Joint Interpretation Library

Biometric Card - Guidelines

Version 1.1
September 2023

This page is intentionally left blank

Table of contents

1 Introduction

1.1 Document Scope and Overview

1 The scope of this document is the Biometric Cards, such as cards embedding a fingerprint Sensor and performing a match on card.

2 The objective of this document is twofold:

1. Build a common understanding of what a biometric card would require in terms of security assessment,
2. Provide specific guidelines regarding attacks that would be specific to such biometric cards.

3 This document identifies:

- A list of possible architectures and the architecture relevant to the scope of this document in Section 3,
- The sensitive assets which are specific to the biometric subsystem of a biometric card in Section 3.6,
- The threats on bio-related assets that shall, or not, be considered in Section 0, and
- A consistent scope of evaluation in Section 6.

4 The attack paths and threats in this document have been derived from the classical 'lost and stolen' scenario. The case of a biometric product that should be resistant to an evaluation laboratory which is granted access to the genuine cardholder's Template has not been considered here. This document does not either consider the case where the fingerprint is assumed to be publicly known and available.

5 This document should help answering the following questions:

- Are the sample and/or candidate to be considered as sensitive assets?
    - Not sensitive: the sample in transit can be captured at many other locations
    - Confidential: the image and/or candidate should not be caught
        - the attacker's potential then propagates to elements involved in the processing
    - Is there any intermediate level of sensitiveness that should be considered?
        - If yes, how will it be nested to the classical attacker's potential AVA_VAN.5?
- Should the MCU be included in the perimeter of the evaluation?
    - Key Recovery if relevant
    - Illegitimate firmware update using a vulnerability/exploit

6 It has been decided by the JHAS that in order to provide necessary examples, the specific use case of biometric *payment* cards will be used, as no other use case is available at the

date of document writing. The output of this document is intended to be applicable to any smart card embedding a fingerprint Sensor together with the matching algorithm.

1.2 References, Acronyms and Definitions

References

[1] ISO/IEC, *Information technology – Biometric performance testing and reporting – Part 1: Principles and framework*, April 2006, ISO/IEC 19975-1

[2] Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA), EU Official Journal (OJ), 31 March 2017

[3] JHAS. Application of Attack Potential to Smartcards. V3.2. November 2022

[4] JHAS. Attack Methods for Smartcards and Similar Devices. v2.5. May 2022

[5] JHAS, Guidance for Vulnerability Analysis and Penetration Testing of a Secure Sub-System within a System-on-Chip, v3.0, March 2023

Acronyms

BC	Biometric Card
CRM	Card Risk Management
FAR	False Acceptance Rate
FRR	False Rejection Rate
FW	Firmware
HW	Hardware
IC	Integrated Circuit
JC	Java Card
L&S	Lost and Stolen
MCU	Microcontroller Unit
OS	Operating System
PIN	Personal Identification Number
RM	Risk Management
RTS	Regulatory Technical Standards
SE	Secure Element
SiP	System in Package
SW	Software

Definitions

(Some of the definitions have been freely inspired from [1].)

Biometric authentication factor

> Generic term to encompass the genuine cardholder's captured Sample, extracted Candidate or stored Template.

Biometric card

In a generic context, a biometric card is a card that embeds a fingerprint Sensor.
It is made of

- An application on top of an OS (JC or not)
- A biometric subsystem (HW+SW) used as a decisional oracle by the application:
  - With dedicated HW (like Sensor and MCU)
  - With dedicated SW spread over the different components (MCU, OS in SE or as an applet on top of a Java Card OS).

Biometric system

In our context, the biometric system is the subsystem of the biometric card which allows to perform the following steps:

1. [data capture] acquires a biometric sample
   a. either for enrolment
   b. or for verification
2. [features extraction] extracts the most characteristic features
   a. [enrolment] either to be stored as a template
   b. [verification] or to be considered as a candidate
3. [verification/matching] performs a match on card between the template and the candidate giving rise to a similarity score
4. [verification/decision] a decision is made based on the similarity score, to accept the candidate or to reject it.

Candidate

The Candidate is the mathematical representation of a fingerprint which is presented by a user. The Candidate in the context of the enrolment process is intended to be (part of) the Template. In the verification process, the Candidate is intended to be compared to the stored Template.

Card Provider

Service Provider entity that issues cards for a specific usage.

Cardholder

Person to whom a card is issued. The cardholder is (contractually) bound to a Card Provider.

Data capture

During data capture a biometric sample is acquired. The latter is used either for enrolment or for verification.

Enrolment

Enrolment is a process which consists in three main steps: data capture, feature extraction and storage for later use. The stored features are called the Template.

Features extraction

The Features extraction step gets the raw image(s) of the fingerprint captured and sent by the Sensor as an input, and outputs the mathematical representation (which may contain a raw image or a part of the raw image or a mix of some parts of the raw image and some additional data such as specific extracted features) of this presented fingerprint. The Features extraction step is a generic term that may include the so-called pre-processing of the raw image which increases for instance the contrast.

MCU-centric

MCU-centric is a hardware and software architecture in which the matching/comparison step is performed inside the MCU (regardless of where and how the Template is stored).

PIN

Personal Identification Number associated to a card and used to authenticate the cardholder.

Sample

The Sample is the raw image(s) captured and sent by the Sensor to the driving component (MCU or SE in this document).

SE-centric

SE-centric is a hardware and software architecture in which the matching/comparison step is performed inside the SE (regardless of where and how the Template is stored).

Sensor

The Sensor is a component embedded on the card which is responsible for capturing the image(s) of the fingerprints when a user puts his finger on it.

Template

The Template is the mathematical representation of a fingerprint of an enrolled user, stored in a long-term memory for later use during the matching/comparison step.

Verification

Verification is a process which consists in four main steps: data capture, feature extraction, comparison with one (or several) Template(s) and decision of acceptance. The extracted features of this process are called the Candidate.

Verification/decision

During verification, a decision follows the matching operation. The decision step accepts or rejects a candidate which has been compared to a (some) template(s). The decision is made by comparing the similarity score provided by the matching step with a threshold. The threshold used for the decision has a direct impact on the so-called FAR and FRR.

2 Biometric Card definition

7 A Biometric Card (BC) is made of possibly several ICs (for instance an SE and optionally an MCU) and a Sensor as illustrated by Figure 1. The main functionalities are dispatched over several components (HW and SW) of the card:

- biometric data capture functionality implemented on and by the Sensor. This module is responsible for acquiring a (set of) sample(s).
- biometric data management application which achieves the
  - features extraction
  - storage of the template
  - verification of a candidate, including decision to accept or to reject

  and is supported in these tasks by several ICs with different embedded software on those ICs.
- application which interacts with the biometric data management application (bio app for short). The application invokes the bio application as a decisional oracle which tells the application whether the submitted candidate is accepted or rejected.

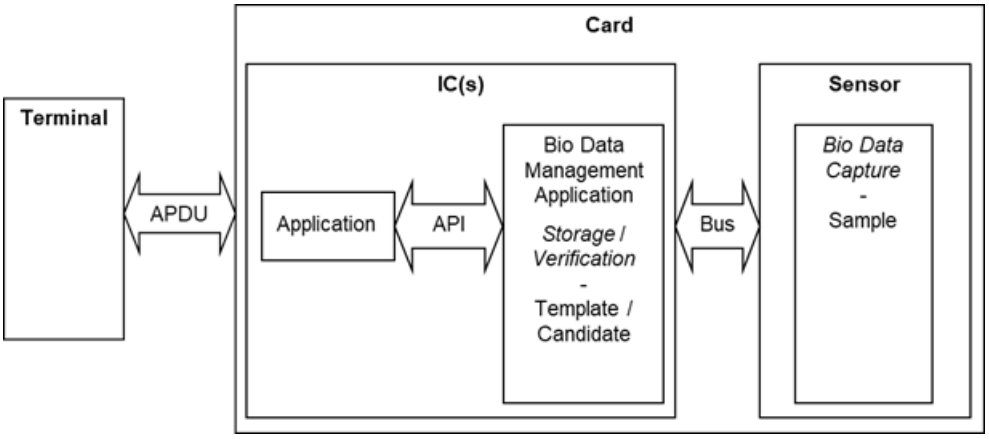

Figure 1: Architecture overview

8 A biometric card can be made of one or several ICs in addition to the Sensor:

- a Secure Element only, or
- a Secure Element and an MCU.

9 It is observed that the feature extraction step (for enrolment or verification) is usually carried out by the MCU (when such a hardware configuration is used). An objective of this document is to determine whether such an architecture is acceptable (in terms of risk) or not.

10 The other steps like

- the storage of the Template,
- the comparison of a Candidate against a Template,
- the decision of acceptance or rejection

could take place in different (HW+SW) locations. Another objective of this document is to determine the different acceptable architectures together with rationales.

11 To determine whether an architecture is acceptable or not, the analysis relies on the impacts of the identified threats. The considered impacts can be financial loss, identity usurpation as well as loss of image and trust.

3 Main architectures

12 This section considers a BC embedding a Sensor, an MCU and an SE and enumerates the possible manners of dispatching the following biometric subsystem functionalities:

- [Data capture]
- [Features extraction]
- [Storage of the template] in case of enrolment
- [Verification of candidate] in case of verification
- [Decision of acceptance or rejection] based on a similarity score and a threshold

among the supporting hardware.

13 The Data capture is always performed on the Sensor and either transmitted to the MCU or to the SE when no MCU is used.

14 In the sequel, different architectures are considered, focusing on:

1. Where matching is carried out, and
2. Where the Template is stored.

15 The impacts (sensitive data exchanged on different communication links, storage on non-secure memory) of each architecture are also considered.

16 To facilitate the listing of the many combinations, it has been chosen to enumerate the different locations where matching could be carried out and then to list the different locations where the Template could be stored.

17 With respect to matching, three main architectures arise that will be detailed in the following sections:

1. MCU-centric: matching occurs on the MCU
2. SE-centric: matching occurs on the SE
3. Mix-matching: matching is split between the MCU and the SE

3.1 MCU-centric architecture

18 Matching occurs on the MCU and the biometric sample is acquired by the Sensor, it is assumed that the sample is sent to the MCU which ‘drives’ the Sensor. Since matching is intended to be performed on the MCU, it is quite natural to require that the features extraction occurs on the MCU as well.

19 Two options arise for the storage of the Template which is intended to be matched against the extracted Candidate:

- the Template is stored on the MCU

- the Template is stored on the SE

20 In the first option, the Template is already available in the MCU which can match it with the Candidate.

21 In the second case, the Template needs to be fetched from the SE to the MCU since matching occurs on the MCU.

22 In both situations, the similarity score or possibly the decision of acceptance (or rejection) must be sent to the application running on the SE.

3.2 SE-centric architecture

23 Matching occurs on the SE and the biometric sample is acquired by the Sensor. It is assumed that the sample is sent to the MCU which still 'drives' the Sensor. Since matching is intended to be performed on the SE, two options may arise:

- The sample is directly sent to the SE (the MCU just drives the Sensor and forwards captured data to the SE). In this case the SE performs the features extraction to recover the Candidate,
- The sample is processed by the MCU to extract a Candidate, meaning that features extraction is carried out on the MCU.

24 As in the MCU-centric case, two options arise for the storage of the Template which is intended to be matched against the extracted Candidate:

- The Template is stored on the MCU: in this case, since the matching is intended to be performed on the SE, the Template must be sent to the SE,
- The Template is stored on the SE: in this case both the Candidate and the Template are available for matching on the SE.

3.3 Mix-matching architecture

25 It may happen that the matching is split between the MCU and the SE. A public Template is then derived, on the SE-side, from the enrolled Template which is stored on the SE-side. This public Template is somehow derived from the enrolled Template in an irreversible manner. Then the following HW+SW architecture may be implemented:

- Features extraction may be performed on the MCU, while
- Public Template derived from the enrolled one is sent to the MCU for a partial matching step. The full Template should not be sent since it will be temporarily stored in MCU.
- The Candidate and/or intermediate results of the partial matching are sent to the SE
- Matching is completed on the SE-side

3.4 Analysis of the architectures

3.4.1 MCU-centric

26 The MCU-centric architecture is discarded because storing and processing a Template on the MCU does not seem relevant. Indeed, in the general case there is absolutely no guarantee on the level of security of an MCU.

27 This architecture is therefore not considered as relevant in the scope of this document.

3.4.2 SE-centric

3.4.2.1 Matching operation processing

28 In this kind of architecture, the processing of the matching operation is performed on the SE side. Because of the security properties of a certified SE, there is a good level of security assurance so that an attacker with a high potential will not be able to recover the Template.

3.4.2.2 Storage of the Template

29 As described in Section 3.2 the storage of the Template can be done in several ways.

30 If the storage is ensured by the SE itself, such devices come with the secure storage as a basic security property. Thus, storage, matching and decision of acceptance are all performed inside the SE.

31 If, for any reason, the Template is stored on the MCU side, its confidentiality and integrity must be ensured. In addition, because matching always occurs on the SE side, the Template must be fetched from the MCU to the SE each time a matching is required, at the cost of extra-exchanges between the SE and the MCU.

32 This option, not being considered efficient from functional point of view, is not relevant in the scope of this document.

3.4.2.3 Features extraction

33 The extraction of features from the sample is either performed directly on the SE or on the MCU. If the features extraction is performed on the MCU, the Candidate is transmitted to the SE for the matching.

3.4.3 Mix-matching

34 In such an architecture, one part of the matching is considered as a public operation whereas the final part is kept confidential. This architecture should not be confused with the one in which the Candidate (features) extraction is performed on the MCU while the (complete) matching is performed on the SE.

35 However, considering the mix-matching architecture raises the question of processing a Template on the MCU. Since MCU-centric architecture was discarded (because of the lack of security assurance on its capacities to preserve confidentiality of manipulated and stored data), it means that the MCU shall only process a public (i.e., blurred/blinded) version of the Template. The practicality of deriving such a public Template from the enrolled one is, at the time of writing this document, unknown. In addition, this

architecture also raises an issue regarding the response time of the Candidate verification, due to extra-exchanges between the SE and the MCU.

36 In such a mix-matching architecture, the lab should assess on a case-by-case basis whether the public part of the matching only processes public information and does not raise any security issue.

37 This architecture thus raises several questions and is only relevant for very specific matching algorithm architectures. It is therefore not considered as relevant in the scope of this document.

3.5 Case of a System in Package (SiP)

38 In such a device, the Sensor, the SE and possibly the MCU are combined into a single hardware package meaning that each component cannot be put apart in an easy manner.

39 From JHAS perspective, this hardware configuration adds some difficulty to the attacker's activities. A dedicated JHAS subgroup (SoC) analysed such kind of architecture. Their work concluded that some additional points should be given to the vendor when such an architecture is used.

40 From [5]: Rating for the removal or penetration of the package is described in the JIL-Application-of-Attack-Potential-to-Smartcards [3] in the "Access to TOE" factor. Indeed, the package can be seen as a barrier that prevents an attacker from accessing the TOE to perform physical or invasive attacks.

3.6 Conclusion on relevant architecture for High attack potential

41 Based on the above analysis, the BC architecture which is the most relevant for resistance to High attack potential is the SE-centric architecture with both matching and storage on the SE side. This architecture only is considered to be in scope of this document.

4 Bio-related Assets

42 This chapter lists the assets related to the biometric subsystem and details their security properties requirements.

4.1 Bio subsystem routines

43 The following routines can be defined:

decision(void): accept or reject API invoked by application)

1. sample := get_sample() {Sensor->MCU | Sensor->SE}
2. candidate := features_extraction(sample) {MCU ; MCU->SE | SE}
3. score := match_Tpl(candidate) {SE}
4. return (score >= threshold) {SE}

match_Tpl(candidate): score

1. template := get_Tpl() {SE}
2. return match(template, candidate) {SE}

store_Tpl(): void

1. sample := get_sample() {Sensor ->MCU [-> SE]}
2. candidate := features_extraction(sample) {MCU ; MCU->SE | SE}
3. set_Tpl(candidate) {SE}

44 Optionally, the biometric subsystem may manage a counter of number of biometric authentications that were attempted, together a dedicated limit. These are denoted:

a. Bio_try_counter (BTC)

b. Bio_try_limit (BTL)

45 These sensitive assets may be directly managed by the application itself. When managed by the biometric subsystem, a set of well identified APIs is provided to the application to perform its CRM. In the context of a BC a part of the CRM may be specific to this kind of product. For this reason, we consider the following additional assets which do not appear in the subroutines above:

- Biometric state machine which formalises the state in which the biometric subsystem is
- Biometric-based risk management of the card which represents the intermediate variables used within the CRM to take into account the state of the biometric subsystem

4.2 Card application

46 The application:

- Invokes the biometric subsystem as a decisional oracle and processes the result,
- Maintains or accesses (through well identified APIs) bio authentication counters (BTC & BTL),
- Performs its risk management and updates counters.

4.3 Enrolment

47 The enrolment step has the following properties:

- Only the authorized person, e.g., genuine cardholder or representative of the issuing entity (*for instance, the cashier at the bank office*) must be able to perform enrolment/re-enrolment.
- Enrolment/re-enrolment can be available in the field but activation of biometric verification functionality using field registered templates must be limited to those who were given such privileges (through different means) and can present a proof of having those privileges (e.g., passcode).
- In the scenario where card application and biometric subsystem application (so called broker) are implemented in the form of two different entities/applications, appropriate mechanism of binding between the applications must be implemented. For example, only trusted application can benefit from the biometric services (incl. matching, enrolment, etc.) provided by biometric subsystem application. Remark: this is an absolute must for products where post issuance is enabled.
- The number of attempts to activate/(re)enable enrolment by all entities other than card provider must be limited by means of a counter limit (or perhaps better to have velocity counter to prevent permanent lock, subject to discussion).

4.4 Assets sensitivity and security properties

48 The assets are detailed in the table below together with their associated security properties:

ASSETS	CONFIDENTIALITY	INTEGRITY
Template	X	X
Score	X	X
Threshold		X
Sample	No but unknown[1]	
Candidate	No but unknown	
Bio Try Counter		X
Bio Try Limit		X
Bio state machine and bio-based risk management		X
Key(s) for Secure Messaging between MCU and SE	X[2]	X[2]
Credentials to gain access to the FW of the MCU	X	X
MCU firmware		X

49 The MCU firmware is listed as an asset for which there is an integrity need. The reason is that if its integrity is harmed, it may be possible to turn the BC into a 'Yes Card' (see Section 5.4.9 for more details).

50 The firmware of the sensor is not listed as it is assumed not to be updatable (see ASSUMPTION 3).

[1] See discussion on 'No but unknown' in ASSUMPTION 2 below.

[2] If the security of the solution relies on secure messaging between the MCU and SE, then the corresponding keys will be in scope for the security evaluation. If secure messaging exists but does not relay assets requiring confidentiality and/or integrity, then the evaluator can conclude it is out of scope.

5 Threats on assets

5.1 Assumptions

ASSUMPTION 1 In order to limit the scope of attacks and to avoid discussions on the strength of biometric-based authentication methods, this section relies on the RTS [2] which states that the cardholder's identity has to be verified, using at least two of the items among possession, knowledge and inherence (see Figure 2).

Figure 2: Factors for customer's authentication

51 Therefore, a BC is compliant with the RTS, relying on the factors of possession and inherence. This couple of factors is a means of authentication that is equivalent to the combination of possession and knowledge factors.

52 N.B.: However, we still do not answer to the question of the sensitiveness of the candidate and sample. To do so, it is proposed to review the threats which are specific to a biometric card and to validate for each identified one:

➔ whether or not it has a practical impact (in terms of financial or image loss).

53 Another way (or maybe a complementary way) of selecting or discarding a threat, is to compare it to an equivalent one in which the classical PIN is involved (it gives us a metric for keeping a threat as relevant or discarding it).

ASSUMPTION 2 The scenario of attack that was chosen to select relevant attack paths in the sequel is the 'lost & stolen' scenario. In this scenario, the attacker steals or finds a stolen card and attempts to tamper with it, to make valid card application features (e.g. *payments*) while neither knowing the PIN nor holding the genuine cardholder's biometrics.

54 Discussion on ASSUMPTION 2 : A consequence of this assumption is that the assets Sample and Candidate, which are derived from the user's fingerprint, are unknown to the attacker at the time he finds or steals the card. In the meantime, these assets do not require confidentiality while they are captured, processed or transmitted by the biometric subsystem. The reason is that requiring confidentiality would then require to implement countermeasures against eavesdropping on the communication buses for instance. Such a requirement would thus lead to a strange situation in which the user (i.e., the genuine cardholder or any attacker) would attempt to spy on the processing or transmission of its own biometrics. The subgroup did not identify any relevant threat in the exploitation phase. However, during the identification phase, this scenario (i.e., spying on its own fingerprint for instance) is still relevant.

ASSUMPTION 3 The sensor is an ASIC (which is assumed to be monolithic), meaning that it has no update capability so that its integrity cannot be harmed.

ASSUMPTION 4 The BC SE development and production phase is performed in a secured environment (covered by Development and Production Site Audit) up to the certification delivery point.

ASSUMPTION 5 At minimum, the BC MCU composite product integration (ensuring Firmware integrity) is performed in a secured environment (covered by Production Site Audit) up to the certification delivery point.

5.2 Surface of attack

5.2.1 Hardware

55 The attack surface is:

- physical contact and/or contactless interfaces
- the circuit design and PCB layout of all components (invasive and non-invasive attacks)
- the plastic body (some latent can be found)

5.2.2 Software

56 The interfaces of the embedded software (for all components composing the biometric card) including

- the card and biometric applications (e.g., capture function, the extraction of features, the matching function and the storage of the template),
- the protocols (e.g., communication links between the Sensor, MCU and SE),
- the data structures and
- all the low-level layers (for example MCU bootloader or/and libs)

are part of the attack surface.

5.3 Threat agents (e.g., attackers)

57 An attacker is defined as having direct physical access to the card including the genuine cardholder.

58 The TOE should be resistant to attacker with High attack potential.

5.4 Threats with supporting paths

5.4.1 Reference (Bio) Template (Disclosure and Modification)

5.4.1.1 Confidentiality:

59 Extraction of the Template during processing (any component)

- Side channel-like attacks which may reveal the template during processing (matching) or comparison.
- Fault Injection attacks which may allow an attacker to dump part of the memory.
- Logical attacks/bad implementations of the SE software which may allow a memory dump.

5.4.1.2 Integrity:

60 Replacement of the Template by a known one.

- For example, by using Fault Injection attacks on the reference to the enrolled Template to point to a known one (for instance, a buffer monitored by the attacker and containing a known Template)
- By means of exploitation of a privileged command to unlock (re-) enrolment
  - Exploit on the embedded software of any component to overwrite the enrolled Template
  - Fault Injection on processing commands (i.e., privileged) to bypass access conditions to write the Template file, unlock the enrolment…

5.4.2 Score

5.4.2.1 Confidentiality:

61 Extraction of the Score during processing

- By means of for example, hill-climbing and side channel attacks an attacker can reveal the score and then tune the presented fingerprint to have a correct match.

5.4.2.2 Integrity:

62 Score modification at runtime processing (good enough, e.g., score ≥ threshold) to pass bio authentication. Such modification of score can be done at any stage of its calculation such as

- matching phase,

- transfer between bio subsystems/modules/computational phases,
- decision taking (score vs threshold).

by means of fault injection.

5.4.3 Threshold

5.4.3.1 Integrity:

63 Threshold modification during runtime processing as well as permanent alteration. Such modification of threshold can be done at any stage of its usage such as

- at rest,
- matching phase,
- decision taking (score vs threshold).

by means of fault injection or logical attacks. This may allow an attacker to modify the threshold and be successfully authenticated with a forged fingerprint.

5.4.3.2 Confidentiality:

N/A

5.4.4 Sample and Candidate

64 Sample and candidate confidentiality is not required but the values are unknown. In this perspective, the following attack paths are considered for the current assessment under the L&S scenario:

- [Lift-up partial attack] Lift-up of the latent prints on the card body and/or sensor surface
    - Example of attacker's aim#1: build a fake fingerprint (2D or 3D) from the latent prints the legitimate cardholder let on the card surface, with the objective to present the fake to the sensor, to pass the cardholder verification step.
- [Reactivation attack] The attacker reactivates the 'Sample acquisition' functionality of the sensor to make it acquire the latent prints that the legitimate cardholder let on the surface of the sensor.
- Interception of the Sample at the Sensor level [enrolment or verification]
    - It requires the genuine user to put his finger while eavesdropping. This attack path is not relevant with ASSUMPTION 2.
    - Supply chain attack, i.e., malicious Sensors are introduced in the supply chain (for instance to always provide the same sample, thus leading to a 'biometric Yes Card'). This attack path is not relevant with ASSUMPTION 3.
- Interception of the Candidate during transmission between components (eavesdropping)

- It requires the genuine user to put his finger while eavesdropping. This attack path is not relevant with ASSUMPTION 2 (same remark as above).
- Supply chain attack, i.e., malicious MCUs are introduced in the supply chain (same attack as above). This attack path is not relevant with ASSUMPTION 5.

- Extraction of the Sample and/or Candidate (any component)
  - It requires the genuine user to put his finger while eavesdropping. This attack path is not relevant with ASSUMPTION 2 (same remark as above).

5.4.5 Bio Try Counter and Limit (BTC and BTL)

5.4.5.1 Integrity:

65 The Biometric Try Counter and Limit are implemented to limit the number of failed biometric authentication attempts. It helps to prevent brute-force attacks.

66 For this reason, attacks attempting to:

- modify the BTC and BTL
- reset the BTC
- bypass the comparison of the counter against its limit

are considered in this document.

67 The integrity of the limit and counter and the comparison results can be modified by means of perturbation or software (logical) attacks for example.

5.4.5.2 Confidentiality:

N/A

5.4.6 Biometric state machine and biometric-based Risk Management of the card

5.4.6.1 Integrity:

68 Modification of the Bio State machine (at any stage of biometric processing, e.g., refer to section 5.4.2 Score) for the attacker to be successfully authenticated with no genuine authentication.

- For example, using fault Injection or logical attacks to change the biometric state machine.

69 Modification of any (intermediate) variable influencing the Risk management of the card, to stay offline instead of requesting an authorisation.

- For example, using fault Injection or logical attacks.

5.4.7 Key(s) for Secure Messaging between MCU and SE

70 In case security of the TOE relies on secure messaging (between MCU and SE), the associated keys should be analysed against disclosure and unauthorized modification.

71 In such a case, this would require the MCU to demonstrate High Assurance.

5.4.8 Credentials to gain access to the FW of the MCU

5.4.8.1 Confidentiality:

72 Recovering MCU credentials may allow an attacker to have access rights on the MCU and be able to write/read the firmware or change credentials data.

5.4.8.2 Integrity:

73 Modification the MCU credentials or change of the program flow when checking credentials to access the FW of the MCU may allow an attacker to have access rights to read/write the firmware.

74 Possible supporting vulnerabilities:

- Using a software (logical) attack (using a software vulnerability).
- Bypassing the credential verification.

75 Note that this asset is strictly related to "MCU firmware" asset. The credentials bypass/modification/disclosure are used with the aim to modify the MCU firmware (see 5.4.9).

5.4.9 MCU firmware

5.4.9.1 Integrity:

76 Modification of MCU firmware

77 Example of attacker's aim#1: to perform replay-like attacks which would allow an attacker to be always successfully authenticated. In a first phase, the attacker updates the firmware with a 'Candidate logger' which records legitimate candidates extracted from the cardholder's fingerprint. In a second phase, upon successful candidate recording the malicious firmware then changes its state to always submit a valid and recorded candidate to the SE. In this way the BC is turned into a 'Yes Card'.

78 *Example of* attacker's aim#1 with *Postal Service attack on MCU FW update capability:*

The *Postal Service attack* is a 2-step attack. The assumption is that the attacker has access to BC, at least during the first step described below, for instance while they are in transit.

- Step 1:
  - The attacker tampers with a large number of those cards and gains access to the MCU FW update feature (getting rid of access controls) to upload

a new but malicious firmware. The malicious firmware consists in recording the next candidate that will be presented by the legitimate Cardholder.

- The transit of those (now maliciously updated) cards continues its way.

- Step 2:
  - The cardholder receives his brand-new card and proceeds to enrolment.
  - Now the card is a 'Yes Card' and vulnerable to lost and stolen fraud.

79 Example of attacker's aim#2: to read the enrolled Template stored on the SE side, if the MCU has the privilege to do so. This privilege may be associated with the capability of the MCU to set up a secure channel with the SE.

6 Evaluation perimeter

80 In this section, the evaluation perimeter for SE-centric architecture which is endorsed by the JHAS is detailed.

81 As detailed in Section 21, a BC can be made of one or several ICs in addition to the Sensor:

- a Secure Element only, or
- a Secure Element and an MCU.

82 The section 3.6 restricts the scope to the BC SE-centric architecture which is the most relevant for resistance to High attack potential. For this architecture, the Secure Element is always evaluated and, depending on some factors, the MCU can be either part of the security evaluation, or out of scope.

83 The evaluation must ensure whether the assumptions listed in Section 5.1 are met. Then only the attacks described in Section 5 that are not covered by assumptions must be considered.

84 The next sections aim at providing some guidance for SE-centric architecture on:

- the MCU test requirements to be performed by the evaluation laboratory
- and the situations where MCU can be excluded from the evaluation scope.

6.1 Considerations on product design and context

85 There are some specific contexts or designs/countermeasures allowing to mitigate the attack paths which are threatening the MCU. In such cases, MCU related attack paths can be put out of scope. To carry out such analysis, the following factors need to be considered during the evaluation of a BC:

- The architectural design:
  - BC architecture and packaging,
  - Biometric subsystem design between the ICs (repartition of the security functions, implementation of the secure messaging, …),
- The vulnerability assessment:
  - Implemented countermeasures,
  - Number of samples required to perform the attack,
- The operational environment and life-cycle:
  - Development and production sites,
  - Issuance process,
  - Enrolment process.

6.2 Architectural design and vulnerability assessment

86 The following situations might lead to discarding some or all attacks on the MCU and therefore, testing will not be required:

1. Attack not applicable:

- no asset, no security function implemented in the MCU,
- no MCU loading capabilities,
- …

2. Attack scenario has theoretical rating above 31:
   - requires several partial attack combinations (e.g., MCU has Hardware tamper-evident feature and has software countermeasures), typically:
     - Physical attack on hardware fuse (disabling READ/WRITE CODE)
     - And fault injections on software countermeasures
3. Hardware is already evaluated as Resistant to high attack potential attackers (Rated >31 points).
   - Countermeasures implementation on modern MCUs:
     - Read/Write encrypted code
     - …
   - Form factors adding point to theoretical rating:
     - Stacked die package
     - …

87 If attack paths cannot be dismissed at an early stage (through the points above) then the lab must derive a penetration test plan for the MCU.

88 If an attack is successful and the MCU is "Not resistant to high attack potential" then mitigation arguments on the possibility of limiting the attacks surface, if applicable, can be used to assess its practicality (such as number of samples, exploitation time, issuance and enrolment process) to possibly dismiss the attack.

6.3 Operational environment and life-cycle

89 The operational environment and life-cycle management of the BC can reduce the risk of some of the attack scenarios. In this case, these scenarios can be put out of the evaluation scope.

90 As examples, the attacks on:

- The MCU firmware (section 5.4.9) based on Postal Service attack for which the following factors need to be considered:
  - Number of samples: lots of samples can be used for the exploitation phase in our scenario, assuming that high volume shipments are not secured. **Secure shipments will discard the attack scenario.**
  - Window of opportunity: should be considered to be *at most* one month to carry out the first step of the attack as **longer attack window will be detected and reported to the card provider**.

- The Sample and Candidate (section 5.4.4)
  - *Attack performed in MCU Supply chain:*

    Those attacks are not relevant if the production environment is covered by guidance and site audit.

91 Based on the security evaluation outcome, the risk management of excluded attack scenario needs to be assessed by the evaluation scheme.

6.4 Conclusion

92 As the BC product is not following a generic standard, many configurations can exist with regard to architectural designs and operational environments. Some specific contexts, guidance or countermeasures can allow to mitigate attack paths on the MCU.

93 It is not possible to cover all details about possible remediations, but the following high-level guidance can put MCU and associated testing out of scope:

- Product and architectural design, not relying on the MCU for the protection of any asset,
- Number of samples required within the specific context of the evaluation (i.e., very restricted number of samples, for any reason),
- Enrolment process, (e.g., MCU not involved in the enrolment process, enrolment ensured by an external device in a secured environment (i.e., *at bank agency only*)),
- Issuance process (e.g., high-volume shipments are secured).