UBREADER2
SECURITY TARGET

VERSION 1.12

2011-12-05

Hitachi-Omron Terminal Solutions, Corp.

.

Table of content

DOCUMENT INTRODUCTION

This Security Target (ST) was developed based on the Biometric Verification Mechanisms Protection Profile v1.3 [BVMPP]. However, it does not claim conformity to this PP.

1. ST INTRODUCTION

1.1. ST AND TOE REFERENCE

ST Title:	UBReader2 Security Target
ST Version:	1.12
ST Date:	2011-12-05
ST Author:	Hitachi-Omron Terminal Solutions, Corp.
CC-Version:	3.1 Release 3
Keywords:	authentication; biometric; identification; verification; finger vein
TOE:	Finger Vein Authentication Device UBReader2 and its related guidance documentation [AGD] <Model: TS-E3F1-700UW / TS-E3F1-700UWP> <Hardware: D, Software: 03-00>
Developer:	Hitachi-Omron Terminal Solutions, Corp.

1.2. TOE OVERVIEW

The scope of this Security Target (ST) is to describe the functionality of the Finger Vein Authentication Device UBReader2 (UBR2) as a biometric system in terms of [CC] and to define functional and assurance requirements for it.

In this context the major scope of the UBR2 as a biometric system is to verify or reject a human being using a pattern of his or her finger vein as unique characteristics of his or her body. The TOE is used by an application (e.g. a portal) which utilizes the functionality of the TOE to verify the identity of a user. The TOE requires other components in its operational environment which are identified in chapter 1.3.6.

Please note that inside this ST the enrolment and the identification process of a biometric system (see also chapter 1.3.2) are not considered. Chapter 1.3 gives a more details overview about the design of the TOE and its boundaries.

1.3. TOE DESCRIPTION

The TOE provides a biometric verification process for the claimed identity of a human being using a pattern of his or her finger vein as unique characteristic of their body.

The basic processes of a biometric system are described in chapter 1.3.2.

This ST describes a biometric system that operates in a verification mode only. Biometric Identification is not addressed with in this ST. Furthermore the enrolment process is out of scope of this ST and it is assumed that all authorized users have been enrolled. Last but not least the TOE aims to verify the identity of a user for the purpose of controlling access to a portal.

Such a portal can be a physical or logical point beyond which information or assets are protected by the biometric system. With failed biometric verification, the portal stays closed for the user. Only after successful biometric verification, the portal will be opened.

Therefore, such a portal requires one of two states after biometric verification: failed or successful authentication of the user. The final decision on the claimed identity of the user (resulting from a biometric probabilistic message into a boolean value) is considered to be part of the TOE. Everything beyond the portal and the control of the portal itself (i.e. which users have access to the portal) is out of the scope of the TOE.

Beside the biometric verification process every biometric system needs to include mechanisms to identify and authenticate an administrator of the system with other means than the biometric mechanism and to limit the access to administrative functions. This is specifically important to limit the ability to change security relevant settings of the biometric functionality to an authorized administrator. The TOE is used as a part of an overall application. Identification and authentication of an administrator needs to be handled by this application, which is part of the operative environment of the TOE. Therefore this requirement is not handled by the TOE but by the operative environment.

1.3.1. Wording in context of Common Criteria

In context of [CC] identification usually means the statement of a claimed identity whole authentication means the confirmation of this identity. In context of biometric technology identification usually means a process as described in chapter 1.3.2. To avoid any misunderstanding: the wording in this ST is as follows:

- Identification: As defined in [CC]
- Authentication: As defined in [CC]
- Biometric identification: Biometric identification as described in chapter 1.3.2
- Biometric verification: Biometric verification as described in chapter 1.3.2

1.3.2. Description of general biometric processes

The general core functionality of biometric systems can be divided into three processes:

- Enrolment[1]:

  Usually, the enrolment process is the first contact of a user with a biometric system. This process is necessary because a biometric system has to 'learn' to verify the identity of each user based on their biometric characteristic.

  During the enrolment process the system captures the biometric characteristic of a user and extracts the features it is working with. This feature vector is then combined with the identity of the user to a biometric reference and stored in a database.

  The quality of the biometric reference has to be assured and quality proofed. In the case of inadequate biometric characteristics or lower reference quality, the person to be enrolled has to repeat the process or is not possible to be enrolled. Only an administrator should be allowed to start the enrolment process. The administrator has to observe the whole process to ensure a correct enrolment. Furthermore, the administrator has to ensure that the user claims his correct identity to the system during the enrolment process.

- Biometric Verification:

  An objective of the biometric verification process is to verify or refuse a claimed identity of a user.

  Therefore the user has to claim an identity to the system. The system gets the biometric reference associated with this identity from the database and captures the biometric characteristic of the user. If the Biometric Live Record (BLR) that is extracted from the characteristic and the biometric reference from the database are similar enough, the claimed identity of the user is verified.

  Otherwise or if no biometric reference was found for the user, the claimed identity is refused. The matching component of a biometric system that decides whether a

---

[1] As mentioned before: Within this ST is assumed that the enrolment process for all users has already been performed.

biometric reference and BLR are similar enough usually uses a threshold value for this decision that can be configured by an administrator. If the matcher finds that the BLR and the biometric reference are more similar than demanded by the threshold, it returns successful verification, otherwise failed verification.

- Biometric Identification[2]:

  An objective of the biometric identification process is quite similar to a biometric verification process. However, in contrast to a biometric verification process there is no claimed identity for the user. The system directly captures the biometric characteristic of a user and compares it to all biometric references in the database.

  If at least one biometric reference is found to be similar enough, the system returns this as the found identity of the user. Biometric identification systems introduce many additional issues in the context of security evaluations. The possibility to find more than one biometric reference that matches or the higher error rates of those systems are only two of them.

[2] The biometric identification process is not part of the TOE and therefore out of scope of this ST.

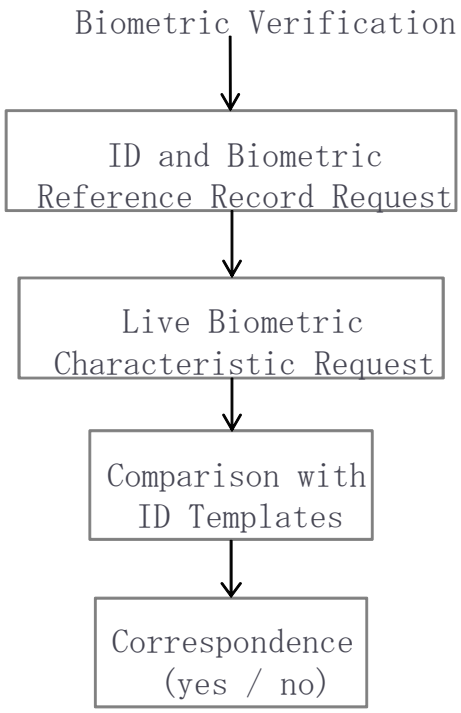

FIGURE 1: VERIFICATION FLOWCHART

1.3.3. TOE CONFIGURATION AND TOE ENVIRONMENT

The [BVMPP] mentioned that a biometric system in general could be realized in two major configurations:

- A Stand-alone solution:

  The stand-alone solution is not integrated into another network and works with one database

- A Network-integrated solution:

  The network-integrated solution is embedded into an existing network.

This ST describes a biometric system for biometric verification.

The performance of biometric systems depends on physical environmental conditions in its environment. This ST specifies how the environment has to be for the TOE. The ST also

specifies the IT components which are necessary to run the TOE (e.g. a PC with a specific operation system).

1.3.4. TOE BOUNDARY

Figure 2 shows the specific function of the TOE.

In this ST, the capture device is a part of the TOE.

The database where the biometric references and other information is stored in, is a part of the TOE.

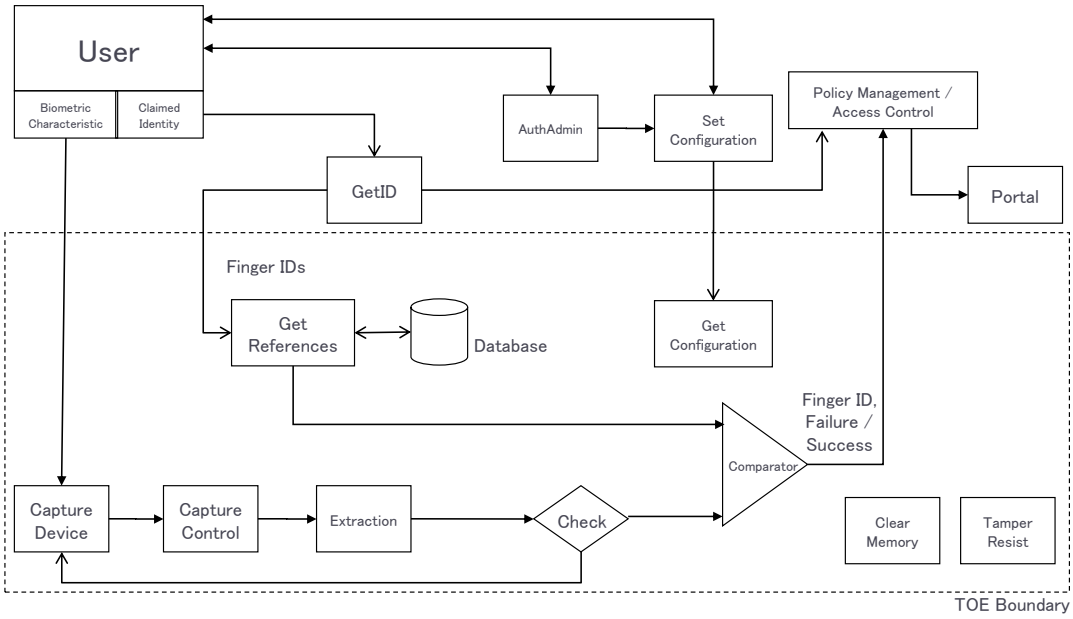

FIGURE 2: SPECIFIC TOE DESIGN FOR BIOMETRIC VERIFICATION

- Get ID:

  When a UserID is inputted into this component, it outputs FingerIDs corresponding to the UserID. The reason why FingerIDs become plural is that one user can enroll his/her vein information for multiple fingers,.

  In this ST, this component is outside of the TOE, the application using the TOE needs handle claimed identities. The application decides Finger IDs (unique ID labeled to biometric references) that corresponds to identity obtained from the user, and sends Finger IDs to the TOE.

- GetReferences (same as GetRef):

  This component receives FingerIDs outputted by GetID and extracts corresponding biometric references from the database.

  In this ST, this is part of the TOE.

  The TOE receives Finger IDs sent from the application and gets corresponding biometric references from a database.

- Extraction:

  In preparation of the biometric verification process a feature vector has to be extracted from the captured data. This is the objective of this component.

  In this ST, this is part of the TOE. In addition to the general model of [BVMPP] the TOE specific Figure 2 contains an additional block called “capture control”. This indicated the fact, that the TOE contains functionality to control the capture device.

- Check:

  This component ensures the minimum quality requirements regarding the biometric references. It can be differentiated into integrity and authenticity check during the process of getting the biometric reference as well as the quality check of the biometric information during the processing of the live biometric characteristics.

  In this ST, the TOE checks integrity and authenticity of all the biometric references stored in a database when the TOE starts. So the TOE does not check integrity and authenticity of the biometric references in each biometric verification process (therefore,

the component “Check” of biometric references is not described in Figure 2). A quality check of live biometric characteristics is done in biometric verification process.

- AuthAdmin:

  This component is responsible for identification and authentication of the administrator with other means than the biometric mechanism itself. This mechanism is a classical identification and authentication component that could for example be realized via a SmartCard/PIN based mechanism. It is necessary to authenticate an administrator before configuring security relevant settings of the TOE.

  In this ST, this component is outside of the TOE scope. The application using the TOE needs to implement this functionality.

- Set Configuration:

  This component provides an interface for the administrator to set security relevant TOE parameters. And this component gets over to Store Configuration. This component is especially used to configure the threshold setting for the comparator component.

  In this ST, this component is outside of the TOE. Therefore the application developer using the TOE needs to implement configuration management in the application.

- Get Configuration:

  This component provides an interface to receive the security relevant TOE parameters which is set by Set Configuration. And this component stores and manages the security relevant TOE parameters in TOE.

  In this ST, this component is a part of TOE.

- Comparator (also called Matcher):

  This component compares biometric references extracted by GetReference with Biometric Live Record (BLR). It corresponds to the Figure 1 on the whole since it takes User ID as argument and compares biometric references with BLR.

  This is an important component regarding the scope of this ST. It compares the enrolled biometric reference with the Biometric Live Record (BLR) and includes the determination whether these records match or not. A comparator produces a value that

shows how well the biometric reference and BLR match. To get a successful/failed return value from the biometric system, the comparator considers a threshold during the matching process. If the biometric reference and the BLR are more similar than demanded by the threshold, the result of matching is success, otherwise it is fail.

The TOE compares biometric references, and returns Finger ID to the application if biometric reference by which the result of matching becomes success is only one.

On the other hand, when there are two or more biometric references by which the result of matching becomes success, or the result of all biometric references becomes fail, the TOE returns "failure" to the application.

When "Exact match" comparison, that is, value that shows how well the biometric reference and BLR match is zero, it is not judged the result success.

- Clear memory:

  In order to protect against attacks, this component clears the content of memory after use. The information that has to be cleared is not limited to the biometric verification result but especially includes the biometric reference, BLR or any biometric raw data.

  In this ST, the biometric references are cleared when the TOE is shut down, and BLR or any biometric raw data is cleared when the biometric verification process is finished.

  Because the memory that has to be cleared could belong to every other component no lines are drawn into the figure for this component.

  For the data under control of the application using the TOE, that application itself is of course responsible.

- Capture Device:

  This component that is also called sensor is responsible for capturing the biometric characteristic from the user. Depending on the used sensor technology also additional processes as a spoof detection or an image enhancement could be performed by this device.

  The capture device is a part of the TOE.

- Policy manager:

  The result of the biometric verification process is passed on to the policy manager of the

environment. This component is responsible for checking the user's rights and opening the portal if the user has sufficient privileges and was successfully verified by the TOE and is therewith realizing an access control mechanism for the portal.

As mentioned before the TOE passes the result of the comparator to the application which uses the TOE. All more specific decisions (whether a user with a specific identity has specific rights for the Portal Service) is up to the application or to the Portal Service itself. In any case the Policy Manager is outside the TOE.

- Storage:

  The TOE has to provide a database. This is used to store the biometric reference of a user but it can be used to store additional information too.

  UBR2 has the case to use database outside and inside. In this ST, only the case with database inside the TOE is targeted.

- Portal:

  The physical or logical point beyond which information or assets are protected by the TOE is controlled by the TOE environment policy management, which gets the biometric verification results ("failed" or "successful") from the TOE.

  As mentioned before the specific connection to the Portal Service is out of scope of the TOE and depends on the overall application using the TOE.

- Transmission / Storage:

  The environment cares for a secure communication and storing where security relevant data is transferred to or from the TOE.

- Tamper Resist:

  This component is responsible for resisting the physical tampering to the UBR2 device while the TOE is running. IF UBReader2 is opened physically, this component deletes data in the SDRAM of the TOE and the authentication engine and templates in flash memory are deleted. Afterwards, UBR2 will be locked even if it is rebooted.

1.3.5. Physical Scope and Logical Scope

A simplified model of the TOE and its boundaries is shown in Figure 3. The capture device is displayed in Figure **4**.

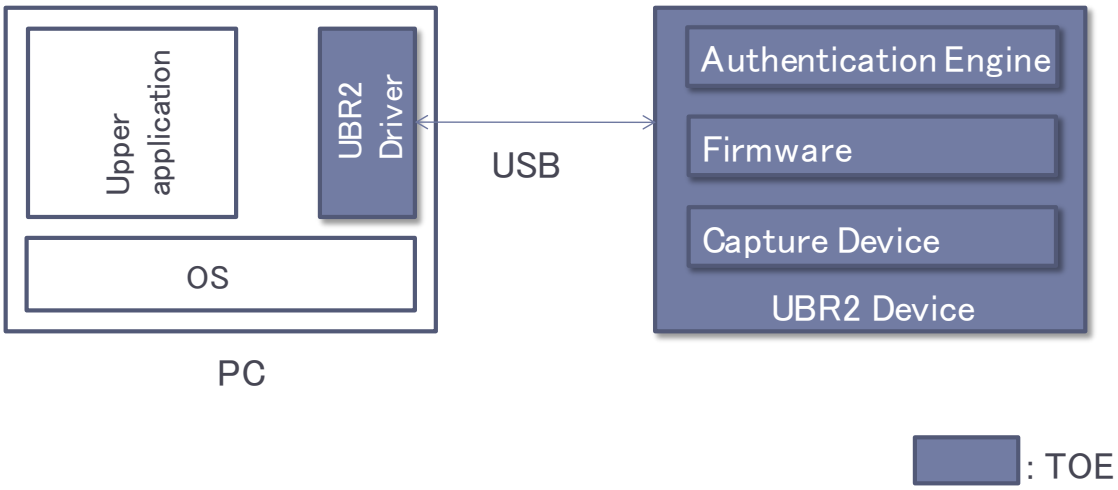

Figure 3: Physical Scope

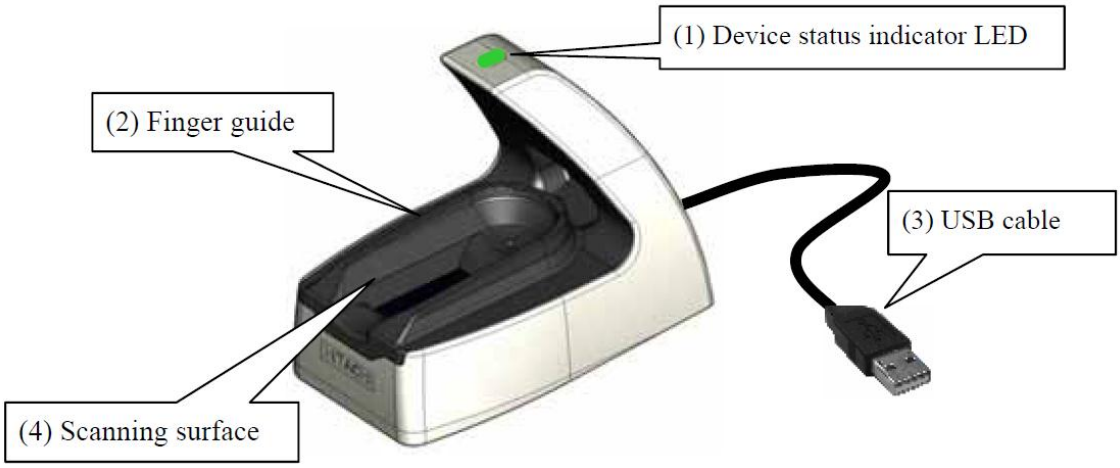

Figure 4: Capture Device

In contrast to the model assumed by the [BVMPP] the capture device is a part of the TOE, see the TOE boundary indicated in Figure **2**. Therefore the TOE is not a pure software system. It therefore consists of two parts as shown in Figure 3.

- The software part of the TOE is a device driver including an API which is used by an application running on a PC.
- The hardware part of the TOE is a device (which itself also contains firmware for its internal operation).

There are two kinds of models of UBR2 device. The difference of each model is only presence of the cable dropout prevention mechanism. The difference is not provided as security functionality in the device.

The TOE is accompanied by its related guidance documentation.

The logical scope of the TOE is best described by enumeration of the provided security functionality:

- Verification of user identity with finger vein patterns (1:1 matching using device internal database)
- Data protection by deletion of residual information
- Protection against physical tampering and replay attacks

Functionality that builds up a trusted channel between UBReader2 device and the device driver is not part of the TOE security functionality.

The TOE contents can be described as follows:

TABLE 1: TOE CONTENTS

TOE contents		Reference / Version
UBReader2 device		TS-E3F1-700UW (USB interface model)
		TS-E3F1-700UWP (USB interface model with cable dropout prevention mechanism)
	Revision	D
	Firmware	020300
	Engine	020300
	Driver	010400
	Firmware INI	010002
UBReader2 Programs & Documents		TS-E3F1-70WCD Ver.03-00
	Device driver	03-00-00
	UBReader2 Users Manual	See [USR_MAN]
	UBReader2 Device Driver Installation Manual	03
	UBReader2 Extra Error Code	02
	UBReader2 Finger Placement Guide	01
	CC Guidance Addendum	See [AGD]

Note: Users shall contact a sales representative of Hitachi-Omron Terminal Solutions in order to learn how to verify the integrity of the CD-ROM. The necessary process is also described in [AGD].

1.3.6. NON-TOE HARDWARE, SOFTWARE, OR FIRMWARE

The following hardware and software is required for the operating environment:

- Hardware (Standard PC)

  Required free RAM: min. 3MB

  Required free HDD memory: min. 5MB (except for log data)

  Connection interface: USB1.1/USB2.0

- Software (OS)

  Windows® XP Professional (32bit), Windows Vista® Business (32bit),

  Windows® 7 Professional (32 bit)

- Software (Application)

  An application that utilizes UBReader2 and integrates its device driver to provide authentication functionality and management functionality to administrators.

2. CONFORMANCE CLAIMS

2.1. CC CONFORMANCE CLAIMS

This ST has been developed using Version 3.1 R3 of Common Criteria [CC].

This ST is conform to part 2 and 3 of [CC]; no extended components have been defined.

2.2. PP CLAIM

This ST does not claim conformance to any Protection Profile.

2.3. PACKAGE CLAIM

This ST conforms to assurance package EAL2 as defined in Common Criteria Part 3.

3. SECURITY PROBLEM DEFINITION

3.1. EXTERNAL ENTITIES

The following external entities interact with the TOE:

- Application developer:

  The application developer integrates the TOE in its own application (e.g. a portal) by accessing the device driver of the TOE.

- Administrator:

  The administrator is authorised to perform the administrative operations and able to use the administrative functions.

  The administrator is also responsible for the installation and maintenance of the TOE and the application.

- User:

  A person who wants access to the portal, which is protected by the TOE.

- Authorised user:

  An enrolled user with an assigned identity.

- Attacker:

  An attacker is any individual who is attempting to subvert the operation of the TOE. The intention may be to gain unauthorized access to the assets protected by the portal.

3.2. ASSETS

The following assets are defined in the context of this ST.

- Primary assets:

  The primary assets which are protected against unauthorised access do not belong to the TOE itself. The portal in the environment permits access only after successful

authentication as a result of the biometric verification. The primary assets, either physical or logical systems, are behind that portal.

- Secondary assets:

  Assets (i.e. TSF data), which are used by the TOE itself. The following assets should be explicitly mentioned:

  ► Biometric Reference Record (BRR):

  This object includes the enrolled biometric data labeled finger ID which is linked with the identity of a user. It is produced during the enrolment process and assumed to be given and quality checked. Finger ID, that is, correspondence between enrolled biometric data and identity of a user is managed by the application which uses the TOE. Therefore, the way of implementation for management is depending on the application, and the protection of the correspondence information is responsibility of the application.

  ► Biometric Live Record (BLR):

  This record includes the live (actual) biometric data (actual biometric characteristic) to be verified against the biometric reference.

  ► Threshold level:

  Threshold level is sent from the application that uses TOE to the TOE each time the biometric verification process is initiated.

  ► Boolean match decision:

  The Boolean match decision is returned by the device to indicate whether a biometric verification was successful or not.

  ► Pairing key:

  The pairing key is used to associate a UBReader2 device with a device driver installed on a PC. The key is generated by the device driver and sent to UBReader2 device during initialization.

3.3. ASSUMPTIONS

A.ADMINISTRATION

The administrator is well trained, non hostile, and reads the guidance documentation carefully, completely understands and applies it.

The administrator is responsible to accompany the TOE installation and oversees the biometric system requirements regarding the TOE as well as the TOE settings and requirements.

A.ENROLMENT

The enrolment is assumed to be already securely performed and therefore, the biometric reference for each authorized user is assumed to be given. The generated reference is of sufficient quality and is linked to the correct user.

A.ENVIRONMENT

It is assumed, that necessary TOE operating equipment and adequate infrastructure is available (e.g.: operating system, database, LAN, and guardian).

Specifically the following things are assumed:

- It is assumed that the direct environment of the TOE supports the functionality of the TOE. Regarding the request of the claimed identity, which is necessary for the biometric authentication, the environment offers the possibility to integrate a claimed identity into the biometric verification process.

- The environment is assumed to implement the access control functionality for the protected portal. Specifically, if the environment has more than one portal that is secured using the services of the TOE the environment is assumed to ensure that after authentication of a user (by the TOE) a portal is only opened if the user has the necessary permission.

- The environment is assumed to ensure a secure communication of security relevant data from and to the TOE.

- The environment ensures a secure communication between the TOE components by physical means.

- It is assumed that the TOE environment is free of viruses, trojans, and malicious software.

- The TOE is a piece of equipment that uses near-infrared light to capture finger vein data without being in physical contact with the finger. Thus the near-infrared light from natural light (sunlight), incandescent lamps, mercury lamp and halogen lamps in the environment can reduce the authentication accuracy. Therefore it is assumed that the capture device is not exposed to direct sunlight, incandescent lamps, mercury lamp and halogen lamps.

- The UBReader2 device is assumed to be stored in a secure environment (e.g. locked storage room) whenever it is not in use and powerless. Before the powerless device is brought into operation, the administrator is assumed to check the security seal and verify that the device has not been opened.

A.PHYSICAL_DRIVER

It is assumed that the UBReader2 device driver installed on the PC is physically protected against unauthorized access or destruction. Physical access to PC is only allowed for authorized administrators. This does not cover the UBReader2 device that has to be accessible for every user.

A.FALLBACK

It is assumed that a fall-back mechanism for the TOE is available that reaches at least the same level of security as the TOE does. This fall-back system is used in cases where an authorized user is rejected by the TOE (False Rejection).

A.ROLES

An application using the TOE shall restrict its management functionality to authenticated and authorized administrators. Other users are not allowed to manage the TOE.

A.AUTH_ADMIN

An application using the TOE shall provide a mechanism to authenticate an administrator with other means than the biometric verification process. This authentication process may be realized via a user name/password or a smartcard/pin based mechanism.

3.4. THREATS

T.BRUTEFORCE

An attacker may perform a brute force attack in order to get verified by the TOE using the identity of another user.

In this way the attacker is trying to get access to the assets residing in the environment that should be protected with the support of the TOE.

This threat considers two different threat agents and corresponding adverse actions:

- A not really hostile user who just tries to get verified with a wrong claimed identity a few times. The motivation of such a user is usually just curiosity. The hostile user does not need specific knowledge about the TOE to perform this attack.
- A real attacker who uses a large amount of biometric characteristics and who really wants to get unauthorized access to the portal. This type of threat agent is supposed to have further public knowledge on biometric systems.

T.MODIFY_ASSETS

An attacker may try to modify secondary assets like biometric references, threshold, pairing key, or the boolean decision.

Such attacks could compromise the integrity of the user security attributes resulting in an incorrect result that might give unauthorized access to the portal.

This threat covers a number of distinct types of attacks:

- An attacker may attempt to modify the threshold level used by the TOE to authenticate users. If the attacker is able to change the threshold (for one or more authorised users), the ability to verify the user(s) will be compromised and the attacker may succeed in gaining access to the portal or an authorised user may be denied entry to the portal.

- An attacker may attempt to modify the Boolean match decision, the pairing key, or the biometric authentication data (the Biometric Reference Record) of an authorised user with the aim of enabling an attacker to masquerade as the authorized user and gain access to the portal. Alternatively, an authorised user may be denied access to the portal. The attacker may be able to insert a new biometric reference, containing biometric data belonging to an attacker, with the aim of enabling the impostor to gain access to the portal.This kind of attack presupposes that the attacker has further knowledge about the TOE and maybe special equipment.

T.REPRODUCE

An attacker may try to record and replay, imitate, or generate the biometric characteristic of an authorised user.

In this way the attacker is trying to get access to the assets residing in the environment that should be protected with the support of the TOE.

The attacker will need further knowledge on biometric systems and the used biometric modality. Attackers may use technical equipment for analysing and generation of the biometric characteristics.

The attacker may also be supported by an authorized user of the TOE (e.g. to imitate his biometric characteristic).

T.RESIDUAL

An attacker may try to take advantage of unprotected residual security relevant data (e.g. biometric data and settings) during a user's session or from a previous, already authenticated user.

In this way the attacker tries to get access to the security relevant settings of the TOE.

This threat covers a following scenario including:

- An attacker takes advantage of the verification memory content (e.g. by reading the memory content, cache or relevant temporary data) using a flaw in a user visible interface of the TOE.

The attacker needs further knowledge about the TOE to find and exploit a vulnerability regarding residual data in memory.

Note: Because the TOE reads biometric characteristics from the vein structure of a finger, residual fingerprint images on the surface of the capture devices cannot be used by attackers to copy or replay the biometric characteristics.

3.5. OSPs

OSP.ERROR

The TOE shall meet recognised national and/or international criteria for its security relevant error rates (e.g. False Accept Rate (FAR) and False Rejection Rate (FRR)).

For the TOE a FAR of less than 0.001 is claimed.

4. SECURITY OBJECTIVES

4.1. SECURITY OBJECTIVES FOR THE TOE

O.BIO_VERIFICATION

The TOE shall provide a biometric verification mechanism to ensure access to a portal with an adequate reliability.

The TOE shall ensure that only suitable biometric references (i.e. records that have been created and stored by the TOE itself) are processed.

An “Exact match” comparison should not be counted as a positive verification as it may be a replay attempt.

The TOE shall meet national and/or international criteria for its security relevant error rates. For the TOE a FAR of less than 0.001 is claimed.

The TOE shall not authenticate forged biometric samples.

O.RESIDUAL

The TOE shall ensure that no residual or unprotected security relevant data remains after operations are completed.

O.PHYSICAL_DEVICE

TOE shall be able to resist physical tampering to the device under operation.

4.2. SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

OE.ADMINISTRATION

It has to be ensured that the administrator is well trained, non-hostile, and has to read the guidance documentation carefully, completely understand and apply it.

The administrator shall be responsible to accompany the TOE installation and oversees the biometric system requirements regarding the TOE as well as the TOE settings and requirements.

OE.ENROLMENT

The enrolment shall be already performed and therefore, the biometric reference for each authorized user is given. The generated references shall be of sufficient quality and linked to the correct user.

OE.ENVIRONMENT

The TOE operating equipment and adequate infrastructure shall be available (e.g.: operating system, database, LAN, public telephone, and guardian).

Specifically the following things have to be ensured:

- The direct environment of the TOE has to support the functionality of the TOE. Regarding the request of the claimed identity, which is necessary for the biometric authentication, the environment shall offer the possibility to integrate a claimed identity into the biometric verification process.
- The environment has to implement the access control functionality for the protected portal. Specifically, if the environment has more than one portal that is secured using the services of the TOE the environment has to ensure that after authentication of a user (by the TOE) a portal is only opened if the user has the necessary permission.
- The environment shall ensure a secure communication of security relevant data from and to the TOE.
- The environment shall ensure a secure communication between the TOE components by physical means.
- The TOE environment has to be free of viruses, trojan horses, and other malicious software.

- The TOE environment shall provide reliable time stamps.

- The TOE is a piece of equipment that uses near-infrared light to capture finger vein data without contacting the finger. Thus the near-infrared light from natural light (sunlight), incandescent lamps, mercury lamp and halogen lamps in the environment can reduce the authentication accuracy. Therefore the capture device is not exposed to direct sunlight, incandescent lamps, mercury lamp and halogen lamps.

- The UBReader2 device shall be stored in a secure environment (e.g. locked storage room) whenever it is not in use and powerless. Before the powerless device is brought into operation, the administrator shall check the security seal and verify that the device has not been opened.

OE.PHYSICAL_DRIVER

The PC installed the UBReader2 device driver shall be physically protected against unauthorized access or destruction. Physical access to the PC may only be allowed for authorized administrators. This may not cover the UBReader2 device that has to be accessible for every user.

OE.FALLBACK

A fall-back mechanism for the TOE shall available that reaches at least the same level of security as the TOE does. This fall-back system is used in cases where an authorized user is rejected by the TOE (False Rejection).

OE.ROLES

An application using the TOE shall restrict its management functionality to authenticated and authorised administrators. Other users are not allowed to manage the TOE.

OE.AUTH_ADMIN

An application using the TOE shall provide a mechanism to authenticate an administrator with other means than the biometric verification process. This

authentication process may be realized via a user name/password or a smartcard/pin based mechanism.

4.3. SECURITY OBJECTIVES RATIONALE

4.3.1. OVERVIEW

The following table gives an overview, how the assumptions, threats, and organisational security policies are addressed by the security objectives. The text of the following subchapters justifies this more detailed.

TABLE 2: SECURITY OBJECTIVES RATIONALE

	O.BIO_VERIFICATION	O.RESIDUAL	O.PHYSICAL_DEVICE	OE.ADMINISTRATION	OE.ENROLMENT	OE.ENVIRONMENT	OE.PHYSICAL_DRIVER	OE.FALLBACK	OE.ROLES	OE.AUTH_ADMIN
T.BRUTEFORCE	X									
T.MODIFY_ASSETS			X			X			X	X
T.REPRODUCE	X		X							
T.RESIDUAL		X								
OSP.ERROR	X									
A.ADMINISTRATION				X						
A.ENROLMENT					X					
A.ENVIRONMENT						X				
A.PHYSICAL_DRIVER							X			
A.FALLBACK								X		
A.ROLES									X	
A.AUTH_ADMIN										X

4.3.2. COVERAGE OF THE ASSUMPTIONS

The assumption A.ADMINISTRATION is covered by security objective OE.ADMINISTRATION as directly follows.

The assumption A.ENROLMENT is covered by security objective OE.ENROLMENT as directly follows.

The assumption A.ENVIRONMENT is covered by security objectives OE.ENVIRONMENT as directly follows.

The assumption A.PHYSICAL_DRIVER is covered by objective OE.PHYSICAL_DRIVER as directly follows.

The assumption A.FALLBACK is covered by objective OE.FALLBACK as directly follows.

The assumption A.ROLES is covered by objective OE.ROLES as directly follows.

The assumption A.AUTH_ADMIN is covered by objective OE.AUTH_ADMIN as directly follows.

For all assumptions, the corresponding objectives are stated in a way, which directly correspond to the description of the assumption. It is clear from the description of each objective that the corresponding assumption is covered.

4.3.3. COUNTERING THE THREATS

The threat T.BRUTEFORCE (using a large amount of possible biometric data to verify against a wrong claimed id) is fully countered by O.BIO_VERIFICATION. O.BIO_VERIFICATION ensures that the biometric verification process itself is done with an appropriate reliability and that the chance of impostor brute force attempts is less than the specified limit for the assurance claim of the TOE.

The threat T.MODIFY_ASSETS is countered by a combination of the objectives O.PHYSICAL_DEVICE, OE.ENVIRONMENT, OE.ROLES, and OE.AUTH_ADMIN. O.PHYSICAL_DEVICE prevents tampering with the database containing the BRRs. OE.ROLES is responsible to limit the access to security relevant objects of the TOE to authorized administrators. OE.AUTH_ADMIN is responsible to authenticate the administrator.

The threat T.REPRODUCE is fully countered by a security objective combination of O.BIO_VERIFICATION, and O.PHYSICAL_DEVICE. O.BIO_AUTHENTICATION ensures that forged biometric samples are not accepted. O.PHYSICAL_DEVICE prevents recording biometric characteristic of authorised user. And O.PHYSICAL_DEVICE prevents fraud such as opening the case and bringing an electrode into contact with the substrate to input counterfeit data, or rewriting BRR.

The threat T.RESIDUAL is fully countered by O.RESIDUAL. O.RESIDUAL directly protects against memory attacks as described in T.RESIDUAL.

4.3.4. COVERAGE OF ORGANISATIONAL SECURITY POLICIES

The organisational security policy OSP.ERROR (the TOE must meet criteria for security relevant error rates) is directly met by O.BIO_VERIFICATION as this objective describes that the biometric verification mechanism has to reach the security relevant error rates as required by OSP.ERROR.

5. EXTENDED COMPONENT DEFINITION

This ST does not use any extended functional or assurance components.

6. SECURITY REQUIREMENTS

This chapter describes the security functional and the assurance requirements which have to be fulfilled by the TOE. Those requirements comprise functional components from part 2 of [CC] and the assurance components as defined for the Evaluation Assurance Level 2 part 3 of [CC].

The following notations are used:

- Refinement operation (denoted by **bold text**): is used to add details to a requirement, and thus further restricts a requirement.
- Refinement operation (denoted by ~~**bold crossed out text**~~): is used to remove unnecessary details of a requirement, though it does not change the meaning of the requirement.
- Selection operation (denoted by underlined text): is used to select one or more options provided by the [CC] in stating a requirement.
- Assignment operation (denoted by *italicised text*): is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- Iteration operation: are identified with a number inside parentheses (e.g. "(1)")

6.1. SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE

The following table summarises all TOE functional requirements of this ST:

TABLE 3: FUNCTIONAL REQUIREMENTS

Class FDP : User Data Protection	
FDP_RIP.1	Subset residual information protection
Class FIA : Identification and Authentication	
FIA_UAU.2	User authentication before any action
FIA_UAU.3	Unforgeable authentication
Class FPT : Protection of the TSF	
FPT_PHP.3	Resistance to physical attack
FPT_RPL.1	Replay detection

6.1.1. USER DATA PROTECTION (FDP)

RESIDUAL INFORMATION PROTECTION (FDP_RIP)

FDP_RIP.1 SUBSET RESIDUAL INFORMATION PROTECTION

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] the following objects: [*authentication functionality using unencrypted biometric data in SDRAM*].

Hierarchical to: No other components

Dependencies: No dependencies

6.1.2. IDENTIFICATION AND AUTHENTICATION (FIA)

USER AUTHENTICATION (FIA_UAU)

FIA_UAU.2 USER AUTHENTICATION BEFORE ANY ACTION

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Hierarchical to: FIA_UAU.1

Dependencies: FIA_UID.1

Application Note: The security relevant error rate of the biometric verification function that is used to realize this authentication has to be lower than or equal to the value for those rates demanded by OSP.ERROR.

UNFORGEABLE AUTHENTICATION (FIA_UAU.3)

FIA_UAU.3 UNFORGEABLE AUTHENTICATION

FIA_UAU.3.1 The TSF shall [detect **and prevent**] use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall [detect **and prevent**] use of authentication data that has been copied from any other user of the TSF.

Hierarchical to: No other components

Dependencies: No dependencies

Application Note: Please note that this SFR refers to authentication data of already enrolled users. The enrollment process is assumed to be secure and will therefore assure that authentication data belongs to a human being.

6.1.3. PROTECTION OF THE TSF (FPT)

TSF PHYSICAL PROTECTION (FPT_PHP)

FPT_PHP.3 RESISTANCE TO PHYSICAL ATTACK

FPT_PHP.3.1 The TSF shall resist [*modifying and reading the security relevant data (i.e. threshold level, Boolean match decision, pairing key and BRR) in physical way*] to the [*device part of the TOE under operation*] by responding automatically such that the SFRs are always enforced.

Hierarchical to: No other components.

Dependencies: No dependencies.

REPLAY DETECTION (FPT_RPL)

FPT_RPL.1 **EXACT MATCH** REPLAY DETECTION

FPT_RPL.1.1 The TSF shall detect **exact match** replay for the following entities: [*biometric live record data*].

FPT_RPL.1.2 The TSF shall ~~**perform**~~ [*reject the replayed data*] when replay is detected.

Hierarchical to: No other components.

Dependencies: No dependencies.

6.2. SECURITY ASSURANCE REQUIREMENTS FOR THE TOE

The TOE assurance requirements for the TOE evaluation and its development and operating environment are taken from Evaluation Assurance Level 2 as shown in the following table:

TABLE 4: ASSURANCE REQUIREMENTS

Assurance Class	ID	Assurance component	Refinement
Development	ADV_ARC.1	Security architecture description	No
	ADV_FSP.2	Security enforcing functional specification	No

Assurance Class	ID	Assurance component	Refinement
	ADV_TDS.1	Basic design	No
Guidance documents	AGD_OPE.1	Operational user guidance	No
	AGD_PRE.1	Preparative procedures	No
Life-cycle support	ALC_CMC.2	Use of a CM system	No
	ALC_CMS.2	Parts of the TOE CM coverage	No
	ALC_DEL.1	Delivery procedures	No
Security Target Evaluation	ASE_CCL.1	Conformance claims	No
	ASE_ECD.1	Extended components definition	No
	ASE_INT.1	ST Introduction	No
	ASE_OBJ.2	Security objectives	No
	ASE_REQ.2	Derived security requirements	No
	ASE_SPD.1	Security problem definition	No
	ASE_TSS.1	TOE summary specification	No
Tests	ATE_COV.1	Evidence of coverage	No
	ATE_FUN.1	Functional testing	No
	ATE_IND.2	Independent testing	No
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis	No

6.3. SECURITY REQUIREMENTS RATIONALE

6.3.1. SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

6.3.1.1. FULFILMENT OF THE SECURITY OBJECTIVES

This chapter proves that the set of security requirements (TOE) is suited to fulfill the security objectives described in chapter 4 and that each SFR can be traced back to the security objectives. At least one security objective exists for each security requirement.

TABLE 5:FULFILMENT OF SECURITY OBJECTIVES

	O.BIO_VERIFICATION	O.RESIDUAL	O.PHYSICAL_DEVICE
FDP_RIP.1		X	
FIA_UAU.2	X		
FIA_UAU.3	X		
FPT_PHP.3			X
FPT_RPL.1	X		

The following paragraphs contain more details on this mapping.

O.BIO_VERIFICATION

- FIA_UAU.2 states that each user has to be successfully authenticated by the biometric mechanism before performing any action.
- FIA_UAU.3 ensures that no forged or copied authentication data can be used for authentication
- FPT_RPL.1 ensures that the TOE rejects biometric authentication data that matches to a biometric reference too well. Such an "exact match" is likely to be the result of a replay attack.

O.RESIDUAL

- This objective is completely covered by FDP_RIP.1 as directly follows.

O.PHYSICAL_DEVICE

- This objective is completely covered by FPT_PHP.3 as directly follows.

6.3.1.2. FULFILLMENT OF THE DEPENDENCIES

The following table summarises all TOE functional requirements dependencies of this ST and demonstrates that they are fulfilled.

TABLE 6: SECURITY FUNCTIONAL REQUIREMENTS

SFR	Dependencies	Fulfilled by
FDP_RIP.1	None	-
FIA_UAU.2	FIA_UID.1	Identification is performed by the application in the operational environment of the TOE.
FIA_UAU.3	None	-
FPT_PHP3.	None	-
FPT_RPL.1	None	-

6.3.2. SECURITY ASSURANCE REQUIREMENTS RATIONALE

The assurance level EAL2 has been chosen, because this is the level defined by the [BVMPP] and is the level, for which comparable biometric devices have been evaluated.

EAL2 has been chosen because it provides a basic assurance that the TOE operates as specified in the ST.

6.3.2.1. DEPENDENCIES OF ASSURANCE COMPONENTS

The dependencies of the assurance requirements taken from EAL2 are fulfilled automatically.

7. TOE SUMMARY SPECIFICATION

This chapter describes how the TOE realises the SFRs defined in chapter 6.1.

The finger vein imaging system and the features of UBReader2 device is described in the following.

- Finger vein imaging system

Blood vessels are not exposed to outer part of human body and their network patterns are normally impossible to see within the range of visible light wavelength. The approximately 0.3 to 1.0 mm vein which constitutes the network patterns are visualized by near infrared rays. It is well known that hemoglobin absorbs near infrared rays more than other substances that comprise human body. Since most of the hemoglobin in human body exists in red blood cells that are flowing inside blood vessels, the blood vessel network patterns can be seen as dark area by infrared imaging systems. Near infrared LEDs and a near infrared camera are used to capture the raw image of finger vein in the imaging systems and a special image processing algorithm is applied to extract the biometric features.

- Features of UBReader2 device

UBReader2 device is so called a “comparison-on-device” finger vein reader. The comparison-on-device reader is equipped with a CPU and memory that executes both enrolment and authentication processes inside the reader itself. The feature of this system is that all algorithms and data required for biometric authentication are enclosed in a tamper-proof casing. UBReader2 device is connected with a PC by a USB cable. The device driver software of UBReader2 installed on the PC controls the UBReader2 device through the cable. Any finger vein images or any finger vein features do not go out from the UBReader2 device because it is a “comparison-on-device” reader described above.

7.1. DATA PROTECTION

FDP_RIP.1, "Subset residual information protection" is realised by the TOE as follows:

The authentication function deletes all unencrypted biometric data (biometric live records, templates) that resides in SDRAM after the authentication finished and before the result is returned.

7.2. I&A

FIA_UAU.2, "User authentication before any action" is realised by the TOE as follows:

The device part of the TOE reads the biometric raw data of the user, processes the raw data and compares the result with the biometrics reference templates stored in the internal database of the device. The ID of the template is provided by the application using the TOE via the driver part of the TOE. The result of the comparison (authentication successful or not) is returned to the application, which can then decide to allow further actions to the user. Which actions these are is up to the application and out of the scope of the TOE.

For the TOE a FAR of less than 0.001 is claimed.

FIA_UAU.3, "unforgable authentication" is realised as follows:

The TOE provides spoof detection to detect and reject forged fingers that bear the biometric characteristics of a real enrolled person. It is an inherent feature of the vein recognition technology.

It is very difficult to create forged fingers, because the vein structure lies inside human bodies and cannot be seen in visible light. Furthermore, there is no residual information left on the capture device that could be used to copy the finger vein structure.

FPT_RPL.1, "Replay detection" is realised as follows:

When a comparison of biometric live data to a reference template yields an "Exact match" the TOE rejects the finger to counter replay attacks.

7.3. TAMPER RESISTANCE

FPT_PHP.3, "Resistance to physical attack" is realised by the TOE as follows:

The device part of the TOE under operation can automatically resist the physical access to internal data. If the device of UBReader2 is opened physically, this component deletes all data in the SDRAM of the TOE and the authentication engine and templates in flash memory are deleted..

8. APPENDIX

8.1. REFERENCES

[CC] Common Criteria for Information Technology Security Evaluation, Ver.3.1R3

[BVMPP] Biometric Verification Mechanisms Protection Profile, Ver.1.3

[AGD] UBReader2 Guidance Documentation Addendum, Version 1.6, 2011-12-05

[USR_MAN] Finger Vein Authentication Device UBReader2 User's Manual, 1st Edition, R5,August 2011.