NRV11

Security Target Lite

Rev. 1.0 — 10 September 2024 **Evaluation document**

NSCIB-2300019-01

Document information

Information	Content
Keywords	Common Criteria, Security Target Lite, NRV11
Abstract	Evaluation of the NRV11, developed and provided by NXP Semiconductors, Business Line Secure Connected Edge (SCE), according to the Common Criteria for Information Technology Evaluation Version 3.1 R5 at EAL6 augmented.

Revision History

Rev.	Date	Description
1.0	2024-09-10	First release, based on full Security Target v1.6

1 Introduction

1.1 ST Reference

Table 1. ST Reference

Title	NRV11 Security Target Lite
Revision	1.0
Date	10 September 2024

1.2 TOE Reference

Table 2. TOE Reference

TOE Name	NRV11
IC Hardware	B0
IC Dedicated Software	Firmware: 2.1.11, Crypto Library: 2.4.2
Operating System	2.0.7
Hardware Major/Minor Version	0xA0 0x00
Software Major/Minor Version	0x00 0x01

Note: *The Hardware and Software Major/Minor Version identifiers listed in the table above represent the IC Hardware, IC Dedicated Software and Operating System version. The corresponding byte values can be checked on the TOE by the customer using the "GetVersion" APDU command as described in [8]. The complete certified response from this command is also documented in [8].*

1.3 TOE Overview

NXP has developed the NRV11 to be used with a host MCU through the I2C interface. The NRV11 can also be used with Proximity Coupling Devices (PCDs, also called "terminal") according to ISO 14443 Type A. It fully complies with the requirements for fast and highly secure data transmission, flexible memory organisation and interoperability with existing infrastructure.

The TOE is a smart card IC comprising a hardware platform and a fixed software package. The software package is stored in ROM memory and provides an operating system with a set of functions, used to manage the various kinds of data files stored in Flash memory. The operating system supports a separation between the data of different applications and provides access control if required by the configuration.

The TOE includes also IC Dedicated Software to support its start-up and for test purposes after production. The Smart Card Controller hardware comprises a 32-bit CPU, volatile and non-volatile memories, cryptographic co-processors, security components and two communication interfaces.

The TOE includes a functional specification and a guidance document. This documentation contains a description of the hardware and software interface, the secure configuration and usage of the product by the terminal designer.

The security measures of the TOE are designed to act as an integral part of the combination of hardware platform and software package in order to strengthen the product as a whole. Several security measures are completely implemented in and controlled by the hardware. Other security measures are controlled by the combination of hardware and software.

1.3.1 Required non-TOE Hardware/Software/Firmware

The TOE requires a host MCU to communicate using its I2C interface. Alternatively, when the TOE is configured to be used via its contactless interface, an ISO 14443 card terminal is required to provide the TOE with power and to receive commands.

1.4 TOE Description

1.4.1 Physical Scope of the TOE

The Target of Evaluation (TOE) is the smart card IC named NRV11 in combination with a fixed software package, the IC Dedicated Software. The TOE includes IC manufacturer proprietary IC Dedicated Test Software and IC Dedicated Support Software, according to the terminology used in the Security IC Protection Profile [6]. The TOE deliverables are mentioned in the table below.

Table 3. TOE deliverables

Type	Name	Version	Form of delivery
IC Hardware	NRV11 Hardware	B0	Sawn wafer, WLCSP
IC Dedicated Test Software	Test Software	2.1.11	On-chip software
IC Dedicated Support Software	Boot Software	2.1.11	On-chip software
	Firmware	2.1.11	On-chip software
	Crypto Library	2.4.2	On-chip software
	Operating System	2.0.7	On-chip software
Document	NRV11, Preliminary data sheet [8]	1.4	Electronic document (PDF via NXP DocStore)
Document	NRV11, Wafer and Delivery Specification, Data sheet addendum [10]	1.1	Electronic document (PDF via NXP DocStore)
Document	NRV11, User Guidance Manual [9]	1.4	Electronic document (PDF via NXP DocStore)

1.4.2 Logical Scope of the TOE

1.4.2.1 Hardware Description

The CPU of the NRV11 has an 32-bit architecture. The on-chip hardware components are controlled by the software via Special Function Registers. These registers are correlated to the activities of the CPU, the memory protection unit, interrupt control, contactless communication, Flash, timers, the AES co-processor and the ECC co-processor. The communication with the NRV11 can be performed through the contactless interface or in specific configurations using the I2C interface.

The ECC co-processor supports ECC operations with a key length of 256 bit over the NIST P-256 and brainpoolP256r1 curves. The AES co-processor supports AES operations with a key length of 128 and 256 bit.

A hardware Random Number Generator provides true random numbers which are used to seed deterministic random number generators, used internally by the operating system for security purposes.

1.4.2.2 Software Description

The IC Dedicated Test Software (Test ROM Software) located in ROM of the TOE is used by the TOE Manufacturer to test the functionality of the chip. The test functionality is disabled before the operational use of the smart card. The IC Dedicated Test Software includes the test operating system, test routines for the various blocks of the circuitry and shutdown functions to ensure that security relevant test operations cannot be executed illegally after phase 3 of the TOE Life cycle.

The TOE also contains IC Dedicated Support Software. The Boot Software which is stored in ROM is part of the IC Dedicated Support Software. This software is executed after each reset of the TOE, i.e. every time when the TOE starts. It sets up the TOE and does some basic configuration. The operating system is also part of the IC Dedicated Software and provides the main functionality of the TOE in the usage phase. The NRV11 is primarily designed for secure contactless transport applications and related loyalty programs as well as access control systems. It fully complies with the requirements for fast and highly secure data transmission, flexible memory organization and interoperability with existing infrastructure. Its functionality consists of:

- Pre-personalized file system with one active application.
- Support for data files and monotonic-counter files.
- ECC-based Card-Unilateral Authentication and generic ECDSA support.
- AES-based Mutual Authentication and Secure Messaging (EV2 Secure Messaging) by default as target, but with optional support for controller command generation and response processing.
- ECC-based mutual authentication through SIGMA-I protocol.
- Two Authority Watchdog Timers, providing the capability to specifiy an expiration time for authentication attempts and/or authentication session duration.
- Authentication on application level with fine-grained access conditions for files.
- Data encryption on the communication path.
- Message Authentication Codes (MAC) for replay attack protection.
- Flexible key management (for symmetric and asymmetric keys).
- ECC keypair generation.
- Unique serial number for each device (UID) with optional random UID.
- ECC-based originality functionality that allows verifying the authenticity of the TOE.
- Secure Dynamic Messaging feature which allows confidential (via AES-based encryption) and integrity protected data (via AES-based CMAC or ECDSA signature) exchange without requiring a preceding authentication.
- Crypto API providing AES, ECDSA, ECDH, SHA, HMAC, and HKDF cryptographic functionality to users.
- Tag-tamper detection.

Asymmetric cryptography features support 256-bit ECC over the NIST P-256 and brainpoolP256r1 curves. Symmetric cryptography features support both AES-128 and AES-256.

With regards to mutual authentication through the SIGMA-I protocol, The TOE implements both Initiator and Responder roles. It can be configured what role to support depending on the use case, protecting the Initiator identity by the protocol design. For the subsequent secure messaging, by default the TOE will act as a target, i.e. processing the provided command and generating a response. Optionally also support for controller can be enabled. This allows to use the TOE to support the command generation towards another TOE (i.e. by applying the secure messaging), and processing the responses (i.e. validating and decrypting the secure messaging).

If privacy is an issue, the TOE can be configured not to disclose any privacy-related information to unauthorized users.

1.4.2.3 Documentation

The data sheet [8] contains a functional description of the communication protocol and the commands implemented by the TOE. The provided documentation can be used by a customer to develop applications using the TOE.

The data sheet is supported by a user guidance manual [9] which gives additional guidance with regards to the secure usage of the TOE.

The Delivery specification data sheet addendum [10] gives additional information regarding the wafer dimensions, TOE identification and delivery processes.

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 NRV11 chip will be embedded on a PCB to communicate with a host MCU, or 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.

Regarding the Application Note 1 of the Protection Profile [6], 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 combined with the embedded software 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 file system content relying on the operational security features of the TOE.

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 software is disabled. Subsequent start-ups of the chip will always enter the user operating mode with the CPU executing the TOE operating system software. The TOE will stay in the user operating mode until the end of its life-time.

The TOE is being locked to the user operating mode before TOE delivery at the end of Phase 6.

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.

The TOE is developed for high-end safeguarded applications, and is designed for embedding in a device with an host MCU communicating with the TOE over I2C. Alternatively, the TOE may communicate using its contactless ISO 14443 interface. Usually the device is assigned to a single individual only and may be used for multiple applications in a multi-provider environment. The secret data shall be used as input for the calculation of authentication data, encryption and integrity protection of data for communication.

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 secure authentication of IoT platforms, electronic accessories, and consumer devices. 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 and do not have any additional functionality used for testing.

1.4.5 Interface of the TOE

The TOE can be connected to a host MCU via the pads dedicated for I2C communication. The functional interface is defined by the commands implemented by the TOE and described in the product data sheet.

Alternatively, 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.

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 Protection Profile Claim

This Security Target claims strict conformance to the following Protection Profile:

- 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 [6].

2.3 Package Claim

This Security Target claims conformance to the assurance package EAL6 augmented with ASE_TSS.2.

2.4 Conformance Claim Rationale

As the Protection Profile [6] requires strict conformance, no conformance claim requirement is needed in this Security Target.

3 Security Problem Definition

This section lists the assets, threats, organisational security policies and assumptions from the Protection Profile [6] and describes extensions to these elements in detail.

3.1 Description of Assets

The assets to be protected (related to standard functionality) are described in Section 3.1 of the Protection Profile [6] and are listed below:

- The user data of the Composite TOE.
- The Security IC Embedded Software, stored and in operation.
- The security services provided by the TOE for the Security IC Embedded Software.

These assets are related to the following high-level security concerns:

- Integrity of user data of the Composite TOE.
- Confidentiality of user data of the Composite TOE being stored in the TOE's protected memory areas.
- Correct operation of the security services provided by the TOE for the Security IC Embedded Software.
- 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, IC Dedicated Software, and configuration data.
- Initialisation Data and Pre-personalisation Data, specific development aids, test and characterisation related data, material for software development support, and photomasks.

For details see Section 3.1 of the Protection Profile [6].

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 4.

Table 4. 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 3.1 of the Protection Profile [6].

The following additional threats are defined in this Security Target:

Table 5. 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 6.

Table 6. Organisational security policies defined in the Protection Profile (PP-0084)

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

For details see Section 3.3 of the Protection Profile [6].

This Security Target defines additional organisational security policies as detailed in the following.

The TOE provides specific security functionality which can used by the operating system. In the following, specific security functionality is listed which is not derived from threats identified for the TOE's environment because it can only be decided in the context of the application against which threats the TOE will use the specific security functionality.

The IC Developer / Manufacturer therefore applies the following policies as specified below.

Table 7. Additional organisational security policies defined in this Security Target

Name	Title
P.Encryption	Confidentiality during communication
P.Integrity	Authenticated integrity during communication
P.Crypto-Service	Cryptographic functionality
P.No-Trace	Untraceability of end-users
P.Tag-Tamper	Tag tamper detection

P.Encryption	**Confidentiality during communication** The TOE shall provide the possibility to protect selected data elements from eavesdropping during contactless communication.
P.Integrity	**Authenticated 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.Crypto-Service	**Cryptographic functionality** The TOE shall provide an API to allow users to use AES, ECDSA, ECDH, SHA, HMAC, and HKDF cryptographic functionality.
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

All assumptions defined in the Protection Profile are valid for this Security Target and are listed in Table 8.

Table 8. Assumptions defined in the Protection Profile (PP-0084)

Name	Title
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation
A.Resp-Appl	Treatment of user data of the Composite TOE

For details see Section 3.4 of the Protection Profile [6].

In compliance with Application Notes 6 and 7 in the Protection Profile [6], this Security Target defines two additional assumptions as follows:

Table 9. 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. Additionally, asymmetric keys may also be generated on the TOE, only exporting the public key. It is assumed that related public keys are properly registered within the system, e.g. by complementing them with a certificate.

A.Terminal-Support	**Terminal Support** The terminal verifies information sent by the TOE in order to ensure integrity and confidentiality of the communication. In case of asymmetric authentication, this may include the verification of a certificate provided by the TOE or via other mechanisms. Furthermore the terminal shall provide random numbers and/or ephemeral ECC keys according to AIS20/31 for the authentication.

The additional assumptions as defined above are required for the correct functioning of the operating system's security functionality. As the Protection Profile [6] does not cover this kind of functionality, the additional assumptions neither mitigate a threat (or a part of a threat) meant to be addressed by security objectives for the TOE in the Protection Profile [6], nor fulfil an OSP (or part of an OSP) meant to be addressed by security objectives for the TOE in the Protection Profile [6].

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 10.

Table 10. 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

Regarding the Application Notes 8 and 9 in the Protection Profile [6], additional security objectives that are based on additional functionality provided by the TOE are defined below:

Table 11. Additional security objectives defined in this Security Target

Name	Title
O.Access-Control	Access Control
O.Authentication	Authentication
O.Encryption	Confidential Communication
O.Integrity	Integrity-Protected Communication
O.Crypto-Service	Cryptographic functionality
O.No-Trace	Preventing Traceability
O.Tag-Tamper	Tag tamper detection
O.Type-Consistency	Data Type Consistency

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.Encryption	**Confidential Communication** The TOE must be able to protect the communication by encryption. This shall be implemented by security attributes that enforce encrypted communication for the respective data elements.
O.Integrity	**Integrity-Protected Communication** The TOE must be able to protect the communication by adding a MAC or signature, ensuring integrity and authentication of the transferred data. 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.Crypto-Service	**Cryptographic functionality** The TOE must be able to provide an API interface to users to perform AES, ECDSA, ECDH, SHA, HMAC, and HKDF cryptographic operations.
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.Tag-Tamper	**Tag tamper detection** The TOE must be able to detect and permanently record tampering status on the tag tamper wire.
O.Type-Consistency	**Data Type Consistency** The TOE must provide a consistent handling of the different supported data types. This comprises over- and underflow checking for values, for data file sizes and record handling.

4.2 Security Objectives for the Security IC Embedded Software

All security objectives for the Security IC Embedded Software which are defined in section 4.2 of the Protection Profile are applied to this Security Target and are listed in Table 12.

Table 12. Security Objectives for the Security IC Embedded Software (PP-0084)

Name	Title
OE.Resp-Appl	Treatment of User Data

4.3 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 13.

Table 13. 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 14. 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 keys may comprise symmetric keys, asymmetric TOE key pairs from which the ECC Private Key is stored on the TOE, and asymmetric key pairs protecting the access to the TOE, i.e. the key pair from which the CA Root Public Key is stored on the TOE, but also the further key pairs that are certified by the CA. These values are generated outside the TOE and are downloaded to the TOE during the personalisation or usage in phase 5 to 7. Asymmetric TOE key pairs can also be generated by the TOE. In this case the environment shall protect the registration of public keys in the system, e.g. by providing the TOE with a certificate. The environment shall ensure that the generated secure values are kept confidential.

The TOE provides specific functionality to verify the success of the application download process. Therefore, OE.Terminal-Support is defined to allow triggering the verification process.

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 and confidentiality of the communication. This may involve the checking of MAC values, signatures and certificates sent by the TOE, and secure closing of the communication session. Furthermore the terminal shall provide random numbers and/or ephemeral ECC keys according to AIS20/31 [1] for the authentication.

The additional security objectives for the operational environment as defined above are required for the correct functioning of the TOE's security functionality. As the Protection Profile [6] does not cover this kind of functionality, the additional objectives neither mitigate a threat (or a part of a threat) meant to be addressed by security objectives for the TOE in the Protection Profile [6], nor fulfil an OSP (or part of an OSP) meant to be addressed by security objectives for the TOE in the Protection Profile [6].

4.4 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. All these items are in line with those in the Protection Profile [6].

Table 15. Security Problem Definition mapping to Security Objective

Security Problem Definition	Security Objective
T.Data-Modification	O.Access-Control O.Type-Consistency
T.Impersonate	O.Authentication
T.Cloning	O.Access-Control O.Authentication
P.Encryption	O.Encryption
P.Integrity	O.Integrity
P.Crypto-Service	O.Crypto-Service
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.

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.Encryption:

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

Justification related to P.Integrity:

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

Justification related to P.Crypto-Service:

Security Objective	Rationale
O.Crypto-Service	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.

The justification of the additional policies and the additional assumptions show that they do not contradict the rationale already given in the Protection Profile [6] for the assumptions, policy and threats defined there.

5 Extended Components Definition

This Security Target defines two additional extended components which are described in the following sections.

Note that the Protection Profile [6] defines extended security functional requirements FCS_RNG.1, FMT_LIM.1, FMT_LIM.2, FAU_SAS.1 and FDP_SDC.1 in chapter 5, which are used in this Security Target but their definitions are not duplicated in this section.

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

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

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.

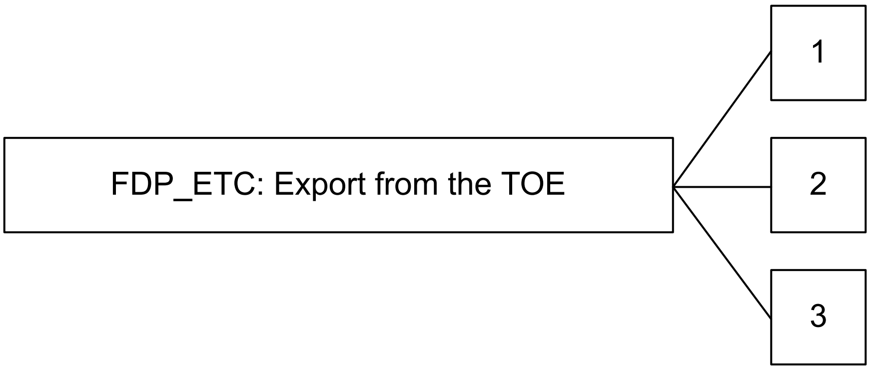

Figure 1. Component levelling of Extended Component FDP_ETC

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 Dynamic Messaging feature provided by the TOE, which allows for the encrypted and 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.

5.2 Authentication Proof of Identity (FIA_API.1)

To define the Transaction Signature functionality of the TOE, an additional family (FIA_API) of the class FIA (Identification and authentication) is taken from Protection Profile PP-0056 [7] and its definition is repeated below. The class behaviour of FIA is defined in CC Part 2 [3].

The family FIA_API describes the functional requirements for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

Family behaviour:

This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.

Component leveling:

Figure 2. Component levelling of Extended Component FIA_API

FIA_API	Authentication Proof of Identity
Management:	FIA_API.1

	The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.
Audit:	FIA_API.1
	There are no actions defined to be auditable.
FIA_API.1	**Authentication Proof of Identity**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	**The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user or role*].**

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 Security Functional Requirements from the Protection Profile

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 FCS_RNG.1/PTG2

The TOE shall meet the requirement "Random number generation (Class PTG.2)" as defined in the PP [6] according to [1] , and as specified below.

FCS_RNG.1/PTG2	**Random number generation (Class PTG.2)**
Hierarchical to:	No other components.

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

Dependencies:	No dependencies.
FCS_RNG.1.1/PTG2	The TSF shall provide a *physical*[3] random number generator that implements:[4]
	(PTG.2.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.
	(PTG.2.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG *prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source*[5].
	(PTG.2.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.
	(PTG.2.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.
	(PTG.2.5) The online test procedure checks the quality of the raw random number sequence. It is triggered *at regular intervals or continuously*[6]. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.
FCS_RNG.1.2/PTG2	The TSF shall provide *octets of bits*[7] that meet:
	(PTG.2.6) Test procedure A[8] does not distinguish the internal random numbers from output sequences of an ideal RNG.
	(PTG.2.7) The average Shannon entropy per internal random bit exceeds 0.997.

6.1.1.3 FCS_RNG.1/DRG4

The TOE shall meet the requirement "Random number generation (Class DRG.4)" as defined in the PP [6] according to [1] , and as specified below.

FCS_RNG.1/DRG4 **Random number generation (Class DRG.4)**

3 [selection: *physical, hybrid physical, hybrid deterministic*]
4 [assignment: *list of security capabilities*]
5 [selection: *prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source, generates the internal random numbers with a post-processing algorithm of class DRG.2 as long as its internal state entropy guarantees the claimed output entropy*]
6 [selection: *externally, at regular intervals, continuously, applied upon specified internal events*]
7 [selection: *bits, octets of bits, numbers [assignment: format of the numbers]*]
8 [assignment: *additional standard test suites*]. Assignment is empty as per Application Note 44 of the PP.

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RNG.1.1/DRG4	The TSF shall provide a *hybrid deterministic*[9] random number generator that implements:[10] (DRG.4.1)The internal state of the RNG shall *use PTRNG of class PTG.2 as random source*[11]. (DRG.4.2) The RNG provides forward secrecy. (DRG.4.3) The RNG provides backward secrecy even if the current internal state is known. (DRG.4.4) The RNG provides enhanced forward secrecy *on demand*[12]. (DRG.4.5) The internal state of the RNG is seeded by an *PTRNG of class PTG.2*[13].
FCS_RNG.1.2/DRG4	The TSF shall provide random numbers that meet: (DRG.4.6) The RNG generates output for which 2^{48} strings[14] of bit length 128 are mutually different with probability *of at least* $1 - 2^{-24}$[15]. (DRG.4.7) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A *and no additional test suites*[16].

6.1.1.4 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.

9 [selection: *physical, hybrid physical, hybrid deterministic*]
10 [assignment: *list of security capabilities*]
11 [selection: *use PTRNG of class PTG.2 as random source, have [assignment: work factor], require [assignment: guess work]*]
12 [selection: *on demand, on condition [assignment: condition], after [assignment: time]*]
13 [selection: *internal entropy source, PTRNG of class PTG.2, PTRNG of class PTG.3, [other selection]*]
14 [assignment: *number of strings*]
15 [assignment: *probability*]
16 [assignment: additional test suites]

FDP_SDC.1.1	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the *RAM and non-volatile memory*[17].

6.1.1.5 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.
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*[18] on all objects, based on the following attributes: *integrity check information associated with the data stored in memories*[19].
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall *perform an error correction if possible or trigger a security reset if not*[20].

6.1.2 Security Functional Requirements regarding Access Control

6.1.2.1 TOE Access Control Policy

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

Subject	AppMgr	Application Manager
Info	The AppMgr is the subject that owns or has access to an AppMasterKey, or has equivalent access rights granted by an AppCA. Note that the TOE supports only a single Application. Within that Application the role can be issued to multiple instances, e.g. through certificates associated with different hosts.	
Info	The AppMgr is the subject that owns or delegates the right to change the AppCARootKeys and their related access rights	

Subject	AppUser	Application User
Info	The AppUser is the subject that owns or has access to an AppKey, or has one or more equivalent access rights granted by an AppCA.	
Info	Note that the TOE supports multiple AppUser within each Application and the assigned rights to the AppUser can be different, which allows to have more or less powerful AppUser.	

17 [assignment: *memory area*]
18 [assignment: *integrity errors*]
19 [assignment: *user data attributes*]
20 [assignment: *action to be taken*]

Subject	AppCA	Application CA
Info	The AppCA is the subject knows the private key related to an AppCARootKey, and therefore can issue certificates holding (a subset of) the access rights related to that AppCARootKey.	
Info	Note that this subject cannot directly authenticate against the TOE, but rather can grant the possiblity to authentication to other subjects via issuing certificates.	

Subject	CryptoChangeUser	CryptoRequest Key Change User
Info	The CryptoChangeUser is the subject that owns or has access to the AppKey required to change CryptoRequest Keys, or has equivalent access rights granted by an AppCA.	

Subject	CryptoUser	CryptoRequest Key User
Info	The CryptoUser is the subject that owns or has access to the AppKey required to issue Crypto Request commands, or has equivalent access rights granted by an AppCA.	

Subject	Anybody	Anybody
Info	Any subject that does not belong to one of the roles AppMgr, AppUser, CryptoChangeUser or Crypto User belongs to the role Anybody. This role includes the device owner (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 explicitly excluded from the role Anybody.	
Info	Additionally, in product configurations with dual interface (I2C and NFC) certain access rights can be granted to Anybody but restricted to one of the interfaces. If only free access over I2C is configured, it means the access right is granted to Anybody over the I2C interface, but not over the NFC interface. If only free access of NFC configured, Anybody can access over NFC but not over I2C.	

Subject	Nobody	Nobody
Info	Any subject that does not belong to one of the roles AppMgr, AppUser, CryptoChangeUser, Crypto User 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	Application	Application
Info	The TOE holds one Application which stores a number of Files.	
Operation	Modify	Modify attribute of an Application.
Operation	Freeze	Freeze attribute of an Application.
Operation	Select	Select an Application.
Attribute	ECCKeyManagement	ECC key management access conditions.
Attribute	CertificateManagement	Certificiate management access conditions.
Attribute	CryptoAPIManagement	Crypto API management access conditions.

Object	File	File
Info	An Application can store a number of Files of different types.	
Operation	Create	Create a File.
Operation	Freeze	Freeze attributes of a File.
Operation	Read	Read operations accessing the content of a File.
Operation	Write	Write operations accessing the content of a File.
Operation	Change	Change operation to change the attribute File.AccessRights.
Attribute	AccessRights	Generic access rights for a File.

Object	CounterFile	Counter File
Info	The Counter File is a specific File type that holds a 4-byte monotonic counter.	
Operation	Create	Create a CounterFile.
Operation	Freeze	Freeze attributes of CounterFile.
Operation	Read	Read the CounterFile.
Operation	Increment	Increment the CounterFile.
Operation	Change	Change operation to change the attribute Counter File.AccessRights.
Attribute	AccessRights	Generic access rights for CounterFile.

Object	AppCertRepo	Application Certificate Repository
Info	An Application can store one or more certificate repositories holding the certificate or certificate chain to authenticate the device.	
Operation	Create	Create a AppCertRepo.
Operation	Read	Read operations accessing the content of a AppCertRepo.
Operation	Write	Write operations accessing the content of a AppCertRepo, including activation and reset of the repository.

Object	AppMasterKey	Application Master Key
Info	The Application Master Key.	
Operation	Change	Change the AppMasterKey.
Operation	Freeze	Freeze the AppMasterKey.

Object	AppKey	Application Key
Info	Application Key that can be used for authentication.	
Operation	Change	Change the AppKey.

Object	CryptoRequestKey	Crypto Request Key
Info	Application Key that can only be used for generic cryptographic operations, but not for authenticaton.	
Operation	Change	Change the CryptoRequestKey.
Operation	Use	Use the CryptoRequestKey.

Object	AppCARootKey	Application CA Root Key
Info	CA Root Key at Application level	
Operation	Create	Create the AppCARootKey and its related attributes.
Operation	Change	Change the AppCARootKey and its related attributes.
Attribute	AccessRights	Access rights granted to this AppCARootKey
Attribute	WriteAccess	Access condition for AppCARootKey.Change.

Object	AppECCPrivateKey	Application ECC Private Key
Info	ECC Private Key at Application level	
Operation	Change	Change the AppECCPrivateKey and/or its related attributes.
Attribute	KeyPolicy	Key policy defining the operations allowed with this App ECCPrivateKey.
Attribute	WriteAccess	Access condition for AppECCPrivateKey.Change.

Note that subjects are authorized by cryptographic keys and certificates. These keys are considered as authentication data and not as security attributes of the subjects. There is one Application available at a time. The Application has 5 AppKeys (from which the one with KeyNo 0x0 is the AppMasterKey) and up to 5 AppCARootKeys. These keys are used to authorise operations on Files. For the AppCARootKeys, this is done indirectly by issuing one or more certificates. Keys are persistent and stored in the non-volatile memory.

6.1.2.2 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*[21] on *all subjects, objects, operations and attributes defined by the TOE Access Control Policy*[22].

21 [assignment: *access control SFP*]
22 [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

6.1.2.3 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*[23] to objects based on the following: *all subjects, objects and attributes*[24].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:[25] 1. *The AppMgr is allowed to perform File.Create.* 2. *The AppMgr is allowed to perform CounterFile.Create.*
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:[26] 1. *The AppMgr or AppUser is allowed to perform File.Read or File.Write or File.Change on a File if the File.AccessRights grant these rights.* 2. *The AppMgr or AppUser is allowed to perform CounterFile.Read or CounterFile.Increment or CounterFile.Change on a CounterFile if the CounterFile.AccessRights grant these rights.* 3. *The AppMgr or CryptoUser is allowed to perform CryptoRequestKey.Use if the Application.CryptoAPIManagement grant this right.* 4. *The Anybody is allowed to perform File.Read or File.Write or File.Change if the File.AccessRights grant these rights.* 5. *The Anybody is allowed to perform CounterFile.Read or CounterFile.Increment or CounterFile.Change on a CounterFile if the CounterFile.AccessRights grant these rights.* 6. *The Anybody is allowed to perform CryptoRequestKey.Use if the Application.CryptoAPIManagement grant this right.* 7. *The AppMgr or AppUser is allowed to perform AppCertRepo.Create if Application.CertificateManagement grants this right. In the default configuration, this is granted to the Admin.* 8. *The Anybody is allowed to perform AppCertRepo.Create if Application.CertificateManagement grants this right.* 9. *The AppMgr or AppUser is allowed to perform AppCertRepo.Read or AppCertRepo.Change if respectively AppCertRepo.ReadAccess or AppCertRepo.WriteAccess grants this right.*

23 [assignment: *access control SFP*]
24 [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*]
25 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
26 [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

	10. *The Anybody is allowed to perform AppCertRepo.Read or AppCertRepo.Change if respectively AppCertRepo.ReadAccess or AppCertRepo.WriteAccess grants this right.*
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules:[27] 1. *No one but Nobody is allowed to perform File.Read or File.Write or File.Change if the File.AccessRights do not grant this right.* 2. *No one but Nobody is allowed to perform CounterFile.Read or CounterFile.Increment or CounterFile.Change if the CounterFile.AccessRights do not grant this right.* 3. *No one but Nobody is allowed to perform CryptoRequestKey.Use if the Application.CryptoAPIManagement do not grant this right.*

6.1.2.4 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].

6.1.2.5 FMT_MSA.1

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

FMT_MSA.1	**Management of security attributes**

27 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
28 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
29 [assignment: *additional importation control rules*]

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
FMT_MSA.1.1	The TSF shall enforce the *TOE Access Control Policy*[30] to restrict the ability to *change or freeze*[31] the security attributes *the security attribute File.AccessRights*[32] to *AppMgr or AppUser respectively*[33].
Refinement:	The detailed management abilities are: 1. *Only the AppMgr is allowed to perform Application.Modify or Application.Freeze on Application.ECCKeyManagement, Application.CertificateManagement and Application.CryptoAPIManagement.* 2. *The AppMgr or AppUser with Change access rights is allowed to perform File.Change and File.Freeze on File.AccessRights at Application level.*

6.1.2.6 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*[34] to provide *permissive*[35] 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*[36] to specify alternative initial values to override the default values when an object or information is created.
Application Note:	The file 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.

6.1.2.7 FMT_MTD.1

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

30 [assignment: *access control SFP(s), information flow control SFP(s)*]
31 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
32 [assignment: *list of security attributes*]
33 [assignment: *the authorised identified roles*]
34 [assignment: *access control SFP, information flow control SFP*]
35 [selection, choose one of: *restrictive, permissive, [assignment: other property]*]
36 [assignment: *the authorised identified roles*]

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 *perform*[37] the *Create and Change operations for Keys*[38] to *specific roles depending on the targeted Key and certain attributes.*[39].
Refinement:	The detailed management abilities are: 1. *The AppMgr is allowed to perform AppMasterKey.Change.* 2. *The AppMgr is allowed to perform AppKey.Change.* 3. *The Admin or CryptoChangeUser is allowed to perform CryptoRequestKey.Change if Application.CryptoAPIManagement grants this right.* 4. *The Anybody is allowed to perform CryptoRequestKey.Change if Application.CryptoAPIManagement grants this right.*

6.1.2.8 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.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions:[40] • *Authenticate a user.* • *Invalidating the current authentication state based on the functions: Selecting and reselecting an application or the card, Changing the key corresponding to the current authentication, Occurence of any error during the execution of a command, Starting a new authentication and Reset.* • *Changing a security attribute.* • *Performing File.Create or CounterFile.Create.*

6.1.2.9 FMT_SMR.1

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

FMT_SMR.1	**Security roles**

37 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
38 [assignment: *list of TSF data*]
39 [assignment: *the authorised identified roles*]
40 [assignment: *list of management functions to be provided by the TSF*]

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles *AppMgr, AppUser, CryptoChangeUser, CryptoUser and Anybody*[41].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.1.2.10 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, but regarded as Anybody by the TOE. This means that the TOE cannot determine if it is used by its intended end-user.
- AppMgr has to authenticate with the AppMasterKey to change the AppMasterKey and AppKeys.
- The TOE does not offer any functionality to read out symmetric keys or asymmetric private keys.

6.1.3 Security Functional Requirements regarding Confidentiality, Authentication and Integrity

6.1.3.1 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 and cipher based MAC for authentication and communication*[42] in accordance with the specified cryptographic algorithm *Advanced Encryption Standard AES in one of the following modes of operation: CBC, CMAC, CCM, GCM*[43] and cryptographic key sizes *128 bits and 256 bits*[44] that meet the following:[45] • *FIPS PUB 197 [13] (AES)* • *NIST SP 800-38A [15] (CBC mode)* • *NIST SP 800-38B [16] (CMAC mode)* • *NIST SP 800-38C [17] (CCM)* • *NIST SP 800-38D [18] (GCM)*

41 [assignment: *the authorised identified roles*]
42 [assignment: *list of cryptographic operations*]
43 [assignment: *cryptographic algorithm*]
44 [assignment: *cryptographic key sizes*]
45 [assignment: *list of standards*]

6.1.3.2 FCS_COP.1/ECDSA

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

FCS_COP.1/ECDSA	**Cryptographic Operation (ECDSA)**
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/ECDSA	The TSF shall perform *signature generation and verification*[46] in accordance with the specified cryptographic algorithm *ECDSA / ECC over GF(p) (i.e. NIST P-256 or brainpoolP256r1)*[47] and cryptographic key sizes *256 bits*[48] that meet the following:[49] *FIPS PUB 186-5 [12]*.

6.1.3.3 FCS_COP.1/ECDH

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

FCS_COP.1/ECDH	**Cryptographic Operation (ECDH)**
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/ECDH	The TSF shall perform *Diffie-Hellman Key Exchange*[50] in accordance with the specified cryptographic algorithm *ECDH / ECC over GF(p) (i.e. NIST P-256 or brainpoolP256r1)*[51] and cryptographic key sizes *256 bits*[52] that meet the following:[53] *NIST SP800-56A [19]*.

6.1.3.4 FCS_COP.1/SHA

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

FCS_COP.1/SHA	**Cryptographic Operation (SHA)**
Hierarchical to:	No other components.

46 [assignment: *list of cryptographic operations*]
47 [assignment: *cryptographic algorithm*]
48 [assignment: *cryptographic key sizes*]
49 [assignment: *list of standards*]
50 [assignment: *list of cryptographic operations*]
51 [assignment: *cryptographic algorithm*]
52 [assignment: *cryptographic key sizes*]
53 [assignment: *list of standards*]

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/SHA	The TSF shall perform *hashing*[54] in accordance with the specified cryptographic algorithm *SHA-256, SHA-384*[55] and cryptographic key sizes *none*[56] that meet the following:[57] *FIPS 180-4 [11]*.

6.1.3.5 FCS_COP.1/HMAC

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

FCS_COP.1/HMAC	**Cryptographic Operation (HMAC)**
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/HMAC	The TSF shall perform *hash-based message authentication code calculation*[58] in accordance with the specified cryptographic algorithm *HMAC-SHA256 and HMAC-SHA384*[59] and cryptographic key sizes *up to 224 byte*[60] that meet the following:[61] *FIPS 198-1 [14]*.

6.1.3.6 FCS_COP.1/HKDF

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

FCS_COP.1/HKDF	**Cryptographic Operation (HKDF)**
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

54 [assignment: *list of cryptographic operations*]
55 [assignment: *cryptographic algorithm*]
56 [assignment: *cryptographic key sizes*]
57 [assignment: *list of standards*]
58 [assignment: *list of cryptographic operations*]
59 [assignment: *cryptographic algorithm*]
60 [assignment: *cryptographic key sizes*]
61 [assignment: *list of standards*]

FCS_COP.1.1/HKDF	The TSF shall perform *HMAC-based Extract-and-Expand Key Derivation Function*[62] in accordance with the specified cryptographic algorithm *HKDF*[63] and cryptographic key sizes *up to 224 byte*[64] that meet the following:[65] *RFC 5869 [20]*.

6.1.3.7 FCS_CKM.1/Session_AES

The TOE shall meet the requirement "Cryptographic key generation (Session AES)" as specified below.

FCS_CKM.1/ Session_AES	**Cryptographic key generation (Session AES)**
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/ Session_AES	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *AES-based Symmetric Authentication Session Key Generation*[66]and specified cryptographic key sizes *128 bits and 256 bits*[67]that meets the following: *NRV11 refarch section 3.6.4 [8]*[68].

6.1.3.8 FCS_CKM.1/Session_SIGMA

The TOE shall meet the requirement "Cryptographic key generation (Session SIGMA)" as specified below.

FCS_CKM.1/ Session_SIGMA	**Cryptographic key generation (Session SIGMA)**
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/ Session_SIGMA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *SIGMA-I Authentication Session Key Generation*[69]and specified cryptographic key sizes *128 bits or 256 bits*[70]that meets the following: *DA OS req section 4.7.2.5*[71].

62 [assignment: *list of cryptographic operations*]
63 [assignment: *cryptographic algorithm*]
64 [assignment: *cryptographic key sizes*]
65 [assignment: *list of standards*]
66 [assignment: *cryptographic key generation algorithm*]
67 [assignment: *cryptographic key sizes*]
68 [assignment: *list of standards*]
69 [assignment: *cryptographic key generation algorithm*]
70 [assignment: *cryptographic key sizes*]
71 [assignment: *list of standards*]

6.1.3.9 FCS_CKM.1/ECC

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

FCS_CKM.1/ECC	**Cryptographic key generation (ECC)**
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/ECC	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDSA (ECC over GF(p))*[72]and specified cryptographic key sizes *256 bits*[73]that meets the following: *FIPS PUB 186-5 [12]*[74].

6.1.3.10 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*[75] that meets the following: *none*[76].

6.1.3.11 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.

72 [assignment: *cryptographic key generation algorithm*]
73 [assignment: *cryptographic key sizes*]
74 [assignment: *list of standards*]
75 [assignment: *cryptographic key destruction method*]
76 [assignment: *list of standards*]

6.1.3.12 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*[77] use of authentication data that has been forged by any user of the TSF.
FIA_UAU.3.2	The TSF shall *detect and prevent*[78] use of authentication data that has been copied from any other user of the TSF.

6.1.3.13 FIA_UAU.5

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

FIA_UAU.5	**Multiple authentication mechanisms**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1	The TSF shall provide *'none', AES-based symmetric mutual authentication, SIGMA-I authentication*[79] to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the *following rules:*[80] • *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 'Everybody' subject.* • *The AES-based symmetric mutual authentication and SIGMA-I authentication is used to authorise the Application Manager and Application User.*

6.1.3.14 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**

77 [selection: *detect, prevent*]
78 [selection: *detect, prevent*]
79 [assignment: *list of multiple authentication mechanisms*]
80 [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

Hierarchical to:	FIA_UID.1 Timing of identification
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 currently selected context and: • for AES-based symmetric mutual authentication: the key number. For example, if an authentication request for key number 0 is issued after selecting a specific application, the user is identified as the Application Manager of the respective application. • SIGMA-I authentication: the access rights granted from the targeted CARootKey and presented certificates. For example, if an authentication request, issued after selecting a specific application, targets a CARootKey that is associated with ACMap where bit 0 is set, and also the presented certificates either implicitly inherit or have this access right explicitly encoded, the user is identified as the Application Manager of the respective application. Before any authentication request is issued the user is identified as "Everybody".

6.1.3.15 FIA_API.1/ECDSA

The TOE shall meet the requirement "Authentication Proof of Identity (ECDSA)" as specified below.

FIA_API.1/ECDSA	**Authentication Proof of Identity (ECDSA)**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1/ECDSA	The TSF shall provide a *generic ECDSA signature functionality*[81] to prove the identity of the *TOE*[82].

6.1.3.16 FIA_API.1/InternAuth

The TOE shall meet the requirement "Authentication Proof of Identity (ISOInternalAuthenticate)" as specified below.

FIA_API.1/InternAuth	**Authentication Proof of Identity (ISOInternalAuthenticate)**
Hierarchical to:	No other components.
Dependencies:	No dependencies.

81 [assignment: *authentication mechanism*]
82 [assignment: *authorized user or role*]

FIA_API.1.1/InternAuth	The TSF shall provide a *ECC-based Card Unilateral Authentication*[83] to prove the identity of the *TOE*[84].

6.1.3.17 FMT_SAE.1/AWDT1

The TOE shall meet the requirement "Time-limited authorisation (AWDT1)" as specified below.

FMT_SAE.1/AWDT1	**Time-limited authorisation (AWDT1)**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles, FPT_STM.1 Reliable time stamps
FMT_SAE.1.1/AWDT1	The TSF shall restrict the capability to specify an expiration time for *an authentication attempt using SIGMA-I or AES-based Symmetric Authentication of any user role* [85] to *the AppMgr*[86].
FMT_SAE.1.2/AWDT1	For each of these security attributes, the TSF shall be able to *abort the authentication attempt*[87] after the expiration time for the indicated security attribute has passed.

6.1.3.18 FMT_SAE.1/AWDT2

The TOE shall meet the requirement "Time-limited authorisation (AWDT2)" as specified below.

FMT_SAE.1/AWDT2	**Time-limited authorisation (AWDT2)**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles, FPT_STM.1 Reliable time stamps
FMT_SAE.1.1/AWDT2	The TSF shall restrict the capability to specify an expiration time for *a secure channel initiated by SIGMA-I or AES-based Symmetric Authentication of any user role*[88] to *the AppMgr*[89].
FMT_SAE.1.2/AWDT2	For each of these security attributes, the TSF shall be able to *reset the authentication and thus remove the access rights granted to the authenticated user role*[90] after the expiration time for the indicated security attribute has passed.

83 [assignment: *authentication mechanism*]
84 [assignment: *authorized user or role*]
85 [assignment: *list of security attributes for which expiration is to be supported*]
86 [assignment: *the authorised identified roles*]
87 [assignment: *list of actions to be taken for each security attribute]*
88 [assignment: *list of security attributes for which expiration is to be supported*]
89 [assignment: *the authorised identified roles*]
90 [assignment: *list of actions to be taken for each security attribute]*

6.1.3.19 FPT_STM.1

The TOE shall meet the requirement "Reliable time stamps" as specified below.

FPT_STM.1	**Reliable time stamps**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.

6.1.3.20 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.
FPT_TDC.1.1	The TSF shall provide the capability to consistently interpret *data files and monotonic counters*[91] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2	The TSF shall use *the following rules:*[92] • *data files or monotonic counters can only be modified by their dedicated type-specific operations honouring the type-specific boundaries.* • *monotonic counters can only be incremented.* when interpreting the TSF data from another trusted IT product.

6.1.3.21 FTP_TRP.1

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

FTP_TRP.1	**Trusted path**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_TRP.1.1	The TSF shall provide a communication path between itself and *remote*[93] users that is logically distinct from other communication paths and provides assured

91 [assignment: *list of TSF data types*]
92 [assignment: *list of interpretation rules to be applied by the TSF*]
93 [selection: *remote, local*]

	identification of its end points and protection of the communicated data from *modification, disclosure, or only modification*[94].
FTP_TRP.1.2	The TSF shall permit *remote users*[95] to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for *authentication requests with AES or ECC, confidentiality and/or integrity verification for data transfers protected with AES based on a setting in the file attributes, confidentiality and/or integrity protection for data transfers initiated by ProcessSM command exchanges*[96].

6.1.4 Security Functional Requirements regarding Robustness

6.1.4.1 FPR_UNL.1

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

FPR_UNL.1	**Unlinkability**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPR_UNL.1.1	The TSF shall ensure that *unauthorised subjects other than the card holder*[97] are unable to determine whether *any operation of the TOE*[98] *were caused by the same user*[99].

6.1.4.2 FPT_RPL.1

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

FPT_RPL.1	**Replay detection**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_RPL.1.1	The TSF shall detect replay for the following entities: *authentication requests with AES or ECC, confidentiality and/or data integrity verification for data transfers protected with AES and based on a setting in the file attributes*[100].

94 [selection: *modification, disclosure, [assignment: other types of integrity or confidentiality violation]*]
95 [selection: *the TSF, local users, remote users*]
96 [selection: *initial user authentication, [assignment: other services for which trusted path is required]*]
97 [assignment: *set of users and/or subjects*]
98 [assignment: *list of operations*]
99 [selection: *were caused by the same user, are related as follows[assignment: list of relations]*]
100 [assignment: *list of identified entities*]

FPT_RPL.1.2	The TSF shall perform *rejection of the request*[101] when replay is detected.

6.1.5 Security Functional Requirements regarding Secure Dynamic Messaging

6.1.5.1 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 file data*[102] with the following user data's associated security attributes: *confidentiality, authenticity and replay protection for the configurable subset of the file data*[103].
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: *plain export of file data in case that Secure Dynamic Messaging is not activated for the file*[104].

6.1.6 Security Functional Requirements regarding Tag Tamper

6.1.6.1 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*[105] unauthorised modifications to the stored audit records in the audit trail.

101 [assignment: *list of specific actions*]
102 [assignment: *pieces of user data*]
103 [assignment: *list of security attributes*]
104 [assignment: *additional exportation control rules*]
105 [selection, choose one of: *prevent, detect*]

FAU_STG.2.3	The TSF shall ensure that *permanent 1-byte status TTPermStatus*[106] stored audit records will be maintained when the following conditions occur: *failure and attack*[107].

6.2 Security Assurance Requirements

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

Table 16. Security Assurance Requirements

Name	Title
ADV_ARC.1	Security architecture description
ADV_FSP.5	Complete semi-formal functional specification with additional error information
ADV_IMP.2	Complete mapping of the implementation representation of the TSF
ADV_INT.3	Minimally complex internals
ADV_SPM.1	Formal TOE security policy model
ADV_TDS.5	Complete semiformal modular design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.5	Advanced support
ALC_CMS.5	Development tools CM coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.2	Sufficiency of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.3	Compliance with implementation standards - all parts
ASE_INT.1	ST introduction
ASE_CCL.1	Conformance claims
ASE_SPD.1	Security problem definition
ASE_OBJ.2	Security objectives
ASE_ECD.1	Extended components definition
ASE_REQ.2	Derived security requirements
ASE_TSS.2	TOE summary specification with architectural design summary
ATE_COV.3	Rigorous analysis of coverage
ATE_DPT.3	Testing: modular design
ATE_FUN.2	Ordered functional testing
ATE_IND.2	Independent testing - sample
AVA_VAN.5	Advanced methodical vulnerability analysis

106 [assignment: *metric for saving audit records*]
107 [selection: *audit storage exhaustion, failure, attack*]

In the set of assurance components chosen for EAL6, only ADV_SPM.1 requires an assignment. This assignment is given below.

ADV_SPM.1	**Formal TOE security policy model**
ADV_SPM.1.1D	The developer shall provide a formal security policy model for the *following SFRs:*[108] • *TOE Access Control Policy: FDP_ACC.1, FDP_ACF.1, FDP_ITC.2, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1*
ADV_SPM.1.2D	For each policy covered by the formal security policy model, the model shall identify the relevant portions of the statement of SFRs that make up that policy.
ADV_SPM.1.3D	The developer shall provide a formal proof of correspondence between the model and any formal functional specification.
ADV_SPM.1.4D	The developer shall provide a demonstration of correspondence between the model and the functional specification.

6.2.1 Refinements of the TOE Security Assurance Requirements

In compliance to Application Note 23 in the Protection Profile [6], this Security Target has to conform to all refinements of the security assurance requirements in the Protection Profile. Because the refinements in the Protection Profile are defined for the security assurance components of EAL4 (augmented by ALC_DVS.2 and AVA_VAN.5), some refinements have to be applied to assurance components of the higher level EAL6 stated in the Security Target.

Most of the security assurance components mentioned in the Protection Profile and in this Security Target have the same component level and therefore for these components the refinements from the Protection Profile are valid for this Security Target without change. The following subsections apply the refinements for the Security Assurance Requirements that are different between the Protection Profile and this Security Target.

6.2.1.1 Refinements regarding ADV_FSP

The refinement in Section 6.2.1.6 of the Protection Profile [6] regarding ADV_FSP.4 addresses the complete representation of the TSF, the purpose and method of use of all TSFIs, and the accuracy and completeness of the SFR instantiations. The refinement is not a change in the wording of the action elements, but a more detailed definition of the items above.

Compared to ADV_FSP.4 component ADV_FSP.5 requires a Functional Specification in a semi-formal style (ADV_ FSP.5.2C). In addition, component ADV_FSP.5 extends the scope of the error messages to be described from those resulting from an invocation of a TSFI (ADV_FSP.5.6C) to also those not resulting from an invocation of a TSFI (ADV_FSP.5.7C). For the latter a rationale shall be provided (ADV_FSP.5.8C).

Since the higher level ADV_FSP.5 only affects the style of description and the scope of and rationale for error messages, the refinement in the Protection Profile regarding ADV_FSP.4 can be applied without changes and is valid for ADV_FSP.5.

108 [assignment: *list of policies that are formally modelled*]

6.2.1.2 Refinements regarding ADV_IMP

The refinement in Section 6.2.1.7 of the Protection Profile [6] regarding ADV_IMP.1 states that it must be checked that the provided implementation representation is complete and sufficient to ensure that analysis activities are not curtailed due to lack of information.

This Security Target targets assurance level EAL6 augmented, which requires access to all source code of the TOE so that the above refinement is implicitly fulfilled.

6.2.1.3 Refinements Regarding ALC_CMC

The refinement in Section 6.2.1.4 of the Protection Profile [6] regarding ALC_CMC.4 is a clarification of the 'TOE' and the term 'configuration items'.

Since the higher level ALC_CMC.5 requires a higher assurance regarding the defined TOE and the configuration items, the refinement in the Protection Profile regarding ADV_CMC.4 can be applied without changes and is valid for ADV_CMC.5.

6.2.1.4 Refinements Regarding ALC_CMS

The refinement in Section 6.2.1.3 of the Protection Profile [6] regarding ALC_CMS.4 is a clarification of the configuration item 'TOE implementation representation'.

Compared to ALC_CMS.4 component ALC_CMS.5 only adds the requirement for a new configuration item to be included in the configuration list (ALC_CMS.51C) so that the refinement in the Protection Profile regarding ADV_CMS.4 can be applied without changes and is valid for ADV_CMS.5.

6.2.1.5 Refinements Regarding ATE_COV

The refinement in Section 6.2.1.8 of the Protection Profile [6] regarding ATE_COV.2 defines that test coverage must include different operating conditions and 'ageing' and that existence and effectiveness of countermeasures against physical attacks cannot be tested but must be given by evidence.

The refinement regarding test coverage is not a change in the wording of the action elements, but a more detailed definition of the items to be applied, so that it can be applied without changes and is valid for ATE_COV.3. The refinement regarding existence and effectiveness of countermeasures against physical attacks is implicitly fulfilled since this Security Target targets assurance level EAL6 augmented, which requires access to all source code and layout data.

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 17. Security Functional Requirements mapping to Security Objectives

Name	Title
O.Access-Control	FCS_CKM.4 FDP_ACC.1 FDP_ACF.1

Table 17. Security Functional Requirements mapping to Security Objectives*...continued*

Name	Title
	FDP_ITC.2 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1
O.Authentication	FCS_COP.1/AES FCS_COP.1/ECDSA FCS_COP.1/ECDH FCS_COP.1/SHA FCS_CKM.1/Session_AES FCS_CKM.1/Session_SIGMA FIA_API.1/ECDSA FIA_API.1/InternAuth FIA_UID.2 FIA_UAU.2 FIA_UAU.3 FIA_UAU.5 FMT_SAE.1/AWDT1 FMT_SAE.1/AWDT2 FMT_SMF.1 FMT_SMR.1 FPT_STM.1 FPT_RPL.1 FTP_TRP.1
O.Encryption	FCS_CKM.1/Session_AES FCS_CKM.1/Session_SIGMA FCS_CKM.4 FCS_COP.1/AES FTP_TRP.1 FDP_ETC.3
O.Integrity	FCS_CKM.1/ECC FCS_CKM.1/Session_AES FCS_CKM.1/Session_SIGMA FCS_CKM.4 FCS_COP.1/AES FCS_COP.1/ECDSA FCS_COP.1/SHA FPT_RPL.1 FTP_TRP.1 FDP_ETC.3
O.Crypto-Service	FCS_COP.1/AES FCS_COP.1/ECDSA FCS_COP.1/ECDH FCS_COP.1/SHA FCS_COP.1/HMAC FCS_COP.1/HKDF

Table 17. Security Functional Requirements mapping to Security Objectives...*continued*

Name	Title
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 SFRs together provide an access control mechanism as required by the objective O.Access-Control.

Justification related to Authentication (O.Authentication)

For authentication, FCS_COP.1/AES requires that the TOE provides the basic cryptographic algorithm that can be used to perform the authentication. The SFRs FCS_CKM.1/Session_AES and FCS_CKM.1/Session_SIGMA generates the session keys used after the authentication.

For asymmetric authentication, the basic cryptographic algorithms are provided by FCS_COP.1/ECDSA, FCS_COP.1/ECDH, FCS_COP.1/SHA, FCS_COP.1/AES and the session keys to be used during and after the authentication are generated by FCS_CKM.1/Session_SIGMA.

The SFR FIA_UID.2, FIA_UAU.2 and FIA_UAU.5 together define that users must be identified and authenticated before any action. This authentication also associates users with the roles as defined in FMT_SMR.1. The SFR FIA_UAU.3 prevents that forged authentication data can be used. 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, these SFRs fulfill the objective O.Authentication.

FMT_SAE.1/AWDT1 allows to limit the time that can be used for an authentication attempt. FMT_SAE.1/AWDT2 allows to limit the time an authentication session remains active. Therefore, these SFRs further strengthen the objective. FPT_STM.1 fulfills the dependency of FMT_SAE.1/AWDT1 and FMT_SAE.1/AWDT2 by providing reliable time stamps.

Justification related to Confidential Communication (O.Encryption)

The SFR FCS_COP.1/AES requires that the TOE provides the basic cryptographic algorithm AES that can be used to protect the communication by encryption. FTP_TRP.1 requires a trusted communication path between the TOE and remote users, FTP_TRP.1.3 especially requires "confidentiality and/or data integrity verification for data transfers protected with AES and based on a setting in the file attributes".

The SFRs FCS_CKM.1/Session_AES and FCS_CKM.1/Session_SIGMA generates the session key used for encryption. FCS_CKM.4 requires that cryptographic keys used for encryption have to be removed after usage.

The TOE also provides Secure Dynamic Messaging service which allows encrypted data to be read without being in the authenticated state. FDP_ETC.3 requires confidential user data export in unauthenticated state, and hence models the requirements to reach O.Encryption.

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

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. FCS_COP.1/SHA and FCS_COP.1/ECDSA provide the algorithms for signature calculation and validation. FTP_TRP.1 requires a trusted communication path between the TOE and remote users, FTP_TRP.1.3 especially requires "confidentiality and/or data integrity verification for data transfers on request of the file owner". The SFRs FCS_CKM.1/Session_AES and FCS_CKM.1/Session_SIGMA generate the session keys used for the MAC calculation. FCS_CKM.1/ECC generates the static key used for the calculation of signatures. FCS_CKM.4 requires that cryptographic keys used for MAC or signature operations can be removed after usage. FPT_RPL.1 requires a replay detection for these data transfers.

The TOE also provides Secure Dynamic Messaging service which allows MACed or signed data to be read without being in the authenticated state. FDP_ETC.3 requires user data export in unauthenticated state, and hence models the requirements to reach O.Integrity.

Justification related to Cryptographic functionality (O.Crypto-Service)

The SFRs FCS_COP.1/AES, FCS_COP.1/ECDSA, FCS_COP.1/ECDH, FCS_COP.1/SHA, FCS_COP.1/HMAC and FCS_COP.1/HKDF require that the TOE provides the related cryptographic functionality for use by the end-user.

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

The SFR FPT_TDC.1 requires the TOE to consistently interpret data files and values. The TOE will honor the respective file formats and boundaries (i.e. upper and lower limits, size limitations). 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 fulfillment are listed in the tables below:

Table 18. Dependencies of Security Functional Requirements (PP-0084)

SFR	Dependency	Fulfilled in ST
FAU_SAS.1	No dependencies.	No dependency
FCS_RNG.1/PTG2	No dependencies.	No dependency
FCS_RNG.1/DRG4	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

Table 18. Dependencies of Security Functional Requirements (PP-0084)*...continued*

SFR	Dependency	Fulfilled in ST
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 19. Dependencies of Security Functional Requirements (Security Target)

SFR	Dependency	Fulfilled in ST
FAU_STG.2	FAU_GEN.1 Audit data generation	See discussion below.
FCS_CKM.1/Session_AES	[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.1/Session_SIGMA	[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_COP.1/ECDH, FCS_COP.1/SHA, FCS_CKM.4
FCS_CKM.1/ECC	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_ CKM.4 Cryptographic key destruction	Yes, by FCS_COP.1/ECDH, FCS_COP.1/ECDSA, 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/Session_AES, FCS_CKM.1/Session_SIGMA, FCS_CKM.1/ECC
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.1/Session_AES, FCS_CKM.4.
FCS_COP.1/ECDH	[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.1/ECC, FCS_CKM.4.
FCS_COP.1/ECDSA	[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.1/ECC, FCS_CKM.4.
FCS_COP.1/SHA	[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	As no key is used, there is no need for key-related dependencies.
FCS_COP.1/HMAC	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or	Yes, by FDP_ITC.2, FCS_CKM.4

Table 19. Dependencies of Security Functional Requirements (Security Target)...continued

SFR	Dependency	Fulfilled in ST
	FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	
FCS_COP.1/HKDF	[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, FMT_MSA.3
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_API.1/ECDSA	No dependencies.	No dependency.
FIA_API.1/InternAuth	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.
FIA_UID.2	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_SAE.1/AWDT1	FMT_SMR.1 Security roles, FPT_STM.1 Reliable time stamps	Yes, by FMT_SMR.1, FPT_STM.1.
FMT_SAE.1/AWDT2	FMT_SMR.1 Security roles, FPT_STM.1 Reliable time stamps	Yes, by FMT_SMR.1, FPT_STM.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_STM.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 aims 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 underlying Protection Profile [6]. The Security Target uses the same augmentations as the PP (and the addition of augmentation ASE_TSS.2), but chooses a higher assurance level. The level EAL6 is chosen in order to meet assurance expectations of access control applications and automatic fare collection systems. Additionally, the requirement of the PP to choose at least EAL4 is fulfilled.

The rationale for the PP augmentations is the same as in the PP. The assurance level EAL6 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 requirements chosen for augmentation do not add any dependencies, which are not already fulfilled for the corresponding requirements contained in EAL6. Therefore, these components add additional assurance to EAL6, but the mutual support of the requirements is still guaranteed.

As stated in the Section 6.3.3 of the Protection Profile [6], the TOE is intended to defend against sophisticated attacks. Therefore specifically AVA_VAN.5 was chosen by the PP in order to assure that even attackers with high attack potential cannot successfully attack the TOE.

In addition to the SARs introduced by EAL6, ASE_TSS.2 was chosen as augmentation to include architectural information on the security functionality of the TOE in the ST.

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. For example, O.Encryption states that the communication can be protected by encryption. While this ensures the rather high-level goal that the communication can not be eavesdropped, the overall goal that the communication is confidential is ensured with the help of the Protection Profile objective that prevent attacks on the key and the cryptographic implementation like probing or fault injection attacks.

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 20. Portions of the TSF

TSF portion	Title	Description
TSF.Service	Service functionality supporting other TSF	This portion of the TSF comprises services like random number generation and provides mechanisms to store initialization, pre-personalization, 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. It defines resets in case an error or attack was detected.
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.Encryption	Encryption	This portion of the TSF provides cryptographic operations to protect communication against eavesdropping.
TSF.Integrity	Integrity-Protected Communication	This portion of the TSF allows both the TOE and the terminal to detect integrity violations, replay or man-in-the-middle attacks.
TSF.Crypto-Service	Cryptographic Functionality	This portion of the TSF provides a cryptographic API to be used by the end-user.
TSF.Monotonic-Count	Monotonic Counters	This portion of the TSF ensures that certain counter objects can only be incremented, but never decremented.
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.Encryption	TSF.Integrity	TSF.Crypto-Service	TSF.Monotonic-Count	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
FCS_RNG.1/PTG2	X											Random number generation (Class PTG.2)
FCS_RNG.1/DRG4	X											Random number generation (Class DRG.4)
Security Functional Requirements regarding Access Control												
FDP_ACC.1				X								Subset access control
FDP_ACF.1				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								Security roles
Security Functional Requirements regarding Confidentiality, Authentication and Integrity												
FCS_COP.1/AES					X	X	X	X				Cryptographic Operation (AES)
FCS_COP.1/ECDSA					X		X	X				Cryptographic Operation (ECDSA)
FCS_COP.1/ECDH					X			X				Cryptographic Operation (ECDH)
FCS_COP.1/SHA					X		X	X				Cryptographic Operation (SHA)
FCS_COP.1/HMAC								X				Cryptographic Operation (HMAC)

SFR	TSF.Service	TSF.Protection	TSF.Control	TSF.Access-Control	TSF.Authentication	TSF.Encryption	TSF.Integrity	TSF.Crypto-Service	TSF.Monotonic-Count	TSF.No-Trace	TSF.Tag-Tamper	Description
FCS_COP.1/HKDF								X				Cryptographic Operation (HKDF)
FCS_CKM.1/Session_ AES					X	X	X					Cryptographic key generation (Session AES)
FCS_CKM.1/Session_ SIGMA					X	X	X					Cryptographic key generation (Session SIGMA)
FCS_CKM.1/ECC							X					Cryptographic key generation (ECC)
FCS_CKM.4				X		X	X					Cryptographic key destruction
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
FIA_API.1/ECDSA					X							Authentication Proof of Identity (ECDSA)
FIA_API.1/InternAuth					X							Authentication Proof of Identity (ISOInternal Authenticate)
FMT_SAE.1/AWDT1				X	X							Time-limited authorisation (AWDT1)
FMT_SAE.1/AWDT2				X	X							Time-limited authorisation (AWDT2)
FPT_STM.1				X	X							Reliable time stamps
FPT_TDC.1				X					X			Inter-TSF basic TSF data consistency
FTP_TRP.1					X	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 Dynamic Messaging												
FDP_ETC.3						X	X					Export of user data in unauthenticated state
Security Functional Requirements regarding Tag Tamper												
FAU_STG.2											X	Guarantees of audit data availability

7.2.2 TSF.Service

TSF.Service provides the following functionality:

TOE identification

FAU_SAS.1 is implemented by a test function that allows to store identification and/or pre-personalization data (including a unique ID for each die) for the TOE in the non-volatile memory (NVM) at the end of the tests in Phase 3.

Random Number Generation

The TOE provides a hardware (physical) random number generator (RNG) according to PTG.2 as described in [1]. The physical RNG comprises a hardware and software test functionality to detect faults in the circuitry of the RNG (total failure test). Therefore this functionality meets FCS_RNG.1/PTG2.

The TOE also provides a hybrid deterministic RNG according to DRG.4 as described in [1]. This functionality therefore meets FCS_RNG.1/DRG4. This hybrid deterministic RNG is seeded by the hardware (physical) PTG.2 RNG and is responsible for providing random numbers for the cryptographic protocols.

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 any kind of attack. Its functionality mainly addresses self-protection 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:

Integrity protection of memories

As required by FDP_SDI.2, TSF.Protection supports the integrity of the ROM, RAM and NVM. The NVM is able to perform error correction. The ROM, RAM and NVM provide parity protection.

Furthermore, TSF.Protection also implements integrity protection during start-up. 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.

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.

The aspect of TSF.Protection is further supported by FPT_FLS.1 which controls the environmental conditions and triggers a reset in case these are out of bounds.

Logical protection

TSF.Protection prevents the reconstruction of TOE internal information that can be found by analysis of external measured signals like power or clock. 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.

In addition, TSF.Protection encrypts contents stored in RAM and NVM memory and applies memory address scrambling. This ensures the confidentiality of user data stored in RAM and NVM memory as required by FDP_SDC.1.

Cryptographic co-processors and cryptographic library

The cryptographic co-processors (AES, ECC) as well as the cryptographic library implement countermeasures against fault injection and information leakage. Another implemented mechanism to protect User Data from unwanted disclosure is an automatic clean-up of relevant registers (key and data registers of the used coprocessor) after usage and before changing the TOE mode. Therefore, all FCS_COP.1 and FCS_CKM.4 iterations indirectly support TSF.Protection.

7.2.4 TSF.Control

TSF.Control addresses those aspects the TSF controls, e.g., the secure operating conditions or access to specific memory addresses. Its functionality mainly addresses non-bypassability of the TSF. TSF.Control provides the following functionality.

Control of operating conditions

TSF.Control ensures the correct operation of the TOE hardware (functions offered by the micro-controller including the standard CPU, the cryptographic coprocessors, the memories, registers, I/O interfaces and the other system peripherals) during the execution of the IC Dedicated Support Software and Security IC Embedded Software. For this the TOE comprises filters for power supply and clock input. In addition, TSF.Control controls the allowed secure range of temperature, clock frequency, voltage and light.

The filters support the correct function of the TOE within the limits of the secure operating conditions. This robustness implements FRU_FLT.2 and ensures that the processing is performed without failure that may be caused by interference of any external communication interface or other external influences.

FPT_FLS.1 is implemented by sensors that limit the temperature, clock frequency, and voltage to a secure upper and lower threshold. These sensors detect whether the TOE is operating outside its specified secure range. Light sensors distributed over the chip surface detect abnormal light intensities. The secure state required by FPT_FLS.1 is realized by an internal reset of the TOE.

Mode control

TSF.Control realizes the control within the TOE testing phases (phase 3 of the life-cycle) and afterwards. The life-cycle 'Wafer Test' is available for testing purposes in the phases before TOE delivery and disabled before the TOE is delivered from NXP to the customer.

The test concept with specific hardware operations initiated by the test software cannot be used to read out directly any data stored in one of the memories 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 wafer test the access to the IC Dedicated Test Software is disabled. TSF.Control ensures that it is not possible to switch back and reuse the test functions again. In addition, the test functions of the IC Dedicated Test Software require a special sequence to execute a dedicated test routine. Therefore, TSF.Control limits the availability of the test functions as stated by FMT_LIM.2.

7.2.5 TSF.Authentication

TSF.Authentication provides an authentication mechanism to separate authorised subjects from unauthorised subjects. The authentication of subjects is performed by either a challenge-response-based mutual authentication protocol using symmetric cryptography, or the asymmetric SIGMA-I protocol, which is an mutual authenticated Diffie-Hellman key agreement protocol. The TOE supports the cryptographic algorithms AES (128 and 256 bits) for the symmetric authentication and ECC (256 bits) for the asymmetric authentication. By this TSF.Authentication meets FCS_COP.1/AES, FCS_COP.1/ECDSA, FCS_COP.1/ECDH, FCS_COP.1/SHA, FCS_CKM.1/Session_AES and FCS_CKM.1/Session_SIGMA.

TSF.Authentication also identifies the user to be authenticated by the currently selected context (card or specific application) and the key number. This meets FIA_UID.2. The cryptographic authentication is used for the *AppMgr* or *AppUser*. Since the TOE can be used without authentication the "none" authentication is used to "authenticate" *Anybody*. Therefore it implements FIA_UAU.2, FIA_UAU.5 and FMT_SMR.1.

The symmetric authentication protocol requires the user to proof knowledge of a secret key by applying it on a freshly generated random challenge, generated to the TOE. The asymmetric authentication protocol requires the user to proof knowledge of a private key by applying it on the public key of a freshly generated ephemeral key pair used for the key agreement. This ensures that the authentication requests itself cannot be forged or circumvented by attacks like replay or man-in-the-middle. Therefore these protocols meet FIA_UAU.3 and the relevant parts of FTP_TRP.1 and FPT_RPL.1 with respect to the authentication requests.

Authentication of a user is initiated by an authentication request and the authentication state is reset if one of the following events occurs: selecting an application or the card, changing the key corresponding to the current authentication, occurrence of any error during the execution of a command, starting a new authentication, rolling a key set, failed proximity check, deleting an *Application* as *AppMgr*, and reset. By this FMT_SMF.1 is also implemented.

The authentication functionality also provides an authentication mechanism to authenticate the TOE. While this is also provided by the mutual authentication mechanisms discussed in the previous section, the TOE also supports TOE-unilateral authentication mechanisms. These mechanisms are based on asymmetric cryptography and do not require any secret key material in the terminal. This method can also be used for originality checking, verifying the authenticity of the TOE immediately after manufacturing, i.e. before further personalization. In this case, one relies on a key pair and certificate injected in the TOE during manufacturing.

For TOE-unilateral authentication, the TOE implements a dedicated unilateral authentication protocol, but also provides generic ECDSA signature support. With this, FIA_API.1/InternAuth and FIA_API.1/ECDSA are implemented.

The TOE supports two Authority Watchdog Timers (AWDT). AWDT1 limits the time that can be used by a user to authenticate to the TOE using the SIGMA-I authentication or the AES-based symmetric authentication. Once enabled, the timer is started when the challenge (i.e. ephemeral public key in case of SIGMA-I authentication) is sent by the TOE. If the user does not properly authenticate before the timer expires, the authentication attempt is reset by the TOE, meaning that the user needs to start over and request a new challenge. Once authenticated, AWDT2 limits the time a user remains authenticated. If the timer expires, the authentication session is reset, meaning that the user loses the access rights granted by the authentication and a new authentication is required. An internal timer provides reliable timestamps as required by SFR FPT_STM.1.

7.2.6 TSF.Access-Control

TSF.Access-Control provides an access control mechanism to the objects and Security Attributes that are part of the TOE Access Control Policy. The access control mechanism assigns subjects - (possibly multiple) *AppUser* - to 4 different groups of operations on *Files*. The operations on *Files* are File.Read, File.Write and File.Change. One subject can be assigned to each group of *File* operations. The special subjects *Anybody* and *Nobody* can also be assigned. Therefore this functionality maintains the roles as required by FMT_SMR.1.

Since TSF.Access-Control also maintains the objects and Security Attributes as stated in the TOE Access Control Policy, it also implements FDP_ACC.1, FDP_ACF.1 and FMT_MSA.1. Management of authentication data is necessary to separate the roles, therefore it also implements FMT_MTD.1.

A primary use of the TOE is storage of data on behalf of the authorised 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 FDP_ITC.2 is also implemented. This applies to the operations *File.Create* or *CounterFile.Create*.

The TOE supports operations to change keys. If keys used to authenticate roles like the AppMgr or AppUser are changed, the existing role instances are replaced by new instances. This implements FCS_CKM.4.

TSF.Access-Control also controls access to the security attributes. Because it also controls create operations, it implements part of FMT_SMF.1.

Finally the type consistency of the file types stored by the TOE is ensured. It ensures that values can not over- or underflow. Furthermore size limitations of files are obeyed. By this FPT_TDC.1 is implemented.

7.2.7 TSF.Encryption

TSF.Encryption provides a mechanism to protect the communication against eavesdropping by encryption. The encryption is requested by the file owner (i.e. the subject *AppUser* that has the right to perform *File.Change* on a *File*) by setting an option in the attributes of that *File*.

The encryption is using the AES algorithm and by this the functionality implements FCS_COP.1/AES. The SFRs FCS_CKM.1/Session_AES and FCS_CKM.1/Session_SIGMA generates the session keys used during the encryption, after the symmetric AES-based authentication or asymmetric ECC-based authentication respectively. The SFR FCS_CKM.4 removes the used cryptographic keys after encryption. Note that the encryption functionality is active after an authentication is performed. If an authorised user sets the access control permissions in a way that an object is accessible to *Anybody* (refer to Access Control) this object can be accessed without authentication and therefore also without protection by this functionality.

TSF.Encryption also adds data to the communication stream that enables the terminal to detect integrity violations, replay attacks or man-in-the-middle attacks. If an encrypted communication is requested, it also 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 up to the current encrypted frame. Therefore it can detect any injected/modified frame in the communication before the transfer of the encrypted frame.

The encryption for communication and the information to detect integrity violations implement FTP_TRP.1 with respect to the confidentiality and/or data integrity verification for data transfers both on request of the File owner or initiated by the ProcessSM command.

When using the Secure Dynamic Messaging functionality, the TOE encrypts a configurable part of the File to be read when required by the File security attributes, therefore implementing FDP_ETC.3.

7.2.8 TSF.Integrity

TSF.Integrity adds data to the communication stream that enables the terminal to detect integrity violations, replay attacks or man-in-the-middle attacks. Vice-versa it verifies the data sent by the terminal and returns an error code if such an attack is detected. When applied on data exchanged after an authentication, it uses the cryptographic algorithm 128-bit AES CMAC. TSF.Integrity therefore implements FCS_COP.1/AES. The SFRs FCS_CKM.1/Session_AES and FCS_CKM.1/Session_SIGMA generate the session keys used during the calculation, after the symmetric AES-based authentication or asymmetric ECC-based authentication respectively. The SFR FCS_CKM.4 removes the used cryptographic keys after calculation.

The detection mechanism covers all frames exchanged between the terminal and the card up to last frame with a MAC. Depending on the selected mode it can also detect what frame was injected/modified. By this FPT_RPL.1 is implemented.

The information to detect integrity violations implement FTP_TRP.1 with respect to the confidentiality and/or data integrity verification for data transfers both on request of the File owner or initiated by the ProcessSM command.

When using the Secure Dynamic Messaging functionality, the TOE provides a mechanism for integrity protection for the File to be read when required by the File security attributes, therefore implementing FDP_ETC.3. This can be based on an AES CMAC, implementing FCS_COP.1/AES as above, or an ECDSA signature using SHA-256 for hashing, therefore implementing FCS_COP.1/ECDSA and FCS_COP.1/SHA. FCS_CKM.1/ECC generates the key used for this calculation.

7.2.9 TSF.Crypto-Service

The TOE provides an API to the end-user to perform cryptographic operations. The following operations are supported.

AES

The TOE provides AES calculations, supporting the following modes: ECB, CBC, CMAC, GCM and CCM. The underlying basic cryptographic function provides the AES algorithm as defined by [13]. The TOE uses the AES hardware coprocessor to provide AES encryption and decryption functionality using 128 or 256 bit keys. The TOE implements additional countermeasures that are configurable and provides functionality for handling checksums over loaded keys. The interface to the AES operations allows execution with static keys stored upfront in NVM, or with run-time keys stored in a generic transient or static buffer as the result of preceding operations. This security functionality covers FCS_COP.1/AES.

ECDSA

The TOE provides functions to perform ECDSA Signature Generation and Signature Verification according to FIPS PUB 186-5 [12]. Hashing of the message can be done beforehand or by the provided API. The supported key length is 256 bits as NIST P-256 and brainpoolP256r1 curves are supported. This security functionality covers FCS_COP.1/ECDSA.

ECDH

The TOE provides a function to perform Diffie-Hellman key agreement according to NIST SP800-56A [19]. The key agreement can either be executed with a static key stored upfront in NVM or an ephemeral key pair generated by the TOE at run-time. The generated shared secret can be outputted, or written to the TOE's internal transient or static buffer. This security functionality covers FCS_COP.1/ECDH and FCS_CKM.1/ECC.

SHA

The TOE provides a function to compute the Secure Hash Algorithms SHA-256 and SHA-384 according to FIPS 180-4 [11]. The generated digest can be outputted, or written to the internal transient or static buffer of the TOE. This security functionality covers FCS_COP.1/SHA.

HMAC

The TOE provides a function to perform HMAC, i.e. Keyed-Hash Message Authentication Code algorithm according to FIPS 198-1 [14]. The TOE supports the calculation of HMAC authentication code with SHA-256 and SHA-384. The interface to the HMAC operations allows execution with static keys (128 or 256 bit) stored upfront in NVM, or with run-time keys (up to 224 byte) stored in a generic transient or static buffer as the result of preceding operations. The result can be outputted, or written to the internal transient or static buffer of the TOE. This security functionality covers FCS_COP.1/HMAC.

HKDF

The TOE provides a function to perform HKDF, i.e. HMAC-based Extract-and-Expand Key Derivation Function algorithm according to RFC 5869 [20]. The TOE supports the calculation of HKDF with SHA-256 and SHA-384. The interface to the HMAC operations allows execution with static keys (128 or 256 bit) stored upfront in NVM, or with run-time keys (up to 224 byte) stored in a generic transient or static buffer as the result of preceding operations. The result can be outputted, or written to the internal transient or static buffer of the TOE. This security functionality covers FCS_COP.1/HKDF.

7.2.10 TSF.Monotonic-Count

The TOE provides one or more monotonic counter via *CounterFiles*.

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.

One of the counters potentially can be related to the authentication, meaning that it will automatically be incremented each time a symmetric or asymmetric mutual authentication is initiated.

7.2.11 TSF.No-Trace

TSF.No-Trace provides an option to the Admin to use a random UID during ISO14443 anti-collision sequence. By this the device cannot be traced any more by simply retrieving its UID. Device specific information can be read out only by the *AppMgr* and *AppUser* if this option is set.

The card specific information is protected and therefore FPR_UNL.1 is implemented. This functionality does not cover the data in the TOE file system. This data is protected by the TOE Access Control Policy and the tracing protection depends on the access control configuration created by the authorised subjects.

In the default configuration, the TOE is injected with a key pair and certificate for originality checking, i.e. allowing to verify that the TOE was manufactured by the certified manufacturer. This key pair and certificate are shared per production batch, therefore preventing the traceability of individual users. If preferred, this functionality can also be disabled after further personalization, i.e. before distributing the TOE to the device owner in the field.

7.2.12 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, the TOE protects the tag tamper status in case of failure or attack. Hence, this functionality implements FAU_STG.2.

8 References

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.

[7] Common Criteria Protection Profile, Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012, Version 1.3.2, 5 December 2012.

8.2 Developer documents

[8] NRV11 family, Secure Authenticator with NFC T4T compliant, Preliminary data sheet, DocStore number 842714, NXP Semiconductors, Revision 1.4, 2 September 2024.

[9] NRV11, Information on Guidance and Operation, User manual, DocStore number 976314, NXP Semiconductors, Revision 1.4, 2 September 2024.

[10] NRV11, Wafer and delivery specification, Product data sheet addendum, DocStore number 977211, NXP Semiconductors, Revision 1.1, 26 July 2024.

8.3 Standards

[11] FIPS PUB 180-4: Secure Hash Standard (SHS), Federal Information Processing Standards Publication, US Department of Commerce/National Institute of Standards and Technology, August 2015.

[12] FIPS PUB 186-5: Digital Signature Standard (DSS), Federal Information Processing Standards Publication, US Department of Commerce/National Institute of Standards and Technology, 3 February 2023.

[13] 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.

[14] FIPS PUB 198-1: The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, US Department of Commerce/National Institute of Standards and Technology, July 2008.

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

[16] 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.

[17] NIST SP 800-38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, Morris Dworkin, National Institute of Standards and Technology, May 2004.

[18] NIST SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Morris Dworkin, National Institute of Standards and Technology, November 2007.

[19] NIST SP 800-56A Revision 3: Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, National Institute of Standards and Technology, April 2018.

[20] RFC 5869: HMAC-based Extract-and-Expand Key Derivation Function (HKDF), Internet Engineering Task Force (IETF), Request For Comments, May 2010.

Legal information

Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

Disclaimers

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

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

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

Suitability for use in non-automotive qualified products — Unless this document expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

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

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

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

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

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.

Tables

Figures

Contents

Date of release: 10 September 2024
Document identifier: NRV11