OPTIGA™ Trust M v3 SLS 32AIA010MK Trusted subsystem

SESIP Security Target

Table of contents

1 Introduction

1.1 ST reference

This ST's title is "OPTIGA™ Trust M v3 SLS 32AIA010MK Trusted subsystem" version 1.5 dated 2024-03-11.

1.2 SESIP Profile Reference

Table 1 SESIP Profile Reference

Reference	Value
PP name	SESIP Profile for PSA Certified™ RoT Component Level 3
PP version	V1.0 REL 02
Assurance Claim	SESIP Assurance Level 3 (SESIP 3)
Optional and additional SFRs	none

1.3 Platform Reference

Table 2 Subsystem Reference

Reference	Value
TOE name	OPTIGA™ Trust M v3 SLS 32AIA010MK
TOE version	V3.00.2440
Hardware reference	IFX_CCI_00000Bh design step G13 with libraries RSA2048 V2.08.007 Toolbox V2.08.007, HSL V02.01.6634 and with specific IC dedicated software
Software Reference	V3.00.2440
TOE type	Processor with interal hardware isolation

1.4 Included Guidance Documents

Table 3 Guidance Documents

Reference	Name	Version
[RefMan]	SLS 32AIA010MH/S/K/L OPTIGA™ Trust M, Solution Reference Manual	v3.60, 2023-12-04
[AddSecGuid]	OPTIGA™ Trust M V3 Additional security-related guidelines,	V1.0, 2024-03-04
[DeliveryGuid]	OPTIGA™ Trust M V3 SLS 32AIA010MK Trusted subsystem Delivery guidance	V1.0, 2024-03-07

Reference	Name	Version
[KeysCert]	SLS 32AIA010MK/L OPTIGA™ Trust M Product Version: V3	V3.10, 2020-09-21
[Dsheet]	SLS 32AIA010MH/S/K/L OPTIGA™ Trust M, Datasheet	V3.40, 2022-06-21
[I2C]	IFX I2C Protocol, Protocol Specification	V2.03, 2020-09-22
[GettingStarted]	SLS 32AIA010MH/S/K/L OPTIGA™ Trust M, Getting Started Guide	v3.10, 2020-09-21
[RelNotes]	Release Notes for SLS 32AIA010MK/L OPTIGA™ Trust, Product Version: V3	V3.00, 2020-10-01

1.5 Platform Functional Overview and Description

1.5.1 TOE type

The TOE type is

a Secure Element, i.e. a secure microcontroller, which can be used as a trusted subsystem for providing cryptographic services and internal trusted storage to a secure connected IOT device.

1.5.2 TOE Physical Scope

The TOE consists of a combination of software, hardware and guidance documents:

- Hardware: Infineon smart card IC (Security Controller) IFX_CCI_00000Bh design step G13 with libraries RSA2048 V2.08.007 Toolbox V2.08.007, HSL V02.01.6634 and with specific IC dedicated software. The hardware part and cryptographic libraries are certified claiming strict conformancy to [PP0084]: https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/CC/SmartCards_IC_Cryptolib/0961_0961V2_0961V3_0961V4_0961V5_0961V6.html; https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0084.html
- Software: Babylon-OS 2020.01 + Trust-M application V3.00.2440
- Guidance documents: see section 1.4

Note: *The Trust-M application software version implicitly also identifies the Babylon-OS version, because OS version is bound to one specific application version.*

1.5.3 Usage and Major Security Features

The platform supports the major security features:

- I2C interface with shielded connection with pre-shared secret (encrypted and MAC-ed communication)
- Cryptographic store for keys and data with integrity and confidentiality protection
- Cryptographic support:
  - RSA 2048 Encryption/Decryption/Signature generation and verification/key generation
  - ECDH, ECDSA, ECC signature generation/verification, key generation; supported curves:
    - NIST P-256/384/521

    - Brainpool P256r1/P384r1/P512r1
- RNG:
    - Physical RNG: PTG.2
- AES 128/192/256 key generation; encryption/decryption/MAC generation/verification with BCM: ECB, CBC, CBC-MAC, CMAC
- HMAC generation/verification based on SHA-256, SHA-384, SHA-512

1.5.4 None TOE Hardware/Software/Firmware

None

2 Security Objectives

For the platform to fulfill its security requirements, the operational environment (technical or procedural) must fulfill the following objectives:

Table 4

ID	Description	Reference
KEY_MANAGEMENT	Cryptographic keys and certificates outside of the platform are subject to secure key management procedures.	[AddSecGuid] section 1 “Security-related guidelines”
TRUSTED_USERS	Actors in charge of platform management, for instance pairing process for secure channel protocol, are trusted	[AddSecGuid] section 1 “Security-related guidelines”
PRESHAREDSECRET	The pre-shared secret needs to be kept in a confidential way by the application.	[AddSecGuid] section 1 “Security-related guidelines”
SHIELDEDCONNECTION	The application must setup data objects accordingly to enforce shielded connection with pre-shared secret upon these objects	[AddSecGuid] section 1 “Security-related guidelines”

Note:

- UNIQUE_ID is not a security objective for this platform, because identification data is already added before customer delivery by the developer of this TOE.
- TRUSTED_USERS was changed to reflect TOE use case (no firmware update possible)

3 Security Requirements and Implementation

3.1 Security Assurance Requirements

The claimed assurance requirements package is SESIP3.

3.2 Flaw Reporting Procedure (ALC_FLR.2)

In accordance with the requirement for a flaw reporting procedure (ALC_FLR.2), including a process to report a flaw and generate any needed update and distribute it, the developer has defined the following procedure:

Flaws can be reported following the procedures as described in https://www.infineon.com/cms/en/about-infineon/company/cybersecurity/

Note: *The platform does not provide any update functionality. The hardware and cryptographic libraries are CC certified with high assurance of EAL6+ targeting a security lifespan of many years (latest certificate from March 2022). The secure subsystem is a closed system, which means it does not allow any software extensions or modifications, effectively preventing loading of malicious (or other) code. Further the strict "need to know" policy applied during development and manufacturing significantly increases the effort for attackers to obtain security critical TOE knowledge.*

3.3 Security Functional Requirements from Base PP

3.3.1 Verification of Platform Identity

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

Conformance rationale: The command GetDataObject allows to extract the TOE version (ESW build number). The ESW build number can be retrieved via [RefMan] section 4.4.1.3 "GetDataObject" on Object ID Tag "0xE0C2 Coprocessor UID Optiga Trust Family" [RefMan], Table 71). The ESW build number can be found in the returned Data Structure in [RefMan], Table 79 Coprocessor UID Optiga Trust Family" at offset 25 with the Name rgbESWBuild and must contain the value 0x2440. Additionally only products, which support "Elliptic Curve Key on NIST P256 curve", are considered as TOE. The Metadata of Data Object Tag = 0xE0F0 [RefMan], Table 71) must contain Metatdata Tag "0xE0 Algorithm associated with key container" ([RefMan], Table 74) with the value "0x03 Elliptic Curve Key on NIST P256 curve" ([RefMan], Table 60). MetaData can be retrieved via [RefMan] section 4.4.1.3 "GetDataObject" with "Param=0x01 Read metadata".

3.3.2 Secure Update of Platform

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

The platform does not meet this functional requirement.

Rationale: see note from chapter 3.2

3.3.3 Physical Attacker Resistance

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

Conformance rationale: The hardware part and cryptographic libraries are certified claiming strict conformancy to [PP0084]: https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/CC/SmartCards_IC_Cryptolib/0961_0961V2_0961V3_0961V4_0961V5_0961V6.html; https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0084.html; The Babylon OS and the Trust-M application follow the user guidance from the hardware certificate.

3.3.4 Secure Initialization of Platform

The platform ensures its authenticity and integrity during the platform initialization. If the platform authenticity or integrity cannot be ensured, the platform will go to **a state where no other operation except optionally Secure Update of Platform (with Physical Attacker Resistance) can be performed**.

Conformance rationale: The IC dedicated software implements several redundancies to protect integrity during hardware boot. The integrity during startup was extensively validated during CC certification. Further the IC embedded software performs a selfcheck, to validate the integrity of specific security features (UMSLC = User Mode Security Life Control). The platform does not allow any updates in the field. Therefore authenticity is not explicitly checked, but implicitly: authentic platform software is loaded during initialization of platform within the secure manufacturing premises of the developer. The high level of integrity protection and non updateability prevent the platform to transition from an authentic to a non authentic state.

3.3.5 Cryptographic Operation

The platform provides the application with Operations in Table 5 functionality with algorithms in Table 5 as specified in specifications in Table 5 for key lengths described in Table 5 and modes described in Table 5.

Table 5 Cryptographic Operation

Algorithm	Operations	Specification	Key lengths	Modes
ECDSA	Sign, Verify	[IETF5639], [N186-4]	NIST: P-256/384/521 Brainpool: P256r1/P384r1/P512r1	-
RSA[1]	Sign, Verify, Encrypt, Decrypt	[RSA-PKCSB]	2048	EXP
AES	Confidentiality: Encrypt/Decrypt	[N197], [ISO9797-1], [N800-38A]	128, 192, 256	ECB, CBC
AES	Integrity: MAC generation/verification	[N-800-38B]	128, 192, 256	CBC-MAC, CMAC
HMAC	Generate, Verify	[N198-1]	256, 384, 512	SHA-256/384/512
Shielded connection with pre-	Key agreement	Based on Pseudo Random Function (PRF) P_SHA256 of [RFC5246]	256	

[1] although RSA2048 is below 128 bit security level according to NIST RSA2048 is still sufficient for federal Government use: see NIST-SP-800-131A Revision 2

Algorithm	Operations	Specification	Key lengths	Modes
shared secret	Encryption & MAC	AES-CCM for encryption & integrity protection: [N197], [N800-38C]	128	CCM

Conformance rationale: These cryptographic claims are partly implemented by the Trust-M application, partly by the cryptographic libraries of the hardware and partly by the Babylon OS. The Babylon OS uses the cryptographic libraries for provisioning cryptographic primitives in a harmonized interface to the application. The application then uses these cryptographic primitives to implement cryptographic protocols like the Shielded connection with pre-shared secret, or provides API's to use the cryptographic primitives directly. In total these were designed to meet the standards mentioned under "Specification".

3.3.6 Cryptographic Random Number Generation

The platform provides the application with a way based on

- Physical noise source

to generate random numbers to as specified in

- PTG.2 according to [BSI_RNGs]

Conformance rationale: The PTG.2 is implemented by the hardware and CC certified.

3.3.7 Cryptographic Key Generation

The platform provides the application with a way to generate cryptographic keys for use in cryptographic operations in Table 6 as specified in specifications in Table 6 for key lengths described in Table 6.

Table 6 Cryptographic Key Generation

ID	Algorithm	Specification	Key lengths
ECDSAKEY	ECDSA keypair generation	Method of generation: ECC curves over prime fiel Fp as well as over GF(2^n) finite field are supported. The generated secret key sk is derived from a random candidate c, sk = c mod (n-1) + 1 with n corresponding to the BasepointOrder of the ECC curve provided.	NIST: P-256/384/521 Brainpool: P256r1/P384r1/P512r1
ECDH	ECDH	[N800-56A], section 5.7.1.2	NIST: P-256/384/521 Brainpool: P256r1/P384r1/P512r1
RSAKEY	RSA	Length of the primes p and q and public exponent is provided by the user. Based on this information the CC certified TRNG is used to generate numbers of that length, which are subsequently checked for primality	2048

ID	Algorithm	Specification	Key lengths
		using Miller Rabin algorithm. From p and q and public exponent, a RSA key pair is derived.	
AESKEY	AES	Directly taken from random output of the CC certified TRNG.	128, 192, 256

Conformance rationale:

- ECDSA key generation is based on the CC certified cryptographic library function "ECC_ECDSAKeyGen" using the CC certified TRNG as entropy source.
- ECDH key generation is based on the certified cryptographic library function "ECC_DHMask".
- RSA key pair generation is based on the CC certified cryptographic library function "CryptoRsaKeyGen" using the CC certified TRNG as entropy source.

3.3.8 Cryptographic KeyStore

The platform provides the application with a way to store cryptographic keys and other protected data objects such that not even the application can compromise the integrity, confidentiality of this data. This data can be used for the cryptographic operations ECDSA, RSA, AES, Shielded connection with pre-shared secret, HMAC.

Conformancy rationale: The TOE offers functionality to use its own trust anchor for integrity protection. Confidentiality during transmission is protected by shielded connection with pre-shared secret (the data objects need to be configured accordingly to enforce shielded connection with pre-shared secret based n pre-shared secret). Confidentiality during storage is inherently protected. For further information see [RefMan] section 5 "OPTIGA™ Trust M Data Structures".

3.4 Additional Security Functional Requirements

3.4.1 Secure Communication Support

The platform provides the application with one or more secure communication channel(s).
The secure communication channel authenticates the application, platform and protects against disclosure, modification of messages between the endpoints, using Shielded connection with pre-shared secret.

Comformace rationale: The platform sends a challenge and sequence counter to the application. Based on this and shared secret, a session key is generated, which is used for confidentiality and modification protection. For further information see [RefMan] section 6.6 "Shielded Connection V1 Guidance", [RefMan] section 6.5.8 "Shielded Connection" and [I2C] section 6 "Presentation Layer".

3.4.2 Secure Communication Enforcement

The platform ensures that the application can only communicate with **trusted subsystems** over the secure communication channel(s) supported by the platform using Shielded Conection

Conformance rationale: The application is required to configure the data objects, upon which shielded connection with pre-shared secret is enforced. For detailed information see [RefMan] section 5 "OPTIGA™ Trust M Data Structures" especially [RefMan] Table 69 "Access Condition Identifier and Operators".

3.5 Optional Security Functional Requirements

The TOE does not implement any of the optional security functional requirements.

4 Mapping and Sufficiency Rationales

4.1 Assurance

The assurance activities defined in [PSA-EM-L3] fulfil the SESIP3 activities. In particular, the required source code review, vulnerability analysis and testing of the [PSA-EM-L3] is applicable.

Table 7 Assurance – Evidence Mapping

Assurance Class	Assurance Family	Covered by
ASE: Security Target Evaluation	ASE_INT.1 ST Introduction	This document chapter 1
	Rationale: this chapter is dedicated and reviewed to meet these requirements	
	ASE_OBJ.1 Security requirements for the operational environment	This document chapter 2
	Rationale: this chapter is dedicated and reviewed to meet these requirements	
	ASE_REQ.3 Listed Security requirements	This document chapter 3
	Rationale: this chapter is dedicated and reviewed to meet these requirements	
	ASE_TSS.1 TOE Summary Specification	From this document the rationales from chapter 3
	Rationale: TSS is merged with the security requirements, as it also described, how these are implemented	
ADV: Development	ADV_FSP.4 Complete functional specification	This document chapter 1.4, especially [RefMan]; Trust-M_ADV_FSP_IMP_mapping TEM-105 v0.2
	Rationale: the guidance documents describe all interfaces and user functionality of the TOE. There is dedicated mapping table between interface and user guidance reference.	
	ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs	Trust-M_ADV_FSP_IMP_mapping TEM-105 v0.2
	Rationale: there is a dedicated mapping table between source code and TSF	
AGD: Guidance Documents	AGD_OPE.1 Operational user guidance	See [RefMan] section 6.5 “Security Guidance” and [RefMan] section 6.6 “Shielded Connection V1 Guidance”
	Rationale: These guidelines provide sufficient guidance to operate the TOE in a secure way. It is one of the evaluation tasks to assure this.	
	AGD_PRE.1 Preparative procedures	See [RefMan] section 6.6.1 “Setup” (setting up shielded connection with pre-shared secret). See [DeliveryGuidance] for setting up delivery procedure
	Rationale: These guidelines provide sufficient guidance to receive, accept and prepare the TOE in a correct way. It is one of the evaluation tasks to assure this.	
	ALC_CMC.1 Labelling of the TOE	Section 1.4

Assurance Class	Assurance Family	Covered by
ALC: Life-cycle Support	Rationale: The evaluator will determine, whether the provided evidence is suitable to meet the requirement.	
	ALC_CMS.1 TOE CM Coverage	Listing of required CM elements provided to the evaluation lab.
	Rationale: The evaluator will determine, whether the provided evidence is suitable to meet the requirement.	
	ALC_FLR.2 Flaw reporting procedures	This document chapter 3.2
	Rationale: the link provided allows externals to report flaws of the TOE to Infineon Technologies AG. Evidence, how flaws are handled was provided to the evaluation lab.	
ATE: Tests	ATE_IND.1 Independent testing: conformance	Witnessing session performed with the evaluation lab
	Rationale: The evaluator will determine, whether the provided evidence and joint execution of testcases is suitable to meet the requirement.	
AVA: Vulnerability Assessment	AVA_VAN.3 Focused vulnerability analysis	Vulnerability and testing carried out by the laboratory
	Rationale: The evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE.	

4.2 PSA Security Functions Mapping

This section shows the platform mapping to the PSA Security Functions.

Table 8 Functionality Mapping and Sufficiency Rationales

PSA Security Function	Covered by SESIP SFR
F.INITIALIZATION	Secure Initialization
F.SOFTWARE_ ISOLATION	Not covered by the TOE
F.SECURE_ STORAGE	Cryptographic KeyStore
F.FIRMWARE_ UPDATE	Not covered by the TOE
F.SECURE_STATE	Secure Initialization; further SFRs not implemented
F.CRYPTO	Cryptographic Operation Cryptographic KeyStore Cryptographic Random Number Cryptographic Key Generation
F.ATTESTATION	Verification of Platform Identity; further SFRs not implemented
F.AUDIT	Not covered by the TOE
F.DEBUG	Not covered by the TOE
F.PHYSICAL	Physical Attacker Resistance
Additional security functionality	Secure Communication Support Secure Communication Enforcement

5 References

Reference Name	Standard Description
[BSI_RNGs]	A proposal for: Functionality classes for random number generators, Wolfgang Killmann, Werner Schindler, Version 2.0, 18 Sept 2011
[IETF5639]	IETF: RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010, http://www.ietf.org/rfc/rfc5639.txt
[ISO9797B]	ISO/IEC 9797-1: 2011 - Information Technology - Security techniques - Message Authentication Codes - Part 1: Mechanisms using block cipher
[N180-4]	NIST: FIPS publication 180-4: Secure Hash Standard (SHS), August 2015
[N186-4]	NIST: FIPS publication 186-4: Digital Signature Standard (DSS), July 2013
[N197]	Federal Information Processing Standards Publication, U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), Advanced Encryption Standard (AES), FIPS PUB 197, as of 26st November 2001
[N198-1]	FIPS PUB 198-1, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, The Keyed-Hash Message Authentication Code (HMAC), July 2008
[N800-38A]	National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Data Encryption Standard, NIST Special Publication 800-38A, Edition 2001
[N800-38C]	NIST Special Publication 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004
[N800-56A]	NIST Special Publication 800-56A Revision 3; Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, April 2018
[N800-90A]	NIST Special Publication 800-90A Revision 1 Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015
[RFC5246]	The Transport Layer Security (TLS) Protocol Version 1.2 URL: https://datatracker.ietf.org/doc/html/rfc5246
[RSA-PKCSB]	PKCS #1: RSA Cryptography Standard, v2.2, October 27, 2012, RSA Laboratories

6 Revision history

Document version	Date of release	Description of changes
1.5	2024-03-11	Final version

Trademarks
All referenced product or service names and trademarks are the property of their respective owners.

Edition 2024-03-11

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Email: erratum@infineon.com

Document reference

IMPORTANT NOTICE

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics (“Beschaffenheitsgarantie”) .

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

In addition, any information given in this document is subject to customer’s compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer’s products and any use of the product of Infineon Technologies in customer’s applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer’s technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies office (**www.infineon.com**).

WARNINGS

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies’ products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.