ST25TA-E Security Target

SMD_ST25TAE_ST_24_001 rev 1.3

BLANK

Contents

List of tables

1 Introduction

The security target describes the Platform (in this chapter) and the exact security properties of the Platform that are evaluated against SESIP [EN17927] (in chapter “Security requirements and implementation”) that a potential consumer can rely upon the product upholding if they fulfil the objectives for the environment (in chapter “Security Objectives for the operational environment”).

1.1 Security target reference

Table 1: Security target reference

Document identification	Version number	Registration
ST25TA-E Security Target	Rev 1.3	Registered at STMicroelectronics under number SMD_ST25TAE_ST_24_001

1.2 Platform reference

Table 2: Platform reference

Reference	Value	
Platform name	ST25TA-E	
Platform version	1.5.1.0	
Platform identification	IC Ref value	0x9A
	Platform version	0x01050100
	IC Manufacturer code	0x02
Platform Type	NFC secure tag. ISO/IEC 14443-A and NFC tag type 4	

1.3 Profile and conformance claims

The ST25TA-E security target describes the ST25TA-E Platform and the exact security properties of the Platform that are evaluated against European Standard [EN17927] Security Evaluation Standard for IoT Platforms (SESIP).

The conformance claims for this security target are described below.

Table 3: SESIP conformance claims

Reference	Value
SESIP profile	This ST does not claim conformance to any SESIP profile
Assurance claim	SESIP assurance level 1 (SESIP1)

1.4 Included guidance documents

See Table 14.

1.5 Platform functional overview and description

1.5.1 Platform type

Platform is the ST25TA-E IC from STMicroelectronics. This device is a NFC/RFID tag IC with solid security and privacy features.
The contactless interface is compliant with the ISO/IEC 14443 standards, see [ISO/IEC 14443], and NFC Forum Type 4 Tag standards [NFCForum-TS-T4T-1.2], [NFC Forum-T4Tag-OPSN_2.0], [NFC Forum-TS_1.0]. The ST25TA-E devices have a configurable flash memory with 25 years of data retention and work with a 13.56 MHz RFID reader or a NFC-enabled smartphone.

1.5.2 Physical scope

The physical scope of the Platform is implemented in the ST25TA-E. The block diagram below provides an overview of the major features supported by this device.

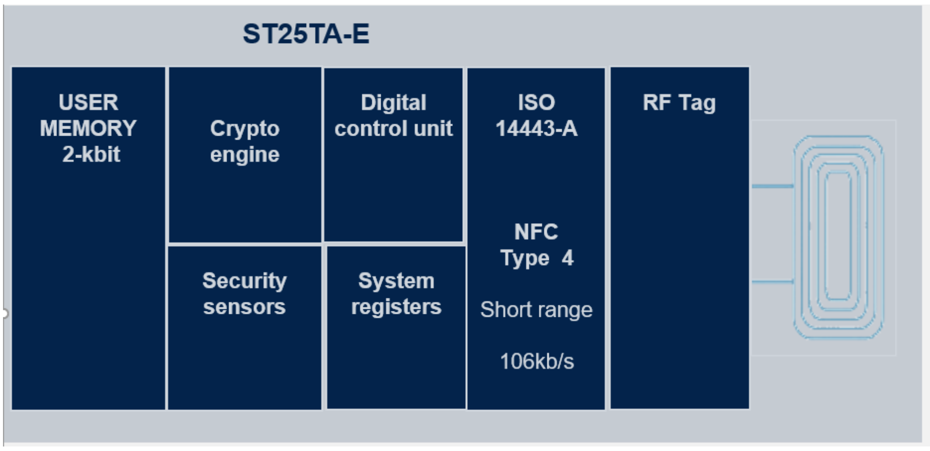

Figure 1: Platform physical scope

1.5.3 Logical scope

The logical scope of the Platform is implemented in the ST25TA-E. The diagram below provides an overview of the major features supported by this device. The Platform evaluation scope is highlighted in pink colour in the figure below.

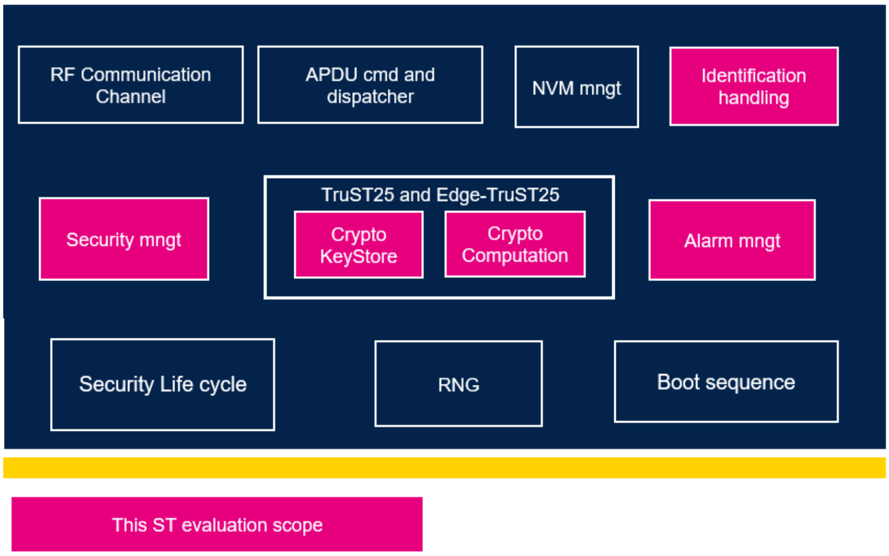

Figure 2: Platform logical scope

1.5.4 Platform usage and major security features

The ST25TA-E Platform is designed to provide identification and Platform instance identification services to the Platform user as detailed in section 3.4.1.1 and section 3.4.1.2 of this security target. Information on such services is also available in [DS_ST25TA-E, section 6].

The Platform includes several tamper resistance mechanisms to provide the Platform user assurance that the user data and security functionality of the device are protected against physical attacks. More information on such physical attacks protections is provided in section 3.4.3.1 which describes the security functional requirement Physical attacker resistance of this SESIP Platform.

The ST25TA-E devices provides cryptographic functionalities such as hash computation, digital signature cryptographic operation and cryptographic keystore. These mechanisms are used for the authentication services named Smart Authentication and Strong Authentication.
Smart Authentication, is using the TruST25 service whereas the Strong authentication is, using the Edge-TruST25 service.

The TrustST25 service ensures that the UID of each NFC/RFID tag device is genuine and can contribute to attest a smart authentication of the chip if the TruST25 services is coupled with other security mechanisms at system level. Performing the TrustST25 service is done with assets stored securely in the Platform thanks to the SFR Cryptographic keyStore detailed in section 3.4.4.2. The TruST25 solution encompasses secure industrialization processes and tools deployed by STMicroelectronics to generate, store and check the signature in the ST25TA-E device. More detailed information on the Smart Authentication service is available in the datasheet of the Platform [DS_ST25TA-E, section 4.4].

The Edge-TruST25 service ensures that each NFC/RFID tag device is genuine and if bond with the final physical product is unique and tamper proof, can prove physical asset authenticity. Performing the Edge-TrustST25 service is done by using the cryptographic operations of the Platform security functional requirement Cryptographic operation in section 3.4.4.1 with the assets stored securely in the Platform thanks to the SFR Cryptographic keyStore detailed in section 3.4.4.2. It encompasses secure industrialization processes and tools deployed by STMicroelectronics to generate, store and check the sensitive assets (needed for this on-chip signature and unique per device) in the device and check each incoming signature from the device. For more detailed information on the Strong authentication please refer to [DS_ST25TA-E, section 4.5].

1.5.5 Product Key Features

The ST25TA-E devices offer a unique combination of high performances and very powerful features such as:

Contactless interface

- Compliant with ISO/IEC 14443 Type A
- NFC Forum Type 4 tag
- Up to 106 kpbs data rate
- Internal tuning capacitance: 68pF +/- 4pF

Memory

- Up to 2048 bits (256 bytes) of secure user Flash memory
- Support NDEF data structure
- Data retention; 25 years
- Minimum endurance : 500 k write cycles.
- Pages erase time down to 0.8 ms.
- Chaining capability
- Augmented NDEF (contextual automatic NDEF message)
- 4-digit unique tap code
- 24-bit general purpose counter with antitearing

Data protection

- Permanent lock file protection for read/write access
- 64-bit password-based file protection for read/write access with diagnosis and mitigation services

Chip identification and protection

- 7-byte unique identifier (UID)
- TruST25 digital signature (off-chip ECDSA)

Product authentication and digitization

- Up to 2-slot secure key storage
- Edge TruST25 digital signature (on-chip ECDSA)
- Compliant with blockchain-backed evidence of authenticity

Security Features

- Active shield
- Monitoring of environmental parameters
- Unique serial number on each die
- Efficient protection against state-of-the-art attacks including hardware, side-channel and fault attacks

Privacy Features

- Scalable NFC-enabled privacy modes:
  - Kill mode and anonymous mode with untraceable UID (fixed or random ID)
  - Configurable kill mode for permanent deactivation of the tag.

Temperature range

- -25°C to +85°C.

The ST25TA-E offers

- Secure high-density Flash memory (NVM).

- A contactless interface including an RF universal Asynchronous Receiver Transmitter (RF UART), enabling communication up to 106 Kbits/s compatible with the ISO/IEC 14443 type A standard.
- A highly reliable True Random Number Generator (TRNG).
- A crypto processor for the ECC computations with a high level of performance and resistant to state-of-the-art side-channel (DPA) and faut attacks.

1.6 Life-cycle

The life cycle actors and phases are summarized in Table 4 and Table 5.

Table 4: Life-cycle actors

Reference	Value
Customer	The final customer (brand) is the actor that owns the certificate authority assets used by the system integrator and provides the final physical product to the NFC tag owner (the end-user).
Inlay Maker	The Inlay Maker is the actor that receives the ST25TA-E Platform from STMicroelectronics and the actor that must perform the delivery conformance with the identification check.
STMicroelectronics	The Platform developer. It is also the actor that performs the Platform pre-personalization and sells the ST25TA-E Platform.
STMicroelectronics subcontractors	Sub-contractors involved by and under supervision of STMicroelectronics during the development of the ST25TA-E Platform.
System Integrator	The system integrator is the actor that manipulates Platform assets to perform the final applicative personalization with the NFC tag assets.
End-user	The end-user is also called **NFC tag owner** and is the actor that buys the final physical product attached to the NFC tag.

Phase 1 is the development of the Platform within STMicroelectronics R&D development centres.

Phase 2 is the IC production environment of the Platform. As high volumes of ICs commonly go through such environments, adequate control procedures are necessary to account for all ICs at all stages of production. Production starts within the Wafer-fab; here the silicon wafers undergo the diffusion processing. Computer tracking at wafer level throughout the process is commonplace. The wafers are then taken into the test area. Testing and pre-personalization of the Platform is done. Pre-personalization of customer assets of each Platform occurs to assure conformance with the device specification and to load the customer information. Finally, the Platform is moved to self-protected mode. Wafers are then scribed and broken such as to separate the functional from the non-functional ICs. The latter is discarded in a controlled accountable manner.

In Phase 3 the good ICs are then packaged, in a back-end plant., ICs are transported and worked on in a secure environment with accountability and traceability of all (good and bad) products.

The Platform is delivered after Phase 3 in packaged form.

Phases 1, 2 and 3 ALC security measures are conformant to Minimum Site Security Requirements [MSSR].

Table 5: Platform life-cycle

Lifecycle phase	Value	Actor
1 Platform Development	Design data, test data	STMicroelectronics
2 Platform production environment	Mask manufacturer, IC manufacturer and IC testing, IC pre-personalization steps. Wafers are ready for packaging phase.	STMicroelectronics
3 IC packaging, pre-personalization if necessary	Packaged Platforms	STMicroelectronics sub-contractors
PLATFORM DELIVERY		
4 Inlay making	Platform at Inlay Maker premises. The NFC tag form factor is achieved.	Inlay Maker
5 ST customer NFC tag integration	Final product maker performs applicative personalization, integrates the NFC tag in its final physical product.	System Integrator (can be the customer)
6 Distribution up to consumers	Customer warehouses, customer distributors	Customer
7 Operational environment	NFC Tag product under final end usage	Customer
8 End-of-life	Product termination	Customer

Before being used by the end-user (also called NFC tag owner), any ST25TA-E chip must follow ST25TA-E guidance [UM_ST25TA-E_GOM]: delivery conformance process and requirements during the production and processing steps of the Platform life cycle.

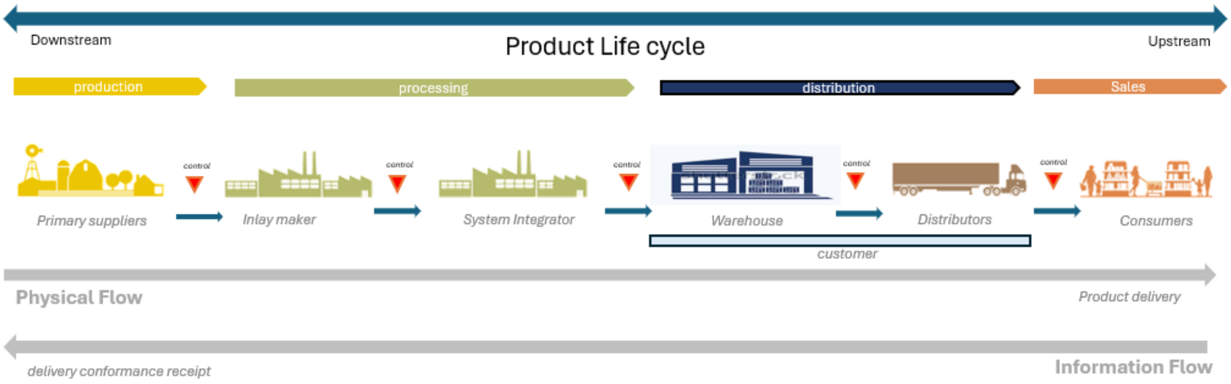

Figure 3: Life cycle

2 Security Objectives for the Operational Environment

2.1 Platform objectives for the operational environment

To fulfil the security requirements of the Platform, the operational environment (technical or procedural) must meet the objectives listed in Table 6.

Table 6: Platform objectives for the operational environment

Reference	Value
Platform verification	The *inlay maker* and *system integrator* check the version of all the Platform components, see [UM_ST25TA-E_GOM, section 2.4 – Delivery and device identification]
Secure use	*Customers* ensure the secure and correct use of the Platform according to the guidance document [UM_ST25TA-E_GOM, section 3.2 Requirements for pre-personalization] and [UM_ST25TA-E_GOM] sections 4.1 to 4.5 included.
Trusted integration	The *inlay maker* must verify the correct identification of the Platform according to the guidance document [UM_ST25TA-E_GOM, section 2.4.1 – Delivery conformance and identification after pre-personalization]. The *system integrator* must verify the correct identification of the Platform according to the guidance document [UM_ST25TA-E_GOM, section 2.4.2 - Delivery conformance and identification at personalization].
Vulnerability handling	The *inlay Maker, the system integrator and the customer* must follow and implement the security requirement updates from the Platform user guidance [UM_ST25TA-E_GOM, section 4.6 - Vulnerability handling] provided by STMicroelectronics to ensure the latest vulnerabilities are always remediated.

2.2 Inherited Objectives for the Operational Environment

The Platform does not include Platform parts that have previously been evaluated under any SESIP certification scheme.

3 Security Requirements and Implementation

3.1 Security Assurance Requirements

The claimed assurance requirements package is SESIP1, as defined in Chapter 8 (section 8.2) of [EN17927].

3.2 Flaw Reporting Procedure (ALC_FLR.SESIP)

In compliance with flaw reporting procedures ALC_FLR.SESIP, the developers have defined the following procedure:

ST's Product Security Incident Response Team (ST PSIRT) supervises the process of accepting and responding to potential security vulnerabilities involving ST hardware and software products. The process is published at Report potential product security vulnerabilities - STMicroelectronics, it is made of the following steps.

Reporting

Vulnerability reporting on the Platform can be done through the PSIRT web page Report potential product security vulnerabilities - STMicroelectronics.
It is recommended to provide the following information when reporting a vulnerability:

- ST product identification: part number or product reference and version (hardware or software)
- Complete technical description of the potential vulnerability, including any related known exploits
- How and when the potential vulnerability was discovered
- Any public information already published or publication planning (CVE, academic paper publication, etc.)
- Your contact information to use during the process

Due to the sensitivity of vulnerability information, it is recommended to provide your findings through encrypted email using the below ST PSIRT PGP/GPG key.

Once submitted, the ST PSIRT will acknowledge the reception of the reported issue.

Evaluation

The ST PSIRT will evaluate the potential vulnerability to understand if there is an issue, analyse it, and set a priority to manage valid issues. ST PSIRT may come back to the submitter in case some information is missing from the original report or if clarification is needed.

Solving

ST PSIRT will investigate potential solutions and mitigations to address the issue.

Communicating

Once a solution is available (fix or mitigation), ST PSIRT will communicate back to the submitter and others where appropriate.

3.3 Vulnerability survey (AVA_VAN.SESIP1)

As defined in Chapter 4 (section 4.7) of [EN17927] the developer has performed a vulnerability survey to demonstrate the resistance of the Platform to the state-of-the-art attacks and known potential vulnerabilities on similar product category in the public domain. The self-assessment done by the developer is detailed in the following:

Table 7: Vulnerability assessment table

Reference	Value
Public vulnerabilities database verification	The developer has verified that the product is resistant to the attack paths listed in the vulnerabilities public databases such as: • Common Vulnerabilities and Exposures (CVE, https://cve.mitre.org) • Common Weakness Enumeration (CWE, https://cwe.mitre.org)
CVE-2021-33881	In particular the following vulnerability On NXP MIFARE Ultralight and NTAG cards, an attacker can interrupt a write operation (aka conduct a "tear off" attack) over RFID to bypass a Monotonic Counter protection mechanism. The impact depends on how the anti-tear-off feature is used in specific applications such as public transportation, physical access control, etc. CVE - CVE-2021-33881 (mitre.org) • MISC:https://blog.quarkslab.com/rfid-monotonic-counter-anti-tearing-defeated.html • MISC:https://www.nxp.com/docs/en/application-note/AN11340.pdf • MISC:https://www.nxp.com/docs/en/application-note/AN13089.pdf • MISC:https://www.sstic.org/2021/presentation/eeprom_it_will_all_end_in_tears/ Internal analysis has concluded the Platform is resistant to this vulnerability.
State-of-the-art on side-channel and fault attacks	• *JIL Attack methods for smartcards v2.5* document contains the list of attacks which can be applied on smartcards like products. It is used as a reference for the evaluation laboratory and part of the SESIP methodology. The developer has checked that the Platform is resistant to the attacks listed in this document even those higher to AVA_VAN.SESIP1. • CHES conference proceedings contain the known side-channel and fault attacks, including recent techniques based on machine learning. The developer has checked that the Platform is resistant to these known attacks when the attack was relevant for this product. • IACR eprint containing former and recent publications on attacks: Cryptology ePrint Archive (iacr.org). The developer has checked that the Platform is resistant to these known attacks when the attack was relevant for this product. Side-channel testing by internal laboratory has been performed to validate the resistance of the Platform to these attacks.
Strength of cryptographic mechanisms	Cryptographic attacks on key-size, choice of the cryptographic algorithm have been reviewed by the developer to ensure no vulnerability is present on the selected algorithm for the cryptographic operations. The following document is the standard for security certification and list the minimal requirement for the cryptographic mechanisms to be embedded in a product. These recommendations have been respected. • SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms version 1.3, February 2023 - SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf
Hardware attacks resistance	The Platform developer has verified the product is resistant to known hardware attacks (physical attacks) as those listed in as those identified in documentation listed below: in *JIL Attack methods for smartcards v2.5* document.
Random number generation attacks	The Platform developer has verified the product is resistant to known attacks on random number generation as those identified in documentation listed below: • in *JIL Attack methods for smartcards v2.5* document.

3.4 Security Functional Requirements

Security Functional Requirements (SFRs) are drawn from [EN17927].

The selected security functional requirements for the Platform, their respective origin and type are summarized in Table 8.

Table 8: Summary of functional security requirements for the Platform

SFR	Addressing	Origin	Type
Verification of Platform identity	Identification and attestation of Platforms and applications	Security target operated	EN 17927:2023
Verification of Platform instance identity		Security target operated	
~~Secure update of Platform~~	Product life cycle	Security target operated	
Physical attacker resistance	Extra attacker resistance	Security target operated	
Cryptographic operation	Cryptographic functionality	Security Target operated	
Cryptographic keyStore			

3.4.1 Identification and attestation of Platform

3.4.1.1 Verification of Platform identity

Requirement

The Platform provides a unique identification of the Platform, including all its parts and their versions.

Refinement

Assets and protections related to this SFRs are:

Asset	Protection required	Comments
Platform identification	Integrity	The modification of the Platform id is impacting the user configuration management.

Conformance rational

Table 9: Platform identification value

Reference	Value	
Platform identification	IC Ref value	0x9A
	Platform version	0x01050100
	IC Manufacturer code	0x02

Identification is done per product with the values given in Table 9 which can be obtained through the command *GetSystemInformation*. See datasheet [DS_ST25TA-E, section 5.4.3.3] and [UM_ST25TA-E_GOM, section 4.1].

Platform identification assets are stored in NVM read-only memory area with high integrity protection to ensure the integrity security attribute property.

The Platform identity SFR is tested by emulation during the design phase and by characterization on silicon samples once they are available.

Additional production tests are performed in production premises prior to shipment to ensure the proper functionality of the product.

3.4.1.2 Verification of Platform instance identity

Requirement
The Platform provides a unique identification of that specific instantiation of the Platform, including all its parts.

Refinement
Assets and protections related to this SFRs are:

Asset	Protection required	Comments
Platform instance identification: UID	Integrity Authenticity	.

Conformance rational

Table 10: Platform identification value

Reference	Value	
Platform instance identity	UID 6 low significant bytes B_1 to B_6 B_0 = 0x02 being the IC manufacturer code byte used in the Platform identity identification.	UID = 0x$B_0B_1B_2B_3B_4B_5B_6$

Instance identification is done per product with the value given in Table 10 which can be obtained through the command *GetSystemInformation*. See datasheet [DS_ST25TA-E, section 5.4.3.3] and [UM_ST25TA-E_GOM, section 4.2].
The ST25TA-E device contains a unique serial ID number programmed in production phase at ST premises. The UID guarantees the uniqueness of each device.

UID is stored in read-only memory area with high integrity protection and protected in authenticity with a ST TruST25 signature and with the Edge-TruST25 P (signed with CA key) as detailed in [UM_ST25TA-E_GOM] section 3.1.

The Platform instance identity SFR is tested by emulation during the design phase and by characterization on silicon samples once they are available.
Additional production tests are performed in production premises prior to shipment to ensure the proper functionality of the product.

~~3.4.2 Product life cycle~~

~~*3.4.2.1 Secure update of Platform*~~

Requirement
~~The Platform can be updated to a newer version in the field such that the <confidentiality,> integrity and authenticity of the Platform is maintained.~~

Conformance rational
The Platform does not support the update or patching for the following reasons:

- The Platform is a closed product that cannot be patched.
- Hardware patching is not possible.

The product is connected to a network temporarily, i.e., only when alimented by a reader else the product is powered off and not connected. Therefore, the timing window for remote connection to attack the product is very limited and the probability of remote attack is very low. Hence, in case of known vulnerability on the product, remote wide-scale attacks have very low probability to happen.

Vulnerability handling is managed by the ALC_FLR.SESIP assurance family and related operational procedures, see section 4.3 in [UM_ST25TA-E_GOM].

3.4.3 Extra attacker resistance

3.4.3.1 Physical attacker resistance

Requirement
The Platform detects or prevents attacks by an attacker with physical access before the attacker compromises any of the other security functional requirements.

Conformance rational
The Platform contains the following security mechanisms to be resistant to physical attacks:

- Active shield
- Memories and buses scrambling to protect the memories content from hardware attacks including reverse engineering attacks.
- Monitoring of environmental parameters active when the Platform is operating.
- Highly efficient hardware protection against perturbation (fault) attacks
- Highly efficient hardware protection against side-channel attacks (SPA, DPA and complex side-channel)
- Algorithmic side-channel countermeasures in the ECC computations
- Algorithmic fault-attacks countermeasures in the ECC computations
- Design development rules have been applied to prevent the Platform from probing, F.I.B and other hardware attacks

The physical attacker resistance security mechanisms are tested by emulation during the design phase and by characterization on silicon samples once they are available with internal and external security laboratories.
Additional production tests are performed in production premises prior to shipment to ensure the proper functionality of the product.

3.4.4 Cryptographic functionality

3.4.4.1 Cryptographic operation

Requirement
The Platform provides the application with cryptographic operations in Table 11 functionality with algorithms in Table 11 as specified in Table 11 for key lengths described in Table 11 and modes described in Table 11.

Table 11: Platform cryptographic operations

Operations	Algorithm	Specification	Key lengths	Modes
Signature generation	ECDSA	NIST FIPS PUB 186-5 SEC1, SEC2 IETF RFC 7027 ANSI X9.62	256 bits	NIST-P256 secp256k1, secp256r1
Hash computation	Keccak	Keccak SHA-3 submission [Keccak]	NA	Keccak-256
	SHA-3	FIPS PUB 202	NA	SHA3-256

Conformance rational

The Platform provides to applications side channel and fault resistant cryptographic algorithms (see vulnerability survey section 3.3), with indicated key size.

Security mechanisms based on hardware side-channel and fault protections are enforced with mathematical blinding operations (randomizations of modulus, points and curve parameters) to protect ECDSA from side-channel and fault attacks.

Cryptographic algorithms are implemented with security requirements conformant to state-of-the-art SOG-IS security standards [SOG-IS].

The cryptographic operations listed in Table 11 is tested by emulation during the design phase and by characterization on silicon samples once they are available.

As for any SFR of the Platform additional production tests are performed in production premises prior to shipment to ensure proper functionality of the product.

3.4.4.2 Cryptographic keyStore

Requirement

The Platform provides a way to store cryptographic keys in Table 12 such that not even the application can compromise the security attributes described in Table 12 of this data. This data can be used for the cryptographic operations from Table 11.

Refinement

Assets and protections related to this SFRs are:

Table 12: Platform cryptographic keystore

Asset	Protection required	Comments
Applicative private keys: Edge-TruST25 K private key	Confidentiality, integrity. authenticity	See [UM_ST25TA-E_GOM, section 3.1] for more detail.
Applicative public keys: Edge-TruST25 K public key	Integrity, authenticity	
Applicative Edge-TruST25 P-signatures	Integrity, authenticity	

Conformance rational

All assets from Table 12 are stored in read only and highly integrity protected NVM memory area. The NVM memory is a secure memory which ensure the confidentiality of the assets stored once they have been loaded in the device. These assets are additionally protected with an on-chip integrity check and loaded in internal secure memory with a cryptographic authentication verification. This authentication operation performed during the asset loading stage in the NVM protected memory of the Platform ensures the authenticity of the loaded assets.

Applicative public keys, called Edge-TruST25 K, are additionally protected in authenticity with signature certificates as detailed in [UM_ST25TA-E_GOM, section 3.1].

The cryptographic keystore listed in Table 12 is tested by emulation during the design phase and by characterization on silicon samples once they are available.
As for any SFR of the Platform additional production tests are performed in production premises prior to shipment to ensure proper functionality of the product.

4 Mapping and sufficiency rationales

4.1 SESIP sufficiency

The claimed assurance requirements package is given in Table 13.

Table 13: Assurance requirements

Assurance class	Assurance family	Covered by	Rationale
ASE: Security Target Evaluation	ASE_INT.SESIP ST Introduction	Section 1 and title page	The ST reference is in the Title, the Platform reference in the "Platform Reference" section 1.2, the Platform overview and description in "Platform Functional Overview and Description" section 1.5.
	ASE_OBJ.SESIP security requirements for the operational environment	Section 2	The objectives for the operational environment in "Security Objectives for the Operational Environment" refer to the guidance documents.
	ASE_REQ.SESIP listed security requirements	Section 3.4	All SFRs in this ST are taken from SESIP. "Verification of Platform Identity" is included. "Secure Update of Platform" is not included and a justification is provided.
	ASE_TSS.SESIP TOE summary specification	Section 3	All SFRs are listed per definition, and for each SFR the implementation and verification are defined in section 3.4.
AGD: Guidance documents	AGD_OPE.SESIP operational user guidance	Guidance documents [UM_ST25_TA-E_GOM] in section 4.	The operational user guidance describes secure usage of the user accessible functions.

	AGD_PRE.SESIP Preparative procedures	Guidance documents [UM_ST25_TA-E_GOM] in section 3.	The preparative procedures describe how the Platform is brought into a secure configuration.
ALC: Life-cycle support	ALC_FLR.SESIP Flaw reporting Procedures	Section "Flaw reporting procedures (ALC_FLR.SESIP)"	The flaw reporting and remediation procedure is described.
AVA_VAN.1	AVA_VAN.SESIP1 Vulnerability survey	Section 3.3	The vulnerability survey and associated tests results are described in section 3.3.

5 References and guidance documents

Table 14: Guidance documents

Reference	Value	Version
UM_ST25TA-E_GOM	ST-25TA-E : Guidance and operational manual – STMicroelectronics.	1.0

Table 15: document references

Reference	Value	Version
EN17927	Security Evaluation Standard for IoT Platforms (SESIP). An effective methodology for applying cybersecurity assessment and re-use for connected products. EN17927:2023 – November 2023	EN17927:2023(E)
DS_ST25TA-E	Datasheet ST25TA_E preliminary - STMicroelectronics.	0.4
MSSR	Minimum Site Security Requirements – Joint Interpretation Library – December 2023.	3.1
SOG-IS	SOG-IS agreed cryptographic mechanisms - Joint Interpretation Library – February 2023. SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf	1.3
[Keccak]	The Keccak SHA-3 submission – STMicroelectronics – January 2011 Keccak-submission-3.pdf	3
ISO/IEC 14443	ISO/IEC 14443-1:2018 Part 1: Physical characteristic – 2018-06 ISO/IEC 14443-2:2020 Part 2: Radio frequency power and signal interface – 2020-07 ISO/IEC 14443-3:2018 Part 3: Initialization and anticollision – 2018-07 ISO/IEC 14443-4:2018 Part 4: Transmission protocol – 2018-06	Edition 4
NFCForum-TS-T4T-1.2	NFC Forum- Technical Specification- Type 4 Tag - [T4T] - 2023.02.10, 02 2023	1.2
NFC Forum-T4Tag-OPSN_2.0	NFC Forum- Technical Specification- Type 4 Tag Operation Specification - [T4TOP 2.0]- 2017-11-13	2.0
NFC Forum-TS_1.0	NFC Forum- Technical Specification – NFC Record Type Definition - Version 1.0 [RTD] - 2020-02-20	1.0

6 Glossary

Term	Definition
Keystore	SESIP term for repository in which certificates, private keys or secrets can be stored.
TruST25	ECDSA off-chip generated signature stored in the SESIP Platform used to prove the origin of the chip UID in identification detection.
Edge-TruST25	ECDSA digital signature on-chip generation service from the SESIP Platform
Platform	SESIP term for hardware and/or software that provides secure services to a connected Platform

7 Abbreviations

Term	Definition
ECDSA	Elliptic curve digital signature algorithm
IC	Integrated circuit
NFC	Near Field communication
RFID	Radio frequency identification
SESIP	Security evaluation standard for IoT Platform
SHA	Secure Hash Algorithm
SFR	Security functional requirement
UID	Unique identifier

MPORTANT NOTICE – PLEASE READ CAREFULLY