Title: Biometric Product Essential Security Requirements
Maintained by: CCDB Work Group for Biometric Product Security
Version: 1.0
Date of issue: 10-Nov.-2016
Supersedes: 0.8

Status

The CCDB Working Group has been requested to develop an Essential Security Requirements (ESR) for biometrics product. This initial draft contains material that was provided by the initiator, IPA (Japan), for a cPP and reviewed by Working Group members (AISEP (Australia), CCN (Spain) and TSE (Turkey)) and initial Biometric Security iTC members (AIST (Japan), Apple (United States), Epoche & Espri and Applus Laboratories (Spain), Safran Identity & Security (France), TUViT (Germany)) then submitted to the CCDB for public review.

Security requirements in this draft don't depend on biometric characteristics (e.g. fingerprint, face and vein). Therefore the cPP that is to be developed based on this ESR does not depend on biometric characteristics either. The evaluation methodology is defined and described in the supporting document for each biometric characteristic if necessary.

It is acknowledged that various PPs for biometric technology are already existing by the time that this document is developed, see [BSI-CC-PP-0043-2008], [BSI-CC-PP-0062-2009], [BSI-PP-0063-2009], [AIST-PP-BVPPP-2016]. However, the authors of this document agree that the development of a cPP for biometrics shall solely start on the basis of this Essential Security Requirements Document and under consideration of the following objectives:

- The current state of the technology in biometrics in all interested countries shall be considered,
- The developed cPP shall be independent of a concrete biometric modality,
- The developed cPP shall be as modular as possible in order to cover all potential application cases.

Accompanying supporting documents are dependent of a concrete biometric modality. Currently supporting documents for fingerprint and finger/palm vein are planned to be developed. CCRA certificates that claim conformance to the cPP shall be issued only for modalities for which CCRA endorsed supporting documents are available.

References:

[BSI-CC-PP-0043-2008] BSI, Biometric Verification Mechanisms Protection Profile, Version 1.3, 2008

[BSI-CC-PP-0062-2009] BSI, Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies (FSDPP_OSP), Version 1.7, 2009

[BSI-PP-0063-2009] BSI, Fingerprint Spoof Detection Protection Profile (FSDPP), Version 1.8, 2009

[AIST-PP-BVPPP-2016] AIST, Protection Profile for Biometric Verification Products, Version 1.2, 2016

Background and Purpose

From ISO/IEC 2382-37 Information technology — Vocabulary — Part 37: Biometrics (cf. http://standards.iso.org/ittf/PubliclyAvailableStandards/c055194_ISOIEC_2382-37_2012.zip), we have the following definitions.

Biometric recognition, biometrics -- *automated recognition of individuals based on their biological and behavioural characteristics*

Biometric System -- *system for the purpose of the biometric recognition of individuals based on their behavioural and biological characteristics*

This document describes the high-level set of security requirements that a biometric product shall satisfy when evaluated against the cPP written for such technology.

The biometric product enrols and/or verifies a user using his/her biometric characteristic. Each process is described in the following paragraphs. A biometric product may implement only one of those functionalities.

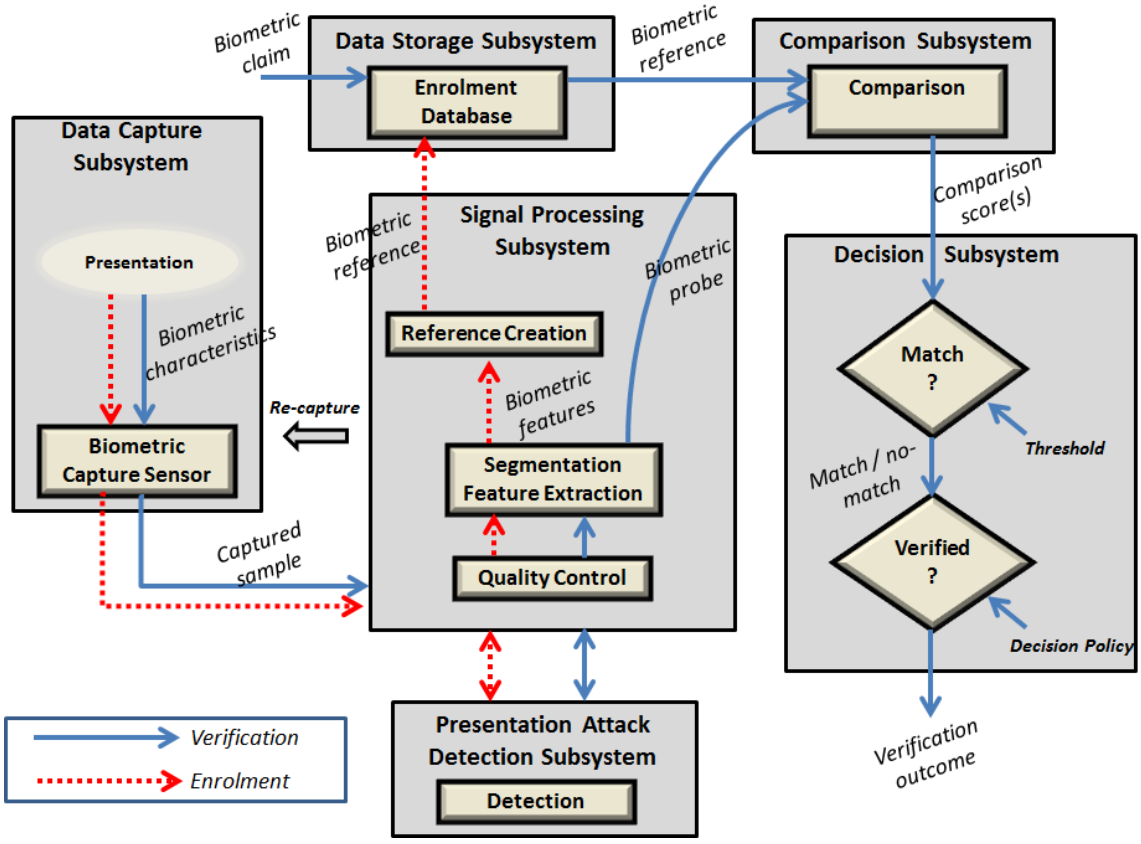
a) Enrolment

During the enrolment process the biometric product captures the biometric raw data of a user and extracts the biometric feature it is working with. The biometric feature is then combined with the identity of the user and stored as a biometric template in a database.

b) Biometric verification

During the verification process the user provides his/her identity and biometric characteristic to the biometric product. The biometric product retrieves the biometric template associated with the identity from the database, compares it with the biometric feature extracted from the captured biometric characteristic of the user to generate the similarity between the two data, and determines whether user is accepted or rejected based on the similarity.

Examples of modalities used by biometric recognition systems are: fingerprint, face, iris, palm print, finger vein, palm vein, speech, signature and so forth. The following figure, inspired from ISO/IEC JTC1 SC37 standards, is a generic representation of a biometric system (other configurations exist). This illustrates the different sub-functionalities on which the biometric enrollment and the biometric verification processes rely on.



When used in a security system, the biometric product needs to take into account the risk of subverting the biometric functionalities. One of the main entry points for an attacker is the biometric capture subsystem where they could present artificial or abnormal biometric traits at the point of presentation and collection of the relevant biometric characteristics, in order to interfere with system policy. As defined in [30107-1], this corresponds to a presentation attack, the "presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system". It can be realized by presenting an artefact or human characteristic which are called presentation attack instruments. Presentation Attack Detection (PAD) refers to the automatic determination of a presentation attack. The PAD subsystem plays an important role in the security of biometric systems, especially when unsupervised.

[30107-1] ISO/IEC 30107-1:2016. Information technology -- Biometric presentation attack detection -- Part 1: Framework

Use Case(s)

Biometric products are used for user authentication for mobile devices such as smartphones, PC login at offices, ATMs at banks, and building or room entrance control, or border security checks.

The configuration of the biometric products is categorized into the following two types:

- Integrated Type: The components of the biometric products are not physically separated, i.e., the components are not connected by USB cables or network.

- Separated Type: The components of the biometric products are physically separated, i.e., the components are connected by USB cables or network.

Resources to be protected

- *Any asset that enrolled users can access after successful biometric verification*
- *Biometric features, templates and security related parameters, such as the threshold value, that are used and referenced for biometric verification*
- *Log data that is produced by the biometric system (if generated by the biometric system)*

Attacker access

- *An attacker can present some biometric characteristics and try to be incorrectly verified as a genuine user.*
- *An attacker can present some biometric characteristics in order trying to disguise her own identity during the enrolment or verification process.*
- *An attacker can present any kind of presentation attack instruments during enrolment and biometric verification for the sake of impersonation.*
  (An attacker may steal biometric features of a genuine user and make any kind of presentation attack instruments based on the biometric features).
- *An attacker can present any kind of presentation attack instruments in order to disguise her own identity during the enrolment or verification process.*
- *An attacker can carry out any kind of logical or physical attacks that do not exceed the attack potential defined in the cPP in order to disguise her own identity during the enrolment or verification process or for the sake of impersonation.*

Attacker Resources

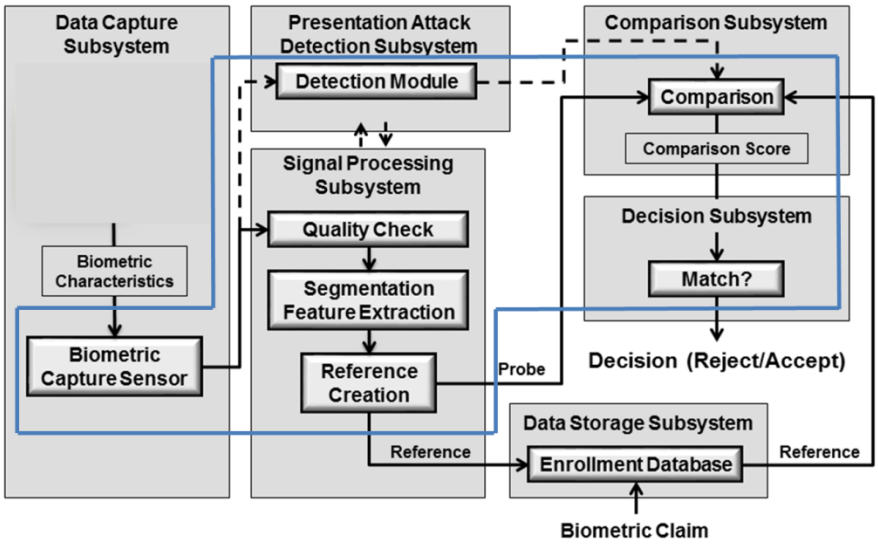
- *An arbitrary amount of time to examine and attack the biometric product, in particular to make artificial biometric characteristics and present them to the biometric product*
- *Commercially and/or publicly available software/knowledge/equipment, and, if it is commercially available, samples of the biometric product to test and attack*

Boundary of Product

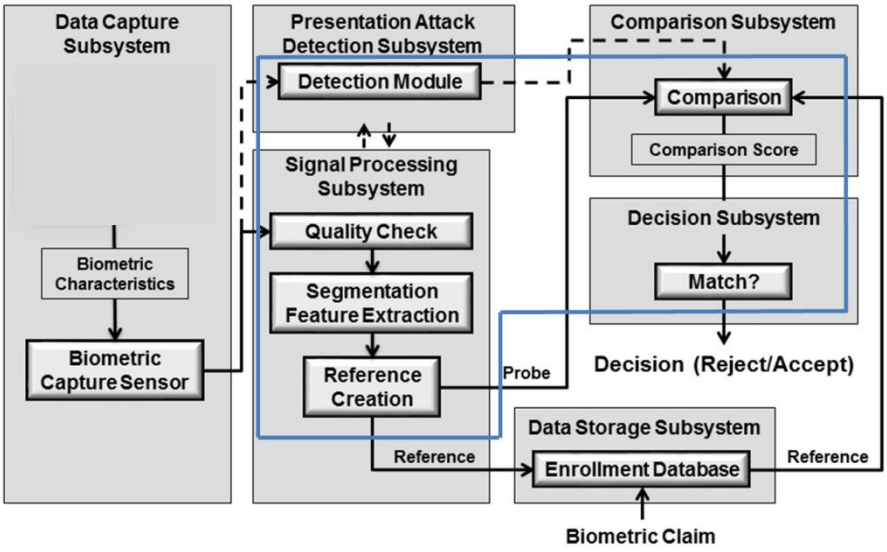
- *The hardware, firmware, software and security functionalities of the biometric product define the boundary*
- *All of the security functionalities are contained and executed within the boundary of the biometric product*

Examples of typical boundary (inside the blue frame) of biometric products (figures are inspired from [30107-1])*:*

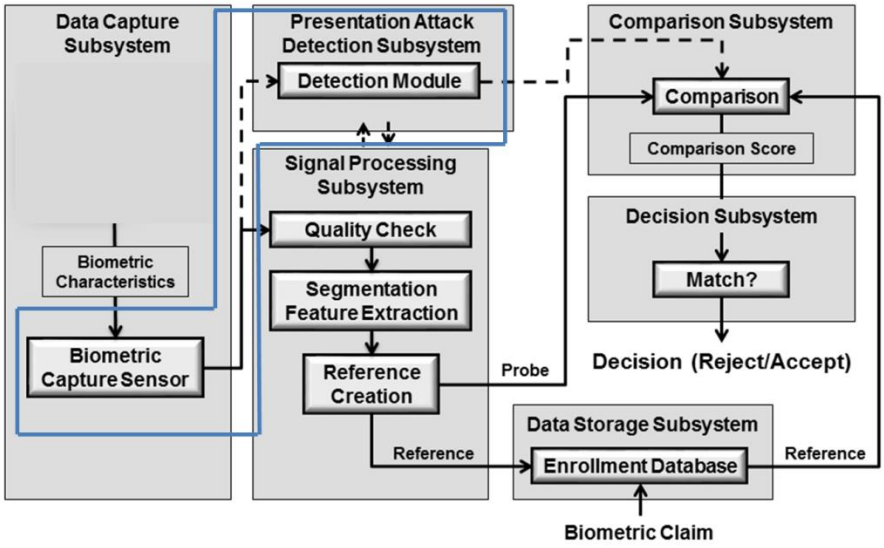
1. *Case of a typical fully integrated biometric product:*



2. *Case of a typical software only product:*



3. *Case of a typical presentation attack detection sensor-based product:*



Essential Security Requirements

- *The biometric product shall enroll users less than a claimed error rate (i.e. FTE)*
- *The biometric product shall verify users less than claimed error rates (i.e. FAR and FRR)*
- *The biometric product shall prevent enrolment nor verification from being successful when presentation attack instruments are used*
- *The biometric product shall counter logical and physical attacks against the TOE that do not exceed the attack potential defined in the cPP*

Assumptions

- *Administrators (if existing) of the biometric product are trustworthy and well trained*
- *Communication between the database and the biometric product is protected*
- *The product is assumed to be used in a semi-controlled and observable environment (i.e. attacks that require extensive time or extensive access to the TOE during exploitation phase or the use of complex tools (in the sense of conspicuous tools) are considered non practical)¶*

Optional Extensions

Requirements captured in this section may already be realized in some products in this technology class, but this ESR is not mandating these capabilities exist in "baseline" level products.

- *The biometric product shall avoid to enroll a user whose biometric feature extracted from her biometric characteristic and a biometric template already stored are determined to be from the same user*
- *The biometric product shall ensure secure communication with the database*
- *The biometric product shall protect the database against modification or eavesdropping*

Outside the Scope of Evaluation

- *Biometric identification*