes *128 bit*[39]that meets the following: *NIST SP 800-108* [19] *(KDF in Counter Mode)*[40].

6.1.4.7 FTP_TRP.1

The TOE shall meet the requirement "Trusted path" as specified below.

FTP_TRP.1	**Trusted path**
Hierarchical to:	No other components.

[36] [assignment: *list of multiple authentication mechanisms*]
[37] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]
[38] [assignment: *cryptographic key generation algorithm*]
[39] [assignment: *cryptographic key sizes*]
[40] [assignment: *list of standards*]

Dependencies:	No dependencies.
FTP_TRP.1.1	The TSF shall provide a communication path between itself and *remote*[41] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification and disclosure for authentication data, and only modification for other data.*[42].
FTP_TRP.1.2	The TSF shall permit *remote users*[43] to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for *AES authentication and, depending on settings in the UserConf, integrity protected data transfers.*[44].

6.1.4.8 FCS_CKM.4

The TOE shall meet the requirement "Cryptographic key destruction" as specified below.

FCS_CKM.4	**Cryptographic key destruction**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwriting*[45] that meets the following: *none*[46].

6.1.4.9 FPT_TDC.1

The TOE shall meet the requirement "Inter-TSF basic TSF data consistency" as specified below.

FPT_TDC.1	**Inter-TSF basic TSF data consistency**
Hierarchical to:	No other components.
Dependencies:	No dependencies.

[41] [selection: *remote, local*]
[42] [selection: *modification, disclosure, [assignment: other types of integrity or confidentiality violation]*]
[43] [selection: *the TSF, local users, remote users*]
[44] [selection: *initial user authentication, [assignment: other services for which trusted path is required]*]
[45] [assignment: *cryptographic key destruction method*]
[46] [assignment: *list of standards*]

FPT_TDC.1.1	The TSF shall provide the capability to consistently interpret *regular data, one-time programmable data and monotonic counters*[47] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2	The TSF shall use *the following rules:* • *regular data, i.e. UserData, UserConf, but also the keys DataProtKey, UIDRetrKey, SUNCMACKey, can be written with any value* • *one-time programmable data bits, i.e. LockBits, BlockBits and OTPBits, can only be changed from '0' to '1'* • *monotonic counters, i.e. NFCCounter and AFCCounterX, can only be incremented* [48] when interpreting the TSF data from another trusted IT product.

6.1.5 Additional SFRs regarding robustness

6.1.5.1 FPT_RPL.1

The TOE shall meet the requirement "Replay detection" as specified below.

FPT_RPL.1	**Replay detection**
Hierarchical to:	No other components.
	No dependencies.
FPT_RPL.1.1	The TSF shall detect replay for the following entities: *authentication requests with AES, data integrity verification for data transfers protected with AES*[49].
FPT_RPL.1.2	The TSF shall perform *rejection of the request*[50] when replay is detected.

6.1.5.2 FPR_UNL.1

The TOE shall meet the requirement "Unlinkability" as specified below.

FPR_UNL.1	**Unlinkability**
Hierarchical to:	No other components.

[47] [assignment: *list of TSF data types*]
[48] [assignment: *list of interpretation rules to be applied by the TSF*]
[49] [assignment: *list of identified entities*]
[50] [assignment: *list of specific actions*]

Dependencies: No dependencies.

FPR_UNL.1.1 The TSF shall ensure that *unauthorised subjects other than the card holder*[51] are unable to determine whether *any operation of the TOE*[52] *were caused by the same user*[53].

Application Note: This SFR is only applicable for the following product variant if Random ID is enabled: MF0AES(H)x0.

6.1.6 Additional SFRs regarding Secure Unique NFC Message (SUN)

6.1.6.1 FDP_ETC.3

The TOE shall meet the requirement "Export of user data in unauthenticated state" as specified below.

FDP_ETC.3 Export of user data in unauthenticated state

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_ETC.3.1 The TSF shall export the following pieces of user data: *a configurable subset of UserData*[54] with the following user data's associated security attributes: *authenticity and replay protection for the configurable subset of the UserData*[55].

FDP_ETC.3.2 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambigously associated with the exported user data.

FDP_ETC.3.3 The TSF shall enforce the following rules when user data is exported from the TOE: *unprotected export of UserData in case that SUN is not activated for the UserData*[56].

Application Note: This SFR is only applicable for the following product variants: NT2H2xy1G, NT2H2xy1S.

6.1.7 Additional SFRs regarding Tag Tampering Feature

[51] [assignment: *set of users and/or subjects*]
[52] [assignment: *list of operations*]
[53] [selection: *were caused by the same user, are related as follows[assignment: list of relations]*]
[54] [assignment: *pieces of user data*]
[55] [assignment: *list of security attributes*]
[56] [assignment: *additional exportation control rules*]

6.1.7.1 FAU_STG.2

The TOE shall meet the requirement "Guarantees of audit data availability" as specified below.

FAU_STG.2	**Guarantees of audit data availability**
Hierarchical to:	FAU_STG.1 Protected audit trail storage
Dependencies:	FAU_GEN.1 Audit data generation
FAU_STG.2.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.2.2	The TSF shall be able to *prevent*[57] unauthorised modifications to the stored audit records in the audit trail.
FAU_STG.2.3	The TSF shall ensure that *permanent Tag Tamper status*[58] stored audit records will be maintained when the following conditions occur: *failure and attack*[59].

6.2 Security Assurance Requirements

The following table lists all security assurance components that are valid for this Security Target. These security assurance components are required by EAL3.

Table 19. Security Assurance Requirements

Name	Title
ADV_ARC.1	Security architecture description
ADV_FSP.3	Functional specification with complete summary
ADV_TDS.2	Architectural design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.3	Authorisation controls
ALC_CMS.3	Implementation representation CM coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.1	Identification of security measures
ALC_LCD.1	Developer defined life-cycle model
ASE_CCL.1	Conformance claims
ASE_INT.1	ST introduction
ASE_SPD.1	Security problem definition
ASE_OBJ.2	Security objectives

[57] [selection, choose one of: *prevent, detect*]
[58] [assignment: *metric for saving audit records*]
[59] [selection: *audit storage exhaustion, failure, attack*]

Table 19. Security Assurance Requirements*...continued*

Name	Title
ASE_ECD.1	Extended components definition
ASE_REQ.2	Derived security requirements
ASE_TSS.2	TOE summary specification with architectural design summary
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: basic design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing - sample
AVA_VAN.2	Vulnerability analysis

6.3 Security Requirements Rationale

6.3.1 Rationale for the Security Functional Requirements

Section 6.3.1 in the Protection Profile provides a rationale for the mapping between security functional requirements and security objectives defined in the Protection Profile. This rationale is not repeated here.

This Security Target defines additional SFRs for the TOE. In addition security requirements for the environment are defined. The following table gives an overview, how the requirements are combined to meet the security objectives.

Table 20. Security Functional Requirements mapping to Security Objectives

Name	Title
O.Access-Control	FCS_CKM.4 FDP_ACC.1 FDP_ACF.1 FDP_ITC.2 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1
O.Authentication	FCS_CKM.1 FCS_CKM.4 FCS_COP.1/AES FIA_UID.2 FIA_UAU.2 FIA_UAU.3 FIA_UAU.5 FMT_SMF.1 FPT_RPL.1 FTP_TRP.1

Table 20. Security Functional Requirements mapping to Security Objectives*...continued*

Name	Title
O.MAC	FCS_CKM.1 FCS_CKM.4 FCS_COP.1/AES FPT_RPL.1 FTP_TRP.1 FDP_ETC.3
O.Type-Consistency	FPT_TDC.1
O.No-Trace	FPR_UNL.1
O.Tag-Tamper	FAU_STG.2

Justification related to Access Control (O.Access-Control)

The SFR FMT_SMR.1 defines the roles of the Access Control Policy. The SFR FDP_ACC.1 and FDP_ACF.1 define the rules and FMT_MSA.3 and FMT_MSA.1 the attributes that the access control is based on. FMT_MTD.1 provides the rules for the management of the authentication data. The management functions are defined by FMT_SMF.1. Since the TOE stores data on behalf of the authorised subjects import of user data with security attributes is defined by FDP_ITC.2. Since cryptographic keys are used for authentication (refer to O.Authentication), these keys have to be removed if they are no longer needed for the access control. This is required by FCS_CKM.4. These nine SFR together provide an access control mechanism as required by the objective O.Access-Control.

Justification related to Authentication (O.Authentication)

The SFR FCS_COP.1/AES requires that the TOE provides the basic cryptographic algorithms that can be used to perform the authentication. FCS_CKM.1 generates the cryptographic keys used during the authentication, while FCS_CKM.4 requires that cryptographic keys have to be removed after usage. The SFRs FIA_UID.2, FIA_UAU.2 and FIA_UAU.5 together define that users must be identified and authenticated before any action. The "none" authentication of FIA_UAU.5 also ensures that a specific subject is identified and authenticated before an explicit authentication request is sent to the TOE. FMT_SMF.1 defines security management functions the TSF shall be capable to perform. FTP_TRP.1 requires a trusted communication path between the TOE and remote users, FTP_TRP.1.3 especially requires "authentication requests". Together with FPT_RPL.1 which requires a replay detection for these authentication requests the eight SFR fulfill the objective O.Authentication.

Justification related to Integrity-protected Communication (O.MAC)

The SFR FCS_COP.1/AES requires that the TOE provides the basic cryptographic algorithms that can be used to compute a MAC which can protect the integrity of the communication. FTP_TRP.1 requires a trusted communication path between the TOE and remote users, FTP_TRP.1.3 especially requires "integrity protected data transfers". FCS_CKM.1 generates the cryptographic keys used to protect the integrity, while FCS_CKM.4 requires that cryptographic keys used for MAC operations have to be removed after usage. FPT_RPL.1 requires a replay detection for these data transfers. FDP_ETC.3 requires user data export in unauthenticated state, and hence models the requirements to reach O.MAC.

Justification related to Data type consistency (O.Type-Consistency)

The SFR FPT_TDC.1 requires the TOE to consistently interpret regular data, one-time programmable data and monotonic counters. The TOE will make sure that one-time programmable memory cannot be unset once set, and that monotonic counters cannot be decremented. This meets the objective O.Type-Consistency.

Justification related to Preventing Traceability (O.No-Trace)

The SFR FPR_UNL.1 requires that unauthorised subjects other than the card holder are unable to determine whether any operation of the TOE were caused by the same user. This meets the objective O.No-Trace.

Justification related to Tag tamper detection (O.Tag-Tamper)

The SFR FAU_STG.2 requires the TOE to prevent unauthorised deletion and modifications to the stored tag tamper status. It also requires the TOE to store the audit records in case of failure or attack. This meets the objective O.Tag-Tamper.

6.3.2 Dependencies of Security Functional Requirements

The dependencies listed in the Protection Profile are independent of the additional dependencies listed in the table below. The dependencies of the Protection Profile are fulfilled within the Protection Profile and at least one dependency is considered to be satisfied. The following discussion demonstrates how the SFR dependencies (defined by Part 2 of the Common Criteria [3]) satisfy the requirements specified in Section 6.1.

The dependencies and their fullfilment are listed in the tables below:

Table 21. Dependencies of Security Functional Requirements (Protection Profile)

SFR	Dependency	Fullfilled in ST
FAU_SAS.1	No dependencies.	No dependency
FDP_ITT.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Yes
FDP_IFC.1	FDP_IFF.1 Simple security attributes	See discussion in the PP
FDP_SDC.1	No dependencies.	No dependency
FDP_SDI.2	No dependencies.	No dependency
FMT_LIM.1	FMT_LIM.2 Limited availability.	Yes
FMT_LIM.2	FMT_LIM.1 Limited capabilities.	Yes
FPT_FLS.1	No dependencies.	No dependency
FPT_ITT.1	No dependencies.	No dependency
FPT_PHP.3	No dependencies.	No dependency
FRU_FLT.2	FPT_FLS.1 Failure with preservation of secure state.	Yes

Table 22. Dependencies of Security Functional Requirements (Security Target)

SFR	Dependency	Fullfilled in ST
FIA_SOS.2	No dependencies.	No dependency
FAU_STG.2	FAU_GEN.1 Audit data generation	See discussion below

Table 22. Dependencies of Security Functional Requirements (Security Target)*...continued*

SFR	Dependency	Fullfilled in ST
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	Yes, by FCS_COP.1/AES, FCS_CKM.4.
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Yes, by FDP_ITC.2, FCS_CKM.1.
FCS_COP.1/AES	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Yes, by FDP_ITC.2, FCS_CKM.4.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Yes, by FDP_ACF.1.
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialisation	Yes, by FDP_ACC.1.
FDP_ITC.2	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], FPT_TDC.1 Inter-TSF basic TSF data consistency	Yes, by FDP_ACC.1, FTP_TRP.1, FPT_TDC.1.
FDP_ETC.3	No dependencies	No dependency
FIA_UID.2	No dependencies.	No dependency
FIA_UAU.2	FIA_UID.1 Timing of identification	Yes, by FIA_UID.2.
FIA_UAU.3	No dependencies.	No dependency
FIA_UAU.5	No dependencies.	No dependency
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions	Yes, by FDP_ACC.1, FMT_SMR.1, FMT_SMF.1.
FMT_MSA.3	FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles	Yes, by FMT_MSA.1, FMT_SMR.1.
FMT_MTD.1	FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions	Yes, by FMT_SMR.1, FMT_SMF.1.
FMT_SMF.1	No dependencies.	No dependency
FMT_SMR.1	FIA_UID.1 Timing of identification	Yes, by FIA_UID.2.
FPR_UNL.1	No dependencies.	No dependency
FPT_RPL.1	No dependencies.	No dependency
FPT_TDC.1	No dependencies.	No dependency
FTP_TRP.1	No dependencies.	No dependency

Part 2 of the Common Criteria defines the dependency of FAU_STG.2 (Guarantees of audit data availability) on FAU_GEN.1 (Audit data generation). The specification of FAU_GEN.1 focusses on the list of data that shall be recorded in each audit record together with its time stamp. However, in the perspective of the TOE, FAU_STG.2

aim at just storing the status of the tag tamper wire in the binary format. In contrast, FAU_GEN.1, specified way more detailed logging information like time stamps than required for the target use-case. Therefore, FAU_GEN.1 is not added.

6.3.3 Rationale for the Assurance Requirements

The selection of assurance components is based on the chosen evaluation assurance level. The level EAL3 augmented is chosen in order to meet assurance expectations of access control applications and automatic fare collection systems. The assurance level EAL3 is an elaborated pre-defined level of the CC, Part 3 [4]. The assurance components in an EAL level are chosen in a way that they build a mutually supportive and complete set of components. The augmentation ASE_TSS.2 is chosen to give architectural information on the security functionality of the TOE.

6.3.4 Security Requirements are Internally Consistent

The discussion of security functional requirements and assurance components in the preceding sections has shown that mutual support and consistency are given for both groups of requirements. The arguments given for the fact that the assurance components are adequate for the functionality of the TOE also show that the security functional and assurance requirements support each other and that there are no inconsistencies between these groups.

The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the cryptographic algorithms and the access control function used to implement the Access Control Policy. The security objectives defined in the Protection Profile can be seen as "low-level protection" objectives, while the additional security objectives defined in this Security Target are "high-level protection" objectives.

7 TOE Summary Specification

7.1 Portions of the TOE Security Functionality

The TOE Security Functionality (TSF) directly corresponds to the TOE security functional requirements defined in Section 6. The table below lists the TSF of the TOE.

Table 23. Portions of the TSF

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.

The TSF are described in more detail in the following sections and the relation to the security functional requirements is shown.

7.2 TOE Summary Specification Rationale

7.2.1 Mapping of Security Functional Requirements and TOE Security Functionality

SFR	TSF.Service	TSF.Protection	TSF.Control	TSF.Access-Control	TSF.Authentication	TSF.MAC	TSF.Monotonic-Count	TSF.OTP	TSF.No-Trace	TSF.Tag-Tamper	Description
Security Functional Requirements from the Protection Profile											
FRU_FLT.2			X								Limited fault tolerance
FPT_FLS.1			X								Failure with preservation of secure state
FMT_LIM.1			X								Limited capabilities
FMT_LIM.2			X								Limited availability
FAU_SAS.1	X										Audit storage
FDP_SDC.1		X									Stored data confidentiality
FDP_SDI.2		X									Stored data integrity monitoring and action
FPT_PHP.3		X									Resistance to physical attack
FDP_ITT.1		X									Basic internal transfer protection
FPT_ITT.1		X									Basic internal TSF data transfer protection
FDP_IFC.1		X									Subset information flow control
Security Functional Requirement regarding Random Numbers											
FIA_SOS.2	X				X						Generation of secrets (random numbers)
Security Functional Requirements regarding Access Control											
FDP_ACC.1				X							Subset access control
FDP_ACF.1				X			X	X			Security attribute based access control
FDP_ITC.2				X							Import of user data with security attributes
FMT_MSA.1				X							Management of security attributes
FMT_MSA.3				X							Static attribute initialization
FMT_MTD.1				X							Management of TSF data
FMT_SMF.1				X	X						Specification of Management Functions
FMT_SMR.1				X	X						Security roles
Security Functional Requirements regarding Confidentiality, Authentication and Integrity											
FCS_COP.1/AES					X	X					Cryptographic Operation (AES)
FCS_CKM.1					X						Cryptographic key generation
FCS_CKM.4				X		X					Cryptographic key destruction

SFR	TSF.Service	TSF.Protection	TSF.Control	TSF.Access-Control	TSF.Authentication	TSF.MAC	TSF.Monotonic-Count	TSF.OTP	TSF.No-Trace	TSF.Tag-Tamper	Description
FIA_UAU.2					X						User authentication before any action
FIA_UAU.3					X						Unforgeable authentication
FIA_UAU.5					X						Multiple authentication mechanisms
FIA_UID.2					X						User identification before any action
FPT_TDC.1				X			X	X			Inter-TSF basic TSF data consistency
FTP_TRP.1					X	X					Trusted path
Security Functional Requirements regarding Robustness											
FPR_UNL.1									X		Unlinkability
FPT_RPL.1					X	X					Replay detection
Security Functional Requirements regarding Secure Unique NFC Message (SUN)											
FDP_ETC.3						X					Export of user data in unauthenticated state
Security Functional Requirements regarding Tag Tampering Feature											
FAU_STG.2										X	Guarantees of audit data availability

7.2.2 TSF.Service

TSF.Services implements a test function that allows storing identification and/or pre-personalization data (including a UID for each die) for the TOE in the configuration area stored in EEPROM at the end of the tests in phase 3. This implements FAU_SAS.1

TSF.Service also provides the TOE with a hardware (physical) random number generator (RNG). The generated random numbers are used internally for use during AES authentication and for the Random ID feature. Therefore this functionality meets FIA_SOS.2.

7.2.3 TSF.Protection

TSF.Protection addresses functionalities of the TOE which are used to protect the TSF, TSF data and user data from attacks. Its functionality mainly addresses selfprotection of the TSF. However, TSF.Protection also addresses non-bypassability as it implements logical protection to avoid information leakage. TSF.Protection provides the following functionality:

Protection against physical manipulations

TSF.Protection protects the TOE against physical manipulation. In case a manipulation is detected, a reset is triggered to return to a secure state. Therefore, TSF.Protection implements FPT_PHP.3, FDP_SDC.1 and FDP_SDI.2

TSF.Protection supports all other SFRs because prevention of successful manipulation of security functionality is a pre-condition for the reliable work of all other functions.

Logical protection

TSF.Protection prevents the reconstruction of TOE internal information that can be found by analysis of externally measured signals like the power supply. Within the different components of the TOE dedicated functions are implemented to sufficiently limit or eliminate the information that might be contained in the shape and amplitude of signals or in the time between events.

Logical protections implemented by TSF.Protection covers the SFRs FDP_ITT.1, FPT_ITT.1 and FDP_IFC.1. They cannot be influenced from outside the TOE.

7.2.4 TSF.Control

TSF.Control addresses those aspects the TSF controls, e.g., the operating conditions or access to specific test functionality.

Control of operating conditions

TSF.Control ensures the correct operation of the TOE hardware during the execution of its functionality. For this the TOE comprises sensors which controls the allowed range of temperature, supply voltage and light.

The sensors support the correct function of the TOE within the limits of the operating conditions. This robustness implements FRU_FLT.2 and ensures that the TOE is executing without main failures that may be caused by interference of any external communication interface or other external influences.

FPT_FLS.1 is implemented by sensors. The sensors detect whether one parameter is outside the specified range. The secure state required by FPT_FLS.1 is realized by an internal reset of the TOE. This secure state is applied as long as sensor identifies an abnormal condition.

An internal reset of the TOE is sufficient to ensure a secure state because all internal operations are stopped. However, security mechanisms detecting faults, go beyond this requirement and implement a transition into a Mute mode in case a non-recoverable error is detected. This is also a part of FPT_FLS.1. The protection mechanisms all aim at providing a baseline protection against an attacker with basic attack potential.

Mode control

TSF.Control realizes the control within the TOE testing phases (phase 3 of the life-cycle) and afterwards. In the phases before packaging and TOE delivery, the TOE is operating in its Initialization mode, in which access to initialization and test functionality is available. After the TOE has been tested and initialized, access to the Initialization mode is no longer possible and the TOE will run in User mode only.

The test concept mentioned above ensures that the test functionality is not available in the operational (User) mode of the TOE. Therefore the capabilities to abuse the test functions for compromising User Data or TSF data is very limited as required by FMT_LIM.1. At the end of the test phase, the access to the test functionality is disabled. TSF.Control ensures that it is not possible to switch back and reuse the test functions again. Therefore TSF.Control limits the availability of the test functions as stated by FMT_LIM.2.

7.2.5 TSF.Authentication

The TOE provides an authentication mechanism to separate authorized subjects from unauthorized subjects. The authentication of subjects is performed by a cryptographic challenge response. The TOE supports the cryptographic algorithms 128-bit AES according to FIPS PUB 197 [16] The authentication mechanism is implemented using the cryptographic coprocessor. A hardware random number generator is used to protect the authentication against attacks like e.g. replay. By this TSF.Authentication meets FIA_SOS.2 and FCS_COP.1/AES. At the end of the authentication, a session key for MAC computation is generated, fulfilling FCS_CKM.1. This session key is destroyed after use, fulfilling FCS_CKM.4.

TSF.Authentication identifies the user to be authenticated by the key number indicated in the authentication request. This meets FIA_UID.2. The cryptographic authentication is used for the AuthUser, UIDRetriever, and OrigKeyUser . Since the TOE can be used without authentication the "none" authentication is used to "authenticate" Anybody. Therefore TSF.Authentication implements FIA_UAU.2 and FIA_UAU.5. TSF.Authentication also meets FMT_SMR.1 with the exception that the role "Nobody" which cannot be authenticated, since this role is solely managed by the access control (TSF.Access-Control).

The authentication protocol requires the user to prove knowledge of a secret key by applying it on a freshly generated random challenge, generated to the TOE. This ensures that the authentication request itself cannot be forged or circumvented by attacks like replay or man-in-the-middle, therefore it meets FIA_UAU.3 and the relevant parts of FTP_TRP.1 and FPT_RPL.1 with respect to the authentication requests. The authentication needs not to be performed again as long as none of the following events occur: occurrence of any error during the execution of a command, starting a new authentication, and Reset/Halt of the card. These events will reset the authentication state to the default (Anybody). By this TSF.Authentication implements these parts of FMT_SMF.1.

Remark

The TOE product variants NT2H2x31G, NT2H2x31S i.e. variants supporting password-based authentication, do not offer TSF.Authentication as the password-based mechanism is outside the certification scope.

7.2.6 TSF.Access-Control

TSF.Access-Control provides an access control mechanism to the subject, objects, operations and attributes that are part of the TOE Access Control Policy. The access control mechanism assigns subjects - AuthUser and UIDRetriever - to different groups of operations. The special subjects Anybody and Nobody can also be assigned. Therefore, TSF.Access-Control maintains the roles as required by FMT_SMR.1.

Since TSF.Access-Control does also maintain the objects and security attributes as stated in the TOE Access Control Policy: it implements FDP_ACC.1, FDP_ACF.1 and FMT_MSA.1. For example, it will depend on a UserConf configuration what part of the UserData can be read by Anybody and what part requires an active AuthUser authentication. Management of authentication data as performed by TSF.Access-Control is necessary to separate the roles, therefore it also implements FMT_MTD.1. If keys (DataProtKey, UIDRetrKey or SUNCMACKey) are changed, the old key values are overridden and thereby destroyed. This implements FCS_CKM.4.

The primary use of the TOE is storage of data on behalf of the authorized users. The rules for data storage are defined by the TOE Access Control Policy. The storage of data is an import of data with security attributes, therefore TSF.Access-Control implements FDP_ITC.2. The memory is fully instantiated during the initialization of the product, thereby implementing FMT_MSA.3.

TSF.Access-Control also controls access to the security attributes and keys. Therefore, it implements part of FMT_SMF.1. Finally, TSF.Access-Control ensures the type consistency of the data types stored by the TOE: regular data, one-time programmable (OTP) memory and monotonic counters. By this FPT_TDC.1 is implemented by TSF.Access-Control.

7.2.7 TSF.MAC

TSF.MAC is supported by two features:

- CMAC-based secure messaging, as supported by MF0AES(H)x0
- Secure Unique NFC Message (SUN), as supported by NT2H2xy1G, NT2H2xy1S

For both features, TSF.MAC uses the cryptographic algorithm 128-bit AES CMAC [18]. Therefore it implements FCS_COP.1/AES. The key used during the calculation is destroyed after use, fulfilling FCS_CKM.4.

CMAC-based secure messaging adds data to the communication stream that enables the terminal to detect integrity violations, replay attacks or man-in-the-middle attacks. Vice versa, the TOE verifies the data sent by the terminal and returns an error code if such an attack is detected. The detection mechanism covers all frames exchanged between the terminal and the card under an active authentication. TSF.MAC can also detect if a frame is replayed. By this TSF.MAC implements FPT_RPL.1. The information to detect integrity violations implements FTP_TRP.1 with respect to the "modification for other data".

While using Secure Unique NFC Message, TSF.MAC provides a mechanism for integrity protection for the data to be read, therefore implements FDP_ETC.3.

7.2.8 TSF.Monotonic-Count

The TOE provides one or more monotonic counters depending on the product variant:

- Three AFCCounterX (with X being 0, 1, or 2), as supported by MF0AES(H)x0
- One NFCCounter, as supported by NT2H2xy1G, NT2H2xy1S

TSF.Monotonic-Count ensures that during the operational lifetime of the TOE, these counters can only be incremented. This is enforced by only offering Read and Increment operations. No Decrement or generic Write operations are supported for these data objects. Therefore TSF.Montonic-Count implements the relevant aspects of FDP_ACF.1 and FPT_TDC.1.

7.2.9 TSF.OTP

The TOE provides three types of one-time programmable memory:

- OTPBits: generic one-time progammable user memory.
- LockBits: set to lock other parts of the memory, i.e. prevent any further updating of it.
- BlockBits: set to lock LockBits, i.e. prevent any further updating of those.

TSF.OTP ensures that cetain parts of the memory can only be written once, i.e. once a '1' bit value has been set, this cannot be unset to '0' anymore. This is enforced by only offering a WriteOnce operation. No generic Write operations are supported for these data objects. Therefore TSF.OTP implements the relevant aspects of FDP_ACF.1 and FPT_TDC.1.

7.2.10 TSF.No-Trace

TSF.No-Trace provides an option to use a random UID during ISO14443 anti-collision sequence[22]. By this, the card cannot be traced any more by simply retrieving its UID. This card specific piece of information can be read out only by the UIDRetriever and AuthUser if this option is set. TSF.No-Trace implements FPR_UNL.1 for this card specific information.

Other data is protected by TSF.Access-Control and the tracing protection depends on the access control configuration and data written by the authorised subjects.

Random ID configuration, and thus TSF.No-Trace, is only supported by the MF0AES(H)x0.

7.2.11 TSF.Tag-Tamper

TSF.Tag-Tamper provides a mechanism for detection and permanent storage of the status of the tag tamper wire. After the detection and storage the status byte cannot be deleted or modified. In addition, TSF.Tag-Tamper protects the tag tamper status in case of failure or attack. Hence, TSF.Tag-Tamper implements FAU_STG.2.

Tamper detection, and thus TSF.Tag-Tamper is only supported by the NTAG 22x StatusDetect (i.e. NT2H2xy1S) variant of the TOE.

7.3 Security Architectural Information

Since this ST claims the assurance requirement ASE_TSS.2, security architectural information on a very high level is supposed to be included in the TSS to inform potential customers on how the TOE protects itself against interference, logical tampering and bypassing. In the security architecture context, this covers the aspects self-protection and non-bypassability.

As described in Section 7.2, the aspects self-protection and non-bypassability are implemented by TSF.Protection and TSF.Control.

TSF.Protection covers the physical protection of the TOE and protects the TOE against tampering and bypassing of the TSFs. TSF.Control contributes by covering the aspects failure with preservation of a secure state and limited fault tolerance. This protects the TOE against interference of security features and security services. TSF.Control limits the capability and availability of the Test Features and protects the TOE against bypassing of security features.

The details are already included in the rationale given above.

8 Bibliography

8 . 1 Evaluation documents

[1] A proposal for: Functionality classes for random number generators, Wolfgang Killmann, T-Systems GEI GmbH, Werner Schindler, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.0, 18 September 2011.

[2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, CCMB-2017-04-001, April 2017.

[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, CCMB-2017-04-002, April 2017.

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, CCMB-2017-04-003, April 2017.

[5] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 5, CCMB-2017-04-004, April 2017.

[6] 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.

8 . 2 Developer documents

[7] MF0AES(H)20, MIFARE Ultralight AES - Contactless ticket IC, Objective data sheet, DocStore number 537911, NXP Semiconductors, Revision 1.1, 20 December 2021.

[8] MF0AES(H)30, MIFARE Ultralight AES - Contactless ticket IC, Objective data sheet, DocStore number 703611, NXP Semiconductors, Revision 1.1, 20 December 2021.

[9] MIFARE Ultralight AES, Information on Guidance and Operation, Guidance and operation manual, DocStore number 708612, NXP Semiconductors, Revision 1.2, 18 January 2022.

[10] NT2H2331G0, NTAG 223 DNA - NFC T2T compliant IC, Objective data sheet, DocStore number 598911, NXP Semiconductors, Revision 1.1, 20 December 2021.

[11] NT2H2331S0, NTAG 223 DNA StatusDetect - NFC T2T compliant IC with StatusDetect feature, Objective data sheet, DocStore number 598811, NXP Semiconductors, Revision 1.1, 20 December 2021.

[12] NT2H2421G0, NTAG 224 DNA - NFC T2T compliant IC, Objective data sheet, DocStore number 599111, NXP Semiconductors, Revision 1.1, 20 December 2021.

[13] NT2H2421S0, NTAG 224 DNA StatusDetect - NFC T2T compliant IC with StatusDetect feature, Objective data sheet, DocStore number 599011, NXP Semiconductors, Revision 1.1, 20 December 2021.

[14] NTAG 22x DNA, Information on Guidance and Operation, Guidance and operation manual, DocStore number 708712, NXP Semiconductors, Revision 1.2, 18 January 2022.

[15] NTAG 22x DNA StatusDetect, Information on Guidance and Operation, Guidance and operation manual, DocStore number 708812, NXP Semiconductors, Revision 1.2, 18 January 2022.

8 . 3 Standards

[16] FIPS PUB 197: Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/National Institute of Standards and Technology, 26 November 2001.

[17] NIST SP 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques, Morris Dworkin, National Institute of Standards and Technology, December 2001.

[18] NIST SP 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Morris Dworkin, National Institute of Standards and Technology, May 2005.

[19] NIST SP 800-108, Recommendation for Key Derivation Using Pseudorandom Functions, revised October 2009, National Institute of Standards and Technology.

[20] ISO/IEC FDIS 14443-1, Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 1: Physical characteristics, March 2016.

[21] ISO/IEC FCD 14443-2, Identification cards - Contactless integrated circuit(s) cards Proximity cards - Part 2: Radio frequency power and signal interface, July 2016.

[22] ISO/IEC FDIS 14443-3 Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 3: Initialization and anticollision, September 2016.

9 Legal information

9.1 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.

9.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. 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.

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

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

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

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

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

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.

9.3 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.

MIFARE Ultralight — is a trademark of NXP B.V.

NTAG — is a trademark of NXP B.V.

Tables

Figures

Contents

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

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 18 January 2022