Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, the 27th July 2012

Reference : ANSSI-CC-NOTE/10EN.01deW10

APPLICATION NOTE

CERTIFICATION OF "OPEN" SMART CARD PRODUCTS

Application : Date of publication – Note for trial use

Diffusion : Public

Courtesy Translation

Document Releases

Edition	Date	Modifications
0	16/12/2010	Creation for trial use
0.1		

This application note will be submitted to the certification management board after its trial phase.

TABLE OF CONTENT

1. CONTEXT AND PURPOSE OF THE DOCUMENT 4

1.1. DEFINITIONS 4
1.2. SCOPE 4
1.3. NOTE'S PLAN 5
1.4. REFERENCES 5

2. OPEN AND ISOLATING PLATFORM 6

2.1. EVALUATION 6
2.1.1. OBJECTIVES 6
2.1.1.1. ANALYSED FUNCTIONALITY 6
2.1.1.2. EVALUATION ENVIRONMENT 6
2.1.2. IDENTIFICATION 7
2.1.3. LIFE CYCLE 7
2.1.4. PRODUCT GUIDANCE 9
2.1.5. EVALUATED CONFIGURATION 9
2.2. OPEN AND ISOLATING PLATFORM CERTIFICATION 10
2.3. OPEN AND ISOLATING PLATFORM MAINTENANCE 12

3. APPLICATIONS ON AN OPEN AND ISOLATING PLATFORM 13

3.1. EVALUATION 14
3.1.1. OBJECTIVES FROM THE PLATFORM CERTIFICATE 14
3.1.2. APPLICATIONS SECURITY FUNCTIONAL COMPATIBILITY 14
3.2. CERTIFICATION 15
3.3. APPLICATION ON OPEN AND ISOLATING PLATFORM MAINTENANCE 15

ANNEX A: REQUIREMENTS AND CONSTRAINTS COMPATIBILITY BETWEEN THOSE DESCRIBED IN THIS NOTE AND THOSE DESCRIBED IN THE "OPEN PLATFORM" PPS THAT ALREADY EXIST 16

1. Context and purpose of the document

1.1. Definitions

The term product here refers to a generic term that corresponds to a TOE associated to an environment.

The term "platform" refers to the terminology used in the note [Compo] about the composition of evaluation results process, applied to the composition evaluation case of an "application on a platform". Thus, a product designated here as a "platform" is an integrated circuit with a software operating system and sometimes with native applicative code.

An "open platform" is a platform that can host new application after its delivery to the end user (i.e. during the 7th phase of the traditional smartcard lifecycle). Such loadings are called "post-issuance" loading (applications loading after delivery of the smartcard to the end user).

Applications may be installed before the 7th phase, we will speak then of "pre-issuance" loading.

A "closed platform" is a platform that can't host new application after its delivery to the end user.

An "isolating platform" is a platform that maintains the separation of the execution domains of all embedded applications on a platform, as of the platform itself. "Isolation" refers here to domain separation of applications as well as protection of application's data.

"Architecture" corresponds to the top level structure of the product, namely the "open platform" with all the applications contained in the product. (whatever they are loaded in pre or post issuance).

As new applications loading could be considered before or after the evaluation process, we will speak of known applications and unknown applications to distinguish applications that have been taken into account during the evaluation process from others.

- "Known applications" correspond to the original architecture of the certified product. They are all taken into account by the ITSEF during the evaluation process.
- "Unknown applications" are applications that were unknown at the moment of evaluation. They correspond to an upgrade of the architecture of the evaluated product, from the one stated in the certification report.

1.2. Scope

This document aims at identifying the certification procedure for open products in order to guarantee that their changed architecture do not affect the effectiveness of the certified security functionality of a certificate already issued for a different architecture of this product. Changed architecture here stands for the addition of applications to the original certified product's architecture (modification of the TOE environment).

Note, that (in contrast to the situation discussed above) a modification of the platform itself will require recertification/assurance continuity of the platform and consequently of the overall product."

In order to take into account, in the certificate, the changed architecture of these products, the platform shall have some properties, notably isolation properties for applications activated on the product. Indeed, only products that offer these isolation properties insure that the activation of a new application does not impact the assurance of the functionality as certified. Those platforms which have been evaluated to demonstrate that they offer (under certain constraints) those guarantees are called "open and isolating platform" in this document.

When new applications are loaded on such an open product, verifications of the fulfilment of the platform security constraints by those new applications are required to ensure that the evaluated product (TOE) reaches the AVA_VAN level aimed in its expected IT-environment extended.

Open platforms that do not guarantee isolation of applications are certified as closed platform. Closed platforms that do not authorize post-issuance loading are out of the scope of this document.

1.3. Note's plan

Chapter 2 defines those guarantees and constraints on platforms and provides input for evaluation and certification of "open and isolating platforms".

Chapter 3 defines those guarantees and constraints on applications and provides input for evaluation of applications on a certified "open and isolating platforms".

1.4. References

- [Compo]: Joint Interpretation Library - Composite product evaluation for smart cards and similar devices, version 1.2, January 2012.
- [JCO/2.6]: Java Card System - Open Configuration Protection Profile, version 2.6. *Certified by ANSSI under the reference ANSSI-CC-PP-2010/03*.
- [JCO/3.0]: Java Card Protection Profile - Open Configuration, version 3.0. *Certified by ANSSI under the reference ANSSI-CC-PP-2010/03-M01*.
- [USIM]: (U)SIM Java Card Platform Protection Profile – Basic and SCWS Configurations, réf. PU-2009-RT-79, version 2.0.2. *Certified by ANSSI under the references ANSSI-CC-PP-2010/04 (Basic Configuration) and ANSSI-CC-PP-2010/05 (SCWS Configuration).*

2. Open and isolating platform

2.1. Evaluation

We will now refer, in this document, to an open and isolating platform for a platform that has been evaluated in accordance with the elements listed here.

2.1.1. Objectives

2.1.1.1. Analysed functionality

An "*open and isolating platform*" shall provide the following functionalities that have to be evaluated

- O1: isolation between all the applications stored on the considered platform, and thus protection against applications that could be hostile;

and

- O2: protection of the post-issuance loading of applications on the considered platform by verification of the integrity and of the authenticity of the verification[1] of each application, before their activation[2] thanks to the evidences defined in the following OE2.

O1 and O2 shall be objectives for the TOE in the security target of the platform.

2.1.1.2. Evaluation environment

An "*open and isolating platform*" is a platform which has been submitted to an evaluation process that makes mandatory the following requirements for all the applications that are loaded on the platform:

- OE1: all applications that will be loaded on the platform have to be verified, before their effective installation (activation), according to the constraints imposed by the targeted platform, related to its isolation properties;

and

- OE2: availability of an integrity evidence for each application to be loaded on the platform (in order to insure that the loaded application has not been changed since the verification of OE1), and also availability of authenticity evidence of those verification.

OE1 and OE2 shall be objectives for the environment in the security target of the platform.

OE1 and OE2 are applicable for all applications, whether they will be evaluated to be certified or not. As such, they are applicable for all known or unknown applications.

For known application, the fulfilment of OE1 and OE2 will be verified by the ITSEF. Nevertheless it is still possible to only verify OE1, and describe the way OE2 shall be fulfilled[3]. Then, the ITSEF will verify the fulfilment of OE1 and evaluate the guidance documentation used to fulfil OE2. In such case, the certificate will unambiguously identify these applications and indicate the usage restriction, requiring the final user to apply the guidance documentations to fulfil OE2.

[1] What is loaded is what have been verified

[2] That is to say before the loaded file becomes an application usable by the end user.

[3] This holds for cases, where OE2 can be fulfilled by organisational measures, which is allowed in certain life-cycle phases, see section 2.1.3.

For unknown application, the verification of the fulfilment of OE1 and OE2 is not possible. It The platform certificate will consist of certificate usage restriction, requiring the final user to apply the guidance documentation to fulfil OE1 and OE2.

2.1.2. Identification

Speaking generally, certification of open platform should allow the identification of the product evaluated by the ITSEF. This identification consists of:

- identification of the product in the state in which it has been submitted for evaluation (given to the ITSEF). It includes all the known applications loaded pre-issuance,
- identification of the all the known applications that can be loaded post-issuance.

Identifiers returned on request by the product shall permit to distinguish the TOE from the product by identifying the platform and listing all the stored applications.

The evaluation shall consider the whole product, whatever the TOE is. Thus, the platform components and the known applications shall be identified in the identification information provided by the security target. These identification information's will be obviously specified in the certification report of the platform.

The developer shall give to the ITSEF means to verify that the product identifiers available to the ITSEF correspond to a set of components known by the ITSEF (whatever if those components belong to the TOE or not).

These requirements permit to avoid the risk of certifying products including applications that do not respect the platform constraints, that is to say which may be hostile for the other applications activated on the product.

2.1.3. Life cycle

The following picture shows a phase model of be the lifecycle of an open platform. It is just an example of such a life cycle: the ALC delivery point related to the platform evaluation may be different from the one identified here.

Note also that the considered point of delivery can be extended from the one considered in the actual evaluation if the evidence for sites certifications or comparable audit results are provided.

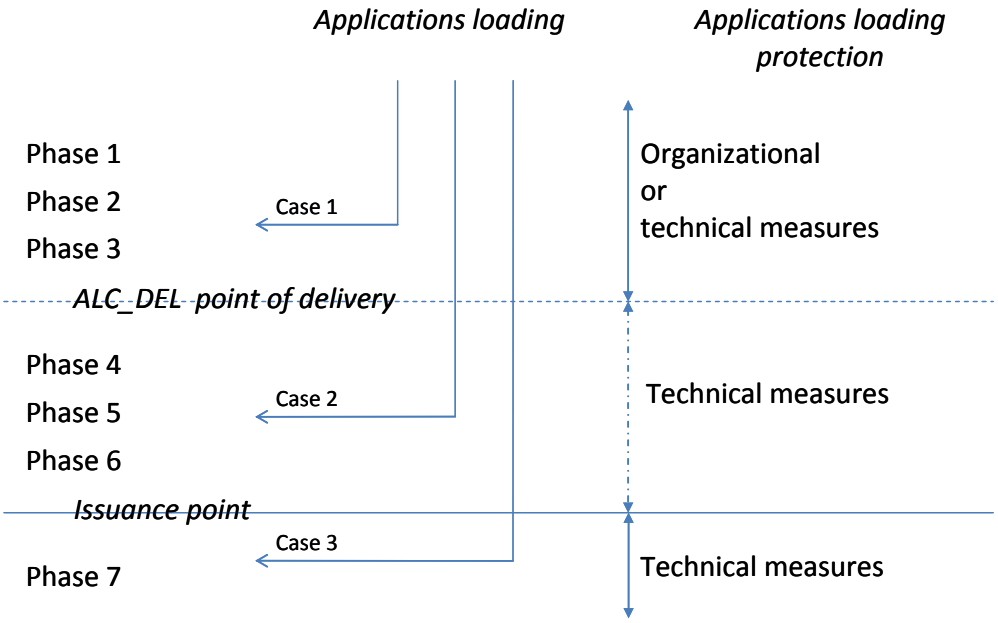


Figure 1 Open and isolating platform life cycle[4]

An "open & isolating platform" product may contain pre-issuance and post-issuance applications.

It is useful to precise that the measures to reach the OE2 objective could be of different natures depending of the moment of the loading.

We distinguish three different cases:

- Case 1: the application is loaded in pre-issuance and before delivery point ; the OE2 objective may be enforced by organizational measures or technical measures ;
- Case 2: the application is loaded in pre-issuance and after the delivery point, organizational measures are not allowed and technical measures must be employed;
- Case 3: the application is loaded in post issuance (after issuance of the product); technical measures associated to OE2 objective must be employed.

By definition all the considered platform allow the case 3 loading (in phase 7 at least).

To precise the way OE1 and OE2 are realized, the security target shall explain the processes implied in the development, in the verification and in the distribution of the application, and the various roles. The security target shall also describe the evaluation scope regarding this detailed lifecycle.

In case known applications are part of the evaluated product the following details of the lifecycle shall also be described in the security target:

- Identification of actors in relation with their role in the management of the processes implied in the application verification;
- Identification of actors in relation with their role in the management of the process implied in the integrity and authenticity protection of applications from their verification to their loading.

[4].Note that the phases 1 to 7 are used as defined in the Protection Profile certified under BSI-CC-PP-0035-2007.

In addition, the ALC delivery point may be different between the certified platform and a subsequent composite certification of applications on top of the certified platform (see Chapter 3). A typical use case might be that the ALC delivery point is moved to a later stage. Thereby, the composite certification would change the classification of phases with respect to whether they belong to Case 1 or Case 2. Platform certification phases of Case 2 could become Case 1 phases of the composite certification, as the point of delivery is postponed, and would then not mandate technical measures. Such a re-classification is accepted and doesn't contradict nor impact the platform certification.

2.1.4. Product guidance

In relation with the evaluation environment identified in chapter 2.1.1.2, the following specific guidance shall be provided by the developer:

- Application development guidance (in relation with OE1), from which are derived the verification guidance that describe the constraints imposed to the application in order to maintain the isolation property of the platform [ISO_VERIF];
- Application loading protection guidance (in relation with OE2), that correspond to:
    - Organizational measures for application loading [ORG_LOAD][5];
    - Technical measures for application loading that shall describe how to activate the related functionality (corresponding to O2) of the platform, associated to measures necessary to guarantee the authenticity of the verifications (Key protection for example) [TECH_LOAD].

As “open and isolating platforms” always allow the case 3 application loading, [ISO_VERIF] and [TECH_LOAD] have always to be provided by the developer.

It won’t be necessary to provide [ORG_LOAD] if the developer doesn’t implement case 1 with organizational measures.

Note that [ISO_VERIF] does not correspond to the guidance mandated by AGD_OPE (guidance documentation for coding of secure applications). [ISO_VERIF] lists all the development rules related to the maintenance of the isolation properties of the platform between application.. Part of AGD_OPE’s guidance dedicated to the application development lists all the development rules related to application that have to provide specific security properties.

Those guidance will have to be evaluated according to AGD or ALC depending of the loading cases considered by the developer.

2.1.5. Evaluated configuration

Depending of the actual lifecycle of the considered product, OE1 and OE2 have to be treated by the ITSEF in the following way:

1. The ITSEF will have to systematically check that all known applications fulfil the the OE1 constraint. The ITSEF may rely on developer evidences to check that the application verification has been done. As it can’t be checked for unknown applications, compliance to [ISO_VERIF] will lead to certificate restrictions.
2. When organizational measures are used before the delivery point, the application loading is under developer’s responsibility, the associated protection that implements OE2 is covered

[5] This guidance is part of ALC security assurance requirements

by ALC Security Assurance Requirement. Therefore, the organizational measures have to be audited.

3. Within the scope of this document, technical measures enforcing OE2 are always used, at least for Case 3. The associated requirements are given in [TECH_LOAD]. Part or all of these requirements can be enforced by ALC Security Assurance Requirements, therefore the corresponding organizational measures have to be audited. Compliance to [TECH_LOAD] that can't be checked will consist of certificate restriction.

Thus OE1 and OE2 have to be verified for all known applications.

2.2. Open and isolating platform certification

A certification report for an open and isolating platform have the following specificities:

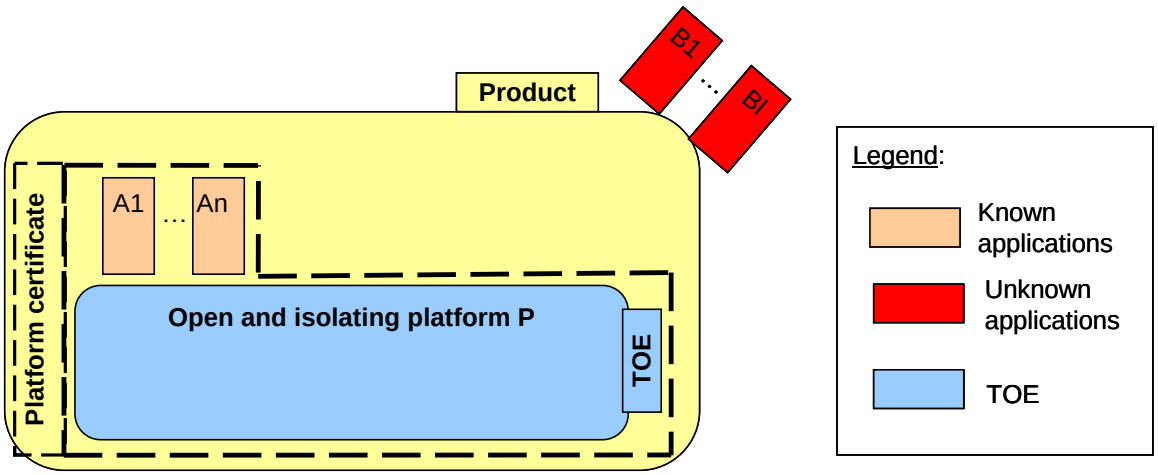
- It will precise that the isolation of applications, and also the protection of post-issuance application loading have been studied in order to identify that this platform is conformant to the concept of "open and isolating platform". The "evaluated configuration chapter" will precise that the evaluated product is an "open and isolating platform".
- It will identify, in the "architecture" and "evaluated configuration" chapters, all the known applications that have been checked by the ITSEF during the evaluation process[6]. It will also precise that all the identified applications in the certification report have been checked according to the OE1 and OE2 objectives.
- The "evaluated configuration" chapters will also precise that products constituted of a subset of known applications are also certified.
- The "usage restrictions" chapter shall state the constraints OE1 and OE2 and the references to the guidance [ISO_VERIF], [ORG_LOAD] and [TECH_LOAD], which apply to any application loaded in the product, in particular any new application unknown at evaluation time. Note that this chapter may also contain usage restrictions that are not linked to the open and isolation properties of the platform.
- It will describe in the "product life cycle" chapter, the different type of application loading applicable to the product and considered by the developer.
- It may contain as well the list of known application for which OE1 only has been verified. In such cases, the certificate will unambiguously identify these applications and indicate the usage restriction, requiring the final user to apply the guidance documentations to fulfil OE2.

The loading of unknown applications as Bi ($i \in [1,l]$) implies that the product no more fully suits the product's architecture stated in the open and isolating platform certificate. The evaluation results are only valid if all the other applications loaded on the platform respect the platform certification constraints. Thus the resulting product architecture which respects the security constraints of the associated certificates can be considered as certified. It is up to the risk manager to rely on the assurance of verification of OE1 and OE2 provided by the actor in charge of the deployment of these applications or to rely on the schema. In this last case (if the CC schema solution is selected), the sponsor will then ask for maintenance as stated in chapter 2.3 hereafter.

[6] Those known applications correspond to applications already hosted by the platform included in the product version available to the ITSEF(post issuance applications) or to applications provided by the developer to the ITSEF that are intended to be loaded post-issuance.

The following picture shows the certified product. Here the TOE only corresponds to the platform. Ai (i ∈ [1,n]) applications correspond to known pre-issuance applications and are then identified in the platform certification report.

Figure 2 Product related to an open and isolating platform TOE



2.3. Open and isolating platform maintenance

The assurance continuity process can be applied to open and isolating platform certificates like any other certificate. This chapter only deals with the specificities of this process for open and isolating platform when no major change of the platform has been performed, and when the developer wants the certified product to include some applications that where unknown during the initial evaluation.

The certificate restrictions concerning these new applications must be checked. When the verification and loading of these new applications is done in the same previously evaluated way than for the known applications, thus responding to OE1 and OE2, a maintenance report can be issued if the site visit report is still valid.

The developer will have to provide the evidences related to those new applications with its impact analysis (same type of evidences than those provided during the initial evaluation process for applications Ai, i ∈ [1,n])). The impact analysis shall also describe the main functionality of the new applications (applications Bj, (j ∈ [1,l])).

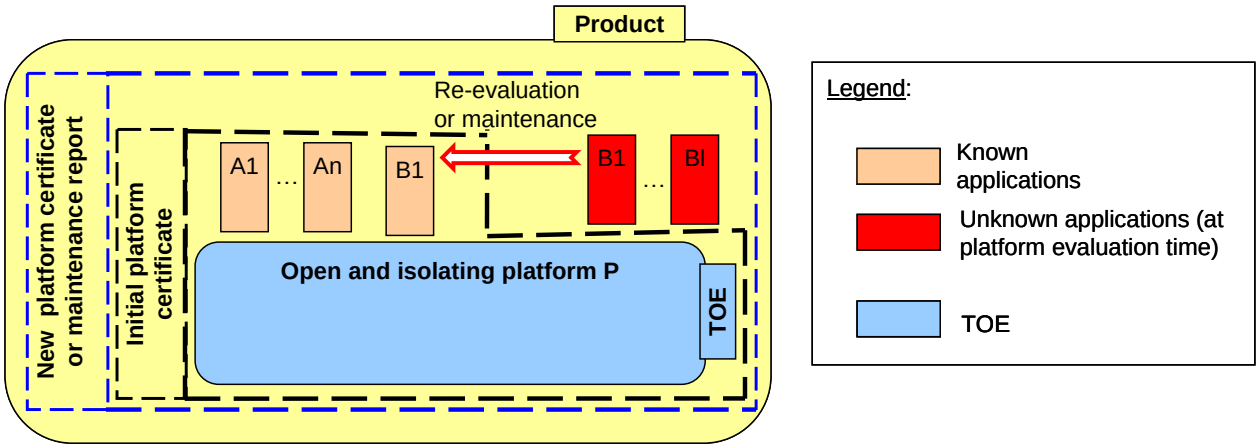


Figure 3 Maintained product related to an open and isolating platform TOE

3. Applications on an open and isolating platform

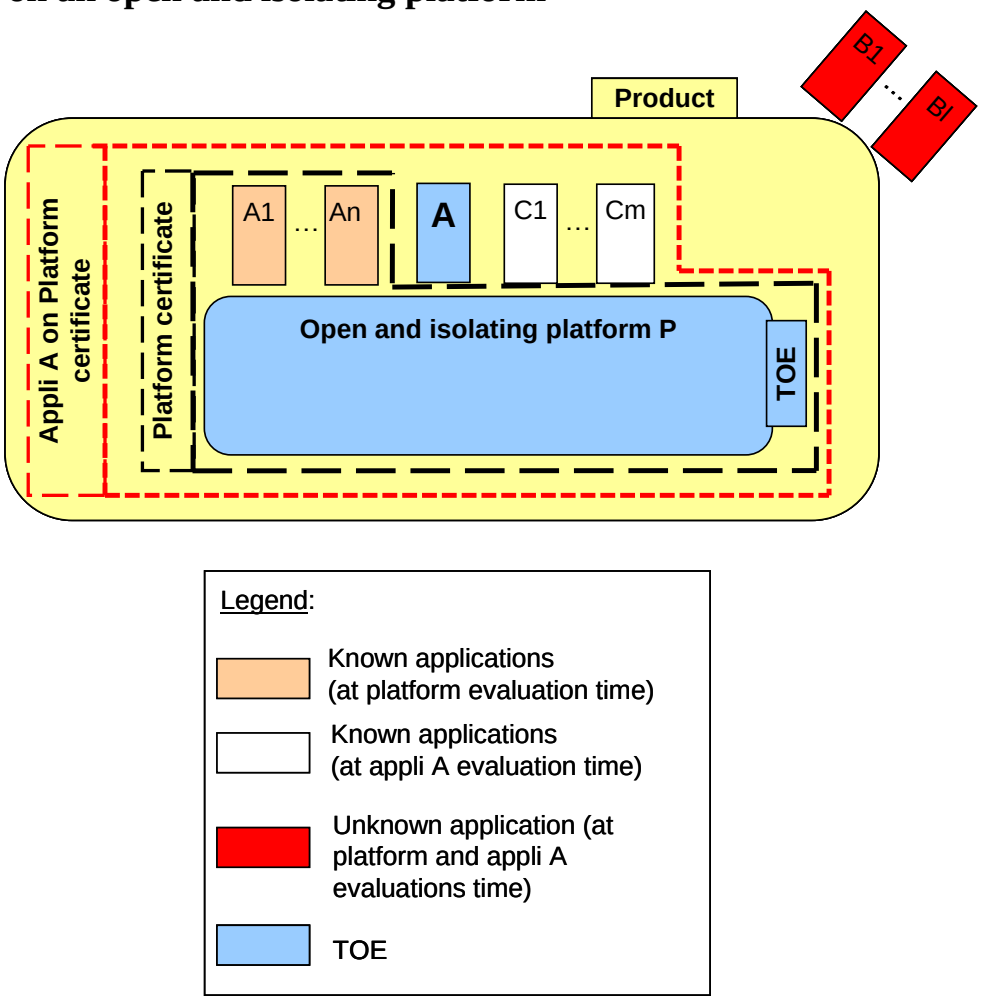


Figure 4 Standard certificate TOE and related product

In this picture, platform P and applications Ai (i ∈ [1,n]) have been evaluated and have led to an open and isolating platform certificate. All Ai applications are identified in the platform certificate.

Applications A and Cj (j ∈ [1,m]) correspond to application loaded after the platform certification but known at application evaluation time. They might either correspond to post (case 3) or pre-issuance (case 1 or 2) applications.

Application A is the application targeted by the application on platform evaluation. We consider here that this evaluation is done according to the composition process [Compo] with reference to:

- the usual security application development guidance for applications that provide security functionality;
- the guide [ISO_VERIF] that describes the constraints imposed to the applications in order to maintain the isolation property;
- and possibly the application loading protection guidance [ORG_LOAD] or [TECH_LOAD].

So the considered TOE here is the “application A on platform P”. Of course other specific CC activities will have to be performed by the ITSEF. This chapter only focus on the requirements imposed by the open and isolating platform evaluation.

3.1. Evaluation

3.1.1. Objectives from the platform certificate

The standard evaluation process requires considering all the known applications. The applications Ai have already been considered at platform evaluation and are identified in the platform certificate report (see 2.2). So in the resulting A on P certification report all the new known applications Cj have to be identified according to the rules defined in 2.1.1.2.

To precise the way OE1 and OE2 are realized, the security target shall detail actors implied in the development, in the verification and in the distribution of the applications, and their roles. The security target should also describe the evaluation scope regarding this detailed lifecycle.

The ITSEF will have to check that all applications respect the platform requirements OE1 and OE2 and that all applications Ai and Cj fulfill the security functional compatibility constraints of application A (see chapter 3.1.2).

For the applications Cj the respect of the requirements OE1 and OE2 shall be evaluated following the same rules than for the known applications Ai at platform evaluation time (see paragraph 2.1.5), with reference to platform guidance (see paragraph 2.1.4).

For the targeted application A the respect of the two requirements OE1 and OE2 shall be realised during the composition activities (see assurance requirements ADV_COMP of [Compo]) and may follow the rules defined in 2.1.5 with reference to platform guidance defined in 2.1.4 as for the Cj applications.

The loading of unknown applications as Bk ($k \in [1,m]$) implies that the product no more fully suit the product's architecture stated in the open and isolating platform certificate of A on P. The evaluation results are only valid if all the other applications loaded on the platform respect the platform certification constraints. The product's architectures which respect the security constraints of the associated certificates can be considered as certified. It is up to the risk manager to rely on the assurance of verification of OE1 and OE2 provided by the actor in charge of the deployment of these applications or to rely on the schema. In this last case, the sponsor will then ask for maintenance as stated in chapter 3.3 hereafter.

3.1.2. Applications security functional compatibility

The targeted A application may require the respect by the co-existing applications of some specific security constraints (for instance, an e-passport application can't coexist with an application that allows the transmission of the user identity without its agreement) that are explicitly described in the application A guide AGD_OPE.

Pre-requisite: The main functionality of application loaded pre-issuance (applications Ai ($i \in [1,n]$)) shall be described in the ETR and ETR-COMP related to the platform evaluation.

The ITSEF will have to check that functionalities of applications Cj and Ai fulfil the security constraint required by application A.

If only some specific product architectures could be certified, regarding the functional compatibility analysis, the ITSEF shall mentioned it to the developer and ask him to provide each of those product's architecture.

3.2. Certification

All coexisting applications[7] with the certified one are identified in such a certification report like in a open and isolating platform (see 2.2). But the "evaluated configuration" chapter of the certification report will precise that products constituted of a subset of known applications are also certified.

3.3. Application on open and isolating platform maintenance

In case the developer wants the certified product include some unknown applications such as Bk too the certificate restrictions concerning these applications must be raised.

A maintenance report may be provided:

- when the verification and loading of these applications is done in the same way than for the known applications Ai or Cj, thus responding to OE1 and OE2 requirements;
- and there is no functional compatibility constraints required by the certified A application.

The developer will have to provide the evidences related to those new applications loading with its impact analysis (same type of evidences than those provided during the initial evaluation process for application Ai or Cj). The impact analysis shall also describe the main functionality of the new applications Bk.

If this loading is made according to organizational measures, the certification body will be able to publish a maintenance report only if the site visit report is still valid.

[7] Known applications.

Annex A: Compatibility with existing “open platform” PPs

The following table identifies the applicability of the open and isolating platform certification approach to the evaluation realised in conformance to the PP [JCO/2.6], [JCO/3.0] or [USIM] and defines the additional requirements that shall be present in the Security Target of the platform.

	[JCO/2.6]	**[JCO/3.0]**	**[USIM]** **(conform to [JCO/2.6])**
O1: isolation between applications	*O.FIREWALL*	*O.FIREWALL*	*O.FIREWALL of [JCO/2.6]*
O2: protection of post issuance loading (authenticity & integrity)	*O.LOAD* ***This objective shall also precise that it is intended to ensure the integrity and authenticity of loaded CAP files, with regards to the verification***	*O.LOAD*	*O.LOAD of [JCO/2.6]* *O.APPLI-AUTH*
OE1: verification of application according to the constraints related to the isolation property of the platform	*OE.VERIFICATION* ***This objective needs to be enlarged to take into account the specific constraints of the considered platform defined in [ISO_VERIF] guide*** *(NB: composition rules will impose this verification to the certified applets, but non-certified applets should also be verified).*	*OE.VERIFICATION*	*OE.VERIFICATION of [JCO/2.6]* *OE.BASIC-APPS-VALIDATION*
OE2: availability of an integrity and of authenticity evidences for each application	***An objective needs to be added in order to allow the evaluation to claim conformance to the open and isolating platform certification approach.*** *(linked with the application note of O.LOAD about the verification of the application integrity)*	*OE.CODE-EVIDENCE*	*OE.VERIFICATION-AUTHORITY*