GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

GlobalPlatform Technology
TEE Biometric System PP-Module
Version 0.0.0.11

Public Review

November 2018

Document Reference: GPD_SPE_091

THIS SPECIFICATION OR OTHER WORK PRODUCT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY IMPLEMENTATION OF THIS SPECIFICATION OR OTHER WORK PRODUCT SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE COMPANY, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER DIRECTLY OR INDIRECTLY ARISING FROM THE IMPLEMENTATION OF THIS SPECIFICATION OR OTHER WORK PRODUCT.

Table des matières

Figures

Tables

1 Introduction

Title:	TEE Biometric System PP-Module (TEE BS PP-Module)
Base PP:	Core TEE PP with Time and Rollback PP-Module, ref. GPD_SPE_021+Time
Identification:	GPD_SPE_091
Sponsor:	GlobalPlatform
Editor:	GlobalPlatform
Date:	November 2018
Version:	0.0.0.11
CC Version:	3.1 Revision 5

This document defines the TEE Biometric System PP-Module, which extends the TEE Protection Profile. The scope of this PP-Module is the biometric verification system on which applications rely for the authentication of an end user and the confirmation of user acceptance. In this context, the major objective of a biometric system is to allow only authorized users to access sensitive information, such as corporate data assets for instance, or sensitive functionality, such as money transfer, bill payment, document signature validation. Biometric systems verify the claimed identity of a human being using unique characteristics of his body and allow or deny him access to sensitive information or functionality based on the results of the biometric verification process.

This PP-Module aims to be applicable to any biometric verification system, independently of the used biometric mode. It is therefore written in a generic way. However, where a certain biometric mode and its specificities have to be considered, this PP-Module focuses on fingerprint recognition.

The biometric services are integrated into the TEE and they may optionally rely on a Trusted User Interface (TUI) to communicate with the end-user. The components needed for capturing the biometric characteristics shall be wired and integral to the device. Their drivers shall be among the TEE components (part of the Trusted OS). The software completing any demanded biometric activity may be implemented as part of the TEE and all data will be processed and stored protected by the TEE. Otherwise, its implementation will ensure an equivalent level of data protection.

The evaluation assurance level applicable to this PP-Module is EAL2+, as defined in the TEE Protection Profile.

This PP-Module is aimed at being used together with the core [TEE PP] and the Time and Rollback PP-Module. The Time and Rollback PP-Module is required for the full protection of the biometric reference database and association store independently of the implementation. The Debug PP-Module is not mandatory but it can be used safely since it does not introduce any consistency issue.

1.1 Audience

This document is dedicated to all actors in the TEE value chain: biometric system developers, integrators (in particular handset makers), service providers (TA developers), as well as ITSEFs, certification bodies and Common Criteria certificate consumers.

1.2 IPR Disclaimer

Attention is drawn to the possibility that some of the elements of this GlobalPlatform specification or other work product may be the subject of intellectual property rights (IPR) held by GlobalPlatform members or others. For additional information regarding any such IPR that have been brought to the attention of GlobalPlatform, please visit https://www.globalplatform.org/specificationsipdisclaimers.asp. GlobalPlatform shall not be held responsible for identifying any or all such IPR, and takes no position concerning the possible existence or the evidence, validity, or scope of any such IPR.

1.3 References

Table 1-1: Normative References

Standard / Specification	Description	Ref
CC Part 1	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, revision 5, April 2017. CCMB-2017-04-001.	[CC1]
CC Part 2	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, revision 5, April 2017. CCMB-2017-04-002.	[CC2]
CC Part 3	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, revision 5, April 2017. CCMB-2017-04-003.	[CC3]
CEM	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, revision 5, April 2017. CCMB-2017-04-004.	[CEM]
GPD_SPE_009	TEE System Architecture, GlobalPlatform (Latest applicable version)	[TEE Arch]
GPD_SPE_010	TEE Internal Core API Specification, GlobalPlatform (Latest applicable version)	[TEE Core API]
GPD_SPE_007	TEE Client API Specification, GlobalPlatform (Latest applicable version)	[TEE Client API]
GPD_SPE_021	TEE Protection Profile v1.2.1 (or Latest applicable version)	[TEE PP]
GPD_SPE_042	TUI Extension: TEE Biometrics API (Latest applicable version)	[TEE BIO API]
GPD_SPE_055	TEE Trusted User Interface Low-level API (Latest applicable version)	[TEE TUI LL API]
ISO/IEC 2382-37/2017	Information technology – Vocabulary – Part 37: Biometrics	[ISOBIO]
RFC2119	Key words for use in RFCs to Indicate Requirement Levels	[RFC 2119]

Table 1-2: Informative References

Standard / Specification	Description	Ref
OMTP ATE TR1	Open Mobile Terminal Platform Advanced Trusted Environment OMTP TR1 v1.1	[OMTP-TR1]

1.4 Terminology and Definitions

The following meanings apply to SHALL, SHALL NOT, MUST, MUST NOT, SHOULD, SHOULD NOT, and MAY in this document (refer to [TEE Arch]):

- **SHALL** indicates an absolute requirement, as does **MUST**.
- **SHALL NOT** indicates an absolute prohibition, as does **MUST NOT**.
- **SHOULD** and **SHOULD NOT** indicate recommendations.
- **MAY** indicates an option.

Selected terms used in this document are included in Table 1-3. CC terminology, defined in [CC1] §4, is not listed here. The following terms come from TEE Protection Profile [TEE PP] and from the ISO biometric vocabulary [ISOBIO].

Table 1-3: Terminology and Definitions

Term	Definition
Application Programming Interface (API)	A set of rules that software programs can follow to communicate with each other.
Biometric Characteristic	The biometric, i.e. unique, physical, feature of interest, e.g. fingerprint, iris, face.
Biometric Comparison	Determination of a biometric comparison score between a biometric probe and a biometric reference or a set of biometric references.
Biometric Comparison Score	Numerical value (or set of values) resulting from a biometric comparison between a biometric probe and a biometric reference or a set of biometric references.
Biometric Probe	The biometric data set extracted from a biometric sample and used for the biometric comparison to a biometric reference or to a set of biometric references.
Biometric Reference	The biometric data set created through an enrolment operation and stored with a unique identifier for use in future biometric identification and verification operations.
Biometric Sample	The raw data set obtained by a sensor during a capture operation. This is subsequently used for creating biometric probes and biometric references.
Capture	The act by which a sensor acquires the raw data set from the biometric characteristic of interest. The raw data set constitutes a biometric sample that can be visualized as an image, e.g. fingerprint, face, or iris.

Term	Definition
Client Application (CA)	An application running outside of the Trusted Execution Environment (TEE) making use of the TEE Client API that accesses facilities provided by the Trusted Applications inside the TEE. Contrast *Trusted Application*.
Consistency	A property of the TEE persistent storage that stands at the same time for runtime and startup consistency. Runtime consistency stands for the guarantee that the following clauses hold: • Read/Read: Two successful readings from the same storage location give the same value if the TEE did not write to this location and the TEE was not reset in between • Write/Read: A successful reading from a given storage location gives the value that the TEE last wrote to this location if the TEE was not reset in between. Startup consistency stands for the guarantee that the following clause holds: • During a given power cycle, the stored data used at startup is the data for which runtime consistency was enforced on the same TEE on a previous power cycle. Consistency implies runtime integrity of what is successfully written and read back – values or code. However, the stored data used at startup may be restored from an old power cycle, not the latest one. It is still consistent at start-up because it corresponds to a memory snapshot at a given time, but it represents an integrity loss compared with the latest power cycle. This notion is weaker than integrity that must be preserved between power cycles.
Device binding	Device binding is the property of data being only usable on a unique given system instance, here a TEE.
Enrolment	The creation of a new biometric reference stored for future usage, defining the authorized user with respect to a biometric feature of interest. enrolment is a prerequisite to Association.
Execution Environment (EE)	A set of hardware and software components that provide facilities (computing, memory management, input/output, etc.) necessary to support applications.
Monotonicity	Monotonicity is the property of a variable whose value is either always increasing or always decreasing over time.
Power cycle	A power cycle is the lapse between the moment a device is turned on and the moment the device is turned off afterwards.
Production TEE	A TEE residing in a device that is in the end user phase of its life cycle
Rich Execution Environment (REE)	An environment that is provided and governed by a Rich OS, potentially in conjunction with other supporting operating systems and hypervisors; it is outside of the TEE. This environment and applications running on it are considered un-trusted. Contrast *Trusted Execution Environment*.

Term	Definition
Rich OS	Typically, an OS providing a much wider variety of features than that of the OS running inside the TEE. It may be very open in its ability to accept applications. It will have been developed with functionality and performance as key goals, rather than security. Due to the size and needs of the Rich OS it will run in an execution environment that may be larger than the TEE hardware (often called an REE – Rich Execution Environment) with much lower physical security boundaries. From the TEE viewpoint, everything in the REE has to be considered un-trusted, though from the Rich OS point of view there may be internal trust structures. Contrast *Trusted OS*.
Root of Trust (RoT)	Generally, the smallest distinguishable set of hardware, firmware, and/or software that must be inherently trusted and which is closely tied to the logic and environment on which it performs its trusted actions.
System-on-Chip (SoC)	An electronic system all of whose components are included in a single integrated circuit.
TA instance time / TA persistent time	Time value available to a Trusted Application through the TEE Internal Core API. The API offers two types of time values: System Time, which exists only during runtime, and Persistent time, which persists over resets. System Time must be monotonic for a given TA instance, and the returned value is called “TA instance time”. Persistent time depends only on the TA but not on a particular instance, it must be monotonic even across power cycles. Its monotonicity across power cycles is related to the Time and Rollback optional PP-Module.
TEE Client API	The software interface used by clients running in the REE to communicate with the TEE and with the Trusted Applications executed by the TEE.
TEE Internal Core API	The software interface exposing TEE functionality to Trusted Applications.
TEE Service Library	A software library that includes all security related drivers.
Trusted Application (TA)	An application running inside the Trusted Execution Environment that exports security related functionality to Client Applications outside of the TEE. Contrast *Client Application*.
Trusted Execution Environment (TEE)	An execution environment that runs alongside but isolated from an REE. A TEE has security capabilities and meets certain security-related requirements: It protects TEE assets from general software attacks, defines rigid safeguards as to data and functions that a program can access, and resists a set of defined threats. There are multiple technologies that can be used to implement a TEE, and the level of security achieved varies accordingly. For more information, see OMTP ATE TR1 [OMTP-TR1]. Contrast *Rich Execution Environment.*

Term	Definition
Trusted OS	The operating system running in the TEE. It has been designed primarily to enable the TEE using security-based design techniques. It provides the GlobalPlatform TEE Internal Core API to Trusted Applications and a proprietary method to enable the GlobalPlatform TEE Client API software interface from another EE. Contrast *Rich OS*.
Trusted Storage	In GlobalPlatform TEE documents, *trusted storage* indicates storage that is protected to at least the robustness level defined for OMTP Secure Storage (in section 5 of [OMTP-TR1]). It is protected either by the hardware of the TEE, or cryptographically by keys held in the TEE. If keys are used they are at least of the strength used to instantiate the TEE. A GlobalPlatform TEE Trusted Storage is not considered hardware tamper resistant to the levels achieved by Secure Elements
Verification	The act of granting or denying access to sensitive data or functionality to a user based on a comparison between a biometric probe and a biometric reference or set of biometric references. The verification is successful if and only if there exists a biometric reference that is similar enough to the biometric probe.

1.5 Abbreviations and Notations

The following abbreviations and notations are used within this Protection Profile Module:

Table 1-4: Abbreviations and Notations

Abbreviation / Notation	Meaning
API	Application Programming Interface
CA	Client Application
CC	Common Criteria (defined in [CC1], [CC2], [CC3])
CEM	Common Evaluation Methodology (defined in [CEM])
CM	Configuration Management (defined in [CC1])
EAL	Evaluation Assurance Level (defined in [CC1])
EE	Execution Environment
ID	Identifier
NA	Not Applicable
OS	Operating System
OSP	Organisational Security Policy (defined in [CC1])
PCB	Printed Circuit Board
PP	Protection Profile (defined in [CC1])

Abbreviation / Notation	Meaning
RAM	Random Access Memory
REE	Rich Execution Environment
RFC	Request For Comments; may denote a memorandum published by the IETF
ROM	Read Only Memory
SAR	Security Assurance Requirement (defined in [CC1])
SFP	Security Function Policy (defined in [CC1])
SFR	Security Functional Requirement (defined in [CC1])
SoC	System-on-Chip
SPD	Security Problem Definition (defined in [CC1])
ST	Security Target (defined in [CC1])
TA	Trusted Application
TEE	Trusted Execution Environment
TOE	Target of Evaluation (defined in [CC1])
TSF	TOE Security Functionality (defined in [CC1])
TUI	Trusted User Interface
TSFI	TSF Interface (defined in [CC1])

1.6 Revision History

GlobalPlatform technical documents numbered *n*.0 are major releases. Those numbered *n*.1, *n*.2, etc., are minor releases where changes typically introduce supplementary items that do not impact backward compatibility or interoperability of the specifications. Those numbered *n.n*.1, *n.n*.2, etc., are maintenance releases that incorporate errata and precisions; all non-trivial revisions are indicated, often with revision marks.

Table 1-5: Revision History

Date	Version	Description
June 2, 2017	0.0.0.*1*	Initial document with TOE description, assets, threats and first draft of objectives
June 26, 2017	0.0.0.*2*	Update following internal review
July 13, 2017	0.0.0.*3*	Update following discussions within TEE SWG and internal review
November, 2017	0.0.0.*4*	Update following reviews, comments and discussions within TEE SWG New SFR chapter
November, 2017	0.0.0.*5*	Update following TEE SWG meeting (Vienna, Nov 8th)

Date	Version	Description
December, 2017	0.0.0.*6*	Updates and SFR chapter revision
Jan-Feb 2018	0.0.0.*7*	Updates and SFR chapter completion
March, 2018	0.0.0.*8*	Global review Draft for TEE Security WG
May, 2018	0.0.0.9	Updates following received comments and discussions during the TEE Security WG meeting
October, 2018	0.0.0.10	Update following TEE PP revision
November, 2018	0.0.0.11	Update following Member Review

2 TOE Overview

This chapter defines the type of the Target of Evaluation (TOE), describes the functional behaviour of the TOE, presents typical TOE architectures, and describes the TOE's main security features and intended usages as well as the TOE's life cycle.

2.1 TOE Type

The TOE type is the GlobalPlatform TEE with a biometric system on which applications rely for the authentication of an end user and the confirmation of user acceptance.

The TOE comprises:

- Any hardware, firmware and software used to provide the biometric functionality, including sensors, drivers, matching, and decision components, and user interfaces;
- Any TA executing on the TEE and implementing security-critical parts of the biometric functionality;
- The guidance for the secure usage of the TEE biometric system after delivery.

The TOE does not comprise:

- The biometric capture functionality of the sensor;
- The Trusted Applications running on top of the TEE that do not implement biometric functionality;
- The Rich Execution Environment (REE);
- The Client Applications running on top of the REE.

Application Note:

This PP-Module does not require full functional compliance with GlobalPlatform APIs specifications.

2.2 TOE Description

2.2.1 Functional Description

The TOE provides core biometric verification functionality that can be divided into two different categories, namely core biometric functionality and administrative functionality. The core biometric functionality includes an implicit capture process and two explicit processes, namely enrolment and verification. The administrative functionality includes an explicit or implicit process which associates (access) rights/authorisations to end users. Optionally, other explicit or implicit administrative processes may be provided, such as for instance a stop function for the biometric processes, the deletion of associations between end users and rights/authorisations, the deletion of data stored during the enrolment process that has subsequently become obsolete, the listing of end users and their specific rights/authorisations, or the global wipe of the biometric system data. Some of the most relevant biometric processes are detailed below.

Application Note:

All the operations provided by a biometric verification system must be described in the STs that are conformant to this PP-Module.

2.2.1.1 Capture

The capture process is the preliminary, necessary step for any direct interaction, i.e. enrolment and verification, of an end user with the biometric system. It is performed by the sensor and consists in acquiring raw data from the physical biometric feature of interest (e.g. fingerprint, iris, face). The captured raw data constitutes a biometric sample (Live Image) that can be visualized as an image. Biometric samples are subsequently used for creating biometric references (Stored Templates) and biometric probes (Live Templates). Biometric samples, biometric references, and biometric probes should never be exported.

The capture function itself lies outside the TOE boundary. However, the biometric system has exclusive access to the sensor/capture peripheral, and therefore to the data, i.e. the captured biometric samples. The exclusive access applies only to the time of usage and only to biometric data.

2.2.1.2 Enrolment

The enrolment process is the first contact of a user with a biometric system. This process is necessary because a biometric verification system has to acquire information regarding each user in order to verify their identity based on their biometric characteristics.

During the enrolment process the system captures the biometric characteristic of a user and extracts the relevant features, i.e. the features it is working with. The quality of the biometric sample has to be assured. If it is inadequate or of low quality, the user to be enrolled has to repeat the process. Optionally, user guidance can be provided during this process. If the quality of the biometric sample is sufficiently high and a biometric reference can be created, a unique identifier for the biometric reference shall be generated. The biometric reference and the identifier shall be combined and stored in a database for subsequent use. Furthermore, following a successful enrolment, an association can be performed. If no biometric reference of sufficient quality can be created an error is returned.

Application Note:

Besides the biometric characteristics, no other data about a user's identity, e.g. name, shall be stored by an enrolment operation.

Application Note:

Like all of the described biometric operations, the enrolment operation should be atomic.

2.2.1.3 Association

The association process is one of the two necessary steps for the authentication of an end user and the confirmation of user acceptance. It is an administrative function that associates specific access rights/authorisations to end users. More specifically, it may link a biometric reference to a TA. The association can be done explicitly and/or implicitly following the enrolment process, the TA installation, or both.

For explicit associations, the user provides a biometric sample (of sufficient quality) giving a biometric probe which is compared against all available biometric references stored in the database. If a *match* is found, then an association between the calling TA and the found matching biometric reference is created. The association is based on the TA and the unique identifier of the found matching biometric reference.

For implicit associations following the enrolment process, an association consisting of the calling TA and the identifier of the biometric reference created during enrolment is created. For implicit associations following the installation of a TA, multiple associations consisting of the installed TA and the identifiers of specific biometric references may be created.

Both explicit and implicit associations must be stored in non-volatile memory, in an association store.

Application Note:

The association process described in the API Biometrics specification GPD_SPE_042 may be implicit at enrolment time or explicit. Associations are stored in an Association Store.

2.2.1.4 Verification

The verification process is the major functionality of a biometric system in the context of this PP-Module. Its objective is to verify or refuse the claimed identity of a user, and consequently to give or deny access to sensitive information or functionality. The user's biometric characteristic has to be captured. The quality of the captured biometric sample has to be assured. If it is inadequate or of low quality, the user to be verified has to repeat the process. A biometric probe is extracted from the biometric sample captured from the user. This is compared against the biometric reference(s) stored in the database and associated to the calling TA in the association store. If there exists one stored biometric reference that is similar enough to the biometric probe, the claimed identity of the user is verified and authentication is successful. Otherwise, i.e. if no adequate biometric reference was found, the claimed identity is refused and authentication fails.

The comparison component of a biometric system computes a comparison score between the biometric probe and the biometric reference. This is then used by the matching component of the biometric system that decides whether a biometric reference and a biometric probe are similar enough. Usually, a threshold value is used for the decision. Default threshold values may be set by the manufacturer.

2.2.1.5 Dissociation

The dissociation process is the converse of the association process. It erases an association kept in the association store that relates a TA and a biometric reference identifier. The dissociation process can be performed explicitly or implicitly during the uninstallation of a TA. When performed explicitly, the unique identifier of a biometric reference is provided and the association between the calling TA and the provided identifier is deleted. When performed implicitly during the uninstallation of a TA, any association linking that specific TA and a biometric reference identifier is deleted. A dissociation operation may trigger an automatic deletion of a biometric reference, when it erases the last association for the biometric reference in question.

The association store must be fully rollback-protected.

2.2.1.6 Biometric Reference Deletion

The biometric reference deletion consists in removing from the database any unused biometric reference. This process could be performed explicitly upon user demand; it should be performed implicitly upon factory reset if such operation is available, or when all associations between its identifier and the existing TAs are garbage collected or deleted from the association store for instance. Additionally, any biometric reference that has become corrupted should be automatically deleted, and subsequent association or verification operations against it should be impossible.

The database in which biometric references are stored must be fully rollback-protected.

A global wipe of the biometric system is a special kind of deletion, which completely removes all the stored biometric system data.

2.2.1.7 Administration

Optionally, a special entity known as the administrator of the biometric verification system may be defined. An administrator is an individual who is authorised to perform specific administrative operations and who is responsible for the installation and maintenance of the biometric system, as well as for the configuration of certain security relevant settings such as the threshold value used during the biometric verification process. Depending on the concrete implementation of a biometric system there may be more than one administrator and also more than one administrative role.

The administrator must be well-trained and non-hostile. He must be supplied with detailed guidance documentation that he will subsequently apply rigorously.

The TOE must provide a mechanism to verify the administrator by other means than the biometric process (e.g. username/password, smartcard/pin etc.).

Specific threats, security objectives and assumptions pertaining to the administrator's interaction with the biometric system have to be considered.

This is not covered by the current version of this PP-Module.

Application Note:

Only some specific authorized end users should have access to the association and dissociation operations described above. Otherwise, if any end user can request an association, the purpose of biometric verification itself is defeated. A malicious or unauthorized user would not need to perform a sophisticated attack: he could simply enroll and then associate his own biometric reference to any applications/services he targets. Similarly, a malicious or unauthorized user could dissociate the associations, i.e. authorisations, of any genuine, authorized user, thus denying him access/rights to information or services to which he has been granted access/rights. Therefore, association, dissociation and listing of existing associations should be available only to specific authorized users, i.e. the equivalent of an administrator. Typical users should only be able to request a biometric verification or enrolment. These aspects are not covered by this PP-Module. However, for the biometric system specified in [TEE BIO API], this is addressed by design since the TEE and the biometric system are not directly accessible to end-users. Access is mediated by TAs, which can access the exposed biometric functionality.

2.2.1.8 Biometric Functionality Overview

Figure 1. illustrates the first four previously described biometric processes: capture, enrolment, association and verification.

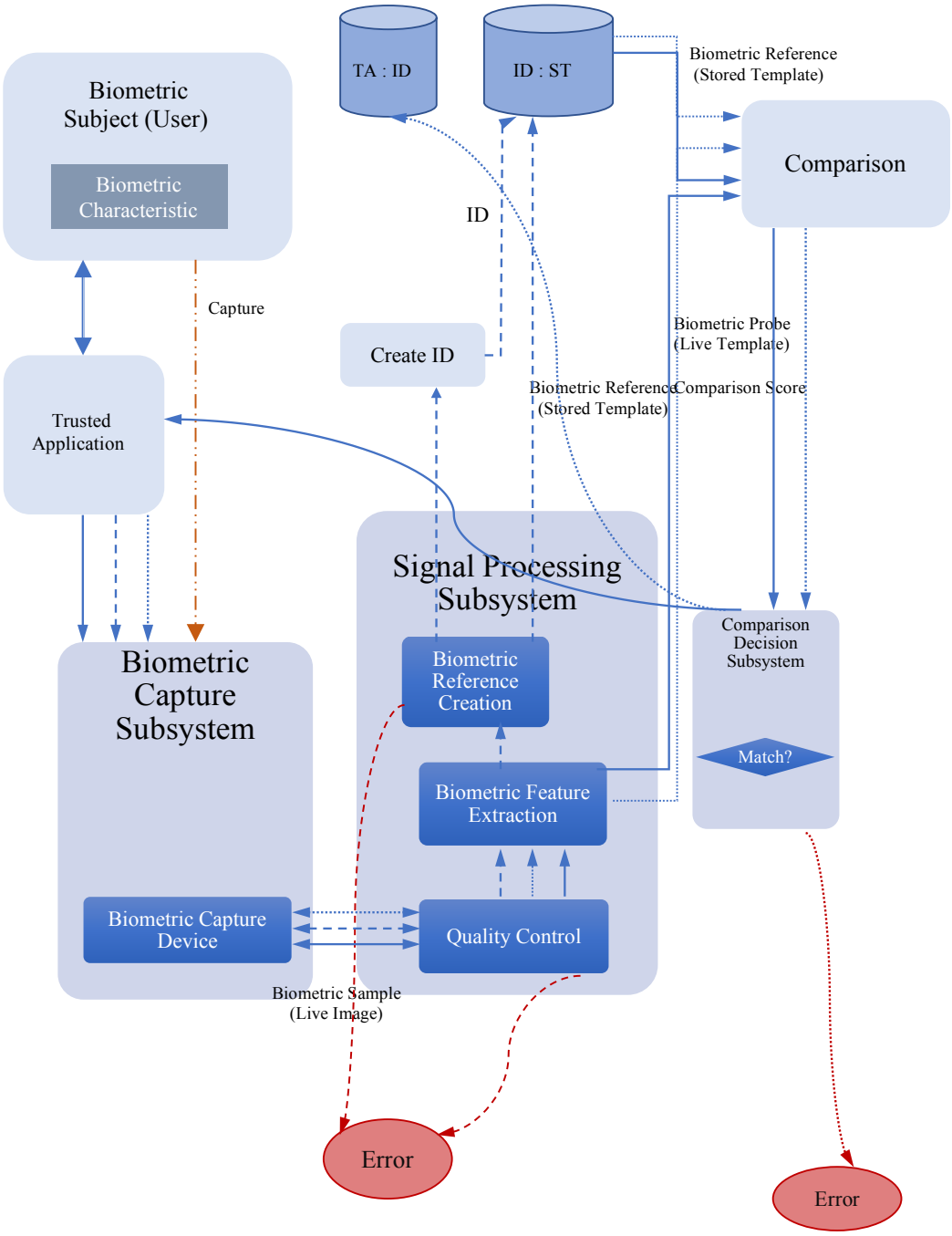
The orange arrow shown only between the biometric subject (user) and the biometric capture subsystem refers to the capture process performed by the sensor. This lies outside the TOE boundaries. It is illustrated by an arrow of the following kind:

The data flow between the different subsystems and components of a biometric system during the enrolment process is illustrated by arrows of the following kind:

The data flow between the different subsystems and components of a biometric system during the association process is illustrated by arrows of the following kind:

The data flow between the different subsystems and components of a biometric system during the verification process is illustrated by arrows of the following kind:

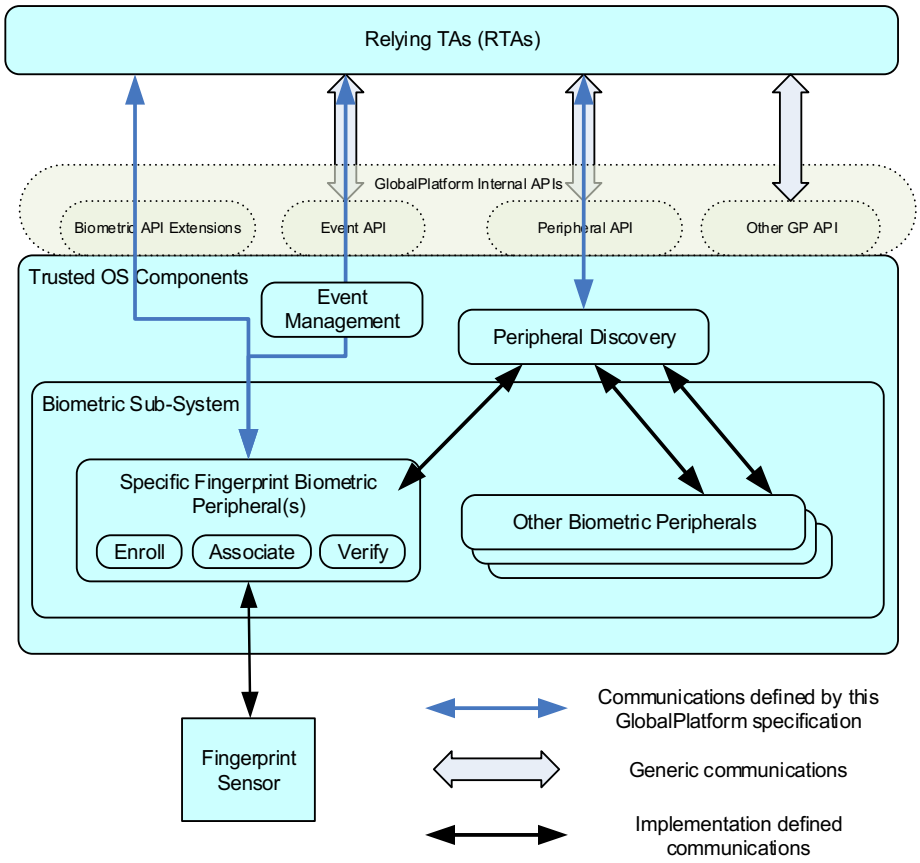
Figure 1 Biometric Functionality – Overview



2.2.2 Architecture

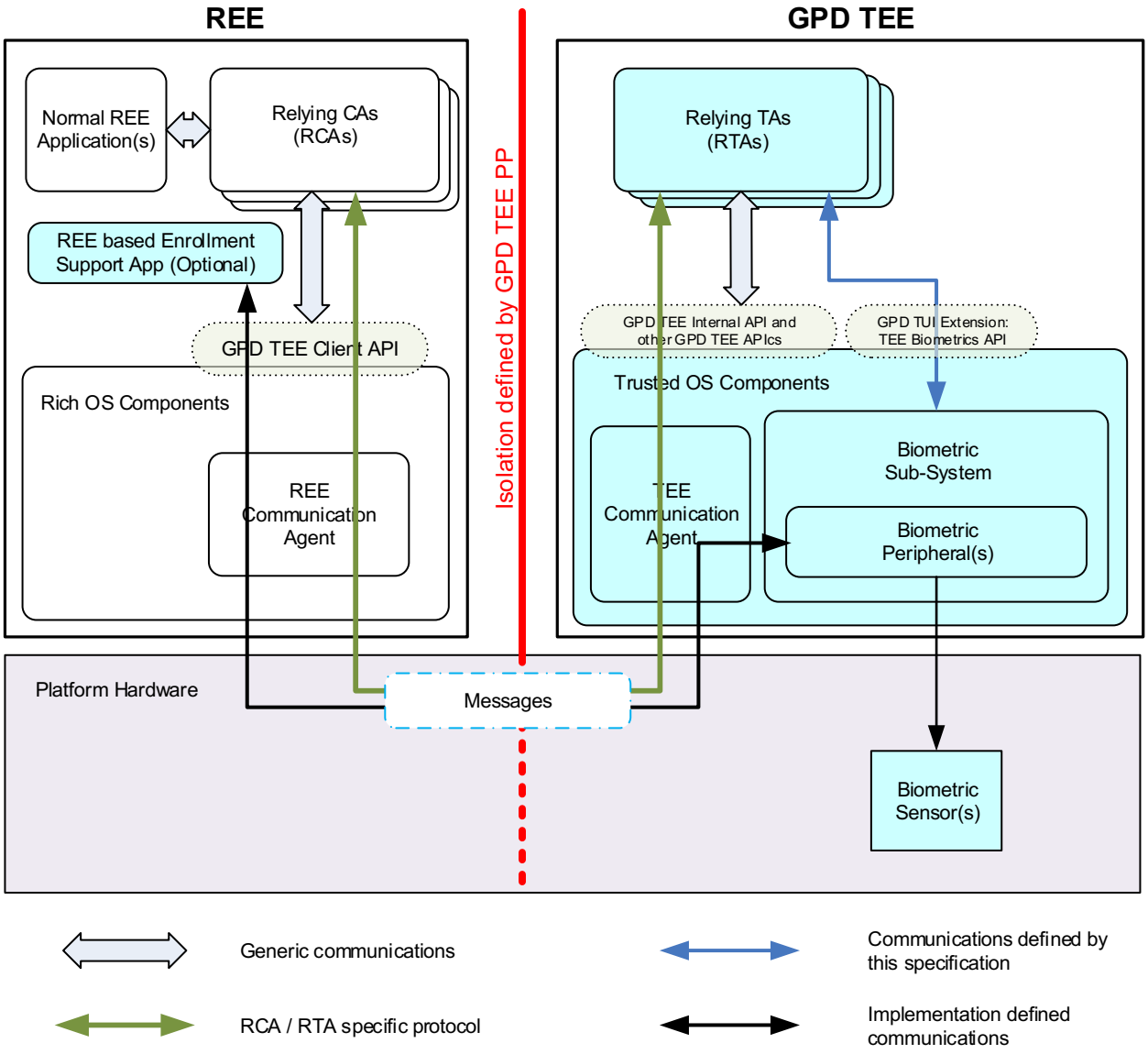
The architecture of the biometric verification system in depicted in Figure 2 and Figure 3.

Figure 2 Architecture Overview -- Multiple Biometrics



The TOE boundary depends on the implementation. Part of the biometric verification system may optionally be implemented as Trusted Applications running in the TEE, or in one of the potentially available SEs, executing as “Match on Card”. Different implementations may choose to allow components in the REE to handle some biometric functionality that is not security-critical. Such architectural choices are made by the device manufacturers. However, regardless of these architectural choices, the execution and all data – persistent and runtime – of a biometric verification system must be protected by enforcing the same criteria as those of the TEE for Trusted Storage.

Figure 3 Architecture Overview -- Biometrics



The hardware components required for providing biometric functionality on a TEE-enabled device are:

- Capture Device(s): the sensors that are in charge of capturing the biometric characteristics from the users[1]. Depending on the used sensor technology, other processes such as liveness detection (to detect and prevent biometric spoof attacks) or image enhancement could be additionally performed by these devices. Any capture device shall be wired and integral to the TEE-enabled device. The capture function itself lies outside the TOE boundary, but at the time of usage, the system has exclusive access to the biometric data. Any other logical functionality pertaining to a biometric system that might be offered by a sensor/capture device lies inside the TOE. The capture device should be started by the TEE. In all cases, the authenticity and integrity of the capture device code shall be ensured. The capture device code may be initialized by the TEE or stored in ROM memory (not loaded by the TEE).

[1] For instance, for fingerprint recognition, various types of solutions exist, such as optical fingerprint readers, silicon fingerprint readers, ultrasonic fingerprint readers.

The drivers for such capture devices shall be among the Trusted OS Components.

Any usage of a capture device is made through an API within the TOE and no access to the captured raw data is given.

- (Optional) Trusted User Interface(s): Typically, devices include a screen and a display controller peripheral. Additionally, a trusted input device (e.g. keyboard, joystick, etc., see [TEE TUI API] for details) should be included for biometric systems that define an administrator role or provide notification function to the user.
- (Optional) Sensor Device for Spoofing Detection: If the main capture device does not have liveness detection capabilities and a software solution for liveness detection is not provided, these can be offered by a separate, dedicated sensor device. This is beyond the scope of this document.

The software components required for providing biometric functionality on a TEE-enabled device are:
- the biometric device drivers;
- the enrolment and authentication functions;
- and the algorithms dedicated to biometric functionality.

Some architectures may rely on:

- Secure Element(s), e.g. for verification ("Match on Card") or for secure storage of all the biometric information transmitted from the capture device and used for creating biometric references;
- Trusted Application(s), e.g. for performing the biometric enrolment and verification functions.

All drivers of biometric devices should be included in the TEE. Algorithms dedicated to biometric functionality can be TEE or TA code depending on the implementation. In both cases, they are inside the TOE boundary.

Biometric references should always be stored in a secure manner, ensuring integrity and confidentiality no matter what type of (non-volatile) storage is used (TEE or SE storage). All biometric information used for biometric reference creation and verification should be transmitted in a secure way (through protected channels ensuring integrity and confidentiality), both in integrated and distributed architectures. No biometric samples and probes should be kept between two consecutive biometric processes. These, i.e. biometric samples and probes, should either be stored in volatile memory or consistently deleted between consecutive capture operations.

2.3 Usage and Major Security Features of the TOE

2.3.1 TOE Security Functionality

The purpose of the TEE biometric verification system is to allow applications to perform biometric user authentication, while ensuring integrity, confidentiality/privacy and device binding of biometric data at rest and at runtime.

The TOE functionality in the end-user phase (cf. section 2.2.1) which is in the scope of the evaluation consists of all the operations on biometric data, including: capture, enrolment, association, verification, dissociation, and global wipe of the biometric system data.

The TOE's interfaces are the Software External Interfaces and the Hardware External Interfaces, introduced in sections 2.2.1 and 2.2.2, respectively.

The following functionality is out of the scope of the TOE:

- PAD (Presentation Attack Detection) system;
- Quality system, e.g. leading to acceptable FAR (False Acceptance Rate).

Application Note:

Security Targets (STs) conformant to this PP-Module shall complete the descriptions of the security functionality with the characteristics of the actual TOE and shall provide the complete set of operations on biometric data, which may include other operations such as deletion of biometric references and administrative commands. If the TOE provides “factory reset” functionality, its consequences on the biometric data must be explicitly described.

2.3.2 TOE Usage

The TOE usage requires confirming the physical presence and acceptance of the authorized users. The main use cases for such user interactions are related to financial services, such as bill payment, money transfer, document signature validation, access control to corporate data assets, etc. In the past, verification of the users of such services has often been performed through PIN or password entry.

2.4 Available Non-TOE Hardware/Software/Firmware

The TOE may require some non-TOE Hardware, Software or Firmware. However, the TOE must be realized in a way such that TOE security functionalities do not rely on proper behavior of non-TOE hardware, software or firmware.

Application Note:

Security Targets conformant to this PP-Module shall complete the descriptions of the available non-TOE hardware/software/firmware with the list of non-TOE resources used by the TOE.

2.5 Reference Device Life Cycle

The generic life cycle defined in the [TEE PP] applies to the TOE as defined in this PP-Module.

Application Note: Security Targets shall describe the actual TOE life cycle, identify the actors and development/manufacturing sites involved; they shall identify the actual integration points of the components (Trusted OS, root of trust, TAs, biometric system’s hardware and software components) into the device, as well as the actual delivery point of the TOE, and precise the process for setting the root of trust of the TEE storage services and the phase in which it occurs.

Security Targets shall also identify the TOE and the components that are delivered with the TOE if any, e.g. the standard OS, pre-installed Trusted Applications or Client Applications. If the TOE provides TA management functionality (i.e. installation of TAs in phase 6 or in general after the delivery point), which is not in the scope of this Protection Profile, it must be described in the ST as well.

3 Conformance Claims

3.1 Conformance Claim to CC

This PP-Module is CC Part 2 [CC2] conformant.

3.2 Conformance Claim to a Package

This PP-Module inherits the assurance level EAL2+ from [TEE PP], which consists of predefined EAL 2 augmented with AVA_TEE.2.

3.3 Conformance Claim to the PP-Module

This PP-Module inherits from [TEE PP] the strict conformance as defined in [CC1] for all Security Targets and Protection Profiles claiming conformance to it.

3.4 Consistency Rationale wrt [TEE PP]

The consistency rationale is given in sections 4.1.3, 4.6, 5.4 and 6.2.

4 Security Problem Definition

This chapter introduces the security problem addressed by the TEE biometric system and its operational environment.

4.1 Assets

The assets can be categorized into primary and secondary assets. Depending on the implementation, primary and secondary assets related to biometric functionality can be either TEE or TA assets (data or code). Furthermore, if the implementation relies on an SE, certain assets related to biometric data can be stored outside the TEE. Independently of the implementation, the TEE/TA assets are in the scope of the evaluation and their security properties should be ensured.

As a general remark, we would like to remind that for **runtime** data, the integrity and consistency properties are equivalent. Some properties are inherited from [TEE PP]. For **TEE runtime data**, these imply: consistency and confidentiality. For **TEE persistent data**, these imply: authenticity, consistency, confidentiality, and device-binding. For **TA code**, these imply authenticity and consistency. For **TA data**, these imply authenticity, consistency, confidentiality, device-binding, and atomicity.

However, some of the runtime data must additionally be *replay-protected*. Such data includes the biometric probes, the verification result. Integrity excludes the possibility of data injection at the level of the TEE memory, which is what replay protection is understood to be. This property is a core TEE property included in [TEE PP].

Application Note:

Terms between brackets come from [TEE BIO API].

4.1.1 Primary Assets

The primary assets refer to the critical information or functionality that can be accessed only by authorized users after a successful biometric verification. In addition, they include the biometric data of end users which is used for authentication.

Primary assets related to the TAs are addressed in the [TEE PP] as **TA code** and **TA data and keys**.

The primary assets related to biometric data are the following:

Biometric Samples (Live Image). Biometric samples represent **runtime** data. They are captured by the capture subsystem and used by the signal processing subsystem to create biometric references and biometric probes.

Properties (in the TOE): consistency (integrity), confidentiality (for privacy).

Application Note:

The communication from sensor to TEE may be in PCB but not physically protected. The TEE will protect this asset against SW attacks.

Biometric References (Stored Templates). Biometric references are created during the enrolment process and they represent **persistent** data. They are used during the biometric verification and association processes. Biometric references are stored together with their unique identifier.

Properties: integrity, rollback protection, authenticity, confidentiality, device-binding.

Application Note:

Integrity requires the Time & Rollback PP-Module.

Biometric Probes (Live Template). Biometric probes are created and used during the biometric verification process and they represent **runtime** data. They are compared against the biometric references.

Properties: consistency (integrity), confidentiality.

For a full TEE implementation, all primary assets related to biometric data are TEE data.

For a TEE/TA implementation, all primary assets related to biometric data may be either TEE or TA data.

For an implementation relying on a Secure Element, biometric references may be SE data.

4.1.2 Secondary Assets

The secondary assets refer to data that is created, generated or manipulated by the TOE itself. Depending on the implementation they represent particular instances of TEE assets or TA assets. They include the following:

Security-relevant TOE configuration data and settings. This type of data is **persistent** and includes **the threshold value** and **the comparison policy** used for deciding during the verification process if a biometric reference and a biometric probe match.

Properties: integrity, authenticity.

Biometric comparison score. This type of data represents **runtime** data. The biometric comparison score is computed by the comparison subsystem during the verification process. The computation is based on a stored biometric reference and a supplied biometric probe.

Properties: consistency (integrity), confidentiality (the comparison score should never be exported).

Biometric verification result. This type of data represents **runtime** data. The biometric verification result (a binary answer, i.e. match/no match) is returned by the comparison decision subsystem based on the biometric comparison score it receives from the comparison subsystem.

Properties: consistency (integrity) (confidentiality and replay protection inherited from the TEE).

Association Store. This constitutes **persistent** data and represents the generic name for the storage of associations. It is manipulated during the association and dissociation processes.

Property: integrity, rollback protection, device-binding, confidentiality.

Biometric system code. The code associated to the biometric system. To a minimum, this includes the drivers of the biometric devices and the algorithms related to the biometric functionality, i.e. the feature extraction code, the biometric verification code, etc. Such data is **persistent** and lies inside the TOE boundary.

Properties: integrity, consistency, authenticity, rollback protection.

Application Note:

In a mixed TEE/TA biometric system implementation, this asset stands as well for the code of any Trusted Application controlling/operating the biometric enrolment and verification processes. The code handling feature extraction can be included at this level. Rollback protection is required in all cases. For a TEE implementation, the rollback protection is inherited. For a TA implementation, rollback protection of TA code must be ensured. Authenticity and consistency of the code for a TA implementation must be ensured as well.

Depending on the implementation, this asset extends **TEE firmware** and / or **TA code** assets as defined in [TEE PP].

Biometric system runtime data. Such data may include handles to events or to biometric runtime data.

Properties: consistency, confidentiality.

Application Note:

In [TEE BIO API], handles to biometric events or handles to biometric probes are instances of biometric system runtime data. Such data can be manipulated to alter the normal behaviour of the biometric verification system.

(optional) Biometric system components identification/authentication data. This type of data is used in distributed architectures. It depends on the implementation.

Properties: integrity, confidentiality, authenticity.

Application Note:

This asset represents **persistent** (e.g. master keys) and **runtime** data (e.g. challenges, session keys). Moreover, such data resides both in Trusted OS and in the components that are distributed across the architecture.

4.1.3 Correspondence to [TEE PP] Assets

For a full TEE implementation, all secondary assets related to biometric functionality are TEE assets (data or code).

For a TEE/TA implementation, all persistent secondary data related to biometric functionality may be either TEE or TA data.

For an implementation relying on a Secure Element, some assets may be SE data. Such kind of implementation is not further discussed in this document.

Table 4-1 shows the relationship between TEE assets as defined in the [TEE PP] and Time & Rollback PP-Module and assets of TEE biometric system defined in this PP-Module. It is applicable to a full TEE implementation. The TEE is considered enriched with all the code and data necessary to handle the biometric authentication of a user.

Table 4-1 Correspondence BS assets - TEE assets

BS Assets \ TEE Assets	TEE identification	TEE initialisation code & data	TEE storage root of trust	RNG	TA code_module	TA data and keys_module	TA instance time	TA persistent time	TEE runtime data	TEE data_module	TEE firmware	TEE rollback detection data
Biometric Samples (Live Image)									X			
Biometric References (Stored Templates)										X		
Biometric Probes (Live Template)									X			
Biometric reference database										X		
Security-relevant TOE configuration data and settings										X		
Biometric comparison score and biometric verification result									X			
Association Store										X		
Biometric system code											X	
Biometric system runtime data									X			

4.2 Users

Legitimate users of the Biometric System are **End Users** who want access to the services of the biometric system and **Enrolled End Users** who have access rights managed by the Biometric System.

Legitimate users interact with the TOE by means of installed **Trusted Applications**, which are considered users of the TOE as well.

Attackers i.e. any individual or application/malware that is attempting to subvert the functionality of the biometric system in order to gain unauthorized access to the assets protected by the TOE, are illegitimate users of the TOE.

4.3 Threats

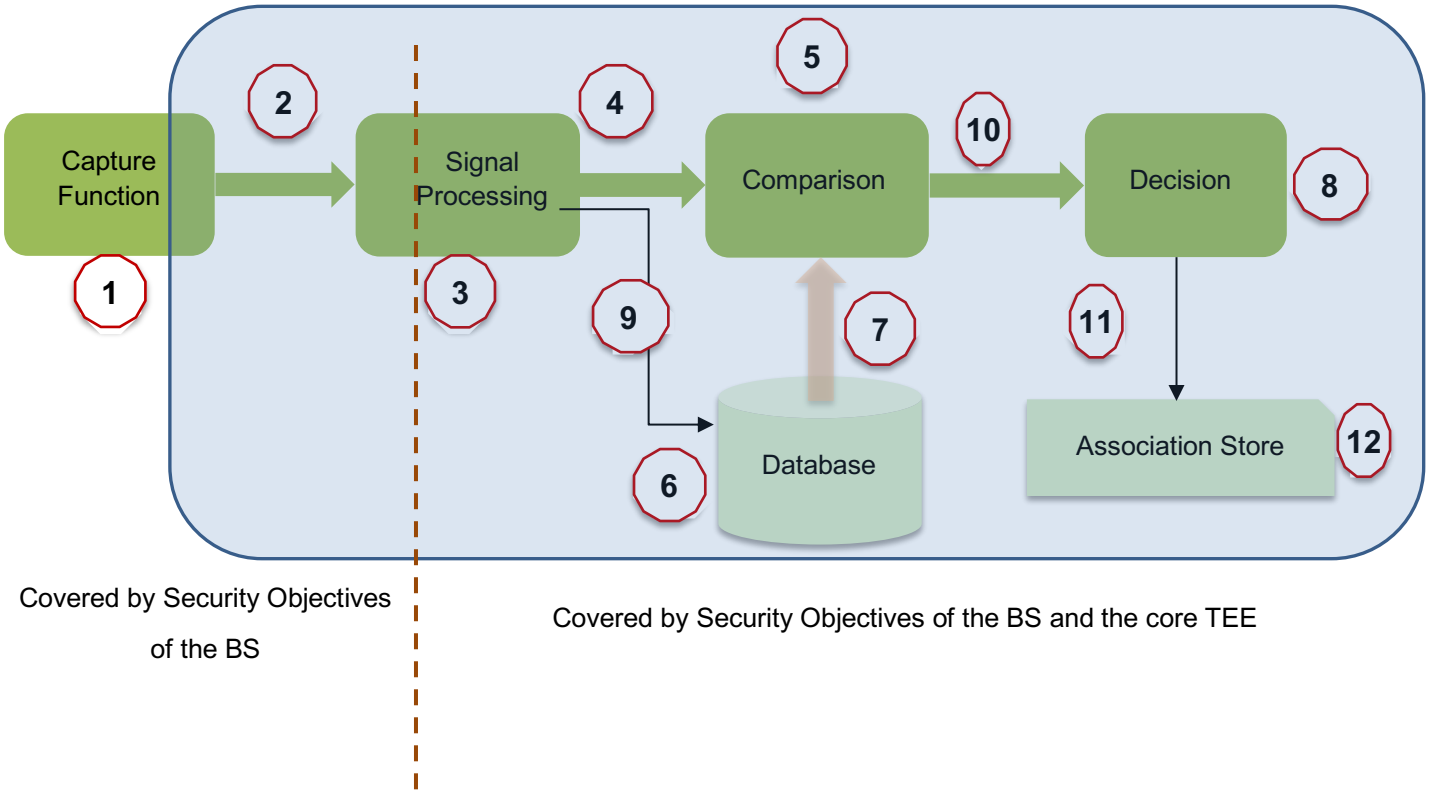
The same threat model and attackers' profiles as included in the [TEE PP] apply. The actual attack surface of the biometric system depends on software and hardware implementation choices.

Application Note:
The following two remarks apply when interpreting / understanding the threat model which introduces a distinction between the sensitivity of biometric samples (i.e. raw capture) and all other forms of biometric data (i.e. probes and references):

a) If the biometric sample is processed within the sensor itself, then protection against attacks of any nature between the sensor and the TEE is required.
b) If the biometric sample is not processed within the sensor itself, then only prevention of software attacks such as eavesdropping/injection of captures between the sensor and the TEE is targeted.

In Figure 5 the main subsystems and components of a biometric system are depicted and the different main points at which attacks on such systems can be conducted are shown[2].

Figure 4 Attack Points -- Overview



Attacks can further be grouped into direct and indirect attacks. Attacks at point 1, i.e. on the capture subsystem and its capture function, are the only direct attacks. They require submitting a fake biometric artefact to the sensor or subverting/replacing the hardware or capture function, but otherwise they require no specific knowledge about the biometric system or its inner working. These types of attacks are external to the TOE and will be presented in further detail in the following section (Attacks external to the TOE). Excepting attacks at point 8 that target the modification of the match/no match answer of the biometric system, all other types of attack (2-7 and 7-12) are feasible only if some knowledge about the biometric system and/or some access privileges are available to the attacker.

Biometric systems are vulnerable to Denial of Service (DoS) attacks. These consist in overwhelming the biometric system with fake requests to the point that all computational resources are engaged and cannot handle valid requests anymore. This type of attack is external to the TOE.

[2] Ratha et al. [RCB] identified the first 8 attack points and described attacks according to the compromised subsystem/component. The last 4 points shown above are specific to biometric systems as depicted in Sec. 2.2.1. [RCB] N. K. Ratha, J. H. Connell, and R. M. Bolle. An analysis of minutiae matching strength. In Audio- and Video-Based Biometric Person Authentication, pages 223–228, 2001.

Attacks at points 1 and 2 are specific to the biometric system and they require specific security objectives. Several of the attacks at points 3-12 are addressed by the TEE and will be covered by security objectives of the TEE as defined in [TEE PP].

4.3.1 Attacks at point 1

The only attack at this point that is internal to the TOE is an attack on the access to the capture function.

T.SHARED_CAPTURE_ACCESS

An attacker intercepts and/or modifies biometric samples, taking advantage of a shared access to the capture function and thus to the captured biometric samples. The objectives of such an attack can be manifold, for instance:

- To extract genuine biometric samples for subsequent replay;
- To alter genuine biometric samples before they are transmitted to the TOE in order to deny access to authorized users.

This attack will be covered by the following objectives:

- O.CAPTURE,
- O.PREVENT_RESIDUAL_BIO_SAMPLES,
- O.PROTECTED_BIO_SAMPLES_COMMUNICATION.

4.3.2 Attacks at point 2

This type of attack targets the communication channel between the sensor and the signal processing or feature extraction subsystem. Depending on the type of hardware used, this may not always be an option as the sensor and the signal processing/feature extraction module are sometimes combined. At this level, an attacker can potentially intercept raw biometric data sent by the sensor. This can subsequently be used for replay attacks or for creating fake biometric images. Alternatively, an attacker can send fake or malicious data to the signal processing subsystem for performing a hill climbing attack. Three different threats are identified at this level.

T.EXTRACT_BIO_SAMPLE

An attacker intercepts and extracts the biometric sample (live image) of a genuine user. The interception is done when the sensor acquires a raw biometric data from a genuine user and sends it to the signal processing subsystem for pre-processing through a communication channel. This attack may be the preliminary step for an impersonation or a replay attack.

Assets threatened indirectly: biometric samples (sent through the communication channel between the sensor and the signal processing unit).

This attack will be covered by the following objectives:

- O.PROTECTED_BIO_SAMPLES_COMMUNICATION.

T.REPLAY_BIO_SAMPLE

This attack consists of two steps. First, an attacker intercepts and steals the biometric sample (live image). The interception is done when the sensor acquires a raw biometric data from a genuine user and then sends it to the signal processing subsystem for pre-processing through a communication channel. As a second step, the attacker injects or replays the stolen biometric sample to the biometric signal processing subsystem. The goal of this attack is to bypass the capture subsystem and to successfully pass the biometric verification process (locally or remotely) thus acquiring access to the primary assets/functionality protected by the TOE.

Assets threatened indirectly: biometric samples (sent through the communication channel between the sensor and the signal processing unit).

This attack will be covered by the following objectives:

- O.PROTECTED_BIO_SAMPLES_COMMUNICATION,
- O.PREVENT_RESIDUAL_BIO_SAMPLES.

T.HILL_CLIMBING_SAMPLE

An attacker repeatedly injects fake biometric samples on the communication channel between the sensor and the signal processing subsystem. For each injected biometric sample, a change or variation is introduced and the effect of this change on the comparison score is observed. The introduced change is kept if the observed comparison score has increased; otherwise, the change is discarded. The procedure is repeated until the attacker obtains a fake biometric probe that passes verification.

The attacker's goal is to iteratively construct a fake biometric probe that will lead to a successful biometric verification. As this type of attack requires observing the comparison score (attack at point 10), this needs to be available or intercepted. However, unlike hill-climbing attacks using biometric probes, at this point the attacker does not need to have information about the used biometric probe format.

Assets threatened indirectly: comparison score and biometric samples (sent through the communication channel between the sensor and the signal processing unit).

This attack will be covered by the following objectives:

- O.PROTECTED_BIO_SAMPLES_COMMUNICATION,
- O.HIDE_COMPARISON_SCORE.

4.3.3 Attacks at point 3

At point 3, attacks consist in manipulating or overriding the feature extraction and biometric template creation performed by the signal processing subsystem. Such attacks usually target the software or the firmware of the biometric system. One threat is identified at this level.

T.OVERRIDE_FEATURE_EXTRACTION

An attacker interferes with/bypasses the feature extraction unit to manipulate or provide false feature values for further processing. A biometric probe may be generated with the characteristics preselected by the attacker.

Assets threatened directly: feature extraction unit (part of the biometric system code), biometric probes.

Application Note: Alternatively, this attack can be used to disable the biometric system and to create a DoS attack, which is out of scope.

This attack will be covered by the following objectives:

- O.BS_INITIALIZATION, which is itself covered by O.INITIALIZATION from [TEE PP],

- O.OPERATION from [TEE PP].

4.3.4 Attacks at point 4

Attacks at this point targets the communication channel between the signal processing subsystem and the comparison subsystem. They target the biometric probe. Two threats are identified at this level. Depending on the system's architecture, attacks at this point may not always be an option.

T.REPLAY_BIO_PROBE

This attack consists of two steps. First, an attacker intercepts the communication channel between the signal processing subsystem and the verification subsystem in order to steal the biometric probe of a genuine, enrolled user. As a second step, this biometric probe can be replayed to the verification subsystem later on. The ultimate goal of the attacker is to be successfully verified by the biometric verification system, thus acquiring access to the primary assets protected by the TOE.

Assets threatened directly: biometric probes.

This attack will be covered by the following objectives:

- O.PROTECTED_DATA_TRANSFER, or
- O.RUNTIME_INTEGRITY and O.RUNTIME_CONFIDENTIALITY from [TEE PP].

T.INJECT_BIO_PROBE

An attacker bypasses the biometric capture and signal processing subsystem(s) and injects an external (malicious) biometric probe. The attacker's aim is to successfully pass the subsequent biometric verification process, and therefore, to be granted access to the primary assets protected by the TOE.

The injected biometric probe can be

- forged;
- generated outside the TOE;
- previously extracted/intercepted from the TOE.

Injecting malicious biometric probes can also be done at this level for brute-forcing the biometric system. This type of attack may require knowledge about the biometric probe format.

Assets threatened directly: biometric probes.

This attack will be covered by the following objectives:

- O.PROTECTED_DATA_TRANSFER, or
- O.RUNTIME_INTEGRITY from [TEE PP].

T.EXTRACT_BIO_PROBE

An attacker extracts a biometric probe outside the TOE. This can be done by intercepting the communication channel between the signal processing subsystem and the comparison subsystem. This attack can have multiple aims:

- subsequent use for replay attacks or impersonation attacks, i.e. masquerading as a genuine, enrolled user;
- extract information about the compared biometric features.

Assets threatened directly: biometric probes.

This attack will be covered by the following objectives:

- O.PROTECTED_DATA_TRANSFER, or
- O.RUNTIME_CONFIDENTIALITY from [TEE PP].

T.HILL_CLIMBING_PROBE

An attacker repeatedly injects fake biometric probes on the communication channel between the signal processing subsystem and the comparison subsystem. For each injected biometric probe, a change or variation is introduced and the effect of this change on the comparison score is observed. The introduced change is kept if the observed comparison score has increased; otherwise, the change is discarded. The procedure is repeated until the attacker obtains a fake biometric probe that passes verification. The attacker's goal is to iteratively construct a fake biometric probe that will lead to a successful biometric verification. As this type of attack requires observing the comparison score, this needs to be available or intercepted. Furthermore, the attacker has to have information about the used biometric probe format.

Assets threatened indirectly: the comparison score and the biometric probes (sent through a communication channel between the signal processing subsystem and the comparison subsystem).

This attack will be covered by the following objectives:

- O.PROTECTED_DATA_TRANSFER,
- O.HIDE_COMPARISON_SCORE,
- O.RUNTIME_INTEGRITY and O.RUNTIME_CONFIDENTIALITY from [TEE PP].

4.3.5 Attacks at point 5

Attacks at this point target the comparison unit and they can be attacks on hardware, software, firmware or the configuration and settings. The main threats identified consist in modifying the comparison threshold or the matching algorithm in order to produce artificially low or high scores.

T.MODIFY_CONFIG_DATA

An attacker modifies security-relevant TOE configuration data and settings such as the comparison policy (high score/low score) or the threshold value used for the comparison in order to bypass the normal verification process. The ultimate goal of the attack is to disrupt the normal verification process by changing the settings to produce a successful match and therefore to gain access to the primary assets protected by the TOE.

An attacker could have multiple immediate goals. One of them consists in changing the comparison threshold in order to facilitate spoofing attacks. Genuine users would not notice such a change because the biometric verification system would continue to grant them access to the primary assets.

Assets threatened directly: configuration data and security-related settings, i.e. comparison policy, threshold values.

This attack will be covered by the following objectives:

- O.TEE_DATA_PROTECTION from [TEE PP].

T.BYPASS_VERIFICATION

An attacker bypasses the biometric verification system and forces the comparison subsystem to generate an artificially high or low comparison score as specified by himself, regardless of the values obtained from the input biometric reference and probe. The ultimate goal of the attacker is to be granted access to the primary assets protected by the TOE.

Assets threatened directly: biometric verification code (part of the biometric system code).

This attack will be covered by the following objectives:

- O.BS_INITIALIZATION, which is itself covered by O.INITIALIZATION from [TEE PP],
- O.OPERATION from [TEE PP].

T.FAULT_INJECTION

An attacker injects a fault at the comparison subsystem level. This attack can have multiple aims:

- corrupt the computation of the comparison score;
- bypass the computation of the comparison score;
- extract security-relevant information;
- modify or alter the comparison score.

Assets threatened directly: comparison score.

This attack will be covered by the following objectives:

- O.BS_INITIALIZATION, which is itself covered by O.INITIALIZATION from [TEE PP],
- O.OPERATION, O.RUNTIME_INTEGRITY, O.RUNTIME_CONFIDENTIALITY, and O.INITIALIZATION from [TEE PP].

4.3.6 Attacks at point 6

Attacks at this point targets the system's database. Depending on how the biometric references are stored, the system's database can be a main target for attacks.

T.CORRUPT_DATABASE

Various attacks are possible at this point such as the injection of a new biometric reference or the modification or removal of an existing one.

Assets threatened directly: list of biometric references in the database, biometric references.

Depending on the implementation, this attack will be covered by the following objectives:

- O.TEE_DATA_PROTECTION or O.TRUSTED_STORAGE from [TEE PP].

T.ROLLBACK_DATABASE

An attacker rollbacks the biometric references database to a genuine previous version.

Assets threatened directly: biometric references database.

Depending on the implementation, this attack will be covered by the following objectives:

- O.ROLLBACK_PROTECTION from [TEE PP].

T.CLONE_DATABASE

An attacker clones the biometric references database of a given device and uses it on another device.

Assets threatened directly: biometric references database.

Depending on the implementation, this attack will be covered by the following objectives:

- O.INITIALIZATION, O.TEE_DATA_PROTECTION or O.TRUSTED_STORAGE from [TEE PP].

4.3.7 Attacks at point 7

Attacks at this point target the communication channel between the system's database and the comparison unit. Various attacks are possible at this level, ranging from stealing the biometric reference of a genuine user, to corrupting or modifying the contents of the transmitted biometric reference.

T.EXTRACT_BIO_REFERENCE

An attacker extracts a biometric reference outside the TOE. This can be done by intercepting the communication channel between the system's database and comparison subsystem and by sniffing the traffic. This attack can have multiple aims:

- acquire information about the biometric system and the compared biometric features;
- acquire biometric reference for subsequently injecting it as a biometric probe;
- acquire necessary information for a subsequent impersonation attack;
- acquire biometric reference for subsequent external modification and reinjection into the database.

Assets threatened directly: biometric references.

This attack will be covered by the following objectives:

- O.PROTECTED_DATA_TRANSFER,
- O.RUNTIME_CONFIDENTIALITY from [TEE PP].

T.INJECT_BIO_REFERENCE

An attacker injects an external biometric reference on the channel between the system's database and the comparison unit. The immediate goal of this attack is to successfully verify a malicious user, ultimately granting him unauthorized access to the primary assets protected by the TOE.

This type of attack assumes that the attacker has knowledge about the TOE and special equipment at his disposal, such as sensors / capture subsystems allowing him to generate new biometric references or to modify existing ones.

Assets threatened directly: biometric references.

This attack will be covered by the following objectives:

- O.PROTECTED_DATA_TRANSFER,
- O.RUNTIME_INTEGRITY from [TEE PP].

T.MODIFY_BIO_REFERENCE

An attacker modifies a biometric reference created during the enrolment process and used by the TOE for the biometric verification process. This can be done by intercepting the communication channel between the system's database and the comparison subsystem during the verification process of a genuine user. Alternatively, this can also be done at point 9, by intercepting the communication channel between the signal processing subsystem and the system's database during the enrolment process of a genuine user.

The immediate goal of this attack is to obtain a forged biometric reference that can be used for a successful verification using biometric probes that are not obtained from a genuine user. By compromising the integrity of such persistent data, the attacker attempts to gain unauthorized access to the primary assets protected by the TOE.

Assets threatened directly: biometric references (integrity, authenticity).

This type of attack assumes that the attacker has knowledge about the TOE and special equipment at his disposal, such as sensors / capture subsystems allowing him to generate new biometric references or to modify existing ones.

Assets threatened directly: biometric references.

This attack will be covered by the following objectives:

- O.PROTECTED_DATA_TRANSFER,
- O.RUNTIME_INTEGRITY from [TEE PP].

4.3.8 Attacks at point 8

Attacks at this point target the decision unit and aim to override the match/no-match result.

T.TAMPER_VERIFICATION_RESULTS

An attacker overwrites the original answer of the decision subsystem and substitutes it with a match/no-match. The match/no-match answer is sent through a communication channel from the comparison decision subsystem to a Trusted Application. This is intercepted and overwritten. The ultimate goal of the attacker is either to gain access to the primary assets protected by the TOE or to force the denial of access to these assets for a genuine user.

A biometric verification system is completely defeated if the system's final decision can be overwritten by an attacker.

Assets threatened directly: biometric verification result.

This attack will be covered by the following objectives:

- O.PROTECTED_DATA_TRANSFER,
- O.RUNTIME_INTEGRITY from [TEE PP].

4.3.9 Attacks at point 9

Attacks at this point target the communication channel between the signal processing subsystem and the system's database that is used during the enrolment process of a genuine user. Various attacks are possible at this level, similar to attacks at point 7; ranging from stealing the biometric reference of a genuine user, to corrupting or modifying the contents of the transmitted biometric reference. However, attacks at this level can have potential longer lasting effects, as an attacker could inject a persistent malicious biometric reference into the system's database.

T.EXTRACT_BIO_REFERENCE_ENROLL

An attacker extracts a biometric reference outside the TOE. This can be done by intercepting the communication channel between the system's database and the signal processing subsystem and by sniffing the traffic. This attack can have multiple aims:

- acquire information about the biometric system and the compared biometric features;

- acquire biometric reference for subsequently injecting it as a biometric probe;
- acquire necessary information for a subsequent impersonation attack;
- acquire biometric reference for subsequent external modification and reinjection into the database.

Assets threatened directly: biometric references.

This attack will be covered by the following objectives:

- O.PROTECTED_DATA_TRANSFER,
- O.RUNTIME_CONFIDENTIALITY from [TEE PP].

T.INJECT_BIO_REFERENCE_ENROLL

An attacker injects an external biometric reference on the channel between the system's database and the signal processing unit. The immediate goal of this attack is to successfully enroll a malicious user, instead of the genuine one, thus bypassing the capture and signal processing subsystems.

This type of attack assumes that the attacker has knowledge about the TOE and special equipment at his disposal, such as sensors / capture subsystems allowing him to generate new biometric references or to modify existing ones.

Assets threatened directly: biometric references.

This attack will be covered by the following objectives:

- O.PROTECTED_DATA_TRANSFER,
- O.RUNTIME_INTEGRITY from [TEE PP].

T.MODIFY_BIO_REFERENCE_ENROLL

An attacker modifies a biometric reference created during the enrolment process and used by the TOE for the biometric verification process. This can be done by intercepting the communication channel between the signal processing subsystem and the system's database during the enrolment process of a genuine user.

The immediate goal of this attack is to obtain a forged biometric reference that can be used for a successful enrolment using a biometric reference that is not obtained from a genuine user. By compromising the integrity of such persistent data, the attacker attempts to gain unauthorized access to the primary assets protected by the TOE.

Assets threatened directly: biometric references.

This type of attack assumes that the attacker has knowledge about the TOE and special equipment at his disposal, such as sensors / capture subsystems allowing him to generate new biometric references or to modify existing ones.

This attack will be covered by the following objectives:

- O.PROTECTED_DATA_TRANSFER,
- O.RUNTIME_INTEGRITY from [TEE PP].

4.3.10 Attacks at point 10

Attacks at this point target the comparison score sent between the comparison and the decision subsystems. Intercepting and extracting the comparison score is a necessary step for hill climbing attacks. Modifications to the comparison score may ultimately lead to false verification/authentication.

T.EXTRACT_COMPARISON_SCORE

An attacker may try to observe and extract the comparison score by intercepting data sent through the communication channel between the comparison and the decision subsystems. This attack is a preliminary step for more advanced attacks, such as hill climbing attacks.

Assets threatened directly: comparison score.

This attack will be covered by the following objectives:

- O.PROTECTED_DATA_TRANSFER,
- O.HIDE_COMPARISON_SCORE,
- O.RUNTIME_CONFIDENTIALITY from [TEE PP].

T.MODIFY_COMPARISON_SCORE

An attacker may try to modify the comparison score by intercepting and altering data sent through the communication channel between the comparison and the decision subsystems. The ultimate goal of the attacker is to be falsely verified and thus to be granted access to the primary assets protected by the TOE.

Assets threatened directly: comparison score.

This attack will be covered by the following objectives:

- O.PROTECTED_DATA_TRANSFER,
- O.RUNTIME_INTEGRITY from [TEE PP].

4.3.11 Attacks at point 11

Attacks at this level target the extraction or the overwriting of the data needed for the association between a biometric reference and a Trusted Application. This is done by intercepting and, in case of overwriting, by altering data transmitted over the communication channel between the decision subsystem and the association store.

T.EXTRACT_ASSOCIATION

An attacker could intercept the communication channel between the decision subsystem and the association store with the goal of extracting information pertaining to an association, i.e. the TA identifier, the unique identifier of a biometric reference, or both. This is a leakage/extraction attack on associations. Such an attack can have multiple aims:

- acquiring preliminary, necessary information for other attacks, including direct attacks;
- acquiring specific information regarding an enrolled user and the user's existing authorisations.

Assets threatened: associations.

This attack will be covered by the following objectives:

- O.PROTECTED_DATA_TRANSFER,
- O.RUNTIME_CONFIDENTIALITY from [TEE PP].

T. OVERWRITE_ASSOC_ID

An attacker could intercept the communication channel between the decision subsystem and the association store with the goal of overwriting either the identifier of a Trusted Application or the unique identifier of a biometric reference used for associating a genuine user to a Trusted Application.

The aim of such an attack can be either acquiring more access rights and privileges by overwriting the identifier of the Trusted Application with the identifier of another, more restrictive Trusted Application. Another aim of such an attack could be to fraudulently associate an enrolled user to an additional Trusted Application.

Assets threatened directly: Trusted Applications identifiers, biometric reference identifiers.

This attack will be covered by the following objectives:

- O.PROTECTED_DATA_TRANSFER,
- O.RUNTIME_INTEGRITY from [TEE PP].

4.3.12 Attacks at point 12

Attacks at this point target the system's association store. New associations could be injected or existing ones could be modified or removed.

T.MODIFY_ASSOCIATION_STORE

An attacker can modify existing associations in the store in order to link an enrolled user to a different Trusted Application than the one he was originally associated to. Alternatively, by modifying the unique identifier to a biometric reference, a user different than the one originally associated to a Trusted Application, could fraudulently be associated to the Trusted Application.

An attacker could add new associations to the store, linking an enrolled user to Trusted Applications to which he was not associated previously, and thus conferring him more access rights or privileges.

By removing existing associations from the store, access rights or privileges of a genuine user can be revoked.

Assets threatened directly: Association store.

Depending on the implementation, this attack will be covered by the following objectives:

- O.TEE_DATA_PROTECTION or O.TRUSTED_STORAGE from [TEE PP].

T.ROLLBACK_ASSOCIATION

An attacker rollbacks the association store to a genuine previous version.

Assets threatened directly: Association Store.

Depending on the implementation, this attack will be covered by the following objectives:

- O.ROLLBACK_PROTECTION from [TEE PP].

T.CLONE_ASSOCIATION

An attacker clones the association store of a given device and uses it on another device.

Assets threatened directly: Association store.

Depending on the implementation, this attack will be covered by the following objectives:

- O.INITIALIZATION and O.TEE_DATA_PROTECTION or O.TRUSTED_STORAGE from [TEE PP].

4.3.13 Other Attacks

T.CORRUPT_RUNTIME_EVENT

An attacker corrupts runtime data, such as a handle to the sensor meant to capture the biometric sample. The attacker's goal is to successfully manage to get a more permissive sensor to do the biometric sample capture.

Assets threatened directly: TOE runtime data.

Application Note: In a GlobalPlatform compliant implementation, this threat stands, for instance, for overwriting the *EventSourceHandle* to get a more permissive sensor to do a verification.

This attack will be covered by the following objectives:

- O.RUNTIME_INTEGRITY from [TEE PP].

T.CORRUPT_RUNTIME_DATA

An attacker corrupts runtime data, such as a handle to a biometric probe or reference provided to the Trusted Application upon capture. Such data can be manipulated to alter the system's expected behavior.

Assets threatened directly: TOE runtime data.

This attack will be covered by the following objectives:

- O.RUNTIME_INTEGRITY from [TEE PP].

T.BS_IMPERSONATION

An attacker impersonates a Trusted Application in order to get unauthorized access to biometric runtime data.

Assets threatened directly: biometric samples, biometric probes, biometric system runtime data.

This attack will be covered by the following objectives:

- O.OPERATION, O.CA_TA_IDENTIFICATION, and O.RUNTIME_INTEGRITY from [TEE PP].

T.RESIDUAL

An attacker extracts unprotected residual security-relevant data during a user's verification session or from the cache, for a previous, successfully verified user. The aim of this attack is to get access to the security-relevant settings of the TOE.

This attack covers multiple scenarios:

- The attacker takes advantage of a flaw in the user interface of the TOE and gets access to the memory content, the cache or relevant temporary data;
- The attacker takes advantage of residual information such as residual biometric samples or probes at the level of the capture and signal processing subsystem.

Assets threatened directly: biometric probes, biometric references, security-relevant configuration data and settings.

The attacker has knowledge about the TOE internal functioning in order to detect and exploit vulnerabilities regarding residual data in memory.

This attack will be covered by the following objectives:

- O.RUNTIME_CONFIDENTIALITY from [TEE PP].

T.REPLAY_EXACT_MATCH[3,4]

An attacker replays a stolen biometric reference as a biometric probe.

This attack will be covered by the following objectives:

- OE.SPOOF_DETECTION and O.PROTECTED_BIO_SAMPLES_COMMUNICATION,
- O.TEE_DATA_PROTECTION, O.TRUSTED_STORAGE, or O.RUNTIME_CONFIDENTIALITY from [TEE PP].

T.UNSAFE_STATE

An attacker forces the system into an unsafe state.

This attack will be covered by the following objectives:

- O.BS_INITIALIZATION,
- O.ATOMIC_BIOMETRIC_OPERATIONS,
- O.UNIQUE_BIO_ID,
- O.ENFORCE_BIOMETRIC_FUNCTIONS.

4.3.14 Attacks External to the TOE

The following attacks apply to the capture function which lies outside the TOE. They will be covered by the objectives on the operational environment, which includes the non-TOE components.

T.BRUTE_FORCE

An attacker performs a brute force attack in order to get verified by the TOE. Thus, the ultimate goal of the attacker is to get access to the primary assets protected by the TOE.

Assets threatened directly: primary assets protected with the support of the TOE.

Application Note:

This threat considers two types of attackers and corresponding adverse actions:

- A hostile attacker who uses a large number of biometric characteristics and who attempts to get unauthorized access to the primary assets protected by the TOE. This type of attacker is supposed to have further than public knowledge on biometric verification systems.
- A hostile, but naïve user who tries to get verified a couple of times hoping to succeed. In this case, the attacker does not need specific knowledge about the TOE in order to perform this type of attack.

This type of attacks depends on the quality imposed for the biometric samples. A high acceptance rate of low-quality biometric samples raises the probability of a successful brute force attack. Thus, a high False Acceptance Rate (FAR) leads to a high probability of successful brute force attacks.

[3] An exact match between a biometric reference and a biometric probe is a strong indicator of a replay attack. The comparison performed between the biometric references and probes is statistical. An exact match between the two is highly probable to be obtained only when the genuine biometric reference stored in the system's database has been stolen and is subsequently used/replayed as a biometric probe.

[4] An upper matching threshold for the comparison score could be defined. Any pair of biometric data that displays a comparison score that is equal or greater than the defined matching threshold should be ignored or rejected. Signatures or time-stamping could be used as well.

T.SPOOF

This type of attack is a direct attack performed at point 1 and it targets the capture functionality of the sensor itself. As the T.BRUTE_FORCE attack presented previously, it lies outside the TOE boundary and it is under the treatment of other international working groups. An attacker may produce a fake artifact in order to successfully pass the biometric capture step.

The attacker's aim can be one of the following:

- to impersonate a specific user of the TOE;
- to impersonate any user of the TOE;
- to disguise their own identity.

For performing this type of attack, the attacker may need the support of an enrolled, genuine user of the TOE (e.g. to imitate his biometric characteristics).

Application Note:

Biometric verification/authentication systems in general are vulnerable to this type of attack. The setup costs of the attack are often low, making the production of fake artifacts worthwhile for impostors for commonly used biometric technologies.

A unit specialized in presentation attacks detection (PAD) should be incorporated in the overall biometric verification system.

4.4 Organisational Security Policies

This PP-Module does not define any organisational security policy for implementation by the TOE and/or its operational environment.

4.5 Assumptions

This section states the assumptions that hold on the non-TOE components and the TOE operational environment

A.NO_RESIDUAL_SAMPLES

The capture function does not store residual biometric samples. The biometric samples are deleted between any two consecutive capture operations.

A.TA_DEVELOPMENT_BS

TA developers are assumed to comply with the biometric system development guidelines set by the TEE provider. In particular, TA developers are assumed to consider the following principles:

1. Verification attempt limit: Attackers must be prevented from gaining access to the primary assets protected by the TOE by making repeated biometric verification attempts. The maximum number of unsuccessful verification attempts (i.e. that lead to a non-match) should be limited according to well-defined policy.
2. Information display: The communication with the end-user of the biometric system should be limited to a minimum and adapted to the kind of supported user interface (trusted or untrusted). This applies in particular to the enrolment, association and biometric verification operations which require capture of end-user biometric data.

Application Note:

This assumption complements A.TA_DEVELOPMENT defined in the [TEE PP].

If the device provides a Trusted User Interface for which TAs can get exclusive access, the Security Target may weaken this assumption (item 2) and require a trusted channel between the biometric system and the TUI.

4.6 Correspondence to [TEE PP] SPD

The following table summarizes the correspondence between the threats, assumptions and OSPs identified for the TEE and those identified for the TOE. A full TEE implementation of the biometric system is considered.

Table 4-2: Correspondence BS SPD - TEE SPD

BS SPD / TEE SPD	T.ABUSE_FUNCT	T.CLONE	T.FLASH_DUMP	T.IMPERSONATION	T.ROGUE_CODE_EXECUTION	T.PERTURBATION	T.RAM	T.RNG	T.SPY	T.TEE_FIRMWARE_DOWNGRADE	T.STORAGE_CORRUPTION	T.ROLLBACK	T.TA_PERSISTENT_TIME_ROLLBACK	OSP_INTEGRATION_CONFIGURATION	OSP.SECRETS	A.PROTECTION_AFTER_DELIVERY	A.TA_MANAGEMENT	A.TA_DEVELOPMENT
T.SHARED_CAPTURE_ACCESS																		
T.REPLAY_BIO_SAMPLE																		
T.EXTRACT_BIO_SAMPLE																		
T.HILL_CLIMBING_SAMPLE																		
T.OVERRIDE_FEATURE_EXTRACTION	X			X	X	X												
T.REPLAY_BIO_PROBE					X		X		X									
T.INJECT_BIO_PROBE					X		X		X									
T.EXTRACT_BIO_PROBE							X		X									
T.HILL_CLIMBING_PROBE					X		X		X									
T.MODIFY_CONFIG_DATA					X	X					X							
T.BYPASS_VERIFICATION	X			X	X	X												
T.FAULT_INJECTION						X												
T.CORRUPT_DATABASE											X							
T.ROLLBACK_DATABASE												X						
T.CLONE_DATABASE		X																
T.EXTRACT_BIO_REFERENCE							X		X									
T.INJECT_BIO_REFERENCE					X		X		X									
T.MODIFY_BIO_REFERENCE					X	X	X											
T.TAMPER_VERIFICATION_RESULTS					X	X	X											
T.EXTRACT_BIO_REFERENCE_ENROLL							X		X									
T.INJECT_BIO_REFERENCE_ENROLL					X		X		X									
T.MODIFY_BIO_REFERENCE_ENROLL					X	X	X											
T.EXTRACT_COMPARISON_SCORE							X		X									
T.EXTRACT_ASSOCIATION							X		X									
T.MODIFY_COMPARISON_SCORE					X	X	X											
T.OVERWRITE_ASSOC_ID					X	X	X											

BS SPD / TEE SPD	T.ABUSE_FUNCT	T.CLONE	T.FLASH_DUMP	T.IMPERSONATION	T.ROGUE_CODE_EXECUTION	T.PERTURBATION	T.RAM	T.RNG	T.SPY	T.TEE_FIRMWARE_DOWNGRADE	T.STORAGE_CORRUPTION	T.ROLLBACK	T.TA_PERSISTENT_TIME_ROLLBACK	OSP_INTEGRATION_CONFIGURATION	OSP.SECRETS	A.PROTECTION_AFTER_DELIVERY	A.TA_MANAGEMENT	A.TA_DEVELOPMENT
T.MODIFY_ASSOCIATION_STORE											X							
T.ROLLBACK_ASSOCIATION												X						
T.CLONE_ASSOCIATION		X																
T.CORRUPT_RUNTIME_EVENT					X	X	X											
T.CORRUPT_RUNTIME_DATA					X	X	X											
T.BS_IMPERSONATION				X														
T.RESIDUAL							X		X									
T.REPLAY_EXACT_MATCH							X		X		X							
T.UNSAFE_STATE																		
A.NO_RESIDUAL_SAMPLES																		
A.TA_DEVELOPMENT_BS																		

Attacks at point 1, i.e. direct attacks on the sensor and T.SHARED_CAPTURE_ACCESS, as well as attacks at point 2, i.e. T.EXTRACT_BIO_SAMPLE, T.REPLAY_BIO_SAMPLE and T.HILL_CLIMBING_SAMPLE are specific to biometric systems.

Attacks at points 3 – 12, as well as attacks described in Section 4.3.13, are specific instances of modification, disclosure, impersonation and perturbation attacks considered in the [TEE PP]. The mapping can be organized in 8 different categories:

- Bypass: linked to T.ABUSE_FUNCT, T.IMPERSONATION, T.ROGUE_CODE_EXECUTION and T.PERTURBATION;
- Modify / tamper / Override / overwrite / Corrupt: linked to T.ROGUE_CODE_EXECUTION, T.PERTURBATION, T.RAM, T.STORAGE_CORRUPTION;
- Inject: linked to T.ROGUE_CODE_EXECUTION, T.RAM and T.SPY;
- Extract: liked to T.RAM and T.SPY;
- Rollback: linked to T.ROLLBACK;
- Clone: linked to T.CLONE;
- Impersonation: linked to T.IMPERSONATION;
- Fault injection: linked to T.PERTURBATION;
- There are two special threats: T.HILL_CLIMBING_PROBE linked to T.ROGUE_CODE_EXECUTION, T.RAM and T.SPY and T.RESIDUAL linked to T.RAM and T.SPY.

5 Security Objectives

5.1 Security Objectives for the TOE

O.BS_INITIALIZATION

The TOE shall ensure that the biometric system is started through a secure initialisation process that ensures the integrity of the biometric subsystems initialisation code and data, and the authenticity of the biometric system firmware.

The TOE shall ensure that all the biometric system code and data are bound to the SoC of the device.

Application Note:

This objective is the extension to the biometric system of the objective O.INITIALIZATION defined in the [TEE PP]. It is included here to highlight the fact that the biometric system is indeed integral to the TEE.

Application Note:

The author of a compliant ST shall describe the capture device(s) initialisation process and how the authenticity of the code running in the device is enforced.

O. CAPTURE

The TOE shall ensure that

- the capture of the raw biometric data is made by the expected wired sensor and that
- at the time of the usage, the biometric system has exclusive access to the capture function, and therefore to the captured data, i.e. the Biometric samples.

O.PROTECTED_BIO_SAMPLES_COMMUNICATION

The TOE shall provide the necessary means for protecting the communication channel between the capture and the signal processing subsystems from unauthorized access by the REE or TAs, which could lead to modification, injection or disclosure of the Biometric samples (live images).

Application Note:

This means that the TOE provides appropriate access control to the communication channel that carries the Biometric samples.

O.PREVENT_RESIDUAL_BIO_SAMPLES

The TOE shall ensure that after the completion of any biometric operation no residual or unprotected biometric sample is stored in memory or at the level of the capture subsystem. Biometric samples must be deleted or invalidated between any two consecutive capture operations.

O.ENFORCE_BIOMETRIC_FUNCTIONS

The TOE shall ensure that the biometric functions have only the expected effects, i.e. modifications, on the state of the biometric system:

- A successful enrolment operation will add a biometric reference and its unique identifier to the biometric reference database, leaving everything else unmodified;
- A verification operation will return a match / no match result, leaving the system's state unmodified;
- An association operation will add an association to the association store if a match has been found in the biometric reference database, leaving everything else unmodified. If a match has not been found, the system's state will not be modified;
- A global wipe of biometric references will erase all biometric data (biometric reference and identifiers, associations);
- (optional) A dissociation operation will delete an association from the association store if the indicated association exists in the association store. Otherwise, the state remains unmodified. If the last association for a specified identifier is deleted, this may lead to a biometric reference deletion;
- (optional) A biometric reference deletion will erase a biometric reference and its unique identifier from the biometric reference database. Any associations for the deleted biometric reference contained by the association store will be deleted. Nothing else in the system's state will be modified;
- Any biometric operation will leave the system in a well-defined safe state.

(optional) Moreover, the TOE shall ensure that any notification about the progress of a biometric operation provided to the user is performed by means of a trusted user interface to which the biometric system has got exclusive access.

Application Note:

An explicit dissociation operation is explicitly requested by a user. An implicit dissociation operation is performed by the system when a TA is uninstalled or upon factory reset if such operation is available.

Application Note:

A global wipe (secure references deletion) shall be performed on factory reset if such operation is available.

Application Note:

A secure deletion of a biometric reference may be performed when the last association for a biometric reference has been deleted. In addition, if corrupted biometric references are detected, a secure deletion of the biometric references should be triggered.

Application Note:

For biometric verification systems which define an administrator role, the TOE shall ensure that the deletion of any rights associated to this role is performed in a secure fashion.

An explicit biometric reference deletion occurs only upon user request. An implicit biometric reference deletion is performed by the biometric system when a biometric reference is no longer in use, i.e. there are no associations linking that particular biometric reference to any existing TA.

Application Note:

The author of a compliant Security Target will indicate if the TOE implements a user notification mechanism, which is optional.

Application Note:

The author of a compliant Security Target will specify the behavior of all other biometric operations performed by the TOE, if applicable.

O.ATOMIC_BIOMETRIC_OPERATIONS

The TOE shall ensure that the biometric operations that impact the persistent state of the biometric system, e.g. enrolment, association and dissociation, are performed atomically. That is, either the operation succeeds or the biometric system's state is unchanged.

Application Note:

This is often described as "rollback to the initial state". However, in this document, rollback designates the unauthorized operation that violates the integrity of data at runtime or at rest.

O.UNIQUE_BIO_ID

The TOE shall ensure that unique biometric reference identifiers are generated and used for any biometric reference stored in the biometric reference database.

O.HIDE_COMPARISON_SCORE

The TOE shall ensure that the biometric comparison score between a biometric reference (stored template) and a biometric probe (live template) is only manipulated internally. This shall not be displayed, exported or returned to the user. The TOE shall ensure that the comparison score cannot be intercepted by a malevolent user. Providing the comparison scores may help attackers to conduct hill climbing attacks by allowing them to observe how close they are to being identified or verified by the biometric system[5].

O.PROTECTED_DATA_TRANSFER

The TOE shall provide the necessary means for ensuring that all biometric data and other assets between the different biometric subsystems are protected when sent between separate entities (if the communicating parties are indeed separate entities). The TOE shall protect against modification, injection or disclosure of the sent biometric data:

This refers to:

- Biometric probes (live templates) sent between the signal processing and comparison subsystems during enrolment or verification;
- Biometric references (stored templates) sent between the signal processing subsystem and the system's database during enrolment on the one hand, and between the system's database and the comparison subsystem during verification on the other hand;
- Biometric comparison score sent between the comparison subsystem and the decision subsystem during verification;
- Associations, Biometric reference identifiers and TA identifiers during association.

Application Note:

This security objective has to be ensured if the biometric functionality is implemented in a distributed manner, comprising different, separate biometric subsystems. TOEs that do not implement physically separated biometric subsystems fulfill this objective by design.

[5] "Biometric System Security". Andy Adler
https://pdfs.semanticscholar.org/3a85/8531c61d98e8c7484ef18df994bb5feb1615.pdf

5.2 Security Objectives for the Operational Environment

This section states the security objectives for the TEE operational environment covering all the assumptions and the organisational security policies that apply to the environment.

The following threats are covered by such kind of objectives:

- T.BRUTE_FORCE;
- T.SPOOF.

OE.SPOOF_DETECTION Spoofing/liveness detection is ensured based on hardware, software or a mix of software and hardware means.

OE.HIGH_QUALITY_CAPTURE A low False Acceptance Rate (FAR) is ensured by capturing biometric samples of sufficiently high quality.

OE.NO_RESIDUAL_SAMPLES The operational environment ensures that no residual biometric samples are stored at the level of the capture device.

OE.TA_DEVELOPMENT_BS

TA developers shall comply with the biometric system development guidelines set by the TEE provider. In particular, TA developers shall consider the following principles:

- Verification attempt limit: Attackers must be prevented from gaining access to the primary assets protected by the TOE by making repeated biometric verification attempts. The maximum number of unsuccessful verification attempts (i.e. that lead to a non-match) should be limited according to a well-defined policy.
- Information display: The communication with the end-user of the biometric system should be limited to a minimum and rely on a trusted interface for which the TA has got exclusive access. This applies in particular to the enrolment, association and biometric verification operations which require capture of end-user biometric data.

Application Note:

This objective completes OE.TA_DEVELOPMENT defined in the [TEE PP].

Characteristics that shall be considered to decide acceptable attempt limit values include (but are not limited to):

- The number of allowed unsuccessful verification attempts;
- The time needed to process a verification attempt.

5.3 Security Objectives Rationale

The following table indicates an overview of how the threats are addressed by the security objectives of the biometric system. The last column of the table indicates whether a threat is covered (partly or completely) by security objectives defined in the [TEE PP]. An orange * indicates that a threat is covered by a conjunction of security objectives specific to the biometric system and security objectives defined in the [TEE PP]. A green * indicates that a threat is either entirely covered by security objectives specific to the biometric system or by objectives defined in the [TEE PP]. A blue * indicates that a threat is completely covered by security objectives defined in the [TEE PP].

Table 5-1: Coverage of BS threats - Part 1

Biometric System Objectives / Biometric System Threats	O.BS_INITIALIZATION	O.CAPTURE	O.PROTECTED_BIO_SAMPLES_COMMUNICATION	O.PREVENT_RESIDUAL_BIO_SAMPLES	O.ENFORCE_BIOMETRIC_FUNCTIONS	O.ATTEMP_LIMIT	O.ATOMIC_BIOMETRIC_OPERATIONS	O.UNIQUE_BIO_ID	O.HIDE_COMPARISON_SCORE	O.PROTECTED_DATA_TRANSFER	OE.SPOOF_DETECTION	OE.HIGH_QUALITY_SAMPLES	OE.NO_RESIDUAL_SAMPLES	OE.TA_DEVELOPMENT_BS	TEE Objectives
T.SHARED_CAPTURE_ACCESS		X	X	X											
T.REPLAY_BIO_SAMPLE			X	X											
T.EXTRACT_BIO_SAMPLE			X												
T.HILL_CLIMBING_SAMPLE			X						X						
T.OVERRIDE_FEATURE_EXTRACTION	X														*
T.REPLAY_BIO_PROBE										X					*
T.INJECT_BIO_PROBE										X					*
T.EXTRACT_BIO_PROBE										X					*
T.HILL_CLIMBING_PROBE									X	X					*
T.MODIFY_CONFIG_DATA															*
T.BYPASS_VERIFICATION	X														*
T.FAULT_INJECTION	X														*
T.CORRUPT_DATABASE															*
T.ROLLBACK_DATABASE															*
T.CLONE_DATABASE															*
T.EXTRACT_BIO_REFERENCE										X					*
T.INJECT_BIO_REFERENCE										X					*
T.MODIFY_BIO_REFERENCE										X					*
T.TAMPER_VERIFICATION_RESULTS										X					*
T.EXTRACT_BIO_REFERENCE_ENROLL										X					*
T.INJECT_BIO_REFERENCE_ENROLL										X					*
T.MODIFY_BIO_REFERENCE_ENROLL										X					*
T.EXTRACT_COMPARISON_SCORE									X	X					*
T.EXTRACT_ASSOCIATION										X					*

Biometric System Objectives / Biometric System Threats	O.BS_INITIALIZATION	O.CAPTURE	O.PROTECTED_BIO_SAMPLES_COMMUNICATION	O.PREVENT_RESIDUAL_BIO_SAMPLES	O.ENFORCE_BIOMETRIC_FUNCTIONS	O.ATTEMP_LIMIT	O.ATOMIC_BIOMETRIC_OPERATIONS	O.UNIQUE_BIO_ID	O.HIDE_COMPARISON_SCORE	O.PROTECTED_DATA_TRANSFER	OE.SPOOF_DETECTION	OE.HIGH_QUALITY_SAMPLES	OE.NO_RESIDUAL_SAMPLES	OE.TA_DEVELOPMENT_BS	TEE Objectives
T.MODIFY_COMPARISON_SCORE										X					*
T.OVERWRITE_ASSOC_ID										X					*
T.MODIFY_ASSOCIATION_STORE															*
T.ROLLBACK_ASSOCIATION															*
T.CLONE_ASSOCIATION															*
T.CORRUPT_RUNTIME_EVENT															*
T.CORRUPT_RUNTIME_DATA															*
T.BS_IMPERSONATION															*
T.RESIDUAL															*
T.REPLAY_EXACT_MATCH				X							X				*
T.UNSAFE_STATE	X				X		X	X							
T.BRUTE_FORCE												X			
T.SPOOF											X				
A.TA_DEVELOPMENT						X								X	
A.NO_RESIDUAL_SAMPLES													X		

The first four threats (attacks at points 1 and 2) are specific to the biometric system and are therefore completely covered by security objectives specific to the biometric system.

T.SHARED_CAPTURE_ACCESS is covered by the following security objectives:

- O.CAPTURE ensures that the biometric sample is captured by the expected wired sensor, and that at the time of usage, the biometric system has exclusive access to the captured biometric samples,
- O.PROTECTED_BIO_SAMPLES_COMMUNICATION ensures that captured biometric samples cannot be intercepted or modified when transmitted by the capture device to the biometric system, and
- O.PREVENT_RESIDUAL_BIO_SAMPLES ensures that no residual biometric samples can be extracted subsequently at the level of the capture subsystem or from memory.

T.EXTRACT_BIO_SAMPLE is covered by the following security objective:

- O.PROTECTED_BIO_SAMPLES_COMMUNICATION ensures that captured biometric samples cannot be intercepted when transmitted by the capture device to the biometric system.

T.REPLAY_BIO_SAMPLE is covered by the following security objectives:

- O.PROTECTED_BIO_SAMPLES_COMMUNICATION ensures that captured biometric samples cannot be intercepted or modified when transmitted by the capture device to the biometric system, and
- O.PREVENT_RESIDUAL_BIO_SAMPLES ensures that no residual biometric samples can be extracted subsequently at the level of the capture subsystem or from memory.

T.HILL_CLIMBING_SAMPLE is covered by the following security objectives:

- O.PROTECTED_BIO_SAMPLES_COMMUNICATION ensures that captured biometric samples cannot be intercepted nor modified when transmitted by the capture device to the biometric system, and
- O.HIDE_COMPARISON_SCORE ensures that the comparison score which offers necessary feedback for performing a hill climbing attack is not exported outside the TOE and cannot be observed or intercepted.

T.UNSAFE_STATE is covered by the following security objectives:

- O.BS_INITIALIZATION,
- O.ENFORCE_BIOMETRIC_FUNCTIONS,
- O.UNIQUE_BIO_ID,
- O.ATOMIC_BIOMETRIC_OPERATIONS.

The following table indicates an overview of how the threats are addressed by the security objectives defined in the [TEE PP].

Table 5-2: Coverage of BS threats - Part 2

TEE Security Objectives / BS Threats	O.CA_TA_IDENTIFICATION	O.KEYS_USAGE	O.TEE_ID	O.INITIALIZATION	O.INSTANCE_TIME	O.OPERATION	O.RNG	O.RUNTIME_CONFIDENTIALITY	O.RUNTIME_INTEGRITY	O.TA_AUTHENTICITY	O.TA_ISOLATION	O.TEE_DATA_PROTECTION	O.TEE_ISOLATION	O.TRUSTED_STORAGE	O.ROLLBACK_PROTECTION	O.TA_PERSISTENT_TIME	OE.INTEGRATION_CONFIGURATION	OE.PROTECTION_AFTER_DELIVERY	OE.SECRETS	OE.TA_MANAGEMENT	OE.TA_DEVELOPMENT
T.SHARED_CAPTURE_ACCESS																					
T.REPLAY_BIO_SAMPLE																					
T.EXTRACT_BIO_SAMPLE																					
T.HILL_CLIMBING_SAMPLE																					
T.OVERRIDE_FEATURE_EXTRACTION						X															
T.REPLAY_BIO_PROBE								X	X												
T.INJECT_BIO_PROBE									X												
T.EXTRACT_BIO_PROBE								X													
T.HILL_CLIMBING_PROBE								X	X												
T.MODIFY_CONFIG_DATA												X									
T.BYPASS_VERIFICATION						X															

TEE Security Objectives / BS Threats	O.CA_TA_IDENTIFICATION	O.KEYS_USAGE	O.TEE_ID	O.INITIALIZATION	O.INSTANCE_TIME	O.OPERATION	O.RNG	O.RUNTIME_CONFIDENTIALITY	O.RUNTIME_INTEGRITY	O.TA_AUTHENTICITY	O.TA_ISOLATION	O.TEE_DATA_PROTECTION	O.TEE_ISOLATION	O.TRUSTED_STORAGE	O.ROLLBACK_PROTECTION	O.TA_PERSISTENT_TIME	OE.INTEGRATION_CONFIGURATION	OE.PROTECTION_AFTER_DELIVERY	OE.SECRETS	OE.TA_MANAGEMENT	OE.TA_DEVELOPMENT
T.FAULT_INJECTION				X		X		X	X												
T.CORRUPT_DATABASE												X		*							
T.ROLLBACK_DATABASE															X						
T.CLONE_DATABASE				X								X		*							
T.EXTRACT_BIO_REFERENCE								X													
T.INJECT_BIO_REFERENCE									X												
T.MODIFY_BIO_REFERENCE									X												
T.TAMPER_VERIFICATION_RESULTS									X												
T.EXTRACT_BIO_REFERENCE_ENROLL								X													
T.INJECT_BIO_REFERENCE_ENROLL									X												
T.MODIFY_BIO_REFERENCE_ENROLL									X												
T.EXTRACT_COMPARISON_SCORE								X													
T.EXTRACT_ASSOCIATION								X													
T.MODIFY_COMPARISON_SCORE									X												
T.OVERWRITE_ASSOC_ID									X												
T.MODIFY_ASSOCIATION_STORE												X		*							
T.ROLLBACK_ASSOCIATION															X						
T.CLONE_ASSOCIATION				X								X		*							
T.CORRUPT_RUNTIME_EVENT									X												
T.CORRUPT_RUNTIME_DATA									X												
T.BS_IMPERSONATION	X					X			X												
T.RESIDUAL								X													
T.REPLAY_EXACT_MATCH								X				X		*							
T.UNSAFE_STATE																					
T.BRUTE_FORCE																					
T.SPOOF																					
A.TA_DEVELOPMENT_BS																					
A_NO_RESIDUAL_SAMPLES																					

The next threats (attacks at points 3 - 12) are covered as follows:

Threats T.OVERRIDE_FEATURE_EXTRACTION and T.BYPASS_VERIFICATION are covered by the following security objectives:

- O.BS_INITIALIZATION that ensures the integrity of the biometric subsystems initialisation code and data, as well as the authenticity of the biometric system firmware, and
- O.OPERATION defined in the [TEE PP] that ensures correct operation of the security functionality, including biometric feature extraction and biometric verification.

Threat T.FAULT_INJECTION is covered by the following security objectives:

- O.BS_INITIALIZATION, and
- O.TEE_ID, O.OPERATION, O.RUNTIME_CONFIDENTIALITY, and O.RUNTIME_INTEGRITY defined in the [TEE PP].

Threat T.REPLAY_BIO_PROBE depends on runtime confidentiality and integrity. Depending on the biometric system's specificities and implementation, they are covered either by a security objective specific to the biometric system or by security objectives defined in the [TEE PP].

For a distributed biometric system in which the biometric functionality is provided by separate biometric subsystems, the threat is covered by the following security objective:

- O.PROTECTED_DATA_TRANSFER that ensures that biometric probes cannot be extracted or modified during their transmission between two separate biometric subsystems.

For a non-distributed biometric system, the threats are completely covered by the following security objectives defined in the [TEE PP]:

- O.RUNTIME_CONFIDENTIALITY that ensures runtime confidentiality preventing exposure of biometric probes, and
- O.RUNTIME_INTEGRITY that ensures runtime integrity and prevents unauthorized modification of biometric probes.

Threats T.INJECT_BIO_PROBE, T.INJECT_BIO_REFERENCE, T.INJECT_BIO_REFERENCE_ENROLL, T.MODIFY_BIO_REFERENCE, T.OVERWRITE_ASSOC_ID, T.TAMPER_VERIFICATION_RESULTS, T.MODIFY_COMPARISON_SCORE, and T.MODIFY_BIO_REFERENCE_ENROLL depend on runtime integrity. Depending on the biometric system's specificities and implementation, they are covered either by a security objective specific to the biometric system or by security objectives defined in the [TEE PP].

For a distributed biometric system in which the biometric functionality is provided by separate biometric subsystems, the threat is covered by the following security objective:

- O.PROTECTED_DATA_TRANSFER that ensures that biometric probes, biometric references, biometric comparison scores, and associations cannot be modified or altered during their transmission between two separate biometric subsystems.

For a non-distributed biometric system, the threats are completely covered by the following security objective defined in the [TEE PP]:

- O.RUNTIME_INTEGRITY that ensures runtime integrity and prevents unauthorized modification of biometric probes.

Threats T.EXTRACT_BIO_PROBE, T.EXTRACT_ASSOCIATION, T.EXTRACT_BIO_REFERENCE, and T.EXTRACT_BIO_REFERENCE_ENROLL depend on runtime confidentiality. Depending on the biometric system's specificities and implementation it is covered either by a security objective specific to the biometric system or by a security objective defined in the [TEE PP].

For a distributed biometric system in which the biometric functionality is provided by separate biometric subsystems, the threat is covered by the following security objective:

- O.PROTECTED_DATA_TRANSFER that ensures that biometric probes, biometric references and associations cannot be extracted during their transmission between two separate biometric subsystems.

For a non-distributed biometric system, the threat is completely covered by the following security objective defined in the [TEE PP]:

- O.RUNTIME_CONFIDENTIALITY that ensures runtime confidentiality preventing exposure or extraction of biometric probes, biometric references, and associations.

Threat T.HILL_CLIMBING_PROBE depends on the confidentiality / non-export outside the TOE of the biometric comparison score, as well as on runtime confidentiality and integrity. The first condition is covered by the following security objective:

- O.HIDE_COMPARISON_SCORE that ensures that the comparison score which offers necessary feedback for performing a hill climbing attack is not exported outside the TOE and cannot be observed or intercepted.

Depending on the biometric system's specificities and implementation, the second condition is covered either by a security objective specific to the biometric system or by security objectives defined in the [TEE PP].

For a distributed biometric system in which the biometric functionality is provided by separate biometric subsystems, the threat is covered by the following security objective:

- O.PROTECTED_DATA_TRANSFER that ensures that biometric comparison scores cannot be extracted or modified during their transmission between two separate biometric subsystems.

For a non-distributed biometric system, the threats are completely covered by the following security objectives defined in the [TEE PP]:

- O.RUNTIME_CONFIDENTIALITY that ensures runtime confidentiality preventing exposure of biometric comparison scores, and
- O.RUNTIME_INTEGRITY that ensures runtime integrity and prevents unauthorized modification of biometric comparison scores.

Threat T.REPLAY_EXACT_MATCH is covered by the following security objectives:

- OE.SPOOF_DETECTION and O.PROTECTED_BIO_SAMPLES_COMMUNICATION preventing replay of exact matches, and
- O.RUNTIME_INTEGRITY from the [TEE PP] ensuring runtime integrity, and
- (for a full TEE implementation) O.TEE_DATA_PROTECTION, or
- (for a TEE/TA implementation) O.TRUSTED_STORAGE.

The next threats are completely covered by security objectives defined in the [TEE PP].

Threats T.CLONE_DATABASE and T.CLONE_ASSOCIATION are covered by the following objectives:

- O.INITIALIZATION, and
- (for a full TEE implementation) O.TEE_DATA_PROTECTION that prevents the TEE from using TEE data that is inconsistent or inauthentic, or
- (for a TEE/TA implementation) O.TRUSTED_PROTECTION that ensures that the trusted storage is bound to the device and that prevents the TEE from using data that is inconsistent or not authentic.

Threats T.ROLLBACK_DATABASE and T.ROLLBACK_ASSOCIATION are covered by the following objective:

- O.ROLLBACK_PROTECTION.

Threats T.CORRUPT_DATABASE and T.MODIFY_ASSOCIATION_STORE are covered by the following security objectives:

- (for a full TEE implementation) O.TEE_DATA_PROTECTION that ensures protection of persistent data, or
- (for a TEE/TA implementation) O.TRUSTED_PROTECTION that ensures protection of the storage.

Threats T.CORRUPT_RUNTIME_EVENT and T.CORRUPT_RUNTIME_DATA are covered by the following security objective:

- O.RUNTIME_INTEGRITY that ensures runtime integrity.

Threat T.MODIFY_CONFIG_DATA is covered by the following security objective:

- O.TEE_DATA_PROTECTION that ensures protection of persistent TEE data.

5.4 Correspondence to [TEE PP] Objectives

The objectives presented in Section 5.1 are specific to the biometric system and they are disjoint from security objectives defined in the [TEE PP].

6 Security Requirements

6.1 Security Functional Requirements

This chapter provides the set of Security Functional Requirements (SFRs) the TOE has to enforce in order to fulfill the security objectives.

The following security functional components defined in CC Part 2 [CC2] are used:

- FDP_ACC.1 Subset access control
- FDP_ACF.1 Security attribute based access control
- FDP_RIP .1 Subset residual information protection
- FDP_ROL.1 Basic Rollback
- FMT_MSA.1 Management of security attributes
- FMT_MSA.2 Secure security attributes
- FMT_MSA.3 Static attribute initialisation
- FPT_FLS.1 Failure with preservation of secure state
- FTP_ITC.1 Inter-TSF trusted channel

6.1.1 Security Policy

This PP-Module requires a security access control policy to the biometric system data, called **Biometric System Access Control SFP**, to enforce the correct behavior of the biometric system functionality.

The subjects, objects, security attributes and operations of this policy are the following:

Subjects: The active entities of the biometric system

- BS (the Biometric System itself)
- TA (Trusted Applications)
- CD (capture device)

Application Note:

The biometric system may rely on a Trusted User Interface (TUI) for direct communication with the user. Therefore, in this case, another active entity of the biometric system is the following:

- TUI (trusted user interface for direct communication with the user)

Using the biometric system with a TUI ensures the following:

- Information entered by users of the biometric system cannot be derived or modified by unauthorized applications in the TEE or by software running within the REE;
- Information displayed to users of the biometric system cannot be accessed, modified, or obscured by an unauthorized application in the TEE or by software running within the REE.

Furthermore, users of a biometric system using a TUI can be confident that the displayed screen and any displayed notification are actually displayed by the TA in charge of the biometric functionality.

Objects: persistent state and a transient state of the biometric system

The minimum persistent state of the biometric system consists of:

- cd_list: a list of authorized capture devices
- bio_ref_list: a list of biometric references
- assoc_store: the association store, i.e. a list of p pairs of TA identifiers and a list of biometric reference identifiers. For each TA, the list of biometric reference identifiers determines the biometric references that are associated to the TA
- bio_threshold_list: a list of thresholds for the biometric comparisons, which depend on the type of biometric data

The minimum transient state of the biometric system consists of:

- calling_TA: the TA that requests a biometric operation
- sample: the captured biometric data
- probe: the biometric data after feature extraction
- bio_ref: the biometric reference
- comparison score: the result of the biometric comparison
- result: the information that is provided to the calling TA, which can hold the following values:
    - if the operation succeeds:
        - MATCH (info), NO_MATCH (info) where info is empty or some code independent of the biometric data
        - SUCCESS (info) where info is empty, or a set of biometric references identifiers, or some code independent of the biometric data
    - if the operation fails: ERROR (info) where info is empty or some error code independent of the biometric data
    - optionally, if the operation is in progress: IN_PROGRESS (info) where info is empty or some progress indicator independent of the biometric data

Application Note:

For biometric systems using TUIs, the minimum persistent state of the biometric system may additionally include the following:

- tui_list: a list of authorized trusted user interfaces

Security attributes:

- cd.status: the status “locked” or “unlocked” of the capture device cd
- bio_ref.id: the unique identifier of the biometric reference bio_ref

Application Note:

For biometric systems using TUIs, an additional security attribute may be the following:

- tui.status: the status “locked” or “unlocked” of the trusted user interface tui

Operations:

- lock (x): locks the capture device or trusted user interface x for exclusive access by the Biometric System
- unlock (x): releases the component x
- capture (cd): request a capture of raw biometric data through the capture function of the capture device cd
- extract: extracts the features of the current biometric sample
- create: creates a biometric reference with unique identification from the current probe
- match (collection): searches in the collection a biometric reference that matches the current probe and provides a result depending on the comparison score and the applicable threshold
- add_assoc: adds the current bio_ref.id to the list of references of the calling TA
- add_bio_ref: adds the current bio_ref to the list of biometric references
- return (info): gives an intermediate or final result to the calling TA
- wipe_bio_ref: globally wipes out all the biometric references, for instance upon factory reset if such operation is available
- remove_assoc (x): removes x from the list of biometric references associated to the calling TA
- read: provides the biometric references associated with the calling TA

Application Note:

These operations must be executed in a specific order to provide the expected service, e.g. enroll, associate, verify. The symbol “;” is used to indicate a sequence of operations. The symbol “+” attached to an operation is used to indicate that the operation can be run one or more times.

Optionally, any operation may implicitly give rise to a notification, i.e. a return of an (intermediate) result to the calling TA

Application Note:

The ST author must complete this list to cover all the biometric operations. For instance, if the TOE allows to remove a biometric reference, the following operation should be added:

- remove_bio_ref (x): removes x from the list of biometric references

Application Note:

For biometric systems using TUIs, an additional operation may be the following:

- notify (tui, info): provides information of in progress operations to the end user through the tui

- (optionally) a direct notification to the user through a trusted interface, e.g. a display.

6.1.2 FDP_ACC.1/BS Subset access control

This SFR contributes to the following security objectives:

- O.CAPTURE
- O.PROTECTED_BIO_SAMPLES_COMMUNICATION
- O.ENFORCE_BIO_FUNCTIONS

FDP_ACC.1/BS Subset access control[6]

Dependencies:

FDP_ACF.1 Security attribute based access control: **FDP_ACF.1/BS**

FDP_ACC.1.1/BS The TSF shall enforce the **Biometric System access control SFP** on

- **Subjects: BS, TA, CD,** ***[assignment: other subjects of the biometric system]***
- **Objects:**
  - **Persistent objects: cd_list, bio_ref_list, assoc_store, bio_threshold_list**
  - **Transient objects: calling_TA, sample, probe, bio_ref, comparison score, result**
  - ***[assignment: other persistent or transient objects of the biometric system]***
- **Operations:**
  - **lock, unlock, capture, extract_feature, create_bio_ref, match, add_bio_ref, add_assoc, return, wipe_bio_ref, remove_assoc, read**
  - ***[assignment: other biometric system operations]***

Application Note:

For biometric systems using a TUI, the **persistent objects** would include **tui_list.**

6.1.3 FDP_ACF.1/BS Security attribute based access control

This SFR contributes to the following security objectives:

- O.CAPTURE
- O.PROTECTED_BIO_SAMPLES_COMMUNICATION
- O.ENFORCE_BIO_FUNCTIONS

FDP_ACF.1/BS Subset access control[7]

[6] FDP_ACC.1.1 The TSF shall enforce the *[assignment: access control SFP]* on *[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].*

Dependencies:

FDP_ACC.1 Subset access control: **FDP_ACC.1/BS**

FMT_MSA.3 Static attribute initialisation: **FMT_MSA.3/BS**

FDP_ACF.1.1/BS The TSF shall enforce the **Biometric System access control SFP** to objects based on the following:

- **cd.status ("locked" or "unlocked")**
- **bio_ref.id**
- ***[assignment: list of additional security attributes]***

FDP_ACF.1.2/BS The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **rule-enroll: [cd.status == unlocked and cd belongs to cd_list] lock (cd); capture+ (cd); extract; create; add_bio_ref; return (result) where result == SUCCESS or ERROR**
- **rule-associate: [cd.status == unlocked and cd belongs to cd_list] lock (cd); capture+ (cd); extract; match (assoc_store); add_assoc; return (result) where result == SUCCESS or ERROR**
- **rule-verify: [cd.status == unlocked and cd belongs to cd_list] lock (cd); capture+ (cd); extract; match (bio_ref_list); return (result) where result == MATCH or NO_MATCH**
- ***[assignment: list of additional rules, including usage conditions of wipe_bio_ref operation if applicable]***

FDP_ACF.1.3/BS The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

- **rule-lock-cd: [cd.status == unlocked] lock (cd)**
- **rule-unlock-cd: [cd.status == locked] unlock (cd)**

---

[7] FDP_ACF.1.1 The TSF shall enforce the [assignment: access control SFP] to objects based on the following: *[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]*.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]*.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]*.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]*.

- **rule-capture: [cd.status == locked and sample's quality is insufficient] capture (cd)**
- **rule-return: [cd.status == locked] return (IN_PROGRESS)**
- **rule-dissociate: remove_assoc; return (SUCCESS or ERROR)**
- **rule-read: read; return (SUCCESS (list of bio_ref identifiers) or ERROR)**
- ***[assignment: list of additional rules, including usage conditions of wipe_bio_ref operation if applicable]***

FDP_ACF.1.4/BS The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- **rule-deny-lock-cd: [cd.status == locked] lock (cd)**
- **rule-deny-capture: [cd.status == unlocked] capture (cd)**
- **rule-deny-extract: [cd.status == locked, sample.quality == insufficient] extract**
- **rule-deny-return: return (IN_PROGRESS or MATCH or NO_MATCH or SUCCESS or ERROR (info)) if info is a biometric system data,**
- ***[assignment: list of additional rules, including usage conditions of wipe_bio_ref operation if applicable]***

where biometric system data stands for samples, probes, bio_refs, association information, comparison_score, threshold or any other persistent or transient data.

Application Note:

The Security Target shall complete the above rules to address all the operations supported by the biometric system and all their usage condition. This holds for wipe_bio_ref, and for any additional operation, for instance **remove_bio_ref(x)**, which can lead to the following rule in FDP_ACF.1.3:

- **rule-unenroll: remove_bio_ref; return (SUCCESS or ERROR)**

Application Note:

For biometric systems using a TUI the following may be included:

- In FDP_ACF.1.1/BS: the security attribute **tui.status ("locked" or "unlocked")**
- In FDP_ACF.1.1/BS**:**
  - **rule-lock-tui: [tui.status == unlocked] lock (tui)**
  - **rule-unlock-tui: [tui.status == locked] unlock (tui)**
- In FDP_ACF.1.4/BS**:**
  - **rule-deny-lock-tui: [tui.status == locked] lock (tui)**
  - **rule-deny-notify-1: [tui.status == unlocked] notify (tui, _)**
  - **rule-deny-notify-2: [tui.status == locked] notify (tui, info) if info is a biometric system data**

6.1.4 FDP_RIP.1/BS Residual information protection

This SFR contributes to the following security objectives:

- O.PREVENT_RESIDUAL_BIO_SAMPLES.

FDP_RIP.1/BS Subset residual information protection[8]

Dependencies: No dependencies.

FDP_RIP.1.1/BS The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource upon from** the following objects:

- **biometric samples as per FDP_ACC.1/BS upon *[selection: capture device lock, capture device unlock]***
- **trusted channel as per FDP_ITC.1/BS_CD upon capture device unlock**

Application Note:

This SFR completes FDP_RIP.1/Runtime as defined in [TEE PP], which covers all the other biometric data: biometric probes, biometric comparison scores, biometric verification results, and any other resource used by the biometric system, such as event handlers, handlers to biometric data, etc.

Application Note:

For biometric systems using a TUI the following objects may be included:

- trusted channel as per FDP_ITC.1/BS_TUI upon trusted user interface unlock

6.1.5 FDP_ROL.1/BS Basic rollback

This SFR contributes to the following security objectives:

- O.BS_ATOMIC_BIO_OPERATIONS.

FDP_ROL.1/BS Basic rollback[9]

---

[8] FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: [assignment: *list of objects*].

[9] FDP_ROL.1.1 The TSF shall enforce [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to permit the rollback of the [assignment: *list of operations*] on the [assignment: *information and/or list of objects*].
FDP_ROL.1.2 The TSF shall permit operations to be rolled back within the [assignment: *boundary limit to which rollback may be performed*].

Dependencies:

[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]: **FDP_ACC.1/BS**

FDP_ROL.1.1/BS The TSF shall enforce **Biometric System Access Control SFP** to permit the rollback of the **add and remove operations** on the **persistent objects bio_ref_list, assoc_store** ***[assignment: list of objects]***.

FDP_ROL.1.2/BS The TSF shall permit operations to be rolled back within the **biometric operation session or upon reset**.

Application Note:

In the context of the biometric system, this means that the TSF shall provide mechanisms to permit the atomic execution of operations on the persistent objects of the biometric system. This includes: enrolment and association, as well as dissociation and delete biometric reference if supported.

6.1.6 FMT_MSA

These SFRs contribute to the following security objectives:

- O.UNIQUE_BIO_ID
- All the objectives linked to FDP_ACF.1/BS.

6.1.6.1 FMT_MSA.1/BS Management of security attributes

FMT_MSA.1/BS Management of security attributes[10]

Dependencies:

[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]: **FDP_ACC.1/BS**

Discarded dependencies:

FMT_SMR.1 Security roles: **since the operations can only be performed by the Biometric System itself**.

FMT_SMF.1 Specification of Management Functions: **since only standard operations are necessary**.

FMT_MSA.1.1/BS The TSF shall enforce the **Biometric Access Control SFP** to restrict the ability to **query and modify** the security attributes

- **cd.status**
- **bio_ref.id**
- ***[assignment: list of security attributes]***

to **the Biometric System**.

Application Note:

[10] FMT_MSA.1.1 The TSF shall enforce the *[assignment: access control SFP(s), information flow control SFP(s)]* to restrict the ability to [*selection: change_default, query, modify, delete, [assignment: other operations]]* the security attributes *[assignment: list of security attributes]* to *[assignment: the authorized identified roles]*.

For biometric systems using a TUI the following security attributes may be included: **tui.status**

6.1.6.2 FMT_MSA.2/BS Secure security attributes

FMT_MSA.2/BS Secure security attributes[11]

Dependencies:

[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]: **FDP_ACC.1/BS**

FMT_MSA.1 Management of security attributes: **FMT_MSA.1/BS**

Discarded dependencies:

FMT_SMR.1 Security roles: **since the operations can only be performed by the Biometric System itself.**

FMT_MSA.2.1/BS The TSF shall ensure that only secure values are accepted for **the following security attributes:**

- **cd.status == locked or unlocked**
- **bio_ref.id == unique identifier within the set of references maintained by the Biometric System**
- ***[assignment: list of security attributes]***

Application Note:

For biometric systems using a TUI the following security attributes may be included:

- **tui.status == locked or unlocked**

6.1.6.3 FMT_MSA.3/BS Static attribute initialisation

FMT_MSA.3/BS Static attribute initialisation[12]

Dependencies:

FMT_MSA.1 Management of security attributes: **FMT_MSA.1/BS**

Discarded dependencies:

FMT_SMR.1 Security roles: **since the operations can only be performed by the Biometric System itself.**

[11] FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for *[assignment: list of security attributes]*.

[12] FMT_MSA.3.1 The TSF shall enforce the [assignment: access control SFP, information flow control SFP] to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: the authorised identified roles] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3.1/BS The TSF shall enforce the **Biometric Access Control SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/BS The TSF shall allow **no role** to specify alternative initial values to override the default values when an object or information is created.

6.1.7 FPT_FLS.1/BS Failure with preservation of secure state

This SFR contributes to the following security objectives:

- O.ENFORCE_BIOMETRIC_FUNCTIONS.

FPT_FLS.1/BS Failure with preservation of secure state[13]

Dependencies: No dependencies.

FPT_FLS.1.1/BS The TSF shall preserve a secure state when the following types of failures occur:

- **a biometric operation is halted**
- **a biometric operation returns an ERROR as per FDP_ACF.1/BS**
- **a trusted channel tampering has been detected as per FTP_ITC.1/BS_CD**
- ***[assignment: list of types of failures in the TSF].***

Application Note:

The ST author shall specify what is meant by “secure state”.

Application Note:

For biometric systems using a TUI, the TSF shall additionally preserve a secure state for the following types of failure:

- **a trusted channel tampering has been detected as per FTP_ITC.1/BS_TUI**

6.1.8 FTP_ITC.1/BS_CD Inter-TSF trusted channel

This SFR contributes to the following security objectives:

- O.CAPTURE,
- O.PROTECTED_BIO_SAMPLES_COMMUNICATION,
- O.ENFORCE_BIOMETRIC_FUNCTIONS.

FTP_ITC.1/BS_CD Inter-TSF trusted channel[14]

[13] FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [assignment: *list of types of failures in the TSF*].

[14] FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

Dependencies: No dependencies.

FTP_ITC.1.1/BS_CD The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

Refinement: “trusted IT product” stands for **capture device**

FTP_ITC.1.2/BS_CD The TSF shall permit **the TSF** to initiate communication via the trusted channel.

FTP_ITC.1.3/BS_CD The TSF shall initiate communication via the trusted channel for **capture biometric data**.

Application Note:

For biometric systems using a trusted user interface, the following additional SFR should be enforced:

FTP_ITC.1/BS_TUI Inter-TSF trusted channel

This SFR contributes to the following security objectives:

- O.ENFORCE_BIOMETRIC_FUNCTIONS.

FTP_ITC.1/BS_TUI Inter-TSF trusted channel

Dependencies: No dependencies.

FTP_ITC.1.1/BS_TUI The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

Refinement: “trusted IT product” stands for **a trusted user interface**

FTP_ITC.1.2/BS_TUI The TSF shall permit **the TSF** to initiate communication via the trusted channel.

FTP_ITC.1.3/BS_TUI The TSF shall initiate communication via the trusted channel for **user notification.**

6.2 Security Objectives Rationale

The following table shows an overview of how the security objectives for the biometric systems are covered by the SFRs.

Table 6-1: Coverage of BS security objectives

Security Objective of the Biometric System	SFRs
O.BS_INITIALIZATION	This objective is fulfilled by the TEE through FPT_INI.1
O. CAPTURE	FDP_ACC.1/BS FDP_ACF.1/BS

FTP_ITC.1.2 The TSF shall permit [selection: *the TSF, another trusted IT product*] to initiate communication via the trusted channel.
FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].

Security Objective of the Biometric System	SFRs
	FMT_MSA.1/BS FMT_MSA.2/BS FMT_MSA.3/BS FTP_ITC.1/BS_CD
O.PROTECTED_BIO_SAMPLES_COMMUNICATION	FDP_ACC.1/BS FDP_ACF.1/BS FMT_MSA.1/BS FMT_MSA.2/BS FMT_MSA.3/BS FTP_ITC.1/BS_CD
O.PREVENT_RESIDUAL_BIO_SAMPLES	FDP_RIP.1/BS
O.ENFORCE_BIOMETRIC_FUNCTIONS	FDP_ACC.1/BS FDP_ACF.1/BS FPT_FLS.1/BS FTP_ITC.1/BS_CD Application Note: For biometric systems using TUIs, the following additional SFR contributes to this objective's fulfilment: FTP_ITC.1/BS_TUI
O.ATOMIC_BIOMETRIC_OPERATIONS	FDP_ROL.1/BS
O.UNIQUE_BIO_ID	FMT_MSA.1/BS FMT_MSA.2/BS FMT_MSA.3/BS
O.HIDE_COMPARISON_SCORE	FDP_ACC.1/BS FDP_ACF.1/BS
O.PROTECTED_DATA_TRANSFER (applicable to a distributed implementation)	This objective is fulfilled by the TEE through FPT_ITT.1.1/Runtime