EUROSMART
The Voice of the Digital Security Industry

Security IC Platform Multi-assurance PP-Configurations

Version 1.0

16 December 2025

developed by

Infineon Technologies AG

NXP Semiconductors

STMicroelectronics

Thales

Registered and certified by
Bundesamt für Sicherheit in der Informationstechnik (BSI)

This page is intentionally left blank.

Table of contents

List of tables

List of Figures

1 Introduction

1 This document defines a set of PP-Modules and a family of multi-assurance PP-Configurations for the Security IC Platform Protection Profile [7], also referred to as PP-0084-v2 in this document.

2 The PP-Modules address functionality that is already in the scope of the PP-0084-v2 but at a strictly higher assurance level including ADV_SPM.1. These are:

- PP-Module Authentication of the Security IC,
- PP-Module Loader 1 (for usage in secured environment only),
- PP-Module Loader 2 (for usage by authorised users only),
- PP-Module Address-based Access Control,
- PP-Module Limited Test Features.

3 The PP-Configurations consist of the core PP-0084-v2[1], possibly including some selected functional packages, and a non-empty subset of PP-Modules.

4 The inclusion (or claim) of functional packages from PP-0084-v2 in the PP-Configurations defined in this document is constrained as follows:

- Package Cryptographic Services can be included in any PP-Configuration,
- Package Authentication of the Security IC can be included if the PP-Module Authentication of the Security IC is not included in the PP-Configuration,
- Packages Loader 1, Loader 2, and Address-based Access Control cannot be included in any PP-Configuration. That is, these can only be included through the corresponding PP-Modules as they define the minimum formal model scope for ADV_SPM.1.

5 The combinatory of functional packages and PP-Modules gives rise to a set of multi-assurance PP-configurations, which are defined altogether in section 2. Each PP-Configuration is identified with a unique reference, which reflects its components. The definition of the PP-Configurations is factorized due to their large number.

2 PP-Configurations

2.1 Identification

6 The reference of a PP-Configuration consists of its name and version, where the name is structured as shown in Table 2-1.

Table 2-1: PP-Configuration with Packages [p] and PP-Modules [m]

Name:	Security IC Platform PP-Configuration with Packages [**p**] and PP-Modules [**m**] where **p** is a subset of the functional packages {Authentication of the Security IC, Cryptographic Services},

[1] Core PP-0084-v2 denotes the PP-0084-v2 without any optional functional package.

	m is a non-empty subset of the PP-Modules {Authentication of the Security IC, Loader 1, Loader 2, Address-based Access Control, Limited Test Features}, and **p** and **m** do not both include Authentication of the Security IC
Version:	1.0
Date:	16/12/2025
Sponsored by:	Infineon Technologies AG, NXP Semiconductors, STMicroelectronics, and Thales
Technical editor:	Internet of Trust, 77 avenue Niel, 75017 Paris, France
CC edition:	CC:2022 Revision 1
Assurance type:	Multi-assurance

7 For example, the following PP-Configuration names are valid:

- Security IC Platform PP-Configuration with Packages [Cryptographic Services] and PP-Modules [Authentication of the Security IC, Loader 1, Loader 2, Address-based Access Control, Limited Test Features],
- Security IC Platform PP-Configuration with Packages [Cryptographic Services] and PP-Modules [Loader 1],
- Security IC Platform PP-Configuration with Packages [none] and PP-Modules [Loader 1, Loader 2, Address-based Access Control].

2.2 Components Statement

2.2.1 PP-Configuration Components

8 The components of a PP-Configuration consist of the core PP-0084-v2 with selected functional packages, and a non-empty set of PP-Modules, as shown in Table 2-2.

Table 2-2: PP-Configuration components

Component name and version		Is a component?
PP	Core PP-0084-v2, optionally including Package Authentication of the Security IC and/or Package Cryptographic Services, v2.0	Yes*
PP-Modules	PP-Module Authentication of the Security IC, v1.0	Optionally**
	PP-Module Loader 1, v1.0	Optionally**
	PP-Module Loader 2, v1.0	Optionally**
	PP-Module Address-based Access Control, v1.0	Optionally**
	PP-Module Limited Test Features, v1.0	Optionally**
* If the PP-Module Authentication of the Security IC is a component of the PP-Configuration, then the Package Authentication of the Security IC is not included. ** At least one PP-Module is included as a component.		

9 Since the selectable PP-Modules have PP-0084-v2 as base PP, the set of components is well-defined.

2.2.2 TSF Organization

2.2.2.1 Overview

10 The TSF of a Security IC Platform Multi-Assurance PP-Configuration consists of the union of its components' sub-TSFs. Figure 1 shows the dependency graph between the sub-TSFs, which is straightforward: all the selectable PP-Modules depend on the core PP-0084-v2, i.e. there is no dependency on the optional functional packages and there is no inter-dependency between the PP-Modules. The Package Authentication of the Security IC can only be included if the corresponding PP-Module is not. All the selectable PP-Modules include higher assurance requirements than PP-0084-v2, i.e. they include ADV_SPM.1.

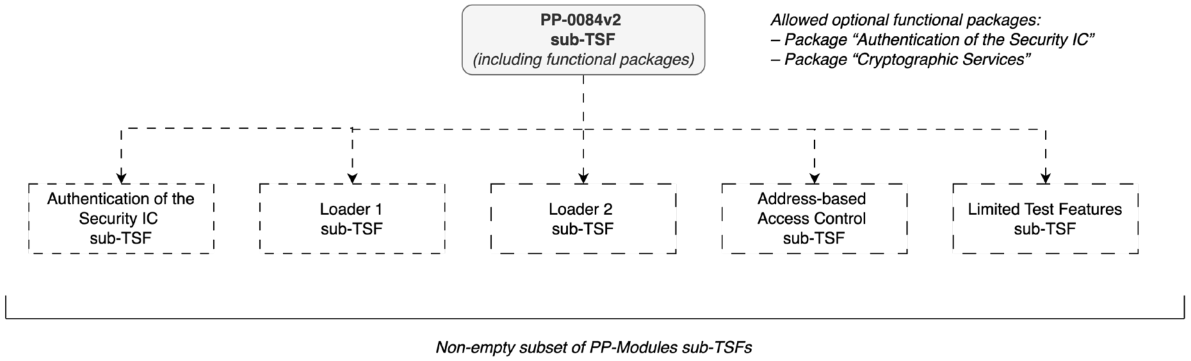
PP-0084v2
sub-TSF
(including functional packages)
Allowed optional functional packages:
– Package "Authentication of the Security IC"
– Package "Cryptographic Services"
Authentication of the Security IC sub-TSF
Loader 1 sub-TSF
Loader 2 sub-TSF
Address-based Access Control sub-TSF
Limited Test Features sub-TSF
Non-empty subset of PP-Modules sub-TSFs

Figure 1: TSF organisation

2.2.2.2 Sub-TSF for PP-0884-v2

11 The sub-TSF defined by the core PP-0084-v2 provides protection of user data confidentiality, integrity, and ensures secure internal data transfer. The TSF protects data stored within protected memory areas and ensures confidentiality and integrity during internal transfer. It provides strong resistance against physical attacks including physical probing, manipulation, forced information leakage, inherent information leakage, and malfunctions induced by environmental stress. Additionally, the TSF implements limited test capabilities and availability after TOE delivery, preventing abuse. It also provides secure random numbers generation.

12 This sub-TSF may also provide cryptographic services and authentication mechanisms to the external entities through the optional functional packages.

2.2.2.3 Sub-TSF Authentication of the Security IC

13 The sub-TSF Authentication of the Security IC provides functionality that enables the TOE to securely authenticate itself to external entities during operational usage. This authentication mechanism ensures that the TOE can unambiguously demonstrate its authenticity by verifying a unique TOE identity.

2.2.2.4 Sub-TSF Loader 1

14 The sub-TSF Loader 1 implements a loading mechanism restricted to usage within secure environments. It provides loading capabilities with limited functionalities, enforced by mechanisms that irreversibly terminate the loader's operation after the necessary loading processes are complete.

2.2.2.5 Sub-TSF Loader 2

15 The sub-TSF Loader 2 provides functionality specifically designed for secure loading operations performed by explicitly authorized users during the operational usage phase of the TOE. It enforces authentication and access controls, ensuring that only authenticated and authorized entities can conduct loading operations post-TOE delivery.

2.2.2.6 Sub-TSF Address-based Access Control

16 The Sub-TSF Address-based Access Control provides security functionality enforcing controlled access to specified addressable areas based on defined security attributes. It ensures that operations on those areas are strictly limited to explicitly authorized subjects.

2.2.2.7 Sub-TSF Limited Test Features

17 The Sub-TSF Limited Test Features provides availability and capability control over the test features after TOE delivery. This sub-TSF is also present in the core part of the PP-0084-v2 sub-TSF.

2.3 TOE Overview

2.3.1 TOE Type

18 The Target of Evaluation (TOE) is a Security IC comprising hardware and IC Dedicated Software as defined in PP-0084-v2.

2.3.2 TOE Usage

19 The TOE is primarily intended as a secure hardware platform for applications requiring high levels of security, such as smart cards and secure elements for payment, identification or electronic signature.

2.3.3 TOE Major Security Features

20 The TOE implements physical protection of its assets and the assets of the Security IC Embedded Software against probing, forced and inherent information leakage, manipulation, and malfunctions induced by environmental stress. The TOE implements secure random number generation and a strict limitation of the test features after delivery.

21 The TOE also implements the additional major security features related to the selected functional packages and the component PP-Modules which are included in the PP-Configuration.

- A TOE that implements cryptographic services for the Security IC Embedded Software and claims the corresponding functional package provides secure cryptographic algorithms to support data confidentiality, integrity, and secure communications.
- A TOE that implements a service for the authentication of the Security IC and claims the corresponding functional package or PP-Module ensures secure and unique identity authentication to external entities.
- A TOE that implements Loader 1 functionality and claims the corresponding PP-Module ensures strictly limited code loading functionalities in controlled environments.
- A TOE that implements Loader 2 functionality and claims the corresponding PP-Module ensures loading is accessible only to authenticated and authorized entities post-delivery.
- A TOE that implements Address-based Access Control and claims the corresponding PP-Module enforces access control on memory regions and possibly other address-based locations/peripherals to prevent unauthorized disclosure, modification, or manipulation of sensitive data.

22 A TOE that claims the PP-Module Limited Test Features does not add functionality to the core functionality expressed in the PP-0084-v2 as this is already included.

2.3.4 Available Non-TOE Hardware/Software/Firmware

23 None.

2.4 Conformance Claims

2.4.1 CC Conformance Claim

24 The PP-Configurations claim conformance to CC:2022 Revision 1[2] as follows:

- CC Part 2-extended,
- CC Part 3-conformant.

25 The conformance claim CC Part 2-extended originates in the PP-Configuration component PP-0084-v2.

26 The CC conformance claim is consistent with the PP-Configurations components, which also claim CC:2022.

2.4.2 Assurance Package claim

27 The PP-Configurations claim conformance to a multi-assurance evaluation level built on top of EAL4-augmented. See 2.6.

2.4.3 Conformance Statement

28 The PP-Configurations require strict conformance of an ST claiming conformance to it.

[2] CC:2022 Revision 1 consists of Parts 1 to 5, cf. [1] to [5].

2.5 Consistency Rationale

2.5.1 TOE Type Rationale

29 The TOE type defined in the PP-Configurations, a Security IC platform is the same as the TOE types specified in PP-0084-v2 and PP-Modules. More specifically:

- the core PP-0084-v2 defines the TOE as a Security IC Platform, including IC hardware and dedicated software for secure storage, secure internal data transfer, and robust physical protection,
- the PP-Modules for Authentication, Loaders, and Address-based Access Control define extensions for Security IC platforms with specific functionalities for robust authentication mechanism, secured loading operations, and rigorous access control to memory and selected address-based locations,
- the PP-Module Limited Test Features covers functionality that is already included in the core PP-0084-v2.

30 Consequently, the TOE type in the PP-Configurations is consistent with the TOE types of its components.

2.5.2 SPD Rationale

31 The SPD of a PP-Configuration is the union of the SPDs of its components. The core SPD from PP-0084-v2 covers generic threats and the RNG service threat, to which each of the PP-Modules included in the PP-Configuration adds specific threats and/or OSPs without contradicting or weakening the core SPD or the SPD of the other PP-Modules. Note that the threats T.Abuse-Loader1 (from PP-Module Loader 1[3]) and T.Abuse-Test (from PP-Module Limited Test Features[4]) are included in the threat T.Abuse-Func defined in the core PP-0084-v2. PP-Modules do not introduce assumptions, thus avoiding any potential conflict with those of the core PP-0084-v2. The SPDs of the PP-Configurations are internally consistent.

2.5.3 Security Objectives Rationale

32 The set of security objectives of a PP-Configuration is the union of the objectives for the TOE and its environment defined in its components, which is internally consistent. The core objectives from PP-0084-v2 cover the generic security properties and the RNG service, to which the each of the PP-Modules included in the PP-Configuration adds some specific objectives without contradicting or weakening the core objectives or the objectives of the other PP-Modules. Note that the objective O.Abuse-Test defined in the PP-Module Limited Test Features is included in the objective O.Abuse-Func defined in the core PP-0084-v2. The sets of security objectives of the PP-Configurations are internally consistent.

2.5.4 SFRs Rationale

33 The set of SFRs of a PP-Configuration is the union of the SFRs of its components. The

[3] The threat T.Abuse-Loader1 is defined in Package Loader 1 and included in PP-Module Loader1.

[4] The threat T.Abuse-Test is defined in PP-Module Limited Test Features.

core SFRs from PP-0084-v2 cover the generic security functionality and the RNG service, to which the each of the PP-Modules included in the PP-Configuration adds specific SFRs without contradicting or weakening the core SFRs or the SFRs of the other PP-Modules. Note that the SFRs defined in the PP-Module Limited Test Features are already included in the core PP-0084-v2. The sets of SFRs of the PP-Configurations are internally consistent.

2.6 SAR Statement

2.6.1 Global SARs for the TOE

34 The global set of Security Assurance Requirements (SARs) for the TOE corresponds to the predefined package EAL4, augmented with ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5, including the refinements defined in PP-0084-v2.

35 Remark: A multi-assurance ST conformant with a PP-Configuration defined in this document can augment the global set of SARs, which is inherited by the SARs of the sub-TSFs.

2.6.2 SARs for Sub-TSFs

36 For the PP-0084-v2 sub-TSF, the set of SARs is identical to the global set of SARs.

37 For the sub-TSFs defined in the PP-Modules, the sets of SARs are EAL4 augmented with ADV_SPM.1, ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5, including the refinements defined in PP-0084-v2.

38 Remark: A multi-assurance ST conformant with a PP-Configuration defined in this document can augment the set of SARs of any sub-TSF. The augmentation can be uniform or not. An augmentation to the global set of SARs leads to the uniform augmentation of the sets of SARs of all the sub-TSFs.

2.6.3 Assurance Rationale

39 The SARs defined for the sub-TSFs of the PP-Configuration are identical to those defined in the corresponding components (PP-0084-v2 and PP-Modules). Therefore, consistency is ensured.

40 The global set of SARs is consistent with the threats as defined in the SPDs of the PP-Configuration components, per PP-0084-v2.

41 Sub-TSF SARs are a superset over the global set targeting formal modelling and proof obligations for the sub-TSF. This keeps a single global assurance baseline while achieving strictly higher assurance where functionality to model is selected through PP-Modules. There is no assurance gap or contradiction between the global set of SARs and the per-PP-Module SARs.

42 Remark: Unlike other PP-Modules, the PP-Module Limited Test Features covers functionality that is part of the core PP-0084-v2. Since the set of SARs of the PP-Module Limited Test Features is a superset of the SARs of PP-0084-v2, in a TOE evaluation the functionality can be evaluated once. If the set of SARs of the PP-0084-v2 is augmented in a multi-assurance ST (without including ADV_SPM.1), then the set of SARs of the PP-Module Limited Test Features should be augmented identically for clarity (in practice the functionality will always be evaluated against all the assurance components that apply to it).

3 PP-Modules

3.1 PP-Module Authentication of the Security IC

3.1.1 Introduction

3.1.1.1 PP-Module Identification

43 The reference of this PP-Module consists of the name and version.

Name:	PP-Module Authentication of the Security IC
Version:	1.0
Date:	16/12/2025
CC edition:	CC:2022 Revision 1

44 This PP-Module is functionally identical to the Package Authentication of the Security IC from PP-0084-v2.

45 From the assurance point of view, it includes a specific set of SARs, which is strictly higher than the one defined in PP-0084-v2.

3.1.1.2 PP-Module Base

46 The PP-Module Base consists of PP-0084-v2 [7].

3.1.1.3 TOE Overview

47 TOE Type: Security IC platform comprising hardware and IC Dedicated Software as defined in PP-0084-v2.

48 TOE Usage: as defined in PP-0084-v2.

49 TOE Major Security Features: authentication of the TOE by external entities.

50 Available Non-TOE Hardware/Software/Firmware: None.

3.1.2 Conformance Claims

3.1.2.1 CC Conformance Claim

51 This PP-Module claims conformance to the CC:2022 Revision 1 as follows:

- CC Part 2-conformant,
- CC Part 3-conformant.

3.1.2.2 Package Claim

3.1.2.2.1 Functional Package Claim

52 This PP-Module claims conformance to functional packages as follows:

- Package-conformant to Package Authentication of the Security IC from PP-0084-

v2.

3.1.2.2.2 Assurance Package Claim

53 This PP-Module claims conformance to the assurance package EAL4 augmented with ADV_SPM.1, ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5, including the refinements defined in PP-0084-v2.

3.1.2.3 Conformance Statement

54 This PP-Module requires strict conformance of a ST or PP claiming conformance to a PP-Configuration that includes it.

3.1.3 Security Problem Definition

55 The asset of this PP-Module is the TOE authentication security service. The SPD is the one defined in the Package Authentication of the Security IC, see PP-0084-v2, section 7.1.3.

3.1.4 Security Objectives

56 The security objectives of this PP-Module are those defined in the Package Authentication of the Security IC, see PP-0084-v2, section 7.1.3.

3.1.4.1 Security Objectives Rationale

57 The rationale for the security objectives of this PP-Module is the one defined in the Package Authentication of the Security IC, see PP-0084-v2, section 7.1.3.

3.1.5 Security Requirements

3.1.5.1 Security Functional Requirements

58 The SFRs of this PP-Module are those defined in the Package Authentication of the Security IC, see PP-0084-v2, section 7.1.4.

3.1.5.2 Security Assurance Requirements

59 The SARs for this PP-Module are those defined in 3.1.2.2.2.

3.1.5.3 Security Requirements Rationale

3.1.5.3.1 SFR Rationale

60 The rationale for the SFRs of this PP-Module, i.e. coverage of the security objectives for the TOE by the SFRs and dependencies analysis, is identical to that provided in the Package Authentication of the Security IC, see PP-0084-v2 section 7.1.4.

3.1.5.3.2 SAR Rationale

61 The SARs of this PP-Module constitute an augmentation of the SARs that apply to the Package Authentication of the Security IC with ADV_SPM.1. This assurance

component requires the formal model of the sub-TSF (the set of SFRs defined in the PP-Module), the proof of the security objectives for the TOE defined in the PP-Module and the relationship between the model and the FSP for that sub-TSF.

62 The augmentation by ADV_SPM.1 has been chosen for higher assurance in the internal consistency of the Security Target and inter-consistency with the FSP.

3.1.5.4 SFR Dependencies

63 The dependencies for this PP-Module are those defined in the Package Authentication of the Security IC, see PP-0084-v2 section 7.1.4.

3.1.6 Consistency Rationale

64 The PP-Module Authentication of the Security IC is consistent with the PP-0084-v2:

- The TOE type defined in the PP-Module is the same as in the PP-0084-v2.
- The asset of this PP-Module is a security service, and as such is included in PP-0084-v2. The threat T.Masquerade-TOE included in this PP-Module extends the threats defined in the core PP-0084-v2. The extension focuses on the risk of claiming genuineness. This PP-Module does not add OSPs or assumptions.
- The additional objective for the TOE O.Authentication ensures that the Security IC can authenticate itself to external entities using Initialisation Data. Additionally, the objective for the environment OE.TOE-Auth requires those external entities to support the verification mechanism and hold the reference data. The objectives introduced in this PP-Module do not contradict or invalidate the objectives of the PP-0084-v2.
- This PP-Module introduces an SFR that completes the SFRs from the core PP-0084-v2. This SFR requires that the TOE provides an authentication mechanism to prove its identity. The SFR introduced in this PP-Module does not contradict or invalidate the SFRs of the PP-0084-v2.
- This PP-Module defines a specific set of SARs, which adds ADV_SPM.1 to the SARs defined in the base PP-0084-v2. All the dependencies of ADV_SPM.1 are included in the set of SARs which is included in PP-0084-v2.

3.2 PP-Module Loader 1 (for usage in secured environment only)

3.2.1 Introduction

3.2.1.1 PP-Module Identification

65 The reference of the PP-Module consists of the name and version.

Name:	PP-Module Loader 1 (for usage in secured environment only)
Version:	1.0
Date:	4/12/2025
CC edition:	CC:2022 Revision 1

66 This PP-Module is functionally identical to the Package Loader 1 (for usage in secured

environment only) from PP-0084-v2.

67 From the assurance point of view, it includes a specific set of SARs, which is strictly higher than the one defined in PP-0084-v2.

3.2.1.2 PP-Module Base

68 The PP-Module Base consists of PP-0084-v2 [7].

3.2.1.3 TOE Overview

69 TOE Type: Security IC platform comprising hardware and IC Dedicated Software as defined in PP-0084-v2.

70 TOE Usage: as defined in PP-0084-v2.

71 TOE Major Security Features: Loading capabilities, to be used in controlled operational environments prior to the end-usage. Its purpose is to load Security IC Embedded Software, user data of the Composite Product, or IC Dedicated Support Software and then have its capability and availability limited so stored data cannot later be disclosed or manipulated.

72 Available Non-TOE Hardware/Software/Firmware: None.

3.2.2 Conformance Claims

3.2.2.1 CC Conformance Claim

73 This PP-Module claims conformance to CC:2022 Revision 1 as follows:

- CC Part 2-conformant
- CC Part 3-conformant.

3.2.2.2 Package Claim

3.2.2.2.1 Functional Package Claim

74 This PP-Module claims conformance to functional packages as follows:

- Package-conformant to Package Loader 1 (for usage in secured environment only) from PP-0084-v2.

3.2.2.2.2 Assurance Package Claim

75 This PP-Module claims conformance to the assurance package EAL4 augmented with ADV_SPM.1, ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5, including the refinements defined in PP-0084-v2.

3.2.2.3 Conformance Statement

76 This PP-Module requires strict conformance of a ST or PP claiming conformance to a PP-Configuration that includes it.

3.2.3 Security Problem Definition

77 The asset of this PP-Module is the user data (Security IC Embedded Software and user data of the Composite TOE). The SPD is the one defined in Package Loader 1, see PP-0084-v2, section 7.2.1.3.

3.2.4 Security Objectives

78 The security objectives of this PP-Module are those defined in the Package Loader 1, see PP-0084-v2, section 7.2.1.3.

3.2.4.1 Security Objectives Rationale

79 The rationale for the security objectives of this PP-Module is the one defined in the Package Loader 1, see PP-0084-v2, section 7.2.1.3.

3.2.5 Security Requirements

3.2.5.1 Security Functional Requirements

80 The SFRs of this PP-Module are those defined in the Package Loader 1, see PP-0084-v2, section 7.2.1.4.

3.2.5.2 Security Assurance Requirements

81 The SARs for this PP-Module are those defined in 3.2.2.2.2.

3.2.5.3 Security Requirements Rationale

3.2.5.3.1 SFR Rationale

82 The rationale for the SFRs of this PP-Module, i.e. coverage of the security objectives for the TOE by the SFRs and dependencies analysis, is identical to that provided in the Package Loader 1, see PP-0084-v2 section 7.2.1.4

3.2.5.3.2 SAR Rationale

83 The SARs of this PP-Module constitute an augmentation of the SARs that apply to the Package Loader 1 with ADV_SPM.1. This assurance component requires the formal model of the sub-TSF (the set of SFRs defined in the PP-Module), the proof of the security objectives for the TOE defined in the PP-Module and the relationship between the model and the FSP for that sub-TSF.

84 The augmentation by ADV_SPM.1 has been chosen for higher assurance in the internal consistency of the Security Target and inter-consistency with the FSP.

3.2.5.4 SFR Dependencies

85 The dependencies for this PP-Module are those defined in the Package Loader 1, see PP-0084-v2, section 7.2.1.4.

3.2.6 Consistency Rationale

86 The PP-Module Loader 1 (for usage in secured environment only) is consistent with the PP-0084-v2:

- The TOE type defined in the PP Module is the same as in the PP-0084-v2.
- The asset of this PP-Module is an asset of PP-0084-v2. The threat T.Abuse-Loader1 and the OSP P.Lim-Block-Loader1 included in this PP-Module extend the SPD defined in the PP-0084-v2. The extension focuses on the secure loading of user data or IC Dedicated Support Software in secured environments. The OSP requires that the Loader capability be limited and then blocked after the intended use. This PP-Module does not add assumptions.
- The additional objective for the TOE O.Cap-Avail-Loader1 provides limited Loader capability and irreversible termination to protect stored user data. Additionally, the objective for the environment OE.Lim-Block-Loader1 is added mandating that the manufacturer protects the Loader, limits its capability and blocks it the after its intended use. The objectives introduced in this PP-Module do not contradict or invalidate the objectives of the PP-0084-v2.
- This PP-Module introduces a set of SFRs that complete the SFRs from the core PP-0084-v2. The SFRs defined in this PP-Module ensures that loading activities are strictly controlled in secure environment.
- This PP-Module defines a specific set of SARs, which adds ADV_SPM.1 to those defined in the base PP-0084-v2. All the dependencies of ADV_SPM.1 are included in the set of SARs which is included in PP-0084-v2.

3.3 PP-Module Loader 2 (for usage by authorized users only)

3.3.1 Introduction

3.3.1.1 PP-Module Identification

87 The reference of the PP-Module consists of the name and version.

Name:	PP-Module Loader 2 (for usage by authorized users only)
Version:	1.0
Date:	16/12/2025
CC edition:	CC:2022 Revision 1

88 This PP-Module is functionally identical to the Package Loader 2 (for usage by authorized users only) from PP-0084-v2.

89 From the assurance point of view, it includes a specific set of SARs, which is strictly higher than the one defined in PP-0084-v2.

3.3.1.2 PP-Module Base

90 The PP-Module Base consists of PP-0084-v2 [7].

3.3.1.3 TOE Overview

91 TOE Type: Security IC platform comprising hardware and IC Dedicated Software as defined in PP-0084-v2.

92 TOE Usage: as defined in PP-0084-v2.

93 TOE Major Security Features: Loader functionality designed for use by authorised entities beyond the manufacturing phases.

94 Available Non-TOE Hardware/Software/Firmware: None.

3.3.2 Conformance Claims

3.3.2.1 CC Conformance Claim

95 This PP-Module claims conformance to CC:2022 Revision 1 as follows:

- CC Part 2-conformant
- CC Part 3-conformant.

3.3.2.2 Package Claim

3.3.2.2.1 Functional Package Claim

96 This PP-Module claims conformance to functional packages as follows:

- Package-conformant to Package Loader 2 (for usage by authorized users only) from PP-0084-v2.

3.3.2.2.2 Assurance Package Claim

97 This PP-Module claims conformance to the assurance package EAL4 augmented with ADV_SPM.1, ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5, including the refinements defined in PP-0084-v2.

3.3.2.3 Conformance Statement

98 This PP-Module requires strict conformance of a ST or PP claiming conformance to a PP-Configuration that includes it.

3.3.3 Security Problem Definition

99 The asset of this PP-Module is the user data (Security IC Embedded Software and user data of the Composite TOE). The SPD is the one defined in the Package Loader 2, see PP-0084-v2, section 7.2.2.3.

3.3.4 Security Objectives

100 The security objectives of this PP-Module are those defined in the Package Loader 2, see PP-0084-v2, section 7.2.2.3.

3.3.4.1 Security Objectives Rationale

101 The rationale for the security objectives of this PP-Module is the one defined in the

Package Loader 2, see PP-0084-v2, section 7.2.2.3.

3.3.5 Security Requirements

3.3.5.1 Security Functional Requirements

102 The SFRs of this PP-Module are those defined in the Package Loader 2, see PP-0084-v2, section 7.2.2.4.

3.3.5.2 Security Assurance Requirements

103 The SARs for this PP-Module are those defined in 3.3.2.2.2.

3.3.5.3 Security Requirements Rationale

3.3.5.3.1 SFR Rationale

104 The rationale for the SFRs of this PP-Module, i.e. coverage of the security objectives for the TOE by the SFRs and dependencies analysis, is identical to that provided in the Package Loader 2, see PP-0084-v2 section 7.2.2.4.

3.3.5.3.2 SAR Rationale

105 The SARs of this PP-Module constitute an augmentation of the SARs that apply to the Package Loader 2 with ADV_SPM.1. This assurance component requires the formal model of the sub-TSF (the set of SFRs defined in the PP-Module), the proof of the security objectives for the TOE defined in the PP-Module and the relationship between the model and the FSP for that sub-TSF.

106 The augmentation by ADV_SPM.1 has been chosen for higher assurance in the internal consistency of the Security Target and inter-consistency with the FSP.

3.3.5.4 SFR Dependencies

107 The dependencies for this PP-Module are those defined in the Package Loader 2, see PP-0084-v2, section 7.2.2.4.

3.3.6 Consistency Rationale

108 The PP-Module Loader 2 (for usage by authorized users only) is consistent with the PP-0084-v2:

- The TOE type defined in the PP Module is as defined in the PP-0084-v2.
- The asset of this PP-Module is an asset of PP-0084-v2. The OSP P.Ctlr-Loader2 included in this PP-Module extends the SPD defined in the PP-0084-v2. The extension requires authorised control of Loader use to protect stored and loaded user data. This PP-Module does not add threats or assumptions.
- The additional objective for the TOE O.Ctrl-Auth-Loader2 provides a trusted communication channel, confidentiality and integrity protection of loaded data, and access control for loader usage. Additionally, the objective for the environment

OE.Loader-Usage2 is added requiring the authorised user to support that trusted channel, provide confidentiality/authenticity of the load data, and meet Loader access conditions. The objectives introduced in this PP-Module do not contradict or invalidate the objectives of the PP-0084-v2.

- This PP-Module introduces a set of SFRs that completes the SFRs from the core PP-0084-v2. The SFRs defined in this PP-Module ensures secure in-field loading operation scenarios.
- This PP-Module defines a specific set of SARs, which adds ADV_SPM.1 to those defined in the base PP-0084-v2. All the dependencies of ADV_SPM.1 are included in the set of SARs which is included in PP-0084-v2.

3.4 PP-Module Address-based Access Control

3.4.1 Introduction

3.4.1.1 PP-Module Identification

109 The reference of the PP-Module consists of the name and version.

Name:	PP-Module Address-based Access Control
Version:	1.0
Date:	16/12/2025
CC edition:	CC:2022 Revision 1

110 This PP-Module is functionally identical to the Package Address-based Access Control, from PP-0084-v2.

111 From the assurance point of view, it includes a specific set of SARs, which is strictly higher than the one defined in PP-0084-v2.

3.4.1.2 PP-Module Base

112 The PP-Module Base consists of PP-0084-v2 [7].

3.4.1.3 TOE Overview

113 TOE Type: Security IC platform comprising hardware and IC Dedicated Software as defined in PP-0084-v2.

114 TOE Usage: as defined in PP-0084-v2.

115 TOE Major Security Features: The Address-Based Access Control functionality lets the Security IC Embedded Software define restricted address areas, including memories and memory-mapped peripherals, and enforces their partitioning so that only permitted operations can be performed on authorised areas.

116 Available Non-TOE Hardware/Software/Firmware: None.

3.4.2 Conformance Claims

3.4.2.1 CC Conformance Claim

117 This PP-Module claims conformance to CC:2022 Revision 1 as follows:

- CC Part 2-conformant,
- CC Part 3-conformant.

3.4.2.2 Package Claim

3.4.2.2.1 Functional Package Claim

118 This PP-Module claims conformance to functional packages as follows:

- Package-conformant to Package Address-based Access Control from PP-0084-v2.

3.4.2.2.2 Assurance Package Claim

119 This PP-Module claims conformance to the assurance package EAL4 augmented with ADV_SPM.1, ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5, including the refinements defined in PP-0084-v2.

3.4.2.3 Conformance Statement

120 This PP-Module requires strict conformance of a ST claiming conformance to a PP-Configuration that includes it.

3.4.3 Security Problem Definition

121 The asset of this PP-Module is the code and data stored in controlled areas. The SPD is the one defined in the Package Address-based Access Control, see PP-0084-v2, section 7.4.3.

3.4.4 Security Objectives

122 The security objectives of this PP-Module are those defined in the Package Address-based Access Control, see PP-0084-v2, section 7.4.3.

3.4.4.1 Security Objectives Rationale

123 The rationale for the security objectives of this PP-Module is the one defined in the Package Address-based Access Control, see PP-0084-v2, section 7.4.3.

3.4.5 Security Requirements

3.4.5.1 Security Functional Requirements

124 The SFRs of this PP-Module are those defined in the Package Address-based Access Control, see PP-0084-v2, section 7.4.4.

3.4.5.2 Security Assurance Requirements

125 The SARs for this PP-Module are those defined in 3.4.2.2.2.

3.4.5.3 Security Requirements Rationale

3.4.5.3.1 SFR Rationale

126 The rationale for the SFRs of this PP-Module, i.e. coverage of the security objectives for the TOE by the SFRs and dependencies analysis, is identical to that provided in the Package Address-based Access Control, see PP-0084-v2 section 7.4.4.

3.4.5.3.2 SAR Rationale

127 The SARs of this PP-Module constitute an augmentation of the SARs that apply to the Package Address-based Access Control with ADV_SPM.1. This assurance component requires the formal model of the sub-TSF (the set of SFRs defined in the PP-Module), the proof of the security objectives for the TOE defined in the PP-Module and the relationship between the model and the FSP for that sub-TSF.

128 The augmentation by ADV_SPM.1 has been chosen for higher assurance in the internal consistency of the Security Target and inter-consistency with the FSP.

3.4.5.4 SFR Dependencies

129 The dependencies for this PP-Module are those defined in the Package Address-based Access Control, see PP-0084-v2, section 7.4.4.

3.4.6 Consistency Rationale

130 The PP-Module Address-based Access Control is consistent with the PP-0084-v2:

- The TOE type defined in the PP-Module is as in the PP-0084-v2.
- The assets of this PP-Module are included in the PP-0084-v2.The threat T.Addr-Access defined in this PP-Module extends the threats defined in the PP-0084-v2. The extension focuses on unauthorized accesses to restricted memory or addressable objects. This PP-Module does not add-OSPs or assumptions.
- The additional objective for the TOE O.Addr-Access aims to restrict access to defined addressable areas. The objective introduced in this PP-Module does not contradict or invalidate the objectives of the PP-0084-v2.
- This PP-Module introduces a set of SFRs that completes the SFRs from the core PP-0084-v2. These SFRs limit the access to addressable areas based on predefined security attributes preventing accidental or deliberate access violations.
- This PP-Module defines a specific set of SARs, which adds ADV_SPM.1 to those defined in the base PP-0084-v2. All the dependencies of ADV_SPM.1 are included in the set of SARs which is included in PP-0084-v2.

3.5 PP-Module Limited Test Features

3.5.1 Introduction

3.5.1.1 PP-Module Identification

131 The reference of the PP-Module consists of the name and version.

Name:	PP-Module Limited Test Features
Version:	1.0
Date:	16/12/2025
CC edition:	CC:2022 Revision 1

132 This PP-Module covers functionality that is included in PP-0084-v2. Nevertheless, this PP-Module includes a specific set of SARs that is strictly higher than the one defined in PP-0084-v2.

3.5.1.2 PP-Module Base

133 The PP-Module Base consists of PP-0084-v2 [7].

3.5.1.3 TOE Overview

134 TOE Type: Security IC platform comprising hardware and IC Dedicated Software as defined in PP-0084-v2.

135 TOE Usage: as defined in PP-0084-v2.

136 TOE Major Security Features: Limitation of the availability and capabilities of test features after TOE delivery.

137 Available Non-TOE Hardware/Software/Firmware: None.

3.5.2 Conformance Claims

3.5.2.1 CC Conformance Claim

138 This PP-Module claims conformance to CC:2022 Revision 1as follows:

- CC Part 2-conformant,
- CC Part 3-conformant.

3.5.2.2 Package Claim

3.5.2.2.1 Assurance Package Claim

139 This PP-Module claims conformance to the assurance package EAL4 augmented with ADV_SPM.1, ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5, including the refinements defined in PP-0084-v2.

3.5.2.3 Conformance Statement

140 This PP-Module requires strict conformance of a ST or PP claiming conformance to a PP-Configuration that includes it.

3.5.3 Security Problem Definition

141 The assets of this PP-Module are of those defined in PP-0084-v2 (user data of the Composite TOE, Security IC Embedded Software, and TOE security services).

142 The TOE shall avert the threat “Abuse of test functionality (T.Abuse-Test)” as specified below.

T.Abuse-Test Abuse of Test Functionality

An attacker may use test features of the TOE which may not be used after TOE Delivery in order to (i) disclose or manipulate user data of the Composite TOE, (ii) manipulate (explore, bypass, deactivate or change) security services of the TOE or (iii) manipulate (explore, bypass, deactivate or change) functions of the Security IC Embedded Software or (iv) enable an attack disclosing or manipulating the user data of the Composite TOE or the Security IC Embedded Software.

143 The threat T.Abuse-Test is included in the threat T.Abuse-Func defined in the base PP-0084-v2.

3.5.4 Security Objectives

144 The TOE shall provide “Protection against Abuse of Test Functionality (O.Abuse-Test)” as specified below.

O.Abuse-Test Protection against Abuse of Test Functionality

The TOE shall prevent that test features of the TOE which may not be used after TOE Delivery can be abused in order to (i) disclose critical user data of the Composite TOE, (ii) manipulate critical user data of the Composite TOE, (iii) manipulate Security IC Embedded Software or (iv) bypass, deactivate, change or explore security features or security services of the TOE.

145 The security objective for the TOE O.Abuse-Test is a specialization of O.Abuse-Func defined in the base PP-0084-v2.

3.5.4.1 Security Objectives Rationale

146 The threat T.Abuse-Test is directly covered by the objective O.Abuse-Test.

3.5.5 Security Requirements

3.5.5.1 Security Functional Requirements

147 This PP-Module uses the following typographic conventions to indicate operations performed on the functional components:

- assignments are denoted by underlined text,
- iterations are indicated by a suffix preceded by the / symbol, following the component identifier.

148 The TOE shall meet the requirement “Limited capabilities (FMT_LIM.1/Test)”. This requirement is replicated from PP-0084-v2.

FMT_LIM.1/Test **Limited capabilities**

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1.1/Test The TSF shall limit its capabilities so that in conjunction with “Limited availability (FMT_LIM.2/Test)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow user data of the Composite TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks[5].

149 The TOE shall meet the requirement “Limited availability (FMT_LIM.2/Test)”. This requirement is replicated from PP-0084-v2.

FMT_LIM.2/Test **Limited availability**

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2.1/Test The TSF shall be designed in a manner that limits its availability so that in conjunction with “Limited capabilities (FMT_LIM.1/Test)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow user data of the Composite TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks[6].

3.5.5.2 Security Assurance Requirements

150 The SARs for this PP-Module are those defined in 3.5.2.2.1.

3.5.5.3 Security Requirements Rationale

3.5.5.3.1 SFR Rationale

151 The objective O.Abuse-Test states that abuse of test functionality shall not be possible in Phase 7 of the life cycle[5] by (i) limiting their capabilities (FMT_LIM.1/Test) or (ii) limiting their availability is limited (FMT_LIM.2/Test). Since these requirements are combined to enforce the policy, both security functional requirements together are suitable to meet the objective.

3.5.5.3.2 SAR Rationale

[5] The life cycle is defined in the base PP-0084-v2.

152 The SARs of this PP-Module augment the PP-0084-v2 baseline with ADV_SPM.1 for the sub-TSF. This assurance component requires the formal model of the sub-TSF (the set of SFRs defined in the PP-Module), the proof of the security objectives for the TOE defined in the PP-Module and the relationship between the model and the FSP for that sub-TSF.

153 The augmentation by ADV_SPM.1 has been chosen for higher assurance in the internal consistency of the Security Target and inter-consistency with the FSP.

3.5.5.4 SFR Dependencies

154 The SFR dependencies are satisfied as shown in Table 3-1.

Table 3-1: PP-Module Limited Test Features - SFR Dependencies

Security Functional Requirement	Dependency	Fulfilled by
FMT_LIM.1/Test	FMT_LIM.2	FMT_LIM.2/Test
FMT_LIM.2/Test	FMT_LIM.1	FMT_LIM.1/Test

3.5.6 Consistency Rationale

155 The PP-Module Limited Test Features is consistent with the PP-0084-v2:

- The TOE type defined in the PP-Module is as in the PP-0084-v2.
- The assets of this PP-Module are those of PP-0084-v2. The threat T.Abuse-Test defined in this PP-Module, which focuses on the abuse of Test features in Phase 7 of the life cycle, is included in PP-0084-v2 as part of the more general threat about the abuse of functionalities (T.Abuse-Func). This PP-Module does not add OSPs or assumptions.
- The additional objective for the TOE O.Abuse-Test aims to prevent the abuse of test functionality. This objective does not contradict or invalidate the objectives of PP-0084-v2 (it is included in the objective O.Abuse-Func).
- This PP-Module includes two SFRs from PP-0084-v2, i.e. FMT_LIM.1/Test and FMT_LIM.2/Test, to control the test functionality.
- This PP-Module defines a specific set of SARs, which adds ADV_SPM.1 to those defined in the base PP-0084-v2. All the dependencies of ADV_SPM.1 are included in the set of SARs which is included in PP-0084-v2.

4 Glossary

The terms defined in PP-0084-v2 [7] apply to this document.

5 Abbreviations

CC	Common Criteria
EAL	Evaluation Assurance Level

PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SPD	Security Problem Definition
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

6 References

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; November 2022, Version CC:2022, Revision 1, CCMB-2022-11-001.

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; November 2022, Version CC:2022, Revision 1, CCMB-2022-11-002

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; November 2022, Version CC:2022, Revision 1, CCMB-2022-11-003.

[4] Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities; November 2022, Version CC:2022, Revision 1, CCMB-2022-11-004.

[5] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements; November 2022, Version CC:2022, Revision 1, CCMB-2022-11-005.

[6] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; Version CC:2022, Revision 1, CCMB-2022-11-006.

[7] Eurosmart, Security IC Platform Protection Profile including Functional Packages, Version 2.0, December 2025.