Global Platform®

The standard for secure digital services and devices

GlobalPlatform Technology

SESIP Profile for ECN

Version 0.0.0.15

Public Review

February 2024

Document Reference: GPT_SPE_152

THIS SPECIFICATION OR OTHER WORK PRODUCT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY IMPLEMENTATION OF THIS SPECIFICATION OR OTHER WORK PRODUCT SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE COMPANY, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER DIRECTLY OR INDIRECTLY ARISING FROM THE IMPLEMENTATION OF THIS SPECIFICATION OR OTHER WORK PRODUCT.

Contents

1 Introduction 7
1.1 Audience 7
1.2 IPR Disclaimer 7
1.3 References 7
1.4 Terminology and Definitions 9
1.5 Abbreviations 11
1.6 Revision History 12
2 Overview 13
2.1 SESIP Profile Reference 13
2.2 Platform Component Functional Overview and Description 13
2.2.1 Usage and Major Security Features 13
2.2.2 Platform Type 14
2.2.3 Available Non-Platform Hardware/Software/Firmware 14
2.2.4 Platform Security Services 14
2.2.5 Life Cycle 15
3 Security Objectives for the Operational Environment 16
4 Security Requirements and Implementation 17
4.1 Security Assurance Requirements 17
4.1.1 Flaw Reporting Procedure (ALC_FLR.2) 17
4.2 Security Functional Requirements for Base-SP 17
4.2.1 Identification and Attestation 17
4.2.1.1 Verification of Platform Identity 17
4.2.1.2 Secure Initialization of Platform 17
4.2.2 Product Life Cycle 18
4.2.2.1 Secure Install of Application 18
4.2.2.2 Secure Update of Platform 18
4.2.2.3 Secure Update of Application 18
4.2.2.4 Factory Reset of Platform 19
4.2.3 Cryptographic Operations 19
4.2.3.1 Cryptographic Key Generation 19
4.2.3.2 Cryptographic Operation 20
4.2.3.3 Cryptographic Random Number Generation 21
4.2.4 Secure Communication 21
4.2.4.1 Secure Communication Support 21
4.2.5 Extra Attacker Resistance 23
4.2.5.1 Software Attacker Resistance: Isolation of Platform 23
4.2.5.2 Software Attacker Resistance: Isolation of Application Parts 23
4.2.6 Compliance Functionality 23
4.2.6.1 Audit Log Generation and Storage 23
4.2.6.2 Reliable Index 25
4.2.7 Access Control 26
4.2.7.1 Authenticated Access Control 26
5 SP-Modules 29
5.1 Secure Boot and File System Secure Storage 29
5.1.1 SESIP References 29
5.1.1.1 Protection Profile Reference 29
5.1.2 Platform Component Functional Overview and Description 29

5.1.2.1 Usage and Major Security Features 30
5.1.2.2 Platform Type 30
5.1.2.3 Available Non-Platform Hardware/Software/Firmware 30
5.1.2.4 Platform Security Services 31
5.1.3 Security Functional Requirements 31
5.1.3.1 Cryptographic Functionality 31
5.1.3.1.1 Cryptographic Key Generation 31
5.1.3.1.2 Cryptographic KeyStore 32
5.1.3.2 Compliance Functionality 33
5.1.3.2.1 Secure Trusted Storage 33
5.1.3.3 Identification and Attestation of Platforms and Applications 34
5.1.3.3.1 Secure Initialization of Platform 34
5.2 Support for HSM-Based Secure Storage and Cryptography 35
5.2.1 SESIP References 35
5.2.1.1 Protection Profile Reference 35
5.2.2 Platform Component Functional Overview and Description 35
5.2.2.1 Usage and Major Security Features 36
5.2.2.2 Platform Type 36
5.2.2.3 Available Non-Platform Hardware/Software/Firmware 36
5.2.3 Security Objectives for the Operational Environment 36
5.2.4 Security Functional Requirements 37
5.2.4.1 Compliance Functionality 37
5.2.4.1.1 Audit Log Generation and Storage 37
5.2.4.2 Identification and Attestation of Platforms and Applications 38
5.2.4.2.1 Secure Initialization of Platform 38
5.2.4.3 Secure Communication 38
5.2.4.3.1 Secure Communication Support 38
5.2.4.3.2 Secure Communication Enforcement 39
5.3 Support for Secure Enclave-Based Secure Storage and Cryptography SP-Module 40
5.3.1 SESIP References 40
5.3.1.1 Protection Profile Reference 40
5.3.2 Platform Component Functional Overview and Description 40
5.3.2.1 Usage and Major Security Features 41
5.3.2.2 Platform Type 41
5.3.2.3 Available Non-Platform Hardware/Software/Firmware 41
5.3.3 Security Objectives for the Operational Environment 41
5.3.4 Security Functional Requirements 42
5.3.4.1 Compliance Functionality 42
5.3.4.1.1 Audit Log Generation and Storage 42
5.3.4.2 Identification and Attestation of Platforms and Applications 43
5.3.4.2.1 Secure Initialization of Platform 43
5.3.4.3 Secure Communication 43
5.3.4.3.1 Secure Communication Support 43
5.3.4.3.2 Secure Communication Enforcement 44

6 Mapping and Sufficiency Rationales 45
6.1 Assurance 45
6.2 Functionality 47
6.2.1 Base-SP 47
6.2.2 Secure Boot and File System Secure Storage SP-Module 49
6.2.3 Support for HSM-Based Secure Storage and Cryptography SP-Module 50
6.2.4 Support for Secure Enclave Secure Storage and Cryptography SP-Module 50

Tables

Table 1-1: References 7
Table 1-2: Terminology and Definitions 9
Table 1-3: Abbreviations 11
Table 1-4: Revision History 12
Table 3-1: Security Objectives for the Operational Environment 16
Table 4-1: Cryptographic Key Generation Details 19
Table 4-2: Cryptographic Operation Details 20
Table 4-3: Allowed TLS Cipher Suites 22
Table 4-4: Auditable Events 24
Table 4-5: Access Isolations by Operation 26
Table 4-6: Management Functions 27
Table 5-1: Cryptographic Key Generation Details for the Secure Boot and File System Secure Storage SP-module 31
Table 5-2: Security Objectives for the Operational Environment 36
Table 5-3: Auditable Events 37
Table 5-4: Security Objectives for the Operational Environment 41
Table 5-5: Auditable Events 42
Table 6-1: Assurance Mapping and Sufficiency Rationales 45
Table 6-2: Functionality Mapping and Sufficiency Rationales for Base-SP 47
Table 6-3: Functionality Mapping and Sufficiency Rationales for SP-module Secure Boot and File System Secure Storage 49
Table 6-4: Functionality Mapping and Sufficiency Rationales for SP-module Support for HSM-Based Secure Storage and Cryptography 50
Table 6-5: Functionality Mapping and Sufficiency Rationales for SP-module Support for Secure Enclave Secure Storage and Cryptography 50

Figures

Figure 2-1: Base Platform Components and Scope....13
Figure 5-1: Edge Compute Node with Software-Based Secure Storage Platform....30
Figure 5-2: Edge Compute Node with HSM-Based Secure Storage and Cryptography....35
Figure 5-3: Edge Compute Node with Secure Enclave Platform....40

1 INTRODUCTION

An Edge Compute Node (ECN) is a device located between a network of IoT leaf devices (an IoT network) and an IoT Edge Cloud. It has the capability of performing local processing of data from IoT leaf devices through a runtime environment offered to developers and of acting as a bridge between the IoT Edge Cloud and IoT leaf devices. The Edge Compute Node can be provisioned and administrated from the IoT Edge Cloud by a trusted administrator.

This profile specifies the security features to be implemented by the ECN Security Manager, a software part of the ECN, to provide the core security features needed by an Edge Compute Node. It describes the essential set of basic security properties that are common to ECN Security Managers and that shall be consistently evaluated. It also specifies three packages extending the basic set of security properties and resulting in the following configurations:

Edge Compute Node with Secure Boot and File System Secure Storage

Edge Compute Node with Support for HSM-Based Secure Storage and Cryptography

Edge Compute Node with Support for Secure Enclave-Based Secure Storage and Cryptography

This profile attempts to be compatible with the Common Criteria Edge Compute Node Protection Profile ([CC Profile]).

If a product is certified compliant to this SESIP profile, customers can rely upon these security features and upon the security assurance provided that they follow user guidance documentation associated to the certified product.

1.1 Audience

This document is intended primarily for the use of the Security Target (ST) writer.

1.2 IPR Disclaimer

Attention is drawn to the possibility that some of the elements of this GlobalPlatform specification or other work product may be the subject of intellectual property rights (IPR) held by GlobalPlatform members or others. For additional information regarding any such IPR that have been brought to the attention of GlobalPlatform, please visit https://globalplatform.org/specifications/ip-disclaimers/. GlobalPlatform shall not be held responsible for identifying any or all such IPR, and takes no position concerning the possible existence or the evidence, validity, or scope of any such IPR.

1.3 References

The tables below list references applicable to this specification. The latest version of each reference applies unless a publication date or version is explicitly stated.

Table 1-1: References

Standard / Specification	Description	Ref
GP_FST_070	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP) v1.2, Public Release, July 2023	[SESIP]

Standard / Specification	Description	Ref
GP_TEN_053	GlobalPlatform Technology Cryptographic Algorithm Recommendations Version 2.0, Public Release, June 2021	[CRYPTO]
GPD_SPE_021	GlobalPlatform Device Committee TEE Protection Profile v1.2.1, November 2016	[TEE PP]
GPD_SPE_	GlobalPlatform Technology TEE Trusted I/O SP-Module v1.0, June 2020	[TEE PP I/O]
CC Profile	Edge Compute Node Protection Profile, Version 1.0.7, 4 September 2020.	[CC Profile]
TCG PP for TPM	TCG, Protection Profile for PC Client Specific TPM 2.0, 16 June 2018, Version 1.1	[TPM PP]
CC collaborative PP	collaborative Protection Profile for Dedicated Security Component, May 1st 2019, Version 1.0d	[DSC PP]
FIPS Pub 140-2	Security Requirements for Cryptographic Modules	[FIPS 140-2]
FIPS Pub 140-3	Security Requirements for Cryptographic Modules	[FIPS 140-3]
FIPS Pub 180-4	Secure Hash Standard	[FIPS 180-4]
FIPS Pub 186-4	Digital Signature Standard (DSS)	[FIPS 186-4]
FIPS Pub 197	Advanced Encryption Standard (AES)	[FIPS 197]
FIPS Pub 198-1	The Keyed-Hash Message Authentication Code	[FIPS 198-1]
IEEE 802.11-2012	Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications	[802.11-2012]
IEEE 802.11ac-2013	Telecommunications and information exchange between systems–Local and metropolitan area networks--Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications--Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz.	[802.11ac-2013]
RFC 7748	Elliptic Curves for Security	[RFC 7748]
NIST Special Publication 800-38A	Recommendation for Block Cipher Modes of Operation: Methods and Techniques	[NIST 800-38A]
NIST Special Publication 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality	[NIST 800-38C]
NIST Special Publication 800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC	[NIST 800-38D]
NIST Special Publication 800-38E	Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices	[NIST 800-38E]

Standard / Specification	Description	Ref
NIST Special Publication 800-38F	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping	[NIST 800-38F]
NIST Special Publication 800-56A	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography	[NIST 800-56A]
NIST Special Publication 800-56B	Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography	[NIST 800-56B]
NIST Special Publication 800-57	Recommendation for Key Management – Part 1 – General	[NIST 800-57]
NIST Special Publication 800-90A	Recommendation for Random Number Generation Using Deterministic Random Bit Generators	[NIST 800-90A]
NIST Special Publication 800-108	Recommendation for Key Derivation Using Pseudorandom Functions	[NIST 800-108]

1.4 Terminology and Definitions

Selected terms used in this document are included in Table 1-2.

Table 1-2: Terminology and Definitions

Term	Definition
Access	Interaction between an entity and an object that results in the flow or modification of data.
Access control	Security service that controls the use of resources1 and the disclosure and modification of data2.
Assurance	A measure of confidence that the security features of an IT system are sufficient to enforce the IT system's security policy
Attack	An intentional act attempting to violate the security policy of an IT system.
Authentication	A security measure that verifies a claimed identity.
Authorization	Permission, granted by an entity authorized to do so, to perform functions and access data.
Availability	Timely3, reliable access to IT resources.
Common Application Developer	Application developers (or software companies) often produce many applications under the same name. ECN allow shared resources by such applications where otherwise resources would not be shared.
Compromise	Violation of a security policy.
Confidentiality	A security policy pertaining to disclosure of data.
Critical cryptographic security parameters	Security-related information appearing in plaintext or otherwise unprotected form and whose disclosure or modification can compromise the security of a cryptographic module or the security of the information protected by the module.

Term	Definition
Cryptographic key (key)	A parameter used in conjunction with a cryptographic algorithm that determines: • the transformation of plaintext data into ciphertext data • the transformation of ciphertext data into plaintext data • a digital signature computed from data • the verification of a digital signature computed from data • a data authentication code computed from data
Cryptographic module	The set of hardware, software, and/or firmware that implements approved security functions, including cryptographic algorithms and key generation, which is contained within the cryptographic boundary.
Cryptographic module security policy	A precise specification of the security rules under which a cryptographic module must operate.
Developer Modes	Developer modes are states in which additional services are available to a user in order to provide enhanced system access for debugging of software.
Enclave	A collection of entities under the control of a single authority and having a homogeneous security policy. They may be logical, or based on physical location and proximity.
General-Purpose Operating System	A general-purpose operating system is designed to meet a variety of goals, including protection between users and applications, fast response time for interactive applications, high throughput for server applications, and high overall resource utilization.
Hardware-protected	Asset (such as a cryptographic key or certificates or cryptographic elements such as a hash) for which storage and processing is done in hardware and result of its usage is provided to software layer. The software layer has a restricted access to the raw data.
Operating environment	The total environment in which a platform operates. It includes the physical facility and any physical, procedural, administrative and personnel controls.
Persistent storage	All types of data storage media that maintain data across system boots (e.g., hard disk, removable media).
Protected data	Protected data is all non-platform data (user data). Protected data includes all keys in secure key storage.
Public object	An object for which the platform unconditionally permits all entities “read” access under the Discretionary Access Control SFP. Only the platform or authorized administrators may create, delete, or modify the public objects.
Security-enforcing	A term used to indicate that the entity (e.g., module, interface, subsystem) is related to the enforcement of the platform security policies.
Security-supporting	A term used to indicate that the entity (e.g., module, interface, subsystem) is not security-enforcing; however, the entity’s implementation must still preserve the security of the platform.

Term	Definition
System services	All services provided by the platform to Edges modules through an application interface. Examples of system services include access to network interface, storage, cryptography. The TSS shall list all system services available for use by Edges modules.
Threat	Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the platform security policy.
Trust Anchor Database	A list of trusted root Certificate Authority certificates.
Trusted endpoints	Servers (IoT Edge Cloud) or IoT leaf devices the platform is designed to communicate with.
Unauthorized individual	A type of threat agent in which individuals who have not been granted access to the platform attempt to gain access to information or functions provided by the platform.
Unauthorized user	A type of threat agent in which individuals who are registered and have been explicitly granted access to the platform may attempt to access information or functions that they are not permitted to access.
Vulnerability	A weakness that can be exploited to violate the platform security policy.

1.5 Abbreviations

Table 1-3: Abbreviations

Abbreviation	Meaning
Base-SP	Base SESIP Profile
ECN	Edge Computer Node
SP-Module	SESIP Profile Module
ST	Security Target

1.6 Revision History

GlobalPlatform technical documents numbered *n*.0 are major releases. Those numbered *n*.1, *n*.2, etc., are minor releases where changes typically introduce supplementary items that do not impact backward compatibility or interoperability of the specifications. Those numbered *n.n*.1, *n.n*.2, etc., are maintenance releases that incorporate errata and precisions; all non-trivial changes are indicated, often with revision marks.

Table 1-4: Revision History

Date	Version	Description
April 2023	v0.0.0.8	Draft provided by NXP Semiconductors and SGS Brightsight
April 2023	v0.0.0.10	Committee Review
June 2023	v0.0.0.11	Member Review (content unchanged since Committee Review)
January 2024	v0.0.0.12	Updates from the editor
February 2024	v0.0.0.15	Public Review
TBD	v1.0	Public Release

2 OVERVIEW

This Profile contains guidance paragraphs:

AN: Application Note: Guidance that must be considered and followed for Security Target writing.

INFO: Additional context information.

2.1 SESIP Profile Reference

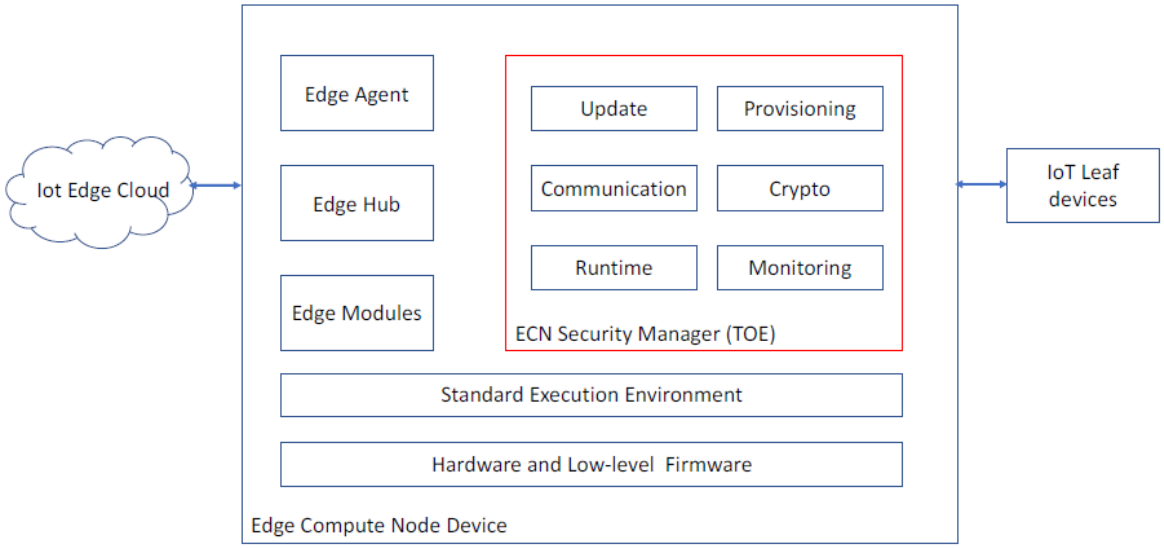
SP name	SESIP Protection Profile for *ECN*
SP version	*Public review v0.0.0.15*
Platform Type	*ECN Security Manager software*
Assurance claim	SESIP2

2.2 Platform Component Functional Overview and Description

In the context of Internet of Things (IoT), an Edge Compute Node (ECN) is a piece of hardware and software located between a network of IoT leaf devices (an IoT network) and an IoT Edge Cloud. It has the capability of performing local processing of data from IoT leaf devices through a runtime environment offered to developers and of acting as a bridge between the IoT Edge Cloud and IoT leaf devices. The Edge Compute Node can be provisioned and administrated from the IoT Edge Cloud by a trusted administrator.

For this Base-SP, the Platform is the ECN Security Manager in charge of providing the core security features needed for an Edge Compute Node. The Platform is illustrated by the red box in Figure 2-1.

Figure 2-1: Base Platform Components and Scope



2.2.1 Usage and Major Security Features

The security features of the ECN Security Manager (Platform) include the following:

The Update function, which provides secure update.

The Edge Runtime, which is the execution runtime for Edge modules.

The Provisioning Library, which provides device identity life-cycle management.

The Secure Communication Library, which provides support of TLS with X.509 certificates.

The Cryptographic Library, which provides cryptographic services for the device, including cryptographic keys.

The Monitoring Library, which generates and monitor security events for the Platform.

2.2.2 Platform Type

The Platform type is a software featuring the security manager for Edge Compute Node.

2.2.3 Available Non-Platform Hardware/Software/Firmware

The execution environment must provide the following:

A supporting Operating System (Standard Execution Environment) for the ECN Security Manager, which provides a runtime environment for the ECN Security Manager and additional services, such as memory isolation or secure storage for cryptographic keys.

The Edge Modules that implement local edge computing functions for the network of leaf devices.

The Edge Hub in charge of communications with the IoT Edge Cloud.

The Edge Agent in charge of Edge module management.

The hardware and low-level firmware supporting the ECN Security Manager, typically based on an Intel or ARM device.

The networked environment with the IoT Edge Cloud and the leaf devices.

2.2.4 Platform Security Services

The security features of the ECN Security Manager include the following:

Security Audit: The ECN Security Manager has the ability to collect audit data, review audit logs, protect audit logs from overflow, and restrict access to audit logs. Audit information generated by the system includes the date and time of the event, the user identity that caused the event to be generated, and other event specific data. Authorized administrators can review audit logs and have the ability to search and sort audit records. Authorized Administrators can also configure the audit system to include or exclude potentially auditable events to be audited based on a wide range of characteristics. In the context of this evaluation, the profile requirements cover generating audit events, selecting which events should be audited, and providing integrity protection for stored audit event entries.

Cryptographic Support: The ECN Security Manager provides cryptographic functions that support encryption/decryption, cryptographic signatures, cryptographic hashing, cryptographic key agreement, and random number generation. The ECN Security Manager additionally provides support for public keys, credential management and certificate validation functions. In addition to using cryptography for its own security functions, the ECN Security Manager offers access to the cryptographic support functions for Edge modules.

Identification and Authentication: The ECN Security Manager provides the ability to use, store, and protect certificates that are used for authentication of the IoT Edge Cloud and to authenticate the ECN Security Manager (static and dynamic attestation).

Self-protection: The ECN Security Manager provides a number of features to ensure the protection of its security functions. It protects against unauthorized data disclosure. The ECN Security Manager ensures process isolation security for all Edge modules, with support from the Standard Execution Environment. The ECN Security Manager includes self-testing features that ensure the integrity of executable program images and its cryptographic functions. Finally, The ECN Security Manager provides a trusted update mechanism to update the ECN Security Manager binaries itself.

Trusted Path for Communications: The ECN Security Manager provides protected communications with the IoT Edge Cloud.

Security Management: The ECN Security Manager provides several functions to manage security policies. This includes management of Edge Modules, cryptographic keys and certificates and auditable events.

2.2.5 Life Cycle

AN In this section, the Security Target shall describe the life cycle of the ECN Security Manager under evaluation.

The description must present an overview of the main phases from the hardware and software design to the product end-of-life; for each phase, all possible ECN Security Manager state(s) must be identified. It must also be explained how transitions between those states are secured.

The description must identify all roots-of-trust integrated to the ECN Security Manager (e.g. for secure boot, for data storage); for each, it must be specified in which phase and under which state the ECN Security Manager integration is performed. It must also be explained how the integration is secured.

The description must additionally include how the provisioning is performed (directly in the ST or referencing the appropriate guidance document).

3 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

For the supervisor to fulfil its security requirements, the operational environment must fulfil the following objectives:

Table 3-1: Security Objectives for the Operational Environment

Description	Reference
ECN Security Manager administrators keep the OS and related library up to date and apply security patches when available. OS updates are verified using digital signature.	*<Reference to the documentation where this is described>*
ECN Security Manager administrators ensure the confidentiality (for symmetric or private keys) and integrity of cryptographic keys and certificates used outside of the ECN Security Manager to encrypt communications or to authenticate the ECN Security Manager.	*<Reference to the documentation where this is described>*
The underlying platform (i.e. OS, hardware, and low-level firmware) provides adequate security, including domain separation (such as a kernel and user mode and isolation between processes) and non-bypassability. In particular, the platform ensures applicative memory separation (no other applicative process can access ECN Security Manager memory). **Application Note** Domain separation and non-bypassability at the OS level should also include anti-exploitation techniques, such as address space layout randomization (ASLR), memory page permissions, stack-based buffer overflow protection	*<Reference to the documentation where this is described>*
The underlying platform (i.e. OS, libraries, hardware, and low-level firmware) provides a secure boot feature which authenticates executable code loaded in memory, from the low-level firmware up to the ECN Security Manager, prior its execution	*<Reference to the documentation where this is described>*
There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the underlying platform (i.e. OS), other than those services necessary for the operation, administration, and support of the ECN Security Manager	*<Reference to the documentation where this is described>*
Those responsible for the ECN Security Manager must ensure that those parts of the ECN Security Manager critical to enforcement of the security policy are protected from physical attacks that might compromise the ECN Security Manager assets, with protections commensurate to the value of those assets.	*<Reference to the documentation where this is described>*
The underlying platform (i.e. OS) provides data-at-rest protection feature for cryptographic keys and certificates used by the ECN Security Manager	*<Reference to the documentation where this is described>*

4 SECURITY REQUIREMENTS AND IMPLEMENTATION

4.1 Security Assurance Requirements

The claimed assurance requirements package is **SESIP2** as defined in [SESIP].

4.1.1 Flaw Reporting Procedure (ALC_FLR.2)

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

<Describe the procedure, including where flaws and security incidents can be reported (website and/or email address), how the reported flaws are handled in a timely manner, and how an application developer/end-user can get informed of the update. If the “Secure update of platform” SFR is removed, you have to provide a strong argumentation here why the platform is not worth getting an update. However, the process to receive the reports of flaws and handling them in a timely manner needs to be described in any case.>

4.2 Security Functional Requirements for Base-SP

In the following Security Functional Requirements, the term **platform** covers the **ECN Security Manager** and the term **application** covers the **Edge Modules**.

4.2.1 Identification and Attestation

4.2.1.1 Verification of Platform Identity

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

Application Note

The user must be able to query:

- The current version of the ECN Security Manager software.
- The current version of the platform firmware/software.
- The current version of the hardware model of the device.
- The current version of the installed applications.

4.2.1.2 Secure Initialization of Platform

The platform ensures its integrity and authenticity during the platform initialization. If the platform integrity and authenticity cannot be ensured, the platform will go to *<list of controlled states>*.

Application Note

- The ECN shall run a suite of self-tests during initial start-up (on power on) to demonstrate the correct operation of all cryptographic functionality.
- The ECN shall transition to non-operational mode and log failures in the audit record and <selection: notify the administrator, <describe any other actions>> when the following types of failure occurs:
  - Failures of the self-test
  - ECN Security Manager software integrity verification failures.

- <If applicable, include additional failures>

4.2.2 Product Life Cycle

4.2.2.1 Secure Install of Application

The application can be installed in the field such that the <*confidentiality,*> integrity and authenticity of the application is maintained.

Application Note

- The platform shall verify that the digital signature verification key used for platform updates is validated to a public key in the Trust Anchor Database.
- The platform shall verify application software using a digital signature mechanism prior to installation.
- The platform shall by default only install applications cryptographically verified by a built-in X.509v3 certificate OR a configured X.509v3 certificate.
- The platform shall not install code if the code signing certificate is deemed invalid.

4.2.2.2 Secure Update of Platform

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

Application Note

- The ECN Security Manager shall verify that the digital signature verification key used for platform updates is validated to a public key in the Trust Anchor Database.
- The ECN Security Manager shall verify application software using a digital signature mechanism prior to installation.
- The ECN Security Manager shall by default only install applications cryptographically verified by a built-in X.509v3 certificate OR a configured X.509v3 certificate.
- The ECN Security Manager shall not install code if the code signing certificate is deemed invalid.
- The ECN Security Manager shall verify that software updates to itself are a current or later version than the current version of the ECN Security Manager.

Guidance Note:

The ST author shall include a reference to the user guidance or provide a description in the “conformance rationale” of how timely security updates are made to the ECN Security Manager. The description shall:

- Include the process for creating and deploying security updates for the platform software. The process description includes the ECN Security Manager developer processes as well as any third-party (carrier) processes. The process description includes each deployment mechanism (e.g., over-the-air updates, per-carrier updates, downloaded updates).
- Express the time window as the length of time, in days, between public disclosure of a vulnerability and the public availability of security updates to the platform.

4.2.2.3 Secure Update of Application

The application can be updated to a newer version in the field such that the <*confidentiality,*> integrity, authenticity of the application is maintained.

Application Note

- The ECN Security Manager shall verify that the digital signature verification key used for ECN Security Manager updates is validated to a public key in the Trust Anchor Database.
- The ECN Security Manager shall not install code if the code signing certificate is deemed invalid.
- The ECN Security Manager shall verify that software updates to the ECN Security Manager are a current or later version of the ECN Security Manager.

4.2.2.4 Factory Reset of Platform

The platform can be reset to the state in which it exists when the product embedding the platform is delivered to the user, before any personal user data, user credentials, or user configuration is present on the platform.

Application Note

The ECN Security Manager shall offer <selection: wipe of protected data, alert the administrator, remove application, list other available remediation actions> upon unenrollment and <selection: other administrator-configured triggers, no other triggers>.

4.2.3 Cryptographic Operations

4.2.3.1 Cryptographic Key Generation

The platform provides a way to generate cryptographic keys for use in *algorithms listed in the table below* as specified in *specifications listed in the table below* for *key lengths listed in the table below*.

Table 4-1: Cryptographic Key Generation Details

Algorithms	Key Lengths	Specifications
RSA schemes	[selection: 2048-bit, 3072-bit]	[FIPS 186-4] Appendix B.3
Elliptic curve-based key establishment schemes	[selection: 256-bit, 384-bit, 521-bit]	[FIPS 186-4] Appendix B.4 or Curve25519 schemes that meet the following: [RFC 7748]
Finite field-based key establishment schemes	[selection: 2048-bit, 3072-bit]	[FIPS 186-4] Appendix B.1

Application Note

Alignment with the CC profile:

- Algorithms and key lengths in Table 4-1 are taken from the [CC Profile]. The choices of the algorithm and key lengths must meet the GP cryptographic algorithm recommendations described in [GP_TEN_053].
- The ST writer may define key lengths greater than the ones defined in Table 4-1.

4.2.3.2 Cryptographic Operation

The platform provides *cryptographic operations listed in the table below* functionality with *algorithms listed in the table below* as specified in *specifications listed in the table below* for key lengths listed *in the table below* and modes listed *in the table below*.

INFO Algorithms under <> are optional and can be removed by the Security Target writer.

Table 4-2: Cryptographic Operation Details

Algorithms / Modes	Operations	Key Size	Specifications
RSA-based key establishment schemes	Key establishment	<selection: 2048-bit, 3072-bit>	[NIST 800-56B]
<Elliptic curve-based key establishment schemes>	Key establishment	<selection: 256-bit, 384-bit, 521-bit>	[NIST 800-56A]
<Finite field-based key establishment schemes>	Key establishment	<selection: 2048-bit, 3072-bit>	[NIST 800-56A]
AES-CBC FIPS	Encryption / Decryption	128-bit and <selection: 256-bit, no other>	[FIPS 197]
AES-CBC	Encryption / Decryption	128-bit and <selection: 256-bit, no other>	[NIST 800-38A]
AES-CCMP	Encryption / Decryption	128-bit and <selection: 256-bit, no other>	[NIST 800-38C] and [802.11-2012]
<AES Key Wrap (KW)>	Encryption / Decryption	128-bit and <selection: 256-bit, no other>	[NIST 800-38F]
<AES Key Wrap with Padding> (KWP)	Encryption / Decryption	128-bit and <selection: 256-bit, no other>	[NIST 800-38F]
<AES-GCM>	Encryption / Decryption	128-bit and <selection: 256-bit, no other>	[NIST 800-38D]
<AES-CCM>	Encryption / Decryption	128-bit and <selection: 256-bit, no other>	[NIST 800-38C]
<AES-XTS>	Encryption / Decryption	128-bit and <selection: 256-bit, no other>	[NIST 800-38E]
<AES-GCMP-256>	Encryption / Decryption	128-bit and <selection: 256-bit, no other>	[NIST 800-38D] and [802.11ac-2013]
<selection: SHA-256, SHA-384, SHA-512>	Cryptographic hashing	None	[FIPS 180-4]
RSA signature schemes	Cryptographic signature services (generation and verification)	<selection: 2048-bit, 3072-bit>	[FIPS 186-4] section 5, The RSA Digital Signature Algorithm

Algorithms / Modes	Operations	Key Size	Specifications
<selection: ECDSA signature schemes>	Cryptographic signature services (generation and verification)	<selection: 256-bit, 384-bit, 521-bit>	[FIPS 186-4] section 6, Elliptic Curve Digital Signature Algorithm (ECDSA)
<selection: HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512>	Keyed-hash message authentication	<key size (in bits) used in HMAC>	[FIPS 198-1] [FIPS 180-4]

Application Note

Alignment with the CC profile:

- Algorithms and key lengths in Table 4-2 are taken from the [CC Profile]. The choices of the algorithm and key lengths must meet the GP cryptographic algorithm recommendations described in [GP_TEN_053].
- The ST writer may define key lengths greater than the ones defined in Table 4-2.

4.2.3.3 Cryptographic Random Number Generation

The platform provides a way based on *an entropy source as described below* to generate random numbers to as specified in *NIST SP 800-90 A* in the following list: *<Hash_DRBG (any), HMAC_DRBG (any) and/or CTR_DRBG (AES)>*.

Entropy source details: source that accumulates entropy from <noise source> with a minimum of <selection: 128 bits, 256 bits> of entropy at least equal to the greatest security strength (according to [NIST 800-57]) of the keys and hashes that it will generate.

Application Note

- Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES) are specified in [NIST 800-90A].
- Noise source can be software-based, or hardware-based if the Platform type from this Base-SP is extended in a SP-Module to also include hardware.
- For the SP-Module “Secure Boot and File System Secure Storage”, the ECN Security Manager shall generate all salts using a RBG that meets this requirement.

4.2.4 Secure Communication

4.2.4.1 Secure Communication Support

The platform provides one or more secure communication channel(s).

The secure communication channel authenticates *another IT trusted product* and protects against *disclosure and modification* of messages between the endpoints, using *the TLS 1.2 cipher suites (RFC 5246) listed below*:

Table 4-3: Allowed TLS Cipher Suites

Cipher Suite	Applicability
TLS_RSA_WITH_AES_128_CBC_SHA256 (RFC 5246)	Mandatory (at least one of them)
TLS_RSA_WITH_AES_256_CBC_SHA256 (RFC 5246)	
TLS_RSA_WITH_AES_256_GCM_SHA384 (RFC 5288)	Optional
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (RFC 5246)	
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (RFC 5246)	
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (RFC 5288)	
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (RFC 5289)	
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (RFC 5289)	
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (RFC 5289)	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (RFC 5289)	
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (RFC 5289)	
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (RFC 5289)	
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (RFC 5289)	
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (RFC 5289)	

Application Notes

Alignment with the CC profile:

- Algorithms and key lengths in Table 4-3 are taken from the [CC Profile]. The choices of the algorithm and key lengths must meet the GP cryptographic algorithm recommendations described in [GP_TEN_053]. The ST writer can add other algorithms in the scope which are not defined in the [CC Profile], e.g. TLS v1.3.

Functionality:

- The ECN Security Manager shall verify that the presented identifier matches the reference identifier according to RFC 6125.
- The ECN Security Manager shall support mutual authentication using X.509v3 certificates.
- The ECN Security Manager shall validate certificates shall be in accordance with the following rules:
  - RFC 5280 certificate validation and certificate path validation.
  - The certificate path must terminate with a certificate in the Trust Anchor Database.
  - The ECN Security Manager shall validate a certificate path by ensuring the presence of the *basicConstraints* extension and that the CA flag is set to TRUE for all CA certificates.
  - The ECN Security Manager shall validate the revocation status of the certificate using [selection: the Online Certificate Status Protocol (OCSP) as specified in RFC 2560, a Certificate Revocation List (CRL) as specified in RFC 5759].
  - The ECN Security Manager shall validate the extendedKeyUsage field according to the following rules:

- Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (idkp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
- Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the *extendedKeyUsage* field.

- The ECN Security Manager shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.
- The ECN Security Manager shall use X.509v3 certificates as defined by RFC 5280 to support authentication for TLS, and [selection: code signing for system software updates, code signing for applications, code signing for integrity verification, [assignment: other uses], no additional uses].
  - When the ECN Security Manager cannot establish a connection to determine the revocation status of a certificate, the ECN Security Manager shall [selection: allow the administrator to choose whether to accept the certificate in these cases, allow the user to choose whether to accept the certificate in these cases, accept the certificate, not accept the certificate].
  - The ECN Security Manager shall not establish a trusted channel if the peer certificate is invalid. It shall provide a certificate validation service to applications and respond to the requesting application with the success or failure of the validation.

A full compliance with the mentioned standards is not required and is restricted only to the specific aspects mentioned above, and compliance is restricted only to the specific aspects mentioned in the SFR.

4.2.5 Extra Attacker Resistance

4.2.5.1 Software Attacker Resistance: Isolation of Platform

The platform provides isolation between the application and itself, such that an attacker able to run code as an application on the platform cannot compromise the other functional requirements.

Guidance Note:

ST author shall describe in the "*conformance rationale*" or provide a reference to the user manual describing the mechanisms in place to prevent Edge modules from modifying the platform software or platform data that governs the behavior of the platform (such as boundary checking of inputs to APIs).

4.2.5.2 Software Attacker Resistance: Isolation of Application Parts

The platform provides isolation between parts of the application, such that an attacker able to run code as one of the *edge modules, edge hub or edge agent* cannot compromise the <*confidentiality and*> integrity of the other application parts.

Application Note:

While memory separation is usually under control of the OS, which is environment, the platform is responsible for separation of other domains, such as filesystem, network, IPC, process identifier. The ST author shall describe in the "*conformance rationale*" the mechanisms in place to provide separation.

4.2.6 Compliance Functionality

4.2.6.1 Audit Log Generation and Storage

The platform generates and maintains an audit log of *events in the table below* and allows access and analysis of these logs following a specific *rules defined in the extra attacker resistance isolation requirements*.

Application Notes

The platform shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions
- All auditable events for the [minimum, basic, detailed, not specified] level of audit
- Administrator management functions, as defined in the fourth column of Table 4-6
- Start-up and shutdown of the OS
- Specifically defined auditable events in the table below
- <add other specifically defined auditable events>
- The platform shall record within each audit record at least the following information:
  - Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event.
  - For each audit event type, based on the auditable event definitions of the functional components included in the SP/ST, <additional information in Table 4-4>.
- The platform shall provide authorized users with the capability to read all audited events and record contents from the audit records.
- The platform shall provide the audit records in a manner suitable for the user to interpret the information.
- The platform shall be able to provide the user a way to select the set of events to be audited from the set of all auditable events based on the following attributes: object identity, user identity, subject identity, host identity, event type (at least one of them must be implemented). If applicable, specify a list of additional attributes that audit selectivity is based upon.
- The platform shall protect the stored audit records in the audit trail from unauthorized deletion.
- The platform shall be able to [prevent] unauthorized modifications to the stored audit records in the audit trail.
- The TSF shall [overwrite the oldest stored audit records] and [no other action] if the audit trail is full.

Table 4-4: Auditable Events

Requirement	Auditable Events	Additional Record Contents
Audit Log Generation and Storage	All modifications to the audit configuration that occur while the audit collection functions are operating.	No additional Information
Cryptographic Key Generation	Failure of key generation activity.	No additional Information
Cryptographic Random Number Generation	Failure of the randomization process.	No additional Information
Secure Communication Support	Failure to establish a TLS session	Reason for failure
	Failure to verify presented identifier	Presented identifier and reference identifier
	Establishment/termination of a TLS session	Non-platform endpoint of connection

Requirement	Auditable Events	Additional Record Contents
	Application initiation of trusted channel	Name of application. Trusted channel protocol. Non-platform endpoint of connection
	Failure to validate X.509v3 certificate.	Reason for failure of validation
	Failure to establish connection to determine revocation status	No additional Information
	Initiation and termination of trusted channel.	Trusted channel protocol. Non-platform endpoint of connection
Software Attacker Resistance: Isolation of Platform Parts Software Attacker Resistance: Isolation of Application Parts	Blocked attempt to modify platform data	Identity of subject. Identity of platform data
Secure Initialization	Measurement of platform software	Integrity verification value
	Initiation of self-test.	None
	Failure of self-test.	None
Secure Update of Platform Secure Install of Application Secure Update of Application	Success or failure of signature verification for software updates.	
	Success or failure of signature verification for Edge modules.	
Authenticated access control	Action performed before authentication.	No additional Information
	Change of settings	Role of user that changed setting. Value of new setting
	Success or failure of function	Role of user that performed function. Function performed. Reason for failure
	Initiation of software update	Version of update
	Initiation of Edge module installation or update	Name and version of Edge module
	Addition or removal of certificate from Trust Anchor Database	Subject name of certificate
Factory Reset of Platform	Unenrollment. Identity of administrator	Remediation action performed

4.2.6.2 Reliable Index

The platform implements a strictly increasing function.

Application Note

The platform shall be able to provide reliable time stamps for its own use.

4.2.7 Access Control

4.2.7.1 Authenticated Access Control

The platform allows only *user, administrator, a common application developer* identified, authenticated, and authorized to allow performing of <*list of allowed resources/operations*>.

Application Note

- The platform shall enforce any information accessible through system services, Edge module data between the platform and Edge module or group of Edge modules. The attributes shall be: Privilege, System service access rights ('No application', 'Privileged' or' All applications'), <*describe the* relevant security attributes>.
- The platform shall:
  - Explicitly authorize access to Edge module or group of Edge modules data is explicitly authorized by <selection: the user, the administrator, Common Application Developer>. The ST author shall include a reference to the user guidance or provide a description in the "conformance rationale" of the rules, based on security attributes, that explicitly authorize access of subjects to objects.
  - The ST author shall include a reference to the user guidance or provide a description in the "conformance rationale" of rules, based on security attributes, that explicitly deny access of Edge module or group of Edge modules to any information accessible through system services and Edge module data.
- The platform shall perform user authentication of the different application and platform part users *as specified in <specifications> enforcing the following access isolations:*

Table 4-5: Access Isolations by Operation

Operations	Users & Privileges
Access to system services with access rights "No application"	None
Access to system services with access rights "Privileged"	Privileged Edge modules
Access to system services with access rights "All applications"	All Edge modules
Access to Edge module private data	Only the Edge module data owner
Access to Edge module public data	Edge module data owner and others
<Others>	

- The platform shall require each user to be successfully identified before allowing any other platform-mediated actions on behalf of that user.
- The platform shall enforce the management access rights related to the users of the different application and platform parts described in the following table:

INFO The Security Target writer must reflect the functions with M Status and identify whether they are User and/or Admin available

Table 4-6: Management Functions

Management Function	Implementation	User	Admin	Only Admin
1. Platform wipe of protected data	M	-	M	-
2. Configure Edge modules installation policy by a) Restricting the sources of Edge modules, b) Specifying a set of allowed Edge modules based on a digital signature or Edge modules name and version (an Edge modules whitelist), c) Denying installation of Edge modules	M	-	M	M
3. Import keys/secrets into the secure key storage	M	O	O	-
4. Destroy imported keys/secrets and any other keys/secrets in the secure key storage	M	O	O	-
5. Import X.509v3 certificates into the Trust Anchor Database	M	-	M	O
6. Remove imported X.509v3 certificates and all X.509v3 certificates in the Trust Anchor Database	M	O	O	-
7. Enroll the ECN Security Manager in management	M	M	-	-
8. Remove Edge modules	M	-	M	O
9. Update ECN Security Manager	M	-	M	O
10. Install Edge modules	M	-	M	O
11. Enable/disable developer modes	M	O	O	O
12. Enable data-at rest protection	O	O	O	O
13. Wipe Edge module data	O	O	O	-
14. Approve import, removal by Edge modules of X.509v3 certificates in the Trust Anchor Database	O	O	O	O
15. Configure whether to establish a trusted channel or disallow establishment if the platform cannot establish a connection to determine the validity of a certificate	M	O	O	O
16. Read audit logs kept by the ECN	O	O	O	-
17. Configure certificate used to validate digital signature on Edge modules	O	O	O	O
18. Configure the auditable events	O	-	O	O
19. Retrieve platform-software integrity verification values	O	O	O	O
Query <other operations> the <set of audit events>	M	-	M	-
<selection: change_default, query, modify, delete, other> security attributes *<list of security attributes>*. **Application Note:** Security attributes shall be initialized with default restrictive values.	M	-	M	-

The first column lists the management functions identified in the SP. In the following columns:

- ‘M’ means Mandatory
- ‘O’ means Optional

The second column, “Implementation”, indicates whether the function is to be implemented. The ST author should select which Optional functions are implemented.

The third column, “User”, indicates functions that are to be restricted to the user (i.e., not available to the administrator).

The fourth column, “Admin”, indicates functions that are available to the administrator. The functions restricted to the user (column 3) cannot also be available to the administrator. Functions available to the administrator can still be available to the user, as long as the function is not restricted to the administrator (column 5). Thus, if the platform must offer these functions to the administrator to perform the fourth column shall be selected.

The fifth column, “Only admin”, indicates whether the function is to be restricted to the administrator when the device is enrolled and the administrator applies the indicated policy. If the function is restricted to the administrator the function is not available to the user. This does not prevent the user from modifying a setting to make the function stricter, but the user cannot undo the configuration enforced by the administrator.

5 SP-MODULES

5.1 Secure Boot and File System Secure Storage

This SP-Module must be flattened with the base-SP for the SP-configuration called Edge Compute Node with Secure Boot and File System Secure Storage.

5.1.1 SESIP References

INFO If the ST writer claims conformance to this SP-Module, this section overwrites section 2.1 “SESIP Profile Reference”.

5.1.1.1 Protection Profile Reference

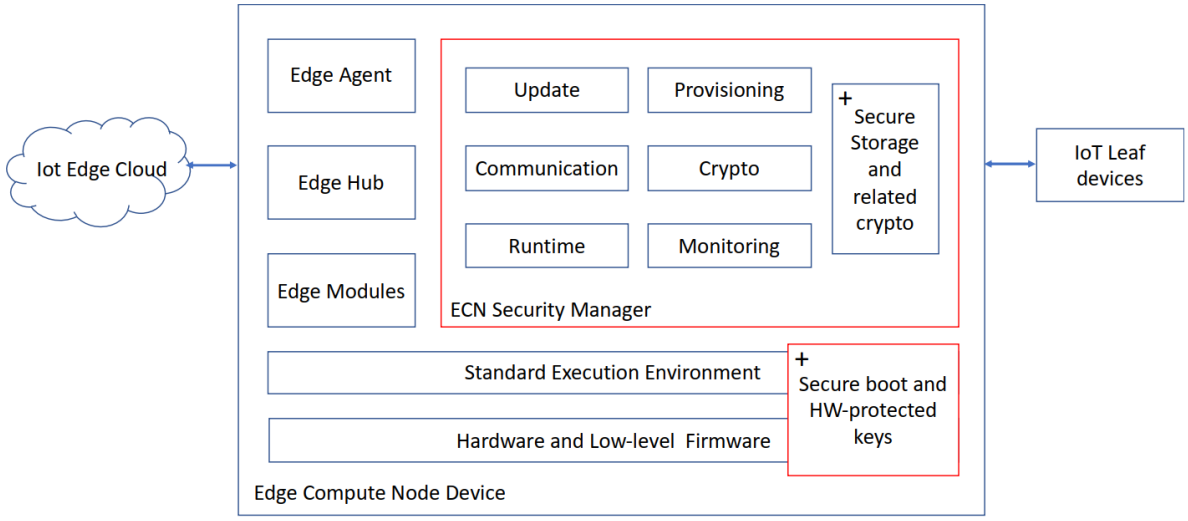
SP name	SESIP Protection Profile for *ECN*
SP-Module name	Secure Boot and File System Secure Storage SP-Module
SP version	*Public review v0.0.0.15*
Platform Type	*ECN Security Manager software*
SP Configuration	*Edge Compute Node with Secure Boot and File System Secure Storage PP-Configuration*
Assurance claim	SESIP2

5.1.2 Platform Component Functional Overview and Description

INFO If the ST writer claims conformance to this SP-Module, this section overwrites section 2.2, “Platform Component Functional Overview and Description”.

This SP-Module extends the Base-SP with a secure boot feature and a secure storage for protected data (data-at-rest protection) on a persistent memory of the Edge Compute Node. The related ECN Security Manager is composed of the ECN Security Manager, as in the Base-SP, extended with the secure boot component and the secure storage component that includes cryptography required for secure storage. The ECN Security Manager is illustrated in red in the following with the additional components for the ECN Security Manager compared to the Base-SP represented with a ‘+’ sign on the corner.

Figure 5-1: Edge Compute Node with Software-Based Secure Storage Platform



5.1.2.1 Usage and Major Security Features

INFO If the ST writer claims conformance to this SP-Module, the content of this section must be added to section 2.2.1, “Usage and Major Security Features”.

The additional security features for the platform of this SP-Module compared to the Base-SP include the following components:

- The Secure storage and related crypto, which protects user data at rest and provides secure storage of cryptographic keys and certificates.
- The Secure boot and hardware-protected keys, which authenticates executable code loaded from boot prior to its execution based on a hardware-protected certificate and provides hardware protection for the cryptographic keys used for secure storage. This low-level firmware and possibly related support from the Standard Execution Environment is outside of the ECN Security Manager and may be device-specific.

5.1.2.2 Platform Type

INFO If the ST writer claims conformance to this SP-Module, this section overwrites section 2.2.2, “Platform Type”.

The platform type is a combination of hardware and software components of an Edge Compute Node featuring a software security manager and hardware support for secure boot and secure storage.

5.1.2.3 Available Non-Platform Hardware/Software/Firmware

INFO If the ST writer claims conformance to this SP-Module, this section overwrites section 2.2.3, “Available Non-Platform Hardware/Software/Firmware”.

Compared to the Base-SP, parts of the hardware and low-level firmware and supporting Operating System related to Secure boot and secure storage are now in the platform.

The available non-platform hardware/software/firmware then consists of:

- The parts of the supporting Operating System (Standard Execution Environment) for the platform not in charge of the secure boot nor secure storage (which have been moved to the platform).
- The Edge Modules that implement local edge computing functions for the network of leaf devices.
- The Edge Hub in charge of communications with the IoT Edge Cloud.

- The Edge Agent in charge of Edge module management.
- The parts of hardware and low-level firmware not in charge of the secure boot (which have been moved to the platform).
- The networked environment with the IoT Edge Cloud and the leaf devices.

5.1.2.4 Platform Security Services

INFO If the ST writer claims conformance to this SP-Module, this security services must be added in section 2.2.4, “Platform Security Services”.

This section summarizes the additional security services provided by the platform along with the ones inherited from the Base-SP and detailed in section 2.2:

User Data Protection: The platform protects user data at rest and provides secure storage of cryptographic keys and certificates.

Secure boot: The platform authenticates executable code loaded from boot prior to its execution.

5.1.3 Security Functional Requirements

INFO This SP-module introduces or refines from the base-SP the following SFRs. All other SFRs from the base-SP also apply to this SP-module.

5.1.3.1 Cryptographic Functionality

5.1.3.1.1 Cryptographic Key Generation

The platform provides a way to generate cryptographic keys for use in *algorithms listed in the table below* as specified in *specifications listed in the table below* for *key lengths listed in the table below*.

Table 5-1: Cryptographic Key Generation Details for the Secure Boot and File System Secure Storage SP-module

ID	Algorithms	Key Lengths	Specifications
Root Encryption Key	<selection: specify one symmetric or asymmetric algorithm>	<specify key lengths with key strength of 112 bits, 128 bits, 192 bits or 256 bits>	<add the specifications>
Data Encryption Keys	AES	128, 256 bits	[NIST 800-57]

ID	Algorithms	Key Lengths	Specifications
Key Encryption Keys	<selection: specify one symmetric or asymmetric algorithm>	<specify key lengths with key strength greater than or equal to 112 bits>	<selection: • generate the KEK using a key generation scheme that meets this profile (as specified in section 4.2.3.1) or • Combine the KEK from other KEKs in a way that preserves the effective entropy of each factor by [selection: using an XOR operation, concatenating the keys and use a KDF (as described in [NIST 800-108]), encrypting one key with another]. >

Application Note:

Alignment with the CC profile:

- Algorithms and key lengths in Table 4-1 are taken from the [CC Profile]. The choices of the algorithm and key lengths must meet the GP cryptographic algorithm recommendations described in [GP_TEN_053].
- The ST writer may define key lengths greater than the ones defined in Table 4-1.

For the Root Encryption Key:

- It shall mutable hardware-protected or immutable hardware-protected.
- It shall not be able to be read from or exported from the hardware.
- Each REK shall be generated by a RBG in accordance with RNG defined in section 4.2.3.3, “Cryptographic Random Number Generation”.

5.1.3.1.2 Cryptographic KeyStore

The platform provides a way to store <list of assets, such as cryptographic keys and passwords> such that not even the application can compromise the *integrity, confidentiality* <selection: authenticity > of this data. This data can be used for the cryptographic operations <list of operations>.

Application Note:

- The ECN Security Manager shall provide Hardware-based or software-based secure key storage
- List of assets must include asymmetric private keys and optionally, symmetric keys and/or persistent secrets.
- ECN Security Manager shall be capable of importing keys/secrets into the secure key storage upon request of <selection: the user or the administrator> and <selection: applications running on the platform, no other subject >

- The ECN Security Manager shall be capable of destroying keys/secrets in the secure key storage upon request of <selection: the user, the administrator].
- The ECN Security Manager shall have the capability to allow only the application that imported the key/secret the use of the key/secret. Exceptions may only be explicitly authorized by <selection: the user, the administrator, a common application developer].
- The ECN Security Manager shall allow only the application that imported the key/secret to request that the key/secret be destroyed. Exceptions may only be explicitly authorized by <selection: the user, the administrator, a common application developer>
- The ECN Security Manager shall encrypt all DEKs and KEKs and <selection: persistent TLS key material, all software-based key storage, no other keys> by KEKs that are protected by the REK with <selection: encryption by a REK, encryption by a KEK chaining to a REK, encryption by a KEK that is derived from a REK>.
- DEKs and KEKs and <selection: persistent TLS key material, all software-based key storage, no other keys> shall be encrypted using one of the following methods: <selection: using a SP800-56B key establishment scheme, using AES in the <selection: Key Wrap (KW) mode, Key Wrap with Padding (KWP) mode, GCM, CCM, CBC mode>>.
- The ECN Security Manager shall protect the integrity of any encrypted DEKs and KEKs and <selection: persistent TLS key material, all software-based key storage, no other keys> by at least one of the following methods:
  - <selection: GCM, CCM, Key Wrap, Key Wrap with Padding> cipher mode for encryption;
  - a hash of the stored key that is encrypted by a key protected by “Cryptographic KeyStore”;
  - a keyed hash using a key protected by a key protected by “Cryptographic KeyStore”;
  - a digital signature of the stored key using an asymmetric key protected according to “Cryptographic KeyStore”.
- The ECN Security Manager shall verify the integrity of the <selection: hash, digital signature, MAC> of the stored key prior to use of the key
- The ECN Security Manager shall not store any plaintext key material in readable non-volatile memory
- The ECN Security Manager shall not transmit any plaintext key material outside the security boundary of the ECN Security Manager
- The ECN Security Manager shall ensure it is not possible for the ECN Security Manager user(s) to export plaintext keys

5.1.3.2 Compliance Functionality

5.1.3.2.1 Secure Trusted Storage

The platform ensures that all data stored, except for <list of data stored in plaintext>, is protected to ensure its integrity, authenticity and binding to the platform instance.

Application Note:

- Encryption shall be performed using DEKs with AES in XTS, CBC or GCM modes.
- The platform shall destroy cryptographic keys in accordance with the specified cryptographic key destruction methods by clearing the KEK encrypting the target key and destroying all plaintext keying material and critical security parameters when no longer needed that meets the following.

Depending of the type of memory, key destruction can be performed by one of the following methods, to be specified in TSS.

- For volatile memory, the destruction shall be executed by a single direct overwrite consisting of a pseudo-random pattern using the platform's RBG or consisting of zeroes.
- For non-volatile EEPROM, the destruction shall be executed by a single direct overwrite consisting of a pseudo random pattern using the platform's RBG (as specified in FCS_RBG_EXT.1), followed by a read-verify.
- For non-volatile flash memory, that is not wear-leveled, the destruction shall be executed by a single direct overwrite consisting of zeros followed by a read-verify or by a block erase that erases the reference to memory that stores data as well as the data itself.
- For non-volatile flash memory, that is wear-leveled, the destruction shall be executed by a single direct overwrite consisting of zeros or by a block erase.
- For non-volatile memory other than EEPROM and flash, the destruction shall be executed by a single direct overwrite with a random pattern that is changed before each write.

- The platform shall wipe all protected data at rest by <describe the data wipe procedure>. The platform shall perform a power cycle on conclusion of the wipe procedure.

5.1.3.3 Identification and Attestation of Platforms and Applications

5.1.3.3.1 Secure Initialization of Platform

The platform ensures its integrity and authenticity during platform initialization. If the platform integrity or authenticity cannot be ensured, the platform will go to <list of controlled states>.

Application Note:

- The ECN Security Manager shall verify the integrity of the bootchain up through the Standard Execution Environment, and <selection: all executable code stored in mutable media, [assignment: list of other executable code], no other executable code>, stored in mutable media prior to its execution through the use of [selection: a digital signature using an immutable hardware-protected asymmetric key, an immutable hardware-protected hash of an asymmetric key, an immutable hardware-protected hash, a digital signature using a mutable hardware-protected asymmetric key].
- The ECN Security Manager shall not execute code if the code signing certificate is deemed invalid.

5.2 Support for HSM-Based Secure Storage and Cryptography

This SP-Module must be flattened with the Base-SP for the configuration called Edge Compute Node with Support for HSM-Based Secure Storage and Cryptography.

5.2.1 SESIP References

INFO If the ST writer claims conformance to this SP-Module, this section overwrites section 2.1 “SESIP Profile Reference”.

5.2.1.1 Protection Profile Reference

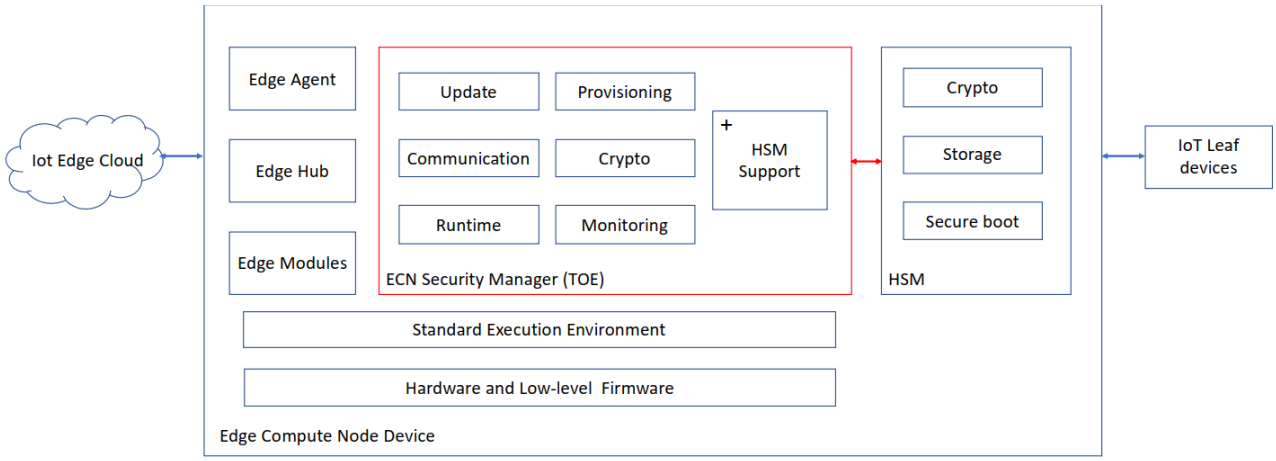
SP name	SESIP Protection Profile for *ECN*
SP-Module name	Support for HSM-Based Secure Storage and Cryptography SP-Module
SP version	*Public review v0.0.0.15*
Platform Type	*ECN Security Manager software extended with secure communication with a trusted IT product*
SP Configuration	*Edge Compute Node with Secure Boot and File System Secure Storage PP-Configuration*
Assurance claim	SESIP2

5.2.2 Platform Component Functional Overview and Description

INFO If the ST writer claims conformance to this SP-Module, this section overwrites section 2.2, “Platform Component Functional Overview and Description”.

This SP-Module extends the Base-SP with a secure boot feature and a secure storage for protected data (data-at-rest protection) supported by a HSM located in the operational environment of the ECN Security Manager. The related platform is composed of the ECN Security Manager, as in the Base-SP, extended with support of the interaction with the HSM. The ECN Security Manager is illustrated in red in Figure 28 where the additional components for the ECN Security Manager compared to the Base-SP are represented with a ‘+’ sign on the corner.

Figure 5-2: Edge Compute Node with HSM-Based Secure Storage and Cryptography



5.2.2.1 Usage and Major Security Features

INFO If the ST writer claims conformance to this SP-Module, the content of this section must be added to section 2.2.1, “Usage and Major Security Features”.

The additional security features for the platform of this SP-Module compared to the Base-SP include the following components:

The Secure storage and related crypto, which protects user data at rest and provides secure storage of cryptographic keys and certificates.

The Secure boot and hardware-protected keys, which authenticates executable code loaded from boot prior to its execution based on a hardware-protected certificate and provides hardware protection for the cryptographic keys used for secure storage. This low-level firmware and possibly related support from the Standard Execution Environment is outside of the ECN Security Manager and may be device-specific.

5.2.2.2 Platform Type

INFO If the ST writer claims conformance to this SP-Module, the content of this section must be added to section 2.2.2, “Platform Type”.

The additional security feature for the platform of this SP-Module compared to the Base-SP includes the following:

Secure communication with trusted IT product (HSM).

5.2.2.3 Available Non-Platform Hardware/Software/Firmware

INFO If the ST writer claims conformance to this SP-Module, this section overwrites section 2.2.3, “Available Non-Platform Hardware/Software/Firmware”.

Compared to the Base-SP, the non-platform hardware/software/firmware is extended with a Hardware Security Module (HSM) peripheral, such as Trusted Platform Module (TPM) or a Dedicated Security Component (DSC).

This HSM is used as a root of trust for the platform and is responsible for:

Contributing to the secure boot of the platform and the platform, by measuring executable code prior to execution and comparing this measure to a reference value;

Managing sensitive assets for the platform, in particular cryptographic keys and certificates;

Offering cryptographic operation services to the platform, based on the keys managed by the HSM.

5.2.3 Security Objectives for the Operational Environment

INFO If the ST writer claims conformance to this SP-Module, the following Security Objectives for the environment must be added to section 3, “Security Objectives for the Operational Environment”.

Table 5-2: Security Objectives for the Operational Environment

Description	Reference
The OS provides data-at-rest protection feature for cryptographic keys and certificates used by the platform in combination with a HSM. The HSM is used as a root of trust by the platform for the operations described in section 5.2.2 (secure boot, cryptographic operation services). The HSM is [FIPS 140-2] or [FIPS 140-3] certified. The HSM is also certified at least EAL3 augmented with ALC_FLR.1 and AVA_VAN.3 according to either [TPM PP] or [DSC PP]	*<Reference to the documentation where this is described>*

5.2.4 Security Functional Requirements

INFO This SP-module introduces or refines from the base-SP the following SFRs. All other SFRs from the base-SP also apply to this SP-module.

5.2.4.1 Compliance Functionality

5.2.4.1.1 Audit Log Generation and Storage

The platform generates and maintains an audit log of *events in the table below* and allows access and analysis of these logs following a specific *rules defined in the extra attacker resistance isolation requirements*.

Application Notes

The platform shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions
- All auditable events for the <selection, choose one of: minimum, basic, detailed, not specified> level of audit
- Administrator management functions, as defined in the fourth column of Table 4-6
- Start-up and shutdown of the OS
- Specifically defined auditable events in Table 4-4 and Table 5-3
- <add other specifically defined auditable events>

The ST must refer to the section of the user guidance describing how the following implementation requirements are met:

- Each record must contain: date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event.
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, additional information in Table 4-4 and Table 5-3.

Table 5-3: Auditable Events

Requirement	Auditable Events	Additional Record Contents
Secure Initialization of Platform	Measurement of platform software	Integrity verification value.
	Initiation of external entity test	None
	Failure of external entity test	None
Secure Communication Support **Secure Communication Enforcement**	Failure of data consistency checks	

5.2.4.2 Identification and Attestation of Platforms and Applications

5.2.4.2.1 Secure Initialization of Platform

The platform ensures its integrity and authenticity during the platform initialization. If the platform integrity or authenticity cannot be ensured, the platform will go to <*list of controlled states*>.

Application Note

- The ECN shall run a suite of self-tests during initial start-up (on power on) to demonstrate the correct operation of all cryptographic functionality.
- The ECN shall transition to non-operational mode and log failures in the audit record <[selection: notify the administrator, [if applicable, define other actions], no other actions> when the following types of failure occurs:
  - Failures of the self-test
  - Platform software integrity verification failures.
  - HSM integrity verification failures
  - <If applicable, include additional failures>
- The ECN shall run a suite of tests <selection: during initial start-up, periodically during normal operation, at the request of an authorized user, <specify other conditions (if applicable)>> to check the fulfilment of integrity of the HSM. If the test fails, it shall be handled as described in this SFR. If applicable, the ST author shall describe in the "*conformance rationale*" any other actions that are implemented after this failure occurs.
- In order to check integrity of the HSM, the platform can for instance check ID of the HSM, use HSM attestation service, read integrity registers, check tamper-detection registers, perform known answer tests for cryptographic operations.

5.2.4.3 Secure Communication

5.2.4.3.1 Secure Communication Support

The platform provides one or more secure communication channel(s).

The secure communication channel authenticates *another IT trusted product* and protects against *disclosure and modification* of messages between the endpoints, using <list of protocols and measures>.

Application Note

- The ECN Security Manager shall provide the capability to consistently interpret data exchanged with the HSM when shared between the platform and another trusted IT product.
- The ECN Security Manager shall use the specification of HSM commands / responses when interpreting the platform data from another trusted IT product.
- The ECN Security Manager shall provide assured identification of its end points and protection of the channel data from modification or disclosure.
- The platform shall permit itself to initiate communication via the trusted channel.
- The ECN Security Manager shall initiate communication via the trusted channel for [all cryptographic and secure storage functions provided by the HSM.

5.2.4.3.2 Secure Communication Enforcement

The platform ensures that communication with *another IT trusted product* can only be done over the communication channel(s) supported by the platform using <*list of protocols and measures*>.

Application Note

- The ECN Security Manager shall provide the capability to consistently interpret data exchanged with the HSM when shared between the platform and another trusted IT product.
- The ECN Security Manager shall use the specification of HSM commands / responses when interpreting the platform data from another trusted IT product.
- The ECN Security Manager shall provide assured identification of its end points and protection of the channel data from modification or disclosure.
- The platform shall permit itself to initiate communication via the trusted channel.
- The ECN Security Manager shall initiate communication via the trusted channel for [all cryptographic and secure storage functions provided by the HSM.

5.3 Support for Secure Enclave-Based Secure Storage and Cryptography SP-Module

This SP-Module must be flattened with the Base-SP for the configuration called Edge Compute Node with Support for Secure Enclave-Based Secure Storage and Cryptography.

5.3.1 SESIP References

INFO If the ST writer claims conformance to this SP-Module, this section overwrites section 2.1 “SESIP Profile Reference”.

5.3.1.1 Protection Profile Reference

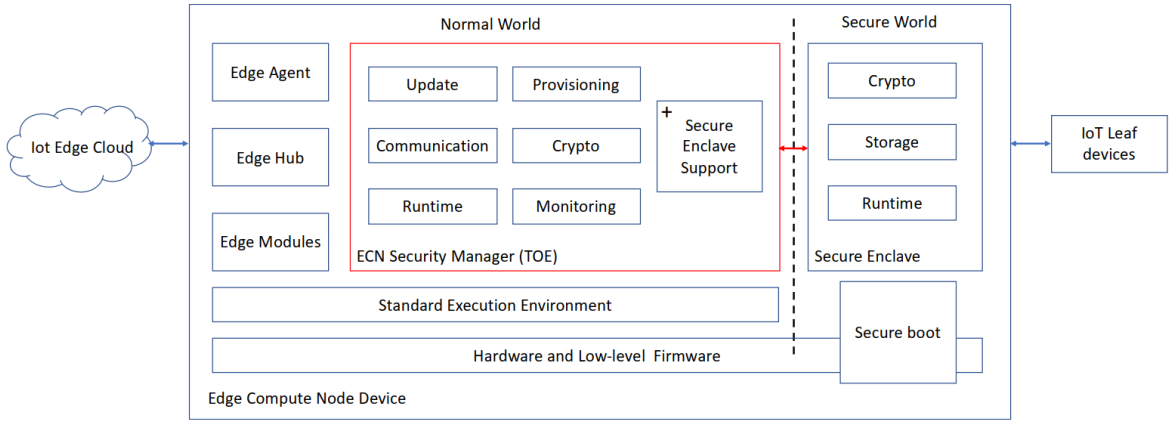
SP name	SESIP Protection Profile for *ECN*
SP-Module name	Support for Secure Enclave-Based Secure Storage and Cryptography SP-Module
SP version	*Public review v0.0.0.15*
Platform Type	*ECN Security Manager software*
SP Configuration	*Edge Compute Node with Secure Boot and File System Secure Storage PP-Configuration*
Assurance claim	SESIP2

5.3.2 Platform Component Functional Overview and Description

INFO If the ST writer claims conformance to this SP-Module, this section overwrites section 2.2, “Platform Component Functional Overview and Description”.

This SP-Module extends the Base-SP with a secure boot feature and a secure storage for protected data (data-at-rest protection) supported by a Secure Enclave located in the operational environment of the platform. The related platform is composed of the ECN Security Manager, as in the Base-SP, extended with support of the interaction with the Secure Enclave. The platform is illustrated in red in the following figure where the additional components for the platform compared to the Base-SP are represented with a ‘+’ sign on the corner.

Figure 5-3: Edge Compute Node with Secure Enclave Platform



5.3.2.1 Usage and Major Security Features

INFO If the ST writer claims conformance to this SP-Module, the content of this section must be added to section 2.2.1, “Usage and Major Security Features”.

The additional security feature for the platform of this SP-Module compared to the Base-SP includes the following:

Secure communication with trusted IT product (Secure Enclave).

5.3.2.2 Platform Type

INFO If the ST writer claims conformance to this SP-Module, this section overwrites section 2.2.2, “Platform Type”.

The platform type is a software featuring the security manager for Edge Compute Node extended with secure communication with a trusted IT product.

5.3.2.3 Available Non-Platform Hardware/Software/Firmware

INFO If the ST writer claims conformance to this SP-Module, this section overwrites section 2.2.3, “Available Non-Platform Hardware/Software/Firmware”.

Compared to the Base-SP, the non-platform hardware/software/firmware is extended with a Secure Enclave isolated from the Standard Execution Environment with hardware support, such as ARM TrustZone® or Intel® SGX (Software Guard Extension).

This Secure Enclave is used as a root of trust for the platform. It is responsible for:

Contributing to the secure boot of the platform and the platform, by measuring executable code prior to execution and comparing this measure to a reference value;

Managing sensitive assets for the platform, in particular cryptographic keys and certificates;

Offering cryptographic operation services to the platform, based on the keys managed by the Secure Enclave.

5.3.3 Security Objectives for the Operational Environment

INFO If the ST writer claims conformance to this SP-Module, the following Security Objectives for the environment must be added to section 3, “Security Objectives for the Operational Environment”.

Table 5-4: Security Objectives for the Operational Environment

Description	Reference
The OS provides data-at-rest protection feature for cryptographic keys and certificates used by the platform in combination with a Secure Enclave. The Secure Enclave is used by the platform for the operations described in section 5.3.2 (secure boot, cryptographic operation services). The Secure Enclave is [FIPS 140-2] or [FIPS 140-3] certified. The Secure Enclave is also certified according to [TEE PP] or [TEE PP] with the Trusted I/O SP-Module [TEE PP I/O].	*<Reference to the documentation where this is described>*

5.3.4 Security Functional Requirements

INFO This SP-module introduces or refines from the base-SP the following SFRs. All other SFRs from the base-SP also apply to this SP-module.

5.3.4.1 Compliance Functionality

5.3.4.1.1 Audit Log Generation and Storage

The platform generates and maintains an audit log of <list of significant security events> and allows access and analysis of these logs following a specific <access control policy>.

Application Notes

The platform shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions
- All auditable events for the <selection, choose one of: minimum, basic, detailed, not specified> level of audit
- Administrator management functions, as defined in the fourth column of Table 4-6
- Start-up and shutdown of the OS
- Specifically defined auditable events in Table 4-4 and Table 5-5
- <add other specifically defined auditable events>

The ST must refer to the section of the user guidance describing how the following implementation requirements are met:

- Each record must contain: date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event.
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, additional information in Table 4-4 and Table 5-3.

Table 5-5: Auditable Events

Requirement	Auditable Events	Additional Record Contents
Secure Initialization of Platform	Measurement of platform software	Integrity verification value.
	Initiation of external entity test	None
	Failure of external entity test	None
Secure Communication Support **Secure Communication Enforcement**	Failure of data consistency checks	

5.3.4.2 Identification and Attestation of Platforms and Applications

5.3.4.2.1 Secure Initialization of Platform

The platform ensures its authenticity and integrity during platform initialization. If the platform authenticity or integrity cannot be ensured, the platform will go to <list of controlled states>.

Application Note

- The ECN shall transition to non-operational mode and log failures in the audit record <[selection: notify the administrator, [if applicable, define other actions], no other actions> when the following types of failure occurs:
  - Failures of the self-test
  - Platform software integrity verification failures.
  - Secure Enclave integrity verification failures
  - <If applicable, include additional failures>
- The ECN Security Manager shall run a suite of tests <selection: during initial start-up, periodically during normal operation, at the request of an authorized user, <specify other conditions (if applicable)>> to check the fulfilment of integrity of the Secure Enclave. If the test fails, it shall be handled as described in this SFR. If applicable, the ST author shall describe in the "*conformance rationale*" any other actions that are implemented after this failure occurs.
- In order to check integrity of the Secure Enclave, the ECN Security Manager can for instance check ID of the Secure Enclave, use Secure Enclave attestation service, read integrity registers, check tamper-detection registers, perform known answer tests for cryptographic operations.

5.3.4.3 Secure Communication

5.3.4.3.1 Secure Communication Support

The platform provides the application with one or more secure communication channel(s).

The secure communication channel authenticates *another IT trusted product* and protects against <list of attacks including disclosure, modification, replay, erasure> of messages between the endpoints, using <list of protocols and measures>.

Application Note

- The ST author shall describe in the "*conformance rationale*" how the platform provides assured identification of its end points and protection of the channel data from modification or disclosure.
- The ECN Security Manager shall provide the capability to consistently interpret data exchanged with the Secure Enclave when shared between the platform and another trusted IT product.
- The ECN Security Manager shall use the specification of Secure Enclave commands / responses when interpreting the platform data from another trusted IT product.

5.3.4.3.2 Secure Communication Enforcement

The platform ensures that the application can only communicate with *another IT trusted product* over the secure communication channel(s) supported by the platform using <list of protocols and measures>.

Application Note

- The ECN Security Manager shall initiate communication via trusted channel for all cryptographic and secure storage functions provided by the Secure Enclave.
- The ECN Security Manager shall provide the capability to consistently interpret data exchanged with the Secure Enclave when shared between the platform and another trusted IT product.
- The ECN Security Manager shall use the specification of Secure Enclave commands / responses when interpreting the platform data from another trusted IT product.

6 MAPPING AND SUFFICIENCY RATIONALES

6.1 Assurance

The assurance activities defined in this document fulfil the SESIP2 activities.

Table 6-1: Assurance Mapping and Sufficiency Rationales

Assurance Class	Assurance Families	Covered by	Rationale
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	Section “Introduction” of the Security Target.	*<The ST writer must complete this rationale.* *Add a reference to the Security Target sections covering the ST reference, the Platform reference, and the Platform description>*
	ASE_OBJ.1 Security requirements for the operational environment	Section “Security Objective for the Operational Environment” of the Security Target.	*< The ST writer must complete this rationale.* *The objectives for the operational environment defined in the Security Target must refer to the guidance documents>*
	ASE_REQ.3 Listed Security requirements	Section “Security Requirements and Implementation” of the Security Target.	*<The ST writer must complete this rationale.* *All the SFRs defined in the Security Target must be defined in this SESIP profile or [GP_FST_070].* *The Security Target must also include the following SFRS: "Identification of Platform Type" and "Secure Update of Platform".>*
	ASE_TSS.1 TOE Summary Specification	Section “Security Requirements and Implementation” of the Security Target.	*< The ST writer must complete this rationale.* *A conformance rationale must be provided by each SFR defined in the Security Target.>*
ADV: Development	ADV_FSP.4 Complete functional specification	Material to be provided to the evaluation laboratory	The security evaluation laboratory will determine if the provided evidence is suitable to meet this requirement.

Assurance Class	Assurance Families	Covered by	Rationale
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	Material to be provided to the evaluation laboratory	The security evaluation laboratory will determine if the provided evidence is suitable to meet this requirement.
	AGD_PRE.1 Preparative procedures	Material to be provided to the evaluation laboratory	The security evaluation laboratory will determine if the provided evidence is suitable to meet this requirement.
ALC: Life-cycle support	ALC_FLR.2 Flaw reporting procedures	Material to be provided to the evaluation laboratory	*<The ST writer must complete this rationale.* *Add a reference to the Security Target sections describing the flaw remediation procedures.>*
ATE: Test	ATE_IND.1 Independent testing: conformance	Laboratory evaluation activities	The security evaluation laboratory will perform functional testing to determine if the platform meets the requirements.
AVA: Vulnerability analysis	AVA_VAN.2 Vulnerability analysis	Laboratory evaluation activities	The security evaluation laboratory will perform penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE. Penetration testing is performed by the evaluator assuming an attack potential of Basic.

6.2 Functionality

6.2.1 Base-SP

Table 6-2: Functionality Mapping and Sufficiency Rationales for Base-SP

SFR from PP	Covered by SESIP SFR	Rationale
FAU_GEN.1	Audit Log Generation and Storage	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FAU_SAR.1	Audit Log Generation and Storage	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FAU_SEL.1	Audit Log Generation and Storage	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FAU_STG.1	Audit Log Generation and Storage	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FAU_STG.4	Audit Log Generation and Storage	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FCS_CKM.1	Cryptographic Key Generation	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FCS_COP.1(KE)	Cryptographic Operation	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FCS_COP.1(SYM)	Cryptographic Operation	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FCS_COP.1(HASH)	Cryptographic Operation	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FCS_COP.1(SIGN)	Cryptographic Operation	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FCS_COP.1(HMAC)	Cryptographic Operation	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FCS_CKM.4	Secure Communication Support Secure Communication Enforcement	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FCS_RBG_EXT.1	Cryptographic Random Number Generation	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FCS_SRV_EXT.1	Cryptographic Operation	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FCS_TLS_EXT.1	Secure Communication Support Secure Communication Enforcement	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FDP_ACC.1	Authenticated access control	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FDP_ACF.1	Authenticated access control	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>

SFR from PP	Covered by SESIP SFR	Rationale
FMT_MSA.1	Authenticated access control	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FMT_MSA.3	Authenticated access control	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FIA_UID.2	Authenticated access control	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FMT_MOF_EXT.1	Authenticated access control	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FMT_MTD.1	Authenticated access control	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FCS_X509_EXT.1	Secure Communication Support Secure Communication Enforcement	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FCS_X509_EXT.2	Secure Communication Support Secure Communication Enforcement	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FCS_X509_EXT.3	Secure Communication Support Secure Communication Enforcement	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FMT_SMF.1	Secure Communication Support Secure Communication Enforcement	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FMT_SMR.1	Secure Communication Support Secure Communication Enforcement	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FMT_SMR.2	Secure Communication Support Secure Communication Enforcement	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FPT_AEX_EXT.1	Software Attacker Resistance: Isolation of Platform Software Attacker Resistance: Isolation of Application Parts	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FPT_FLS_EXT.1	Secure initialization of Platform	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FPT_STM.1	Reliable Index	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FPT_SRA_EXT.1	Factory Reset of Platform	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FPT_TST_EXT.1	Secure initialization of Platform	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FPT_TUD_EXT.1	Verification of Platform Identity	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FPT_TUD_EXT.2	Secure Update of Platform Secure Install of Application Secure Update of Application	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>

SFR from PP	Covered by SESIP SFR	Rationale
FTP_ITC.1	Secure Communication Support Secure Communication Enforcement	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>

6.2.2 Secure Boot and File System Secure Storage SP-Module

Table 6-3: Functionality Mapping and Sufficiency Rationales for SP-module Secure Boot and File System Secure Storage

SFR from PP	Covered by SESIP SFR	Rationale
FCS_CKM_EXT.1	Cryptographic Key Generation	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FCS_CKM_EXT.2	Cryptographic Key Generation	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FCS_CKM_EXT.3	Cryptographic Key Generation	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FCS_CKM_EXT.4	Cryptographic Random Number Generation	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FCS_CKM_EXT.5	Cryptographic Random Number Generation	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FCS_STG_EXT.1	Cryptographic KeyStore	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FCS_STG_EXT.2	Cryptographic KeyStore	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FCS_STG_EXT.3	Cryptographic KeyStore	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FDP_DAR_EXT.1	Secure Encrypted Storage	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FDP_DAR_EXT.2	Secure Encrypted Storage	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FPT_TST_EXT.2	Secure Initialization of Platform	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FPT_KST_EXT.1	Cryptographic KeyStore	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FPT_KST_EXT.2	Cryptographic KeyStore	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FPT_KST_EXT.3	Cryptographic KeyStore	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>

6.2.3 Support for HSM-Based Secure Storage and Cryptography SP-Module

Table 6-4: Functionality Mapping and Sufficiency Rationales for SP-module Support for HSM-Based Secure Storage and Cryptography

SFR from PP	Covered by SESIP SFR	Rationale
FAU_GEN.1	Audit Log Generation and Storage	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FPT_FLS_EXT.1	Secure Initialization	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FPT_TDC.1	Secure Communication Support Secure Communication Enforcement	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FPT_TEE.1	Secure Initialization	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FTP_ITC.1(HSM)	Secure Communication Support Secure Communication Enforcement	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>

6.2.4 Support for Secure Enclave Secure Storage and Cryptography SP-Module

Table 6-5: Functionality Mapping and Sufficiency Rationales for SP-module Support for Secure Enclave Secure Storage and Cryptography

SFR from PP	Covered by SESIP SFR	Rationale
FAU_GEN.1	Audit Log Generation and Storage	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FPT_FLS_EXT.1	Secure Initialization of Platform	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FPT_TDC.1	Secure Communication Support Secure Communication Enforcement	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FPT_TEE.1	Secure Initialization	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>
FTP_ITC.1(Enclave)	Secure Communication Support Secure Communication Enforcement	<Describe how the SESIP SFR covers the SFR defined in [CC Profile]>