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

Reference: ANSSI-CC-NOTE-06/2.0
EN

APPLICATION NOTE

SECURITY REQUIREMENTS FOR POST-DELIVERY CODE LOADING

Application : From date of application.

Circulation : Public.

COURTESY TRANSLATION

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP

Version history

Version	Date	Modifications
1.0	15/05/2006	Creation of the Application Note « Handling patches in software loaded in EEPROM, according to PP 9911 »
2.0	23/01/2015	Update of version 1.0 . Application Note name changed.

TABLE OF CONTENTS

1. INTRODUCTION 4

1.1. Objective 4
1.2. Scope 4
1.3. Terminology 5
1.4. References 6

2. ARCHITECTURE OF THE TOE 6

3. LIFECYCLE OF THE TOE 7

4. SECURITY OBJECTIVES FOR THE INITIAL TOE 9

5. DELIVERIES 10

6. FINAL TOE PREPARATION 10

7. CONSIDERATION OF A MAINTENANCE CODE LOADING 10

1. Introduction

1.1. Objective

A growing number of products like « electronic components, micro-electronic components and embedded software » has a code loading mechanism. If the code loading is not carried out in an environment where the security has been audited during an evaluation, or if this loading mechanism is not itself evaluated, the security of the certified product could be questioned.

So the certification body requires the systematic evaluation of the loading mechanism of products like « electronic components, micro-electronic components and embedded software ». Any product with such mechanism not included in the perimeter of evaluation will carry out the evaluation project to the Failure verdict.

The purpose of this note is to define the concepts and the methodology applicable to the evaluation of a TOE embedding a code loading mechanism ("Loader") and the usage of this Loader as part of the assurance continuity process.

This note is addressed to both developers and evaluators.

1.2. Scope

The current document is applicable for the evaluation of products like « electronic components, micro-electronic components and embedded software » embedding a Loader.

Generally speaking, it means security products (for example smart card composite products, Trusted Platform Modules, digital tachograph cards, etc.) where a significant portion of the required security requirements depend of hardware features of the underlying chip and which embed a software developed by the Product Manufacturer.

The embedded software can be of different types : native software, closed platform with applications, open platform, etc.

The Loader belongs to the embedded software.

This Initial TOE is then updated with a the code called "Additional Code". The certification of this update corresponds to a new TOE called "Final TOE" and is carried out in accordance with the insurance continuity procedure [CC-AC].

The "Additional Code" could be for instance:

- code correcting functional flaws ;
- code correcting security flaws ;
- code adding new functionalities ;
- full operating system.

In the scope of this note, downloading of Additional Code onto the Initial TOE can occur from TOE delivery up to and including the use phase of the product.

Note : the Additional Code loading done during the audited phases of the ALC (before the TOE delivery) is analyzed in the framework of a classical evaluation. It does not require the interpretation and application of this note.

1.3. Terminology

Additional Code	Code activated by the Atomic Activation on the Initial TOE to generate the final TOE. For instance, Additional Code could: correct flaws, add new functionalities, update the operating system.
Additional Code proof	Information generated by the Product Manufacturer which allow to the Initial TOE to verify the authenticity and integrity of the Additional Code.
Atomic Activation	The Loader guarantees at activation time that the loaded Additional Code is activated and that the Identification Data of the TOE are updated. This functionality is called Atomic 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.
Final TOE	The Final TOE is generated from the Initial TOE and the Additional Code. It is the resulting product of the Atomic Activation of the Additional Code onto the Initial TOE.
Initial TOE	The Initial TOE is the product on which the Additional Code is loaded and with the Loader as part of the embedded software.
Loader	The Loader is the software developed by the Product Manufacturer. It is used to load and activate the Additional Code into the Product FLASH or EEPROM memory. The Loader is included in the embedded software and is considered as part of the Initial TOE.
Load Phase	The Load Phase is starting at the beginning of the Additional Code loading and ending at the end of Atomic Activation. During the Load Phase, the Initial TOE shall be in a secure state.
Post-issuance loading	The Additional Code is loaded and installed on Initial TOE during product use (phase 7 of the classical cards life cycle), meaning after the issuance of the product to end user.
Pre-issuance loading	The Additional Code is loaded and installed on Initial TOE before the issuance to the end user and after the delivery point of the TOE.
Product Manufacturer	The Product Manufacturer is the entity which develops the embedded software and manages the cryptographic keys used to generate the proofs of the authenticity and integrity of the Additional Code.
Product TOE Issuance	The time when the Initial TOE, the Additional Code or the Final TOE are delivered to the end user (phase 7 of the cards classical life cycle).
TOE Delivery	The time when Initial TOE and Additional Code delivery is analyzed as

	part of the evaluation process (corresponding to the ALC delivery point). This step delimits the development phases covered by technical and organizational measures (grouped into a phase called ALC) and the phases covered only par technical measures (grouped into a phase called AGD).
TOE Identification Data	Data defined by the Product Manufacturer to identify the Initial TOE, the Additional Code and the Final TOE.
TOE Issuance	The time when the Initial TOE, the Additional Code or the Final TOE are delivered to the end-user.

1.4. References

[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 of the TOE

Figure 1 describes the architecture of the TOE.

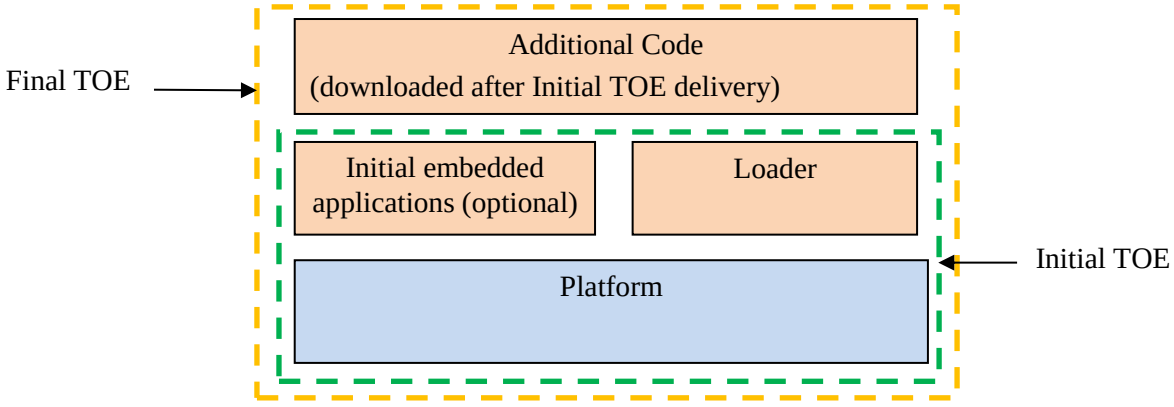

Figure 1: Architecture of the TOE

The Initial TOE (in dashed green line) delivered by the Product Manufacturer is composed of:

- a Platform ;
- a Loader which is a part of the embedded software ;
- optional applications which are parts of the embedded software.

The Final TOE (in dashed yellow line) is composed of:

- Initial TOE ;
- Additional Code, which is a part of the embedded software.

The Additional Code delivered by the Product Manufacturer is a part of the embedded software.

Note : Several loading of Additional Codes can occur during the life of the product and can lead to re-evaluations or maintenances according to [CC-AC]. The Final TOE becomes the Initial TOE for a next load.

3. Lifecycle of the TOE

Figure 2 describes the lifecycle of the TOE.

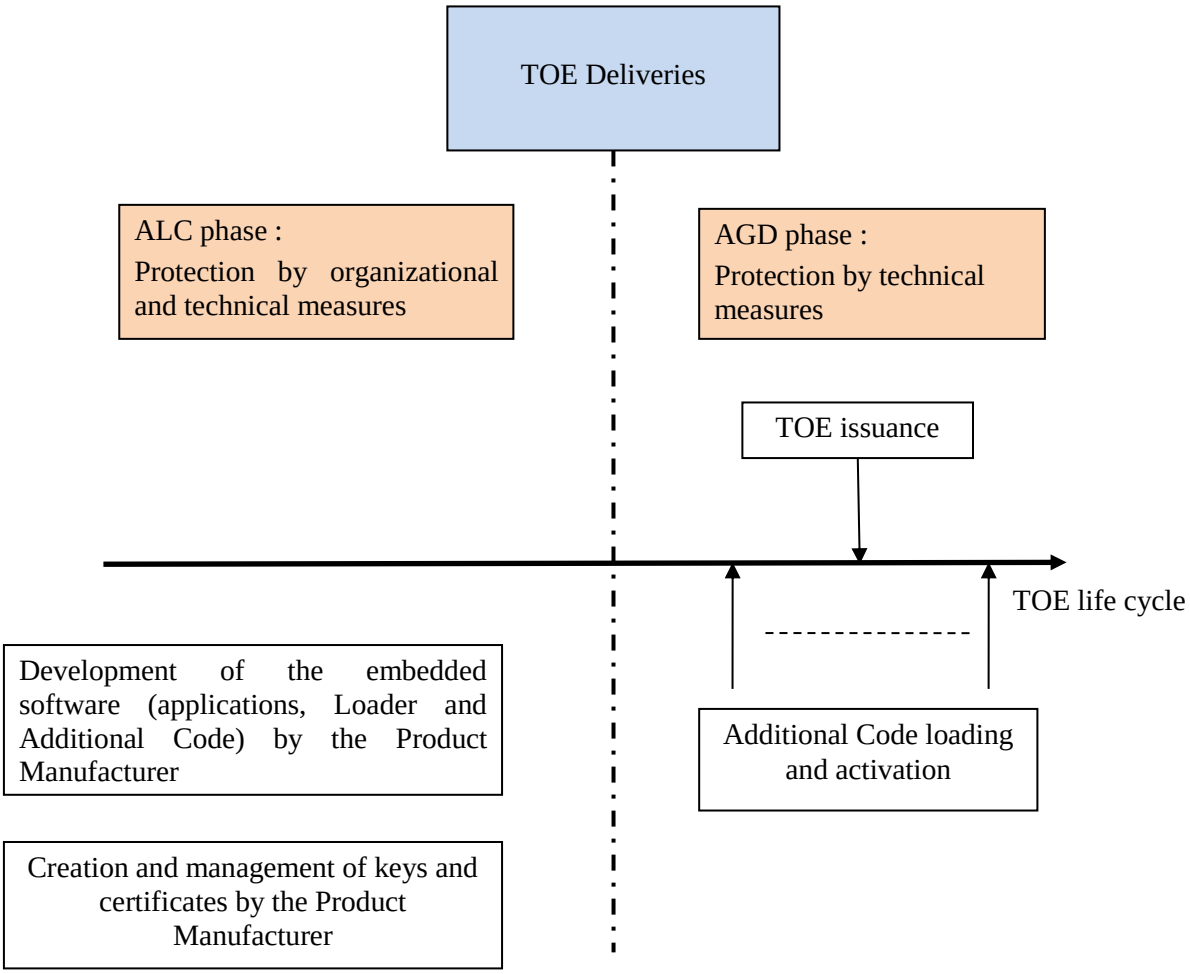

Figure 2: TOE lifecycle

The TOE lifecycle is defined by two phases separated by the TOE Delivery :

- first phase called « ALC phase » corresponding to the product development phases covered by organizational and technical measures ;
- second phase called « AGD phases » corresponding to the operational life of the product covered by guidance and technical measures.

ALC phase:

Initial TOE and Additional codes are developed in a secure and audited environment as part of a CC evaluation.

The Additional code is signed with a cryptographic key and the generated proof is linked to the Additional Code. The cryptographic key shall be of sufficient quality and the process of key generation and proof generation related to the Additional Code will have to be appropriately secured to ensure :

- the confidentiality, authenticity and integrity of the cryptographic key,
- the authenticity and integrity of the proof. The cryptographic keys and proof generation management will be carried out in a secure and audited environment.

Initial TOE stores in its non-volatile memory the cryptographic means allowing to check authenticity and integrity of the loaded Additional Code.

During the product life, several Additional Codes can be developed and loaded onto the TOE (after an Additional Code load, the Final TOE becomes the Initial TOE of the next load).

Each Final TOE (each of them corresponding to the activation of a specific Additional Code) shall be identified with unique identification data.

TOE Delivery :

The Initial TOE, the Additional Codes and the guidance for the Final TOE preparation and use shall be delivered to the user.

AGD phase :

The proof verification functionality linked to the Additional Code is used by the Initial TOE or the Final TOE to check the integrity and authenticity of the Additional Code before its activation.

The activation of the loaded Additional Code is possible if :

- integrity and authenticity of the Additional Code have been successfully checked;
- the loaded Additional code is targeted to the Initial TOE (Identification Data of the Additional Code and the Initial TOE will be used for this check).

Identification Data of the resulting Final TOE shall identify the Initial TOE and the activated Additional Code. Identification Data shall be protected in integrity.

The Additional Codes can be loaded at any time during the AGD phase, in other words, the preparation of the Final TOE can occur before the card delivery (pre-issuance loading) or after the card delivery (post-issuance loading).

4. Security Objectives for the Initial TOE

Security Target of a TOE embedding a Loader shall include the following Security Objectives.

The TOE shall provide "Secure loading of the Additional Code (O.Secure_Load_ACode)" as specified below.

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.

The TOE shall provide "Secure activation of the Additional Code (O.Secure_AC_Activation)" as specified below.

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.

The TOE shall provide "TOE Identification (O.TOE_Identification)" as specified below:

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 shall be able to uniquely identify Initial TOE and Additional Code(s) which are embedded in the Final TOE.

In case a threat of masquerade shall be taken into account, a complementary objective, such as the Initial TOE authentication for example, shall be added to counter this specific threat.

5. Deliveries

The assurance component of the family ALC_DEL (delivery procedure) deals with the TOE delivery or parts of it to the user (smartcard embedder, personalizer, system integrator, end-consumer…) or its site.

Content and presentation elements:

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.**

For the delivery of the Initial TOE, Additional Code and Final TOE, all the guidance describing the delivery procedures shall be taken into account.

They must especially describe the protection measures of the proof associated to the Additional Codes and the protection measures of the cryptographic keys used to generate this proof. The measures described in the guidance will have to be audited.

6. Final TOE preparation

The assurance component AGD_PRE (preparation procedures) describes the procedures of the TOE or part of the TOE. This comprises the verification of the authenticity of the Additional Code and the identification procedures of the Initial TOE and the Final TOE.

Content and presentation elements:

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.**

Preparative user guidance are intended to be used by persons responsible for the following tasks:

- acceptance of the Initial TOE and of the Additional Code ;
- installation of the TOE : download of the Additional Code onto the Initial TOE, activation of the Additional Code, checking of the resulting Identification Data.

7. Consideration of a maintenance code loading

For a certified TOE with a Loader corresponding to the above requirements :

- if the Additional Code loaded in AGD phase corresponds to the evolutions assessed as minor based on [CC-AC], the Certification Body will be dealing with the Final TOE by issuing a maintenance report ;
- if the Additional Code loaded in AGD phase corresponds to the evolutions assessed as major based on]CC-AC], the Certification Body will be dealing with the Final TOE as a new evaluation.