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, le 05 novembre 2014

N° 4758/ANSSI/SDE/PSS/CCN

Référence : ANSSI-CC-NOTE-10/1.0

NOTE D'APPLICATION

CERTIFICATION DE PRODUITS OUVERTS DE TYPE CARTE A PUCE

Application : Dès son approbation.

Diffusion : Publique.

Le directeur général
de l'agence nationale de la sécurité
des systèmes d'information

Guillaume POUPARD

[ORIGINAL SIGNE]

Suivi des modifications

Edition	Date	Modifications
0	16/12/2010	Création pour la phase expérimentale.
1.0	05/11/2014	Mise en cohérence avec la note JIL du 4 février 2013, version 1.1 (for trial use) rédigée sur la base de la version 0 du présent document.

La présente procédure est disponible en ligne sur le site institutionnel de l'ANSSI (www.ssi.gouv.fr).

Table des matières

1. Contexte et objet du document

1.1. Définitions

Le terme « produit » désigne ici un terme générique correspondant à une TOE associée à son environnement.

Le terme « plateforme » est utilisé ici conformément à la terminologie de la note [Compo] sur le processus de composition de résultats d'évaluation, appliquée au cas d'évaluation en composition "application sur plateforme". Ainsi, un produit désigné ici comme "plateforme" correspond à un microcircuit associé à un système d'exploitation logiciel et parfois à du code natif.

Une « plateforme ouverte » correspond à une plateforme qui, après sa livraison à l'utilisateur final (c'est-à-dire à la septième phase du cycle de vie classique d'une carte à puce), permet le chargement de nouvelles applications. De tels chargements sont dénommés chargements « *post-issuance* » (chargements d'applications après livraison du produit à l'utilisateur final).

Des applications peuvent être installées avant la septième phase, il s'agit alors de chargements « *pre-issuance* ».

Une « plateforme fermée » correspond à une plateforme qui ne peut pas accueillir de nouvelles applications après la livraison du produit à l'utilisateur final.

Une « plateforme cloisonnante » correspond à une plateforme qui maintient la séparation des domaines d'exécution de toutes les applications embarquées sur la plateforme et de la plateforme elle-même. Le terme « cloisonnante » s'applique autant au domaine de séparation des applications qu'à la protection de leurs données.

L'« architecture » correspond au plus haut niveau de structure du produit, à savoir la « plateforme ouverte » avec toutes les applications chargées sur le produit (en *pre-issuance* ou *post-issuance*).

Etant donné que le chargement de nouvelles applications peut être pris en considération avant ou après le processus d'évaluation, nous parlerons d'applications connues et d'applications inconnues afin de distinguer les applications qui auront été prises en compte pendant le processus d'évaluation de celles qui ne l'auront pas été.

Les « applications connues » correspondent aux applications présentes dans l'architecture originale du produit certifié. Elles sont toutes prises en compte par le CESTI durant le processus d'évaluation[1].

Les « applications inconnues » sont des applications qui n'étaient pas connues au moment de l'évaluation. Elles constituent une modification de l'architecture du produit évalué, par rapport à celui fixé dans le rapport de certification.

[1]Elles ne font pas nécessairement partie de laTOE.

1.2. Périmètre

Ce document décrit la procédure de certification de produits ouverts permettant de garantir que toute modification d'architecture du produit n'impacte pas les fonctions de sécurité ayant déjà fait l'objet d'un certificat. La modification de l'architecture du produit initial correspond ici à l'ajout d'applications (modification de l'environnement de la TOE).

Il est à noter, contrairement à la situation évoquée ci-dessus, qu'une modification de la plateforme nécessitera une nouvelle certification (et par conséquent de l'ensemble du produit) ou une maintenance.

Afin que le certificat prenne en compte les évolutions du produit, les plateformes doivent disposer de propriétés de sécurité, plus particulièrement de propriétés cloisonnantes, pour les applications activées sur le produit. Seuls les produits offrant ces propriétés cloisonnantes pourront assurer que l'exécution d'une nouvelle application n'aura pas de conséquences sur la fonctionnalité déjà certifiée. Ces plateformes, évaluées dans le but de démontrer qu'elles offrent ces garanties (sous certaines contraintes), sont ici dénommées "plateformes ouvertes cloisonnantes".

Lorsque de nouvelles applications sont chargées sur de tels produits ouverts, des vérifications sur le respect des contraintes de sécurité de la plateforme par ces nouvelles applications sont impératives pour s'assurer que le produit atteigne le niveau AVA_VAN considéré dans le cadre de l'évaluation.

Les plateformes ouvertes qui ne garantissent pas le cloisonnement des applications sont certifiées comme des plateformes fermées. Les plateformes fermées qui n'autorisent pas le chargement *post-issuance* sont exclues du périmètre de ce document.

1.3. Plan

Le chapitre 2 fixe la démarche applicable pour l'évaluation et la certification de « plateformes ouvertes cloisonnantes ».

Le chapitre 3 fixe la démarche applicable pour l'évaluation d'applications sur une « plateforme ouverte cloisonnante » certifiée.

2. Plateforme « ouverte cloisonnante »

2.1. Évaluation

Une plateforme ouverte cloisonnante fera, dans ce document, référence à une plateforme évaluée conformément aux éléments déclinés ci-dessous.

2.1.1. Objectifs

2.1.1.1. Fonctionnalités analysées

Une plateforme ouverte cloisonnante devra disposer des fonctions à évaluer suivantes :

- O1 : le cloisonnement entre toutes les applications chargées sur la plateforme considérée, et donc la protection contre les applications potentiellement hostiles ;

et

- O2 : la protection du chargement *post-issuance* d'applications sur la plateforme considérée, en vérifiant l'intégrité et l'authentification de la vérification[2] de chaque application, avant leur activation[3] grâce aux éléments de preuves définies dans l'OE2 ci-après.

O1 et O2 devront être des objectifs sur la TOE définis dans la cible de sécurité de la plateforme.

2.1.1.2. Environnement de l'évaluation

L'évaluation d'une plateforme ouverte cloisonnante doit imposer, pour toutes les futures applications à charger sur la plateforme, les contraintes suivantes:

- OE1 : toutes les applications qui seront chargées sur la plateforme doivent être vérifiées, vis-à-vis des contraintes et exigences relatives aux propriétés de cloisonnement d'applications imposées par la plateforme, avant leur installation effective (activation) ;

et

- OE2 : la mise à disposition d'une preuve d'intégrité de chaque application chargée sur la plateforme (afin de s'assurer qu'elle n'a pas subi de modifications depuis la vérification des précédentes contraintes OE1), ainsi que d'une preuve d'authenticité de ces vérifications.

OE1 et OE2 devront être des objectifs sur l'environnement et doivent être identifiés dans la cible de sécurité de la plateforme.

Notons que OE1 et OE2 sont applicables à toutes les applications, qu'elles soient évaluées ou non, connues ou inconnues.

Pour les applications connues, le respect des objectifs OE1 et OE2 devra être vérifié par le CESTI. Cependant, il est possible de vérifier seulement OE1 et de décrire comment respecter OE2[4]. Le

[2] Ce qui est chargé est ce qui a été vérifié.

[3] C'est-à-dire avant que le fichier chargé devienne une application exploitable par l'utilisateur final.

[4] Ceci est valable si des mesures organisationnelles permettent le respect d'OE2, ce qui est autorisé dans certaines phases du cycle de vie, voir paragraphe 2.1.3.

CESTI vérifiera alors le respect d'OE1 et évaluera les guides utilisés pour OE2. Dans ce cas, le certificat identifiera clairement les applications connues et indiquera les restrictions d'usage, imposant à l'utilisateur final de se conformer à la documentation pour respecter OE2.

Pour les applications inconnues, la vérification du respect d'OE1 et OE2 n'étant pas possible, elles devront respecter les restrictions d'usage définies clairement dans le certificat, imposant à l'utilisateur final de se conformer à la documentation pour respecter les objectifs OE1 et OE2.

2.1.2. Identification

De manière générale, la certification de plateforme ouverte devrait permettre l'identification du produit évalué par le CESTI, c'est à dire :

- l'identification du produit dans la version soumise à l'évaluation (version fournie au CESTI). Cela inclut toutes les applications connues chargées *pre-issuance* ;
- l'identification de toutes les applications connues susceptibles d'être chargées *post-issuance*.

L'identification de la plateforme et l'inventaire de toutes les applications chargées devront permettre de distinguer la TOE du produit.

L'évaluation devra considérer l'ensemble du produit quelle que soit la TOE. Par conséquent, les données d'identification des composants de la plateforme et des applications connues devront être spécifiées dans la cible de sécurité. Ces éléments seront également spécifiés dans le rapport de certification de la plateforme.

Le développeur devra donner les moyens nécessaires au CESTI pour qu'il vérifie que les références du produit, dont dispose le CESTI, correspondent à un ensemble de composants connus par le CESTI (que les éléments appartiennent ou non à la TOE).

Ces exigences permettent d'éviter la certification de produits comprenant des applications ne respectant pas les contraintes de la plateforme, c'est-à-dire pouvant être hostiles pour d'autres applications déjà chargées sur le produit.

2.1.3. Cycle de vie

La figure ci-dessous présente un modèle des phases du cycle de vie d'une plateforme ouverte : il s'agit d'un exemple illustrant un tel cycle, le point de livraison ALC pourra être différent de celui ici mentionné.

Le point de livraison considéré ici peut également être décalé dans le temps si des éléments probants émanant de certification de sites ou de résultats d'audits comparables sont fournis.

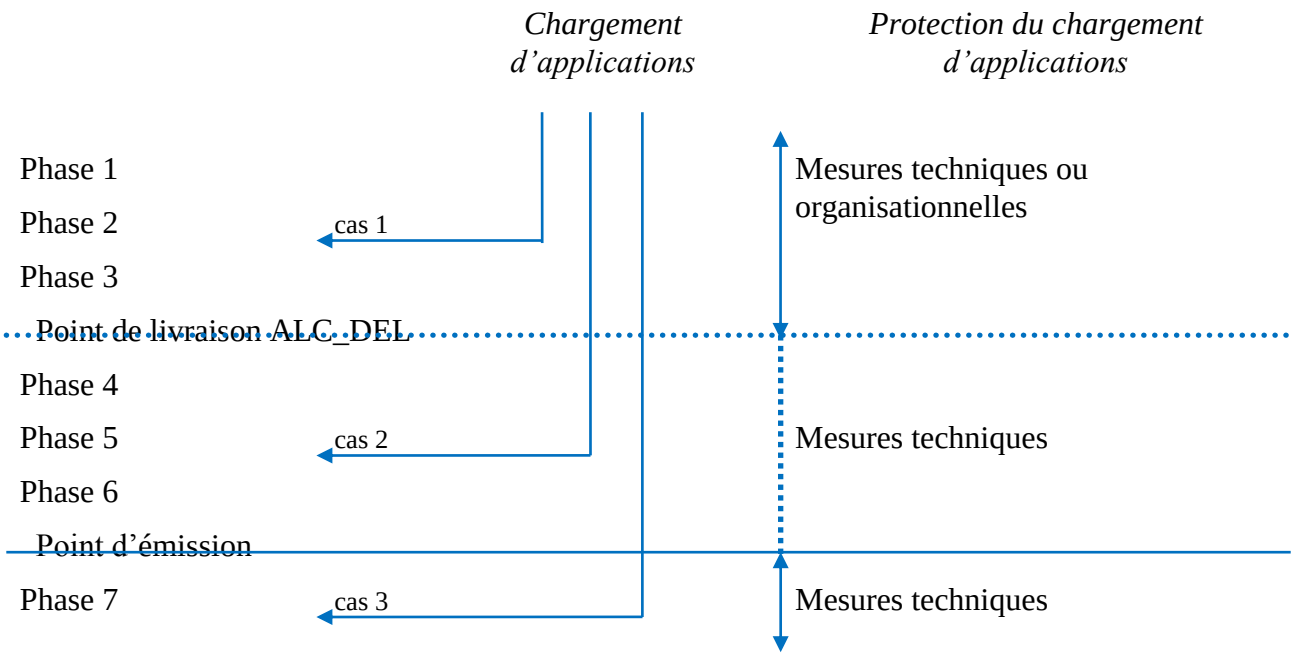

Figure 1 : cycle de vie d'une plateforme ouverte cloisonnante[5]

Une plateforme ouverte cloisonnante peut contenir des applications *pre-issuance* et *post-issuance*.

Les mesures permettant de réaliser l'objectif OE2 peuvent être différentes, en fonction du moment où s'effectue le chargement.

Trois cas sont à distinguer :

- cas 1 : l'application est chargée en *pre-issuance* et avant le point de livraison : des mesures organisationnelles ou techniques peuvent être mises en œuvre pour renforcer l'objectif OE2 ;
- cas 2 : l'application est chargée en *pre-issuance* et après le point de livraison : des mesures organisationnelles ne sont pas acceptées, des mesures techniques doivent être mises en œuvre ;
- cas 3 : l'application est chargée en *post-issuance* (après mise à disposition du produit à l'utilisateur final) : des mesures techniques associées à l'objectif OE2 doivent être mises en œuvre.

Par définition, toutes les plateformes considérées autorisent le chargement d'applications *post-issuance*, cas 3 (au moins en phase 7).

Pour préciser la manière dont OE1 et OE2 sont réalisés, la cible de sécurité devra décrire les processus et leurs différents rôles impliqués dans le développement, la vérification et la distribution de l'application. La cible de sécurité devra également décrire le périmètre d'évaluation en tenant compte de ce cycle de vie détaillé.

[5] Les phases 1 à 7 sont utilisées telles que définies dans le Profil de Protection BSI-CC-PP-00035-2007.

Dans le cas où les applications connues font partie du produit évalué, les détails du cycle de vie suivant doivent donc également être décrits dans la cible de sécurité :

- l'identification des acteurs et de leur rôle dans la gestion des processus de vérification de l'application ;
- l'identification des acteurs et de leur rôle dans la gestion des processus de protection d'intégrité et d'authenticité des applications, de leur vérification à leur chargement.

De plus, le point de livraison ALC peut être différent entre la plateforme certifiée et la certification en composition avec des applications venant s'ajouter sur la plateforme certifiée (voir chapitre 3). Un cas pratique type pourrait être que le point de livraison ALC soit déplacé à une étape ultérieure. De ce fait, la certification en composition changerait la classification des phases en respectant le fait qu'elles se situent dans le cas 1 ou le cas 2. Les phases de certification de la plateforme du cas 2 pourraient devenir celles du cas 1 pour la certification en composition, puisque le point de livraison est reporté, et donc n'exigeraient pas de mesures techniques. Une telle reclassification est acceptée et ne contredit ni n'impacte la certification de la plateforme.

2.1.4. Documentation du produit

Concernant l'environnement de l'évaluation identifié au chapitre 2.1.1.2, les guides spécifiques suivants doivent être fournis par le développeur :

- guide de développement d'application (concernant OE1), où sont définies les règles de vérification d'autorisation décrivant les contraintes de sécurité imposées à l'application pour garder les propriétés cloisonnantes de la plateforme [ISO_VERIF] ;
- guide de protection du chargement d'application (concernant OE2), décrivant :
    - les mesures organisationnelles pour le chargement d'application [ORG_LOAD][6] ;
    - les mesures techniques pour le chargement d'application qui doivent décrire la façon d'activer les fonctions (correspondant à O2) liées à la plateforme, associées aux mesures nécessaires pour garantir l'authenticité des vérifications (par exemple la protection de clefs) [TECH_LOAD].

Comme les plateformes ouvertes cloisonnantes permettent toujours le chargement d'application dans le cas 3, [ISO_VERIF] et [TECH_LOAD] doivent toujours être fournis par le développeur.

Le développeur doit fournir [ORG_LOAD] uniquement s'il est dans le cas 1 et s'il a décidé de répondre aux contraintes définies ici avec des mesures organisationnelles.

A noter que [ISO_VERIF] ne correspond pas aux guides de l'AGD_OPE (guides définissant les règles pour l'implémentation d'applications sécurisées). [ISO_VERIF] liste toutes les règles de développement relatives à la maintenance des propriétés de cloisonnement de la plateforme entre applications. Une partie des guides AGD_OPE dédiée au développement d'application liste toutes les règles de développement relatives à une application devant présenter des propriétés spécifiques de sécurité.

Ces guides devront être évalués suivant les classes AGD ou ALC en fonction des cas de chargement pris en compte par le développeur.

[6] Ce guide fait partie des exigences de sécurité d'assurance ALC.

2.1.5. Configuration évaluée

Selon le cycle de vie du produit considéré, le CESTI devra traiter OE1 et OE2 de la manière suivante :

1. le CESTI devra systématiquement vérifier que toutes les applications connues respectent bien les contraintes OE1. Le CESTI pourra s'appuyer sur les preuves du développeur afin de s'assurer que la vérification de l'application a été effectuée. Comme cela n'est pas vérifié pour les applications inconnues, la conformité à [ISO_VERIF] consistera en une restriction d'usage du certificat ;
2. quand les mesures organisationnelles sont mises en place avant le point de livraison, le chargement de l'application est sous la responsabilité du développeur. La protection associée réalisée par l'objectif OE2 est couverte par les exigences d'assurance ALC. Par conséquent, les mesures organisationnelles doivent être auditées ;
3. dans le périmètre de cette note, les mesures techniques qu'imposent OE2 sont toujours utilisées, au moins pour le cas 3. Les exigences associées sont données dans [TECH_LOAD] et une partie peut être imposée par les exigences d'assurance ALC. De ce fait les mesures organisationnelles correspondantes doivent être auditées. La conformité au [TECH_LOAD] consistera en une restriction d'usage du certificat.

Ainsi OE1 et OE 2 doivent être vérifiés pour toutes les applications connues.

2.2. Certification

Un rapport de certification pour une plateforme ouverte cloisonnante doit comporter les particularités suivantes :

- il précisera que le cloisonnement d'une part et les mécanismes de protection du chargement *post-issuance* d'autre part ont été étudiés, afin d'identifier cette plateforme comme conforme au concept de « plateforme ouverte cloisonnante » décrit ici. Le chapitre « configuration évaluée » précisera que le produit évalué est une « plateforme ouverte cloisonnante » ;
- il identifiera, aux chapitres « architecture du produit » et « configuration évaluée », l'ensemble des applications connues qui ont été vérifiées par le CESTI durant l'évaluation[7]. Il précisera également que toutes les applications identifiées dans le rapport de certification ont été vérifiées conformément aux objectifs OE1 et OE2 ;
- le chapitre « configuration évaluée » précisera que les produits, constitués d'un sous ensemble d'applications connues, sont aussi certifiés ;
- le chapitre « restriction d'usage » doit indiquer les contraintes des objectifs OE1 et OE2 et les références des guides [ISO_VERIF], [ORG_LOAD] et [TECH_LOAD] s'appliquant à toutes les applications chargées sur le produit et, en particulier, à toutes les nouvelles applications inconnues au moment de l'évaluation. Ce chapitre peut également contenir les restrictions d'utilisation qui ne sont pas rattachées aux propriétés de la plateforme ouverte cloisonnante ;

[7] Ces applications connues correspondent soit aux applications déjà présentes sur la plateforme et incluses dans la version du produit mise à disposition du CESTI (application *pre-issuance*) ; soit aux applications fournies par le développeur au CESTI et destinées à être chargées en *post-issuance*.

- il identifiera au chapitre « cycle de vie du produit » les différents modes de chargement d'applications du produit envisagés par le développeur ;
- il pourra aussi contenir la liste des applications connues pour lesquelles seulement OE1 a été vérifié. Dans ce cas, le certificat identifiera clairement ces dernières et indiquera les restrictions d'usages et les guides à appliquer pour l'utilisateur final afin de respecter OE2.

Le chargement d'applications inconnues, nommées Bi (i ∈ [1,I]), induit que le produit ne correspond plus totalement à l'architecture du produit dans le certificat de la plateforme ouverte cloisonnante. Les résultats d'évaluation restent valables uniquement si toutes les applications Bi chargées sur la plateforme répondent aux contraintes de la certification de la plateforme. Ainsi les architectures des produits respectant les contraintes de sécurité des certificats associés peuvent être considérées comme certifiées. Il appartient au gestionnaire de risques de s'appuyer sur l'assurance de la vérification de OE1 et OE2, fournie par les acteurs en charge du développement de ces applications, ou bien sur le schéma de certification. Dans ce dernier cas, le commanditaire demandera une maintenance du certificat suivant les modalités fixées au chapitre 2.3 ci-après.

La Figure 2 montre le produit certifié dans le cas où la TOE correspond à la plateforme. Ai (i ∈ [1,n]) correspondent aux applications connues *pre-issuance* qui sont ensuite identifiées dans le rapport de certification de la plateforme.

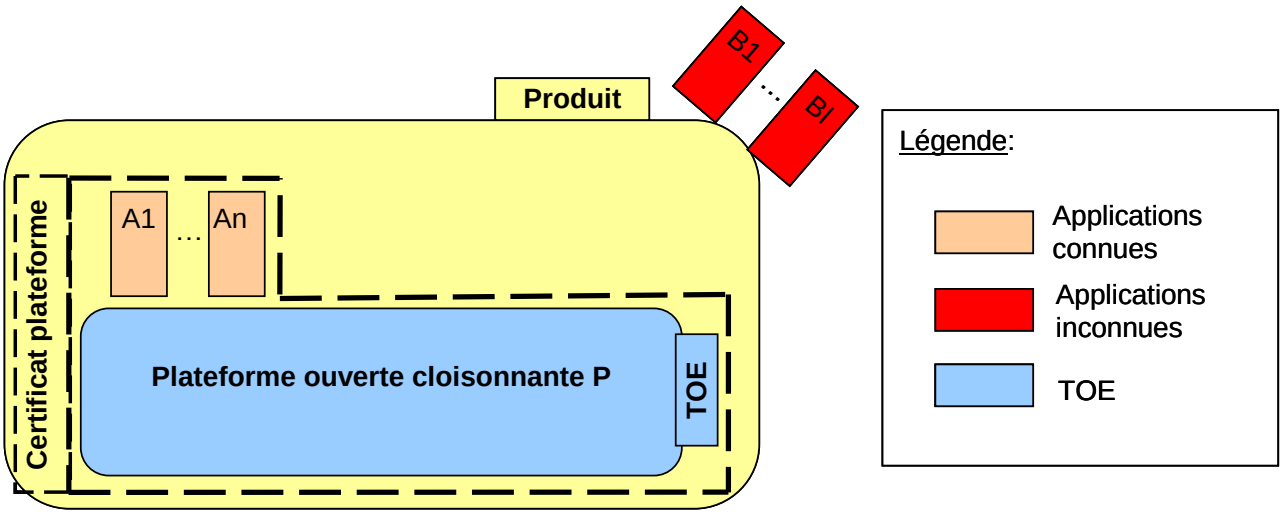

Figure 2 Produit avec une plateforme ouverte cloisonnante en TOE

2.3. Maintenance

Le processus de maintenance peut être appliqué aux certifications de plateforme ouverte cloisonnante comme à tout autre certificat. Ce chapitre ne traite que des spécificités de ce processus pour une plateforme ouverte cloisonnante quand aucun changement majeur n'a été effectué sur la plateforme, et quand le développeur veut que le produit certifié prenne en compte des applications inconnues lors de l'évaluation initiale.

Les restrictions d'usage du certificat concernant ces nouvelles applications doivent être vérifiées. Si la vérification et le chargement de ces nouvelles applications sont effectués de la même manière que pour les applications connues, répondant donc aux objectifs OE1 et OE2, un rapport de maintenance pourra être édité si le rapport de visite de site est encore valide.

Le développeur devra fournir les preuves relatives à ces nouvelles applications chargées ainsi que l'analyse d'impact (avec le même mode de preuve que celles fournies pendant le processus d'évaluation initiale pour les applications Ai, i ∈ [1,n]). L'analyse d'impact doit aussi décrire les fonctions principales des nouvelles applications (applications Bj, j ∈ [1,I]).

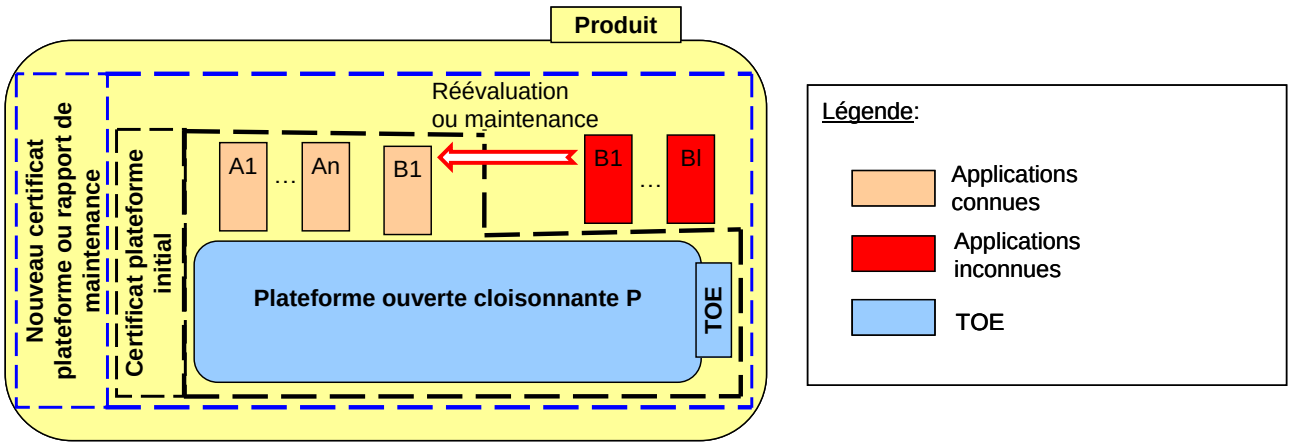

Figure 3 Maintenance de produit avec une plateforme ouverte cloisonnante en TOE

3. Applications sur une plateforme ouverte cloisonnante

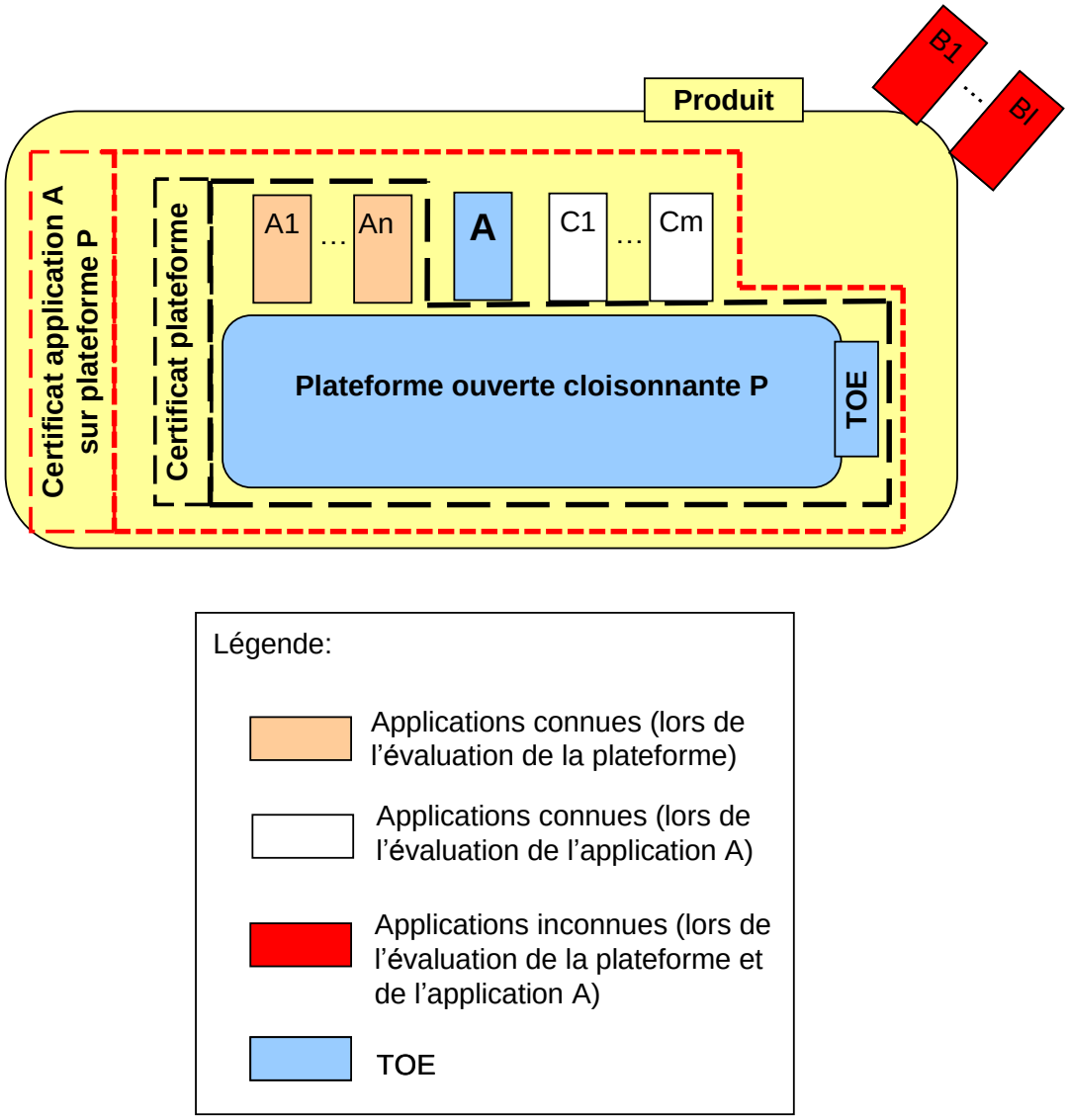

Figure 4 Certification de la TOE

Sur la Figure 4, la plateforme P et ses applications Ai (i ∈ [1,n]) ont été évaluées et ont mené à un rapport de certification de la plateforme ouverte cloisonnante. Toutes les applications Ai sont identifiées dans le certificat de la plateforme.

Les applications A et Cj (j ∈ [1,m]) correspondent aux applications chargées après la certification de la plateforme mais connues lors de l'évaluation de celle-ci. Elles peuvent correspondre aux applications soit *post-issuance* (cas 3), soit *pre-issuance* (cas 1 et 2).

L'application A est l'application ciblée par l'évaluation de la plateforme. On peut envisager ici l'évaluation suivant le processus de composition [Compo] avec les références suivantes :

- le guide de développement courant de sécurité des applications, pour les applications qui fournissent des fonctions de sécurité ;

- le guide [ISO_VERIF] décrivant les contraintes imposées aux applications afin de maintenir les propriétés de cloisonnement ;
- éventuellement les guides [ORG_LOAD] et [TECH_LOAD] de protection du chargement d'applications.

Ainsi, la TOE considérée ici est « l'application A sur la plateforme P ». Bien entendu, d'autres activités spécifiques seront réalisées par le CESTI. Ce chapitre se concentre seulement sur les exigences imposées par l'évaluation de la plateforme ouverte cloisonnante.

3.1. Evaluation

3.1.1. Objectifs issus de l'évaluation de la plateforme ouverte cloisonnante

Le processus traditionnel d'évaluation demande de considérer toutes les applications connues. Les applications Ai ont déjà été considérées dans l'évaluation de la plateforme et sont identifiées dans le rapport de certification de la plateforme (voir 2.2). Dans le rapport de certification de A sur P, toutes les nouvelles applications Cj doivent donc être identifiées suivant les règles définies en 2.1.1.2.

Afin de préciser la façon dont les objectifs OE1 et OE2 sont réalisés, la cible de sécurité devra décrire tous les acteurs et leurs différents rôles impliqués dans le développement, la vérification et la diffusion de l'application. La cible de sécurité doit aussi décrire le périmètre d'évaluation concernant ce cycle de vie.

Le CESTI devra vérifier que toutes les applications répondent bien aux exigences de la plateforme OE1 et OE2 et que toutes les applications Ai et Cj sont, en terme de sécurité, fonctionnellement compatibles avec l'application A (voir chapitre 3.1.2).

Pour les applications Cj, le respect des exigences OE1 et OE2 devra être évalué suivant les mêmes règles que pour les applications connues Ai lors de l'évaluation de la plateforme (voir paragraphe 2.1.5), avec les références au guide de la plateforme (voir paragraphe 2.1.4).

La vérification, pour l'application A visée, du respect des deux exigences OE1 et OE2 devra être réalisée dans le cadre de l'évaluation en composition (au titre des composants d'assurance ADV_COMP de [Compo]) et pourra suivre les règles définies en 2.1.5 avec les références des guides de la plateforme définis en 2.1.4 comme pour les applications Cj.

Le chargement d'applications inconnues, nommées Bk ($k \in [1,m]$) signifie que le produit ne correspond plus totalement à l'architecture du produit dans le certificat de la plateforme ouverte cloisonnante de A sur P. Les résultats d'évaluation restent valables uniquement si toutes les applications chargées sur la plateforme répondent aux contraintes de la certification de la plateforme. Les architectures des produits respectant les contraintes de sécurité des certificats associés peuvent être considérées comme certifiées. Il appartient au gestionnaire de risques de s'appuyer sur l'assurance de la vérification de OE1 et OE2, fournie par les acteurs en charge du développement de ces applications, ou bien sur le schéma de certification. Dans ce dernier cas, le commanditaire demandera une maintenance du certificat suivant les modalités fixées au chapitre 3.3 ci-après.

3.1.2. Compatibilité des applications de sécurité fonctionnelles

L'application A peut nécessiter le respect, pour les applications coexistantes, de certaines contraintes de sécurité (par exemple, une application e-passeport ne peut coexister avec une application permettant la diffusion, à l'insu du porteur, de son identité), ce qui est décrit dans le guide AGD_OPE de l'application A.

Pré-requis : La fonction principale des applications chargées pre-issuance (applications Ai (i ∈ [1,n])) devra être décrite dans le Rapport Technique d'Evaluation (RTE) et le RTE-Comp de l'évaluation plateforme.

Le CESTI devra vérifier que les fonctionnalités des applications Cj et Ai respectent les contraintes de sécurité demandées par l'application A.

Au vu des résultats de l'analyse de la compatibilité des fonctionnalités, si seulement certaines architectures spécifiques de produit ne peuvent être certifiées, le CESTI devra le mentionner au développeur et lui demander de fournir chacune de ces architectures produit.

3.2. Certification

Toutes les applications coexistantes[8] avec l'application certifiée sont identifiées dans le rapport de certification comme dans le cas d'une plateforme ouverte cloisonnante (voir chapitre 2.2). Cependant, le chapitre « configuration évaluée » du rapport de certification précisera que ces produits, qui constituent un sous-ensemble d'applications connues, sont aussi certifiés.

3.3. Maintenance

Dans le cas où le produit inclut certaines applications inconnues comme Bk, et que le développeur veut le faire certifier, les restrictions d'usage du certificat concernant ces applications devront être levées.

Un rapport de maintenance peut être fourni :

- quand la vérification et le chargement de ces applications sont faits de la même manière que pour les applications connues Ai ou Cj, donc répondant aux exigences OE1 et OE2 ;
- s'il n'y a pas de contrainte de compatibilité fonctionnelle demandée par l'application certifiée A.

Le développeur devra fournir les preuves de ces nouveaux chargements d'applications avec leur analyse d'impact (avec le même type de preuves que celles fournies pendant le processus d'évaluation initial des applications Ai et Cj). L'analyse d'impact devra décrire les fonctionnalités principales des nouvelles applications Bk.

Si ce chargement est effectué suivant les mesures organisationnelles, le certificateur pourra publier un rapport de maintenance seulement si le rapport de la visite du site est encore valide.

[8] Applications connues.

4. Références

[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*. Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/03.

[JCO/3.0] *Java Card Protection Profile - Open Configuration, version 3.0*. Certifié par l'ANSSI sous la référence 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.* Certifiés par l'ANSSI sous les références ANSSI-CC-PP-2010/04 (Configuration de Base) et ANSSI-CC-PP-2010/05 (Configuration SCWS).

[JIL] *Joint Interpretation Library – Certification of "open" smart card products*, version 1.1 (for trial use), 4 February 2013.

Annexe : Compatibilité des exigences et contraintes décrites dans cette note avec celles des profils de protection existants

Le tableau suivant identifie l'applicabilité de la démarche de certification d'une plateforme ouverte cloisonnante aux évaluations réalisées en conformité avec les PP [JCO/2.6], [JCO/3.0] ou [USIM]. Il définit aussi les exigences qui devront être présentes dans la cible de sécurité de la plateforme.

	[JCO/2.6]	**[JCO/3.0]**	**[USIM] (conforme à [JCO/2.6]**
O1 : cloisonnement entre les applications	*O.FIREWALL*	*O.FIREWALL*	*O.FIREWALL du [JCO/2.6]*
O2 : protection du chargement *post-issuance* (authenticité et intégrité)	*O.LOAD* ***Cet objectif doit préciser qu'il est destiné à assurer l'intégrité et l'authenticité des fichiers CAP chargés, concernant la verification***	*O.LOAD*	*O.LOAD du [JCO/2.6]* *O.APPLI-AUTH*
OE1 : vérification de la conformité des applications aux contraintes de cloisonnement de la plateforme	*OE.VERIFICATION* ***Cet objectif doit être étendu pour prendre en compte les contraintes spécifiques de la plateforme considérée définie dans le guide [ISO_VERIF].*** *(NB : les règles de composition imposent cette vérification aux applications certifiées, mais les applications non certifiées doivent également y être soumises).*	*OE.VERIFICATION*	*OE.VERIFICATION du [JCO/2.6]* *OE.BASIC-APPS-VALIDATION*
OE2 : mise à disposition de preuves d'intégrité et d'authenticité pour chaque application	***Un objectif doit ici être ajouté pour que l'évaluation puisse se réclamer conforme à la démarche de certification d'applications sur plateformes ouvertes cloisonnantes.*** *(en liaison avec la note d'application de O.LOAD sur la vérification de l'intégrité de l'application).*	*OE.CODE-EVIDENCE*	*OE.VERIFICATION-AUTHORITY*