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 23 janvier 2015

N° 260/ANSSI/SDE/PSS/CCN
Référence :ANSSI-CC-NOTE-06/2.0

NOTE D'APPLICATION

EXIGENCES DE SECURITE POUR UN CHARGEMENT DE CODE EN PHASE D'UTILISATION

Application : Dès son approbation

Diffusion : Publique

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

Signé : Guillaume POUPARD

Suivi des modifications

Version	Date	Modifications
1.0	15/05/2006	Création de la note « Prise en compte de correctifs du logiciel embarqué, chargés en EEPROM , lors de l'évaluation d'une carte à puce selon le PP 9911 »
2.0	23/01/2015	Mise à jour complète de la version 1.0. Renommage de la note.

En application du décret n° 2002-535 du 18 avril 2002 modifié, la présente note d'application a été soumise au comité directeur de la certification, qui a donné un avis favorable.

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

TABLE DES MATIERES

1. Introduction

1.1. Objectif

Un nombre croissant de produits de type « composants électroniques, microélectroniques et logiciels embarqués » dispose de mécanisme de chargement de code. Si ce chargement de code n'est pas réalisé dans un environnement dont la sécurité a été auditée lors d'une évaluation, ou si ce mécanisme de chargement n'est pas lui-même évalué, la sécurité du produit certifié pourrait être remise en question.

Ainsi le centre de certification impose que les mécanismes de chargement de code des produits du type « composants électroniques, microélectroniques et logiciels embarqués » soient systématiquement évalués. Tout produit disposant d'un tel mécanisme non inclus dans le périmètre d'évaluation mènera le projet d'évaluation au verdict Echec.

L'objet de cette note est de définir les concepts et la méthodologie applicables à une évaluation d'une cible embarquant un mécanisme de chargement de code (*Loader*) et l'usage accepté de ce *Loader* dans le cadre du processus de continuité de l'assurance.

Cette note est adressée aux développeurs et aux évaluateurs.

1.2. Périmètre

Ce document est applicable pour l'évaluation de produits de type « composants électroniques, microélectroniques et logiciels embarqués » embarquant un *Loader*.

D'une manière générale, ce sont des produits de sécurité (par exemple des cartes à puce, des *Trusted Platform Modules*, des tachographes…) où une part significative des exigences de sécurité dépend de caractéristiques matérielles du composant sous-jacent et qui embarquent un logiciel développé par le Fabricant du Produit.

Le logiciel embarqué peut être de différents types tels que : code natif, plateforme fermée avec applications, plateforme ouverte, etc.

Le *Loader* fait partie du logiciel embarqué. La TOE considérée dans le cadre de la première évaluation du *Loader* est appelée « TOE Initiale ». Cette TOE Initiale est ensuite mise à jour avec le code appelé « Code Additionnel ». La certification de cette mise à jour, correspondant à une nouvelle TOE appelée « TOE Finale », est effectuée en accord avec la procédure de continuité de l'assurance [CC-AC].

Le Code Additionnel peut être par exemple :

- du code corrigeant des défauts fonctionnels ;
- du code corrigeant des défauts de sécurité ;
- du code implémentant de nouvelles fonctionnalités ;
- un système d'exploitation complet.

Le périmètre de cette note couvre le chargement de Code Additionnel de la phase de livraison de la TOE à la phase d'utilisation comprise.

Remarque : le chargement de Code Additionnel réalisé lors des phases auditées au titre de ALC (i.e. avant la livraison de la TOE) est analysé dans le cadre d'une évaluation classique. Il ne nécessite pas d'interprétation et ne correspond donc pas à l'application de la présente note.

1.3. Terminologie

Activation Atomique	Le *Loader* garantit que, après son activation, le Code Additionnel est opérationnel et que les Données d'Identification de la TOE sont mises à jour. Cette fonctionnalité est appelée Activation Atomique. Si l'Activation Atomique est réussie, alors le résultat est la TOE Finale, sinon (en cas d'interruption du processus ou en cas d'incident empêchant la génération de la TOE Finale), la TOE Initiale doit rester dans son état ou être dans un état sécurisé d'échec.
Preuve associée au Code Additionnel	Informations générées par le Fabricant du produit et qui permettent à la TOE Initiale de vérifier l'authenticité et l'intégrité du Code Additionnel.
Chargement post-émission	Le Code Additionnel est chargé et activé sur la TOE Initiale en phase d'utilisation du produit (i.e. pendant la phase 7 du cycle de vie classique des cartes), c'est-à-dire après l'émission (*issuance*) du produit à l'utilisateur final.
Chargement pré-émission	Le Code Additionnel est chargé et activé sur la TOE Initiale avant l'émission (*issuance*) à l'utilisateur final et après le point de livraison de la TOE.
Code Additionnel	Code activé par l'Activation Atomique sur la TOE Initiale pour générer la TOE Finale. Le Code Additionnel peut par exemple : corriger des défauts, ajouter des fonctionnalités, changer le système d'exploitation…
Emission de la TOE produit	Moment où la TOE Initiale, le Code Additionnel ou la TOE Finale sont livrés à l'utilisateur final (i.e. phase 7 du cycle de vie classique des cartes).
Données d'Identification de la TOE	Données définies par le Fabricant du produit pour identifier la TOE Initiale, le Code Additionnel et la TOE Finale.
Fabricant du Produit	Le Fabricant du Produit est l'entité qui développe du logiciel embarqué et gère les clés cryptographiques utilisées pour générer les preuves d'authenticité et d'intégrité du Code Additionnel.
Livraison de la TOE	Moment où la livraison de la TOE Initiale et du Code Additionnel est analysée dans le cadre du processus d'évaluation (correspond au point de livraison ALC) ; cette étape délimite les phases de développement couvertes par des mesures techniques et organisationnelles (regroupées dans une phase dite phase ALC) et les phases couvertes seulement par des mesures techniques (regroupées dans une phase dite phase AGD).

Loader	Le *Loader* est le logiciel développé par le Fabricant du Produit. Il est utilisé pour charger et activer le Code Additionnel dans la mémoire non volatile (FLASH ou EEPROM) du Produit. Le *Loader* est inclus dans le logiciel embarqué et est considéré comme une partie de la TOE Initiale.
Phase de Chargement	La Phase de Chargement débute au chargement du Code Additionnel et se termine à la fin de l'Activation Atomique. Pendant la Phase de Chargement, la TOE initiale doit être dans un état sécurisé.
TOE Finale	La TOE Finale est générée à partir de la TOE Initiale et du Code Additionnel. C'est le résultat de l'Activation Atomique du Code Additionnel sur la TOE Initiale.
TOE Initiale	La TOE Initiale est le produit sur lequel le Code Additionnel est chargé et qui inclut le *Loader* en tant que logiciel embarqué.

1.4. Références

[CC]	Common Criteria for Information Technology Security Evaluation, version 3.1, revision 4, September 2012. Part 2: Functional security components.
	Common Criteria for Information Technology Security Evaluation, version 3.1, revision 4, September 2012. Part 3: Assurance security components.
[CEM]	Common Methodology for Information Technology Security Evaluation, version 3.1, revision 4, September 2012.
[CC-AC]	Assurance Continuity: CCRA Requirements, version 2.1, June 2012.

2. Architecture de la TOE

La Figure 1 décrit l'architecture de la TOE.

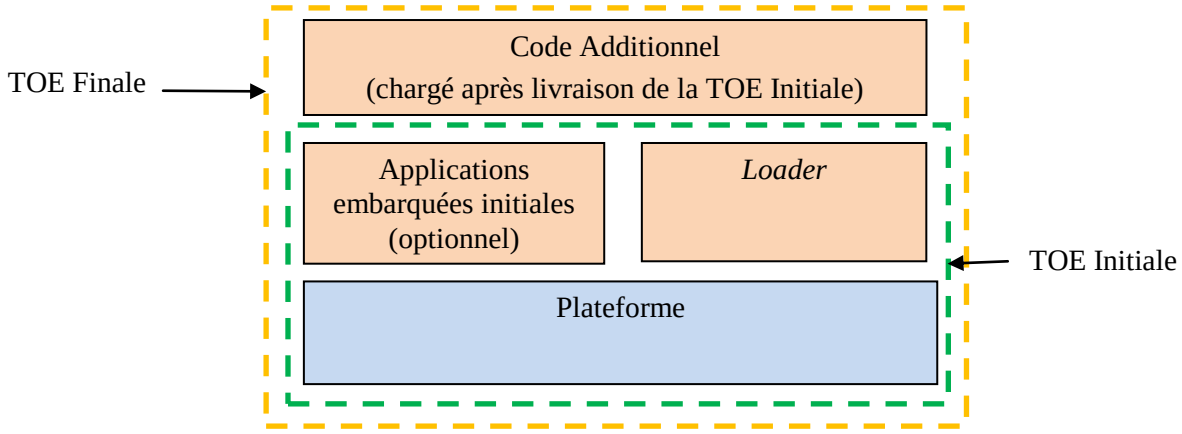

Figure 1: Architecture de la TOE

La TOE Initiale (en ligne pointillée verte), livrée par le Fabricant du Produit est composée :

- d'une Plateforme ;
- d'un *Loader* qui fait partie du logiciel embarqué ;
- d'applications optionnelles qui font partie du logiciel embarqué.

La TOE Finale (en ligne pointillée jaune) est composée :

- de la TOE Initiale ;
- du Code Additionnel qui fait partie du logiciel embarqué.

Note : plusieurs chargements de Code Additionnel peuvent se produire pendant la vie du produit et conduire à des ré-évaluations ou des maintenances selon [CC-AC]. La TOE Finale devient la TOE Initiale pour un prochain chargement.

3. Cycle de vie de la TOE

La Figure 2 décrit le cycle de vie de la TOE.

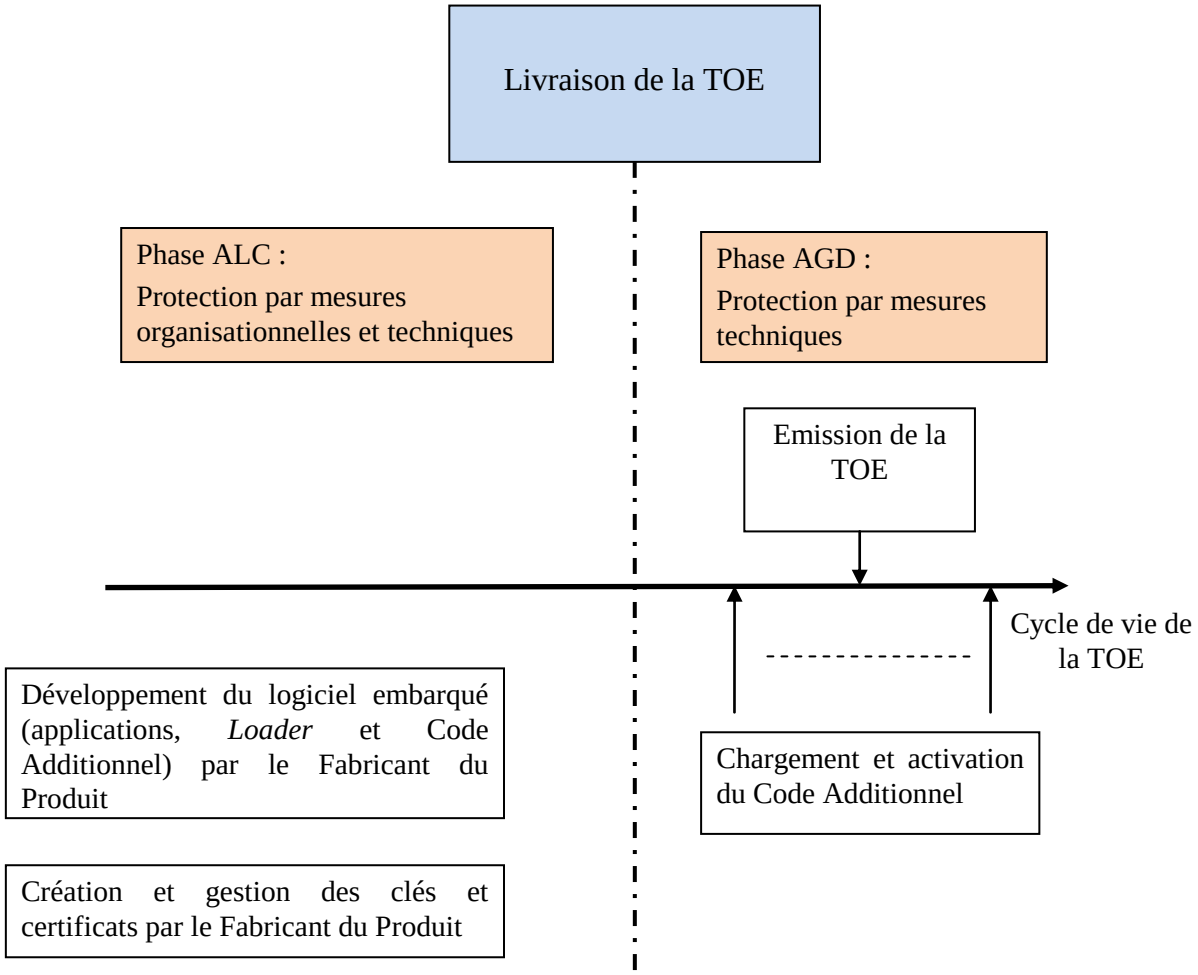

Figure 2: Cycle de vie de la TOE

Le cycle de vie de la TOE est défini par deux phases séparées par la livraison de la TOE :

- la première phase appelée « Phase ALC » correspond aux phases de développement du projet couvertes par des mesures organisationnelles et techniques ;
- la deuxième phase appelée « Phase AGD » correspond à la vie opérationnelle du produit couverte par des guides et des mesures techniques.

Phase ALC :

La TOE Initiale et le Code Additionnel sont développés dans un environnement sécurisé et audité dans le cadre d'une évaluation CC.

Le Code Additionnel est signé avec une clé cryptographique et la preuve générée est associée au Code Additionnel.

Cette clé cryptographique devra être d'une qualité suffisante et les processus de génération de la clé et de génération de la preuve associée au Code Additionnel devront être sécurisés de manière à garantir :

- la confidentialité, l'authenticité et l'intégrité de la clé cryptographique ;
- l'authenticité et l'intégrité de la preuve. Le processus de gestion de clés cryptographiques et de génération des preuves devra être réalisé dans un environnement sécurisé et audité.

La TOE Initiale stocke dans sa mémoire non-volatile les moyens cryptographiques lui permettant de vérifier l'authenticité et l'intégrité du Code Additionnel chargé.

Pendant la vie du produit, plusieurs Codes Additionnels peuvent être développés et chargés sur la TOE (après un chargement de Code Additionnel, la TOE Finale devient la TOE Initiale du chargement suivant).

Chaque TOE Finale (correspondant chacune à l'activation de Code Additionnel spécifique) doit être identifiée avec des Données d'Identification uniques.

Livraison de la TOE :

La TOE Initiale, le Code Additionnel et les guides pour la préparation et l'utilisation de la TOE finale sont délivrés à l'utilisateur.

Phase AGD :

La fonctionnalité de vérification de la preuve associée au Code Additionnel est utilisée par la TOE Initiale pour vérifier l'intégrité et l'authenticité du Code Additionnel avant son activation.

L'activation du Code Additionnel chargé est possible si :

- l'intégrité et l'authenticité du Code Additionnel ont été vérifiées avec succès ;
- le Code Additionnel chargé est destiné à la TOE Initiale (les Données d'Identification du Code Additionnel et de la TOE Initiale participeront à cette vérification).

Les Données d'Identification de la TOE Finale résultante doivent identifier la TOE Initiale et le Code Additionnel activé. Les Données d'Identification doivent être protégées en intégrité.

Le Code Additionnel peut être chargé à n'importe quel moment durant la Phase AGD, en d'autres mots, la préparation de la TOE finale peut être réalisée avant émission de la carte (pré-émission) ou après cette émission (post-émission).

4. Objectifs de sécurité pour la TOE initiale

La Cible de Sécurité d'une TOE embarquant un *Loader* doit contenir les Objectifs de Sécurité suivants.

La TOE doit fournir l'objectif « Secure loading of the Additional Code (O.Secure_Load_ACode) » comme spécifié ci-dessous.

O.Secure_Load_ACode **Secure loading of the Additional Code**

The Loader of the Initial TOE shall check an evidence of authenticity and integrity of the loaded Additional Code.
The Loader enforces that only the allowed version of the Additional Code can be loaded on the Initial TOE. The Loader shall forbid the loading of an Additional Code not intended to be assembled with the Initial TOE.
During the Load Phase of an Additional Code, the TOE shall remain secure.

La TOE doit fournir l'objectif « Secure activation of the Additional Code (O.Secure_AC_Activation) » comme spécifié ci-dessous.

O.Secure_AC_Activation **Secure activation of the Additional Code**

Activation of the Additional Code and update of the Identification Data shall be performed at the same time in an Atomic way.
All the operations needed for the code to be able to operate as in the Final TOE shall be completed before activation.
If the Atomic Activation is successful, then the resulting product is the Final TOE, otherwise (in case of interruption or incident which prevents the forming of the Final TOE), the Initial TOE shall remain in its initial state or fail secure.

La TOE doit fournir l'objectif « TOE Identification (O.TOE_Identification) » comme spécifié ci-dessous.

O.TOE_Identification **Secure identification of the TOE**

The Identification Data identifies the Initial TOE and Additional Code. The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data.
After Atomic Activation of the Additional Code, the Identification Data of the Final TOE allows identifications of Initial TOE and Additional Code. The user must be able to uniquely identify Initial TOE and Additional Code which are embedded in the Final TOE.

Si une menace de mascarade sur la TOE Initiale doit être prise en compte, alors un objectif sera ajouté pour contrer spécifiquement cette menace, tel que l'authentification de la TOE Initiale.

5. Livraisons

Le composant d'assurance ALC_DEL (procédures de livraison) traite de la livraison de la TOE ou des parties de la TOE à l'utilisateur (encarteur, personnalisateur, intégrateur…) ou sur son site.

Eléments de contenu et présentation :

ALC_DEL.1.1C **The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.**

Pour la livraison de la TOE Initiale, du Code Additionnel et de la TOE Finale, tous les guides décrivant les livraisons doivent être pris en compte.

Ils devront notamment décrire les mesures de protection de la génération de la preuve associée aux codes additionnels et les mesures de protection des clés cryptographiques utilisées pour générer cette preuve. Les mesures décrites dans les guides devront être auditées.

6. Préparation de la TOE finale

Le composant d'assurance AGD_PRE décrit les procédures de préparation de la TOE ou de parties de la TOE. Cela comprend les procédures de vérification de l'authenticité du Code Additionnel et les procédures d'identification de la TOE Initiale et de la TOE Finale.

Eléments de contenu et présentation :

AGD_PRE.1.1C **The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.**

AGD_PRE.1.2C **The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.**

Les guides utilisateur de préparation sont destinés à être utilisés par les personnes en charge des tâches suivantes :

- acceptation de la TOE Initiale et du Code Additionnel ;
- installation de la TOE : chargement du Code Additionnel sur la TOE Initiale, activation du Code Additionnel, vérification des Données d'Identification résultantes.

7. Prise en compte d'un chargement de code en maintenance

Pour une TOE certifiée avec un *Loader* correspondant aux exigences ci-dessus :

- si le Code Additionnel chargé en phase AGD correspond à des évolutions jugées **mineures** selon [CC-AC], le Centre de Certification traitera la TOE Finale en émettant un rapport de maintenance ;
- si le Code Additionnel chargé en phase AGD correspond à des évolutions jugées **majeures** selon [CC-AC], le Centre de Certification traitera la TOE Finale en tant que nouvelle évaluation.