Joint Interpretation Library

Security requirements for post-delivery code loading

Version 2.0

September 2024

This page is intentionally left blank

Table of contents

1 Introduction

1.1 Objective

1 A growing number of products like “micro-electronic components embedding software” also embed 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 unless the loading mechanism is effectively deactivated before delivery of the product.

2 So the systematic evaluation of the loading mechanism of these products is required. Any product with such a mechanism not included in the perimeter of evaluation will carry out the evaluation project to the Failure verdict.

3 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.

4 This note is addressed to both developers and evaluators.

1.2 Scope

5 The current document is applicable for the evaluation of products like “smart cards and similar devices” embedding a Loader.

6 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 on hardware features of the underlying chip and which embed a software developed by the Product Manufacturer.

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

8 The Loader belongs to the Initial TOE (which can be for example an IC, an embedded software in composition with an IC, or other).

9 This “Initial TOE” is then updated with the code called “Update Code”. The certification of this update corresponds to a new TOE called “Updated TOE”. **This has to be successfully carried out in accordance with the assurance continuity procedure [CC-AC] / [JIL-AC]**.

10 The “Update Code” could be for instance:

- code correcting functional or security flaws of the IC dedicated software or the embedded software;
- code adding new functionalities to the IC dedicated software or the embedded software;
- full update of the embedded software operating system...

11 In the scope of this note, downloading of Update Code onto the Initial TOE can occur from TOE delivery (as covered by the ALC_DEL evaluation activities) up to and including the use phase of the product.

12 Note: the Update 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

Update Code	Code loaded, installed and activated by the Atomic Activation on the Initial TOE to generate the Updated TOE. Note: Update Code can add, overwrite or remove code. For instance, Update Code could: correct flaws, add new functionalities, update the operating system. Note: The old code of the initial TOE may remain in the TOE, no longer accessible, or may be overwritten, but only if the initial state (or fail secure state) can be reinstated in case of interruption or incident during the atomic activation.
Update Code proof	Information generated by the Product Manufacturer which allows the Initial TOE to verify the authenticity and integrity of the Update Code.
Atomic Activation	The Loader guarantees at activation time that the loaded Update 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 Updated TOE, otherwise (in case of interruption or incident which prevents the forming of the Updated TOE), the Initial TOE shall remain in its initial state or fail secure state.
Updated TOE	The Updated TOE is generated from the Initial TOE and the Update Code. It is the resulting product of the Atomic Activation of the Update Code onto the Initial TOE.
Initial TOE	The Initial TOE is the product on which the Update Code is loaded, and includes the Loader as part of its TSF.
Loader	The Loader is either software developed by the Product Manufacturer, or any other type of instrument or device which makes it possible to load and activate the Update Code into the Product FLASH or EEPROM memory, or the counterpart of these in case of another technology used. Examples of Loaders include, but are not limited to, Loaders provided by an IC platform, provided by the embedded software, or by a joint IC platform/embedded software solution. The Loader is part of the TSF of the Initial TOE.
Load Phase	The Load Phase is starting at the beginning of the Update 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 Update 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 Update 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 Update Code.
TOE Issuance	The time when the Initial TOE, the Update Code or the Updated TOE are delivered to the end user (phase 7 of the cards classical life cycle).
TOE Delivery	The time point at the end of the development phase of the Initial TOE or Update Code as far as covered by analysis within the related evaluation process (corresponding to the delivery point in the sense of ALC). This step delimits the development phases covered by technical and organizational measures (covered by the ALC class) and the phases covered by guidance and technical measures (covered by the AGD class).
TOE Identification Data	Data defined by the Product Manufacturer which identifies the Initial TOE, the Update Code and the Updated TOE.

1.4 References

[CC-AC]	Assurance Continuity: CCRA Requirements, v3.1 2024-02-29
[JIL-AC]	JIL Assurance Continuity, v1.2 March 2024.
[JIL-AC-SCSD]	JIL Assurance Continuity - Practical Cases for Smart Cards and similar devices for CC:2022, v1.1 April 2024

2 Architecture of the TOE

13 Figure 1 describes an example of typical architecture of the TOE.

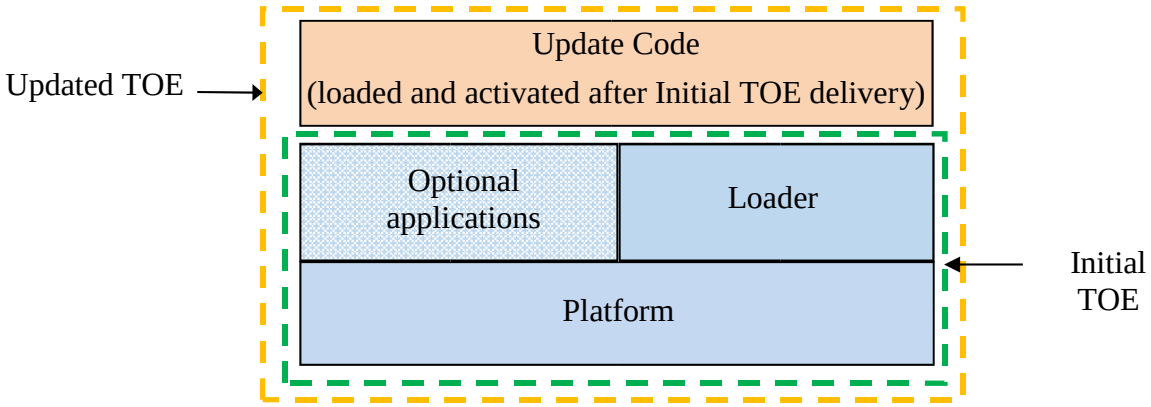

Figure 1: Architecture of the TOE

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

- a Platform, including any dedicated software. Examples of Platform could be:
  - an IC with its dedicated software,
  - an embedded software, running on top of an IC with its dedicated software;
- a Loader, which is a part of the Platform (e.g. part of the IC dedicated software, part of the embedded software, or part of the composition of both IC and embedded software);
- optional applications, which are part of the IC dedicated software or the embedded software.

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

- Initial TOE (including the Loader);
- Update Code, which has been loaded and activated into the Initial TOE to conform the Updated TOE.

16 The Update Code delivered by the Product Manufacturer can update part (or potentially the whole) of the Platform dedicated software, of the embedded software, or a combination of both.

17 Note: Several loading of Update Codes can occur during the life of the product and has to lead to **re-evaluations or maintenances according to [CC-AC] / [JIL-AC]**. The Updated TOE becomes the (certified) Initial TOE for the next load.

3 Lifecycle of the TOE

18 Figure 2 describes an example of typical lifecycle of the TOE.

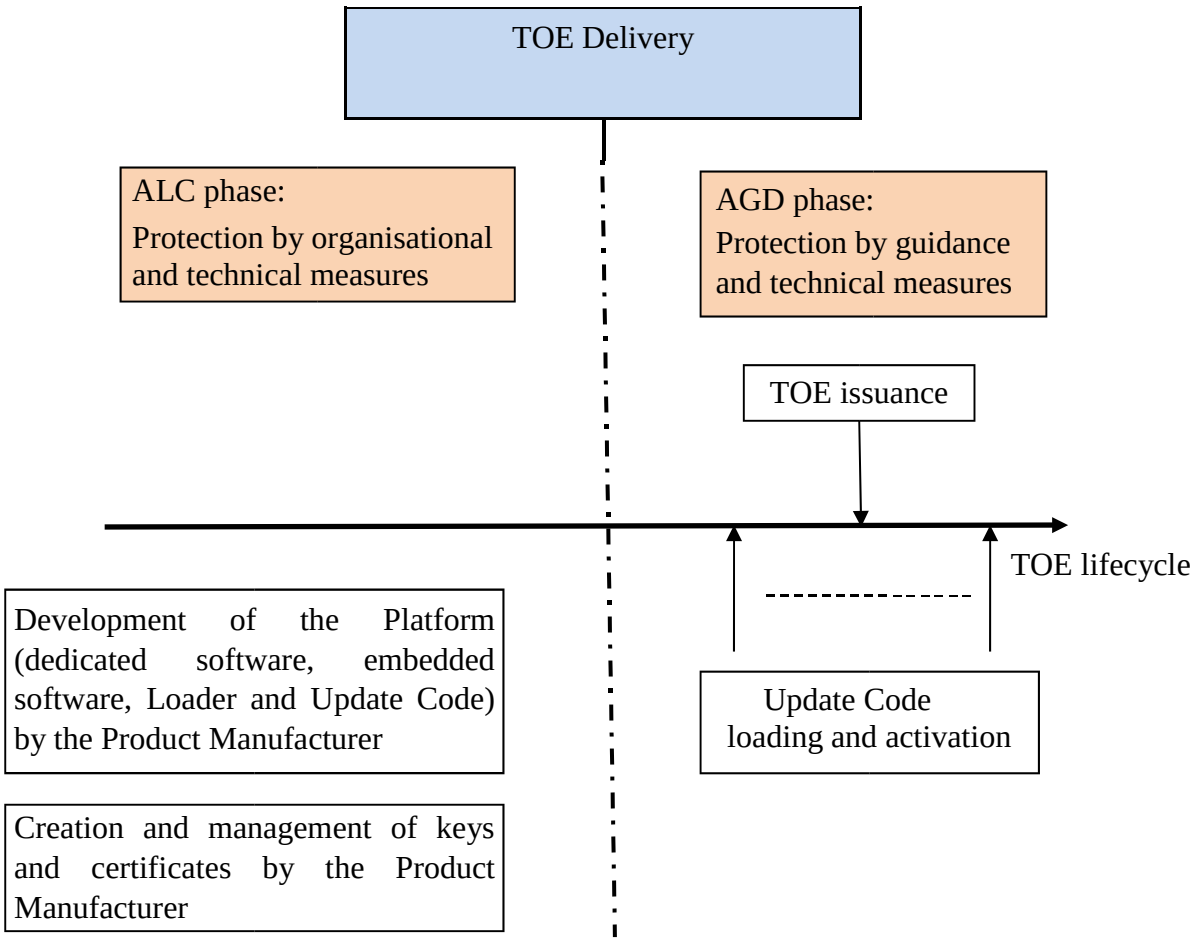

Figure 2: TOE lifecycle

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

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

20 ALC phase:

21 Initial TOE and Update Codes are developed in a secure and audited environment as part of a CC evaluation. Keys and certificates have to be created by the Product Manufacturer and managed in a secure and audited environment. The potential changes of the development environment of the Updated TOE compared with the Initial TOE shall be declared using an Impact Analysis Report, and covered during the assurance maintenance activities of the Updated TOE according to [CC-AC] / [JIL-AC].

22 The Update Code is signed with a cryptographic key and the generated proof is linked to the Update Code. The cryptographic key shall be of sufficient quality and the process of key generation and proof generation related to the Update 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.

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

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

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

26 TOE Delivery:

27 The Initial TOE, the Update Code and the guidance for the Updated TOE preparation and use shall be delivered to the user.

28 The Update Code can be delivered at the same time of the Initial TOE delivery, or at any point during the AGD phase between the Initial TOE delivery and before the loading and activation of the Update Code

29 AGD phase:

30 The Update Code proof linked to the Update Code is used by the Initial TOE Loader to check the integrity and authenticity of the Update Code before its activation.

31 The activation of the loaded Update Code is possible if:

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

32 Identification Data of the resulting Updated TOE shall identify the Initial TOE and the activated Update Code. Identification Data shall be protected in integrity.

33 The Update Codes can be loaded at any time during the AGD phase, in other words, the preparation of the Updated TOE can occur before the card is issued to the end user (pre-issuance loading) or after (post-issuance loading).

4 Security Objectives for the Initial TOE

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

35 The TOE shall provide “Secure loading of the Update Code (O.Secure_UC_Load)” as specified below.

O.Secure_UC_Load **Secure loading of the Update Code**

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

36 The TOE shall provide “Secure activation of the Updated Code (O.Secure_UC_Activation)” as specified below.

O.Secure_UC_Activation **Secure activation of the Update Code**

Activation of the Update 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 Updated TOE shall be completed before activation.
If the Atomic Activation is successful, then the resulting product is the Updated TOE, otherwise (in case of interruption or incident which prevents the forming of the Updated TOE such as tearing, integrity violation, error case…), the Initial TOE shall remain in its initial state or fail secure.

37 The TOE shall provide “Authentication for the Secure loading and activation (O.Auth_Secure_Load)” as specified below.

O.Auth_Secure_Load **Authentication for the Secure loading and activation**

The TOE shall provide mechanisms for the identification and authentication of users for initiating and performing the operations of Secure Loading and Secure Activation of the Update Code. The TOE shall not allow Secure Loading and Secure Activation of the Update Code without preceding identification and authentication of the user.

38 The TOE shall provide “TOE Identification (O.TOE_Identification)” as specified below:

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

The Identification Data identifies the Initial TOE and Update 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 Update Code, the Identification Data of the Updated TOE allows identifications of Initial TOE and Update Code. The user shall be able to uniquely identify Initial TOE and Update Code(s) which are embedded in the Updated TOE.

39 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.

40 Please note: for inclusion of the above security objectives in a ST or PP, the author of the ST/PP shall add into those documents the required SPD elements and SFRs related to the defined security objectives, including mappings and rationales concerning the relationship between SPD and the security objectives, as well as between security objectives and SFRs.

41 For the cases where the TOE ST claims conformance to a Protection Profile that already defines the Loader functionality as part of its requirements (e.g. PP-0084 or PP-0117), the security objectives defined above would not be required, and the definitions of the PP shall be followed instead.

42 Please also note, that the verification of the authenticity of the Additional Code and the identification procedures of the Initial TOE and the Final TOE need to be detailed: How are these tasks requested for the TOE and the user (entity performing / initiating the loading and activation of the Additional Code) linked together?

5 Deliveries

43 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.

44 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.**

45 Refinement: For the delivery of the Initial TOE, Update Code and Updated TOE, all the guidance describing the delivery procedures shall be taken into account.

46 Refinement: They must especially describe the protection measures of the proof associated to the Update Codes and the protection measures of the cryptographic keys used to generate this proof. The measures described in the guidance will have to be evaluated to assess their sufficiency and effectiveness.

6 Updated TOE preparation

47 The assurance family AGD_PRE (Preparative procedures) deals with all acceptance and installation procedures that are necessary to progress the received TOE to the secure configuration as described in the ST. This comprises the secure acceptance of the Initial TOE and Update Code (including the identification procedures, integrity checks and authenticity checks for all items), and the installation procedures required for the Initial TOE and the Updated TOE.

48 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.**

49 Refinement: Preparative user guidance is intended to be used by persons responsible for the following tasks:

- acceptance of the Initial TOE and of the Update Code, including the identification and the integrity and authenticity checks of all their parts;
- installation of the TOE: download of the Update Code onto the Initial TOE, activation of the Update Code, and checking of the resulting Identification Data of the Updated TOE.

50 Note: Updated user guidance specifying the Updated TOE Identification Data have to be re-assessed according to [CC-AC] / [JIL-AC], either by a maintenance process or by a re-evaluation. The Identification Data has to be unique.

7 Assurance continuity process

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

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

52 The JIWG document "Assurance Continuity - Practical cases for Smart Cards and similar devices" [JIL-AC-SCSD] can be used as guidance during the TOE changes assessment process.