



BIOMETRIC TECHNOLOGY SECURITY EVALUATION UNDER THE COMMON CRITERIA

Version 1.2
September 2001

Issued by:
**Communications Security Establishment
Certification Body**
Canadian Common Criteria Evaluation and Certification Scheme

© 2001 Government of Canada, Communications Security Establishment

Electronic Warfare Associates-Canada, Ltd., under contract to the Communications Security Establishment, conducted a study of Biometric Evaluation Methodologies under the Common Criteria and provided the basis for this document.

EXECUTIVE SUMMARY

The purpose of this work is to clarify, modify or define appropriate security functions and assurance requirements for evaluations of biometric products under the Common Criteria (CC). In addition, appropriate evaluation methodologies are also defined. For the purposes of this study, a mature biometric technology (fingerprint) is used as a basis. However, other technologies are also considered.

This study differentiates between performance- and security-oriented testing. Briefly, performance testing is defined as testing to determine which of two or more devices is best, or the most efficient, cost-effective device that meets application requirements. Security testing on the other hand is testing to determine how the device meets security functional and assurance requirements.

Significant findings include:

- Security evaluations of biometric targets of evaluation (TOEs) are not the same as performance evaluations. However, key elements of accepted performance evaluation practices are applicable to security evaluations, namely: modes of operation; uniqueness and robustness; false match (FM) / false non-match (FNM) rates; and environment influences.
- Models representing biometric functions can assist in the identification of applicable functional and assurance requirements.
- The environment has a significant impact in the evaluation of a biometric TOE, in terms of supporting the identification of both functions and vulnerabilities. The characterisation factors defined herein assist in the determination of TOE application as well as associated vulnerabilities.
- Most of the security functions require additional explanation and guidelines in their application to biometric TOEs; in particular: FAU - Security Audit; FCS - Cryptographic Support; FDP – User Data Protection; FIA – Identification and Authentication; FMT – Security Management; FPR – Privacy; FRU – Resource Utilisation; and FTA – TOE Access. FCO – Communication is not considered relevant to biometric TOE security evaluations.
- Assurance requirements are generally applicable to biometric TOEs. However, AGD – Guidance, ATE-Tests, AVA - Vulnerability Assessment, and ALC - Life Cycle Support require significant explanation and guidelines in their application to biometric TOEs.
- The assurance requirements assigned by EAL1 through 4 are applicable to biometric evaluations with the caveat that the recommended guidelines and recommendations be considered.
- The potential strength of function (SOF) of a biometric can be determined in a qualitative fashion, based on the documented evidence of the uniqueness and robustness of the biometric. However, the SOF of the biometric device requires a more rigorous, quantitative approach.
- FM and FNM rates can be used as means of determining SOF.

- FM and FNM rate claims must be supported by appropriate testing that take into account the factors and criteria defined in this report.
- Due to the probabilistic nature of FM and FNM rates, an associated factor is critical with respect to biometric TOE evaluations – threshold settings: their determination, setting and control.
- Testing to determine SOF (through FM and FNM rates) is problematic in terms of sample size, type and quality. Different approaches are provided; however, in the short term, sample size required to determine FM and FNM within a defined confidence interval should be based on the methods presented in section 8.6.
- Many organisations are working to develop best practices in terms of performance evaluations of biometric products. These practices, as they are developed and used, should be reviewed for security evaluation purposes.

This study identifies the CC security functions and assurance requirements, and evaluation methodologies that are considered “weak” with respect to biometric TOE evaluations. The issues are identified and guidelines to address them are provided. However, how best to implement them in the CC is left to the Canadian Scheme certifier. It is recommended that:

- the two representations (context and level 0) of biometric functional models defined herein be adopted for evaluations, especially to assist in the identification of applicable functional and assurance requirements;
- the environment characterisation factors defined herein be adopted to assist in the determination of TOE applications and associated vulnerabilities;
- the following security functions consider the recommended explanation and guidelines provided: FAU - Security Audit; FCS - Cryptographic Support; FDP – User Data Protection; FIA – Identification and Authentication; FMT – Security Management; FPR – Privacy; FRU – Resource Utilisation; and FTA – TOE Access, FPT – Protection of the TSF, FTP- Trusted Path/channels;
- the following assurance requirements adopt the recommended explanations and guidelines provided: AGD – Guidance, ATE-Tests, AVA - Vulnerability Assessment, and ALC - Life Cycle Support;
- the assurance requirements assigned by EAL1 through 4 be deemed applicable to biometric evaluations with the caveat that the recommended guidelines be considered;
- the potential SOF of a biometric be determined in a qualitative fashion, based on the documented evidence of the uniqueness and robustness of the biometric;
- FM and FNM rates be used as means of determining SOF;
- the concept of employing the statistical formula provided herein for determining appropriate sample size for the calculation of FM and FNM rates be adopted until further work in establishing best practices is conducted and accepted by the biometric community; and
- all of the presented conclusions and recommendations be verified during actual biometric TOE evaluations.

TABLE OF CONTENTS

1	INTRODUCTION.....	1
1.1	BACKGROUND.....	1
1.2	PURPOSE.....	2
1.3	REFERENCES.....	2
1.4	ACRONYMS AND DEFINITIONS.....	3
2	CC EVALUATION OBJECTIVES.....	4
3	STUDY METHODOLOGY.....	5
4	SCOPE.....	6
5	BIOMETRIC SYSTEM FUNCTIONS.....	6
5.1	GENERAL.....	6
5.2	BIOMETRIC FUNCTIONAL MODELS.....	7
5.2.1	General.....	7
5.2.2	Capture Biometric Sample.....	9
5.2.3	Extract Biometric Feature.....	10
5.2.4	Create Template.....	10
5.2.5	Create BIR.....	11
5.2.6	Compare Template.....	11
5.2.7	Decide Match.....	11
5.2.8	Decide Acceptance.....	11
5.2.9	Transmit.....	11
5.2.10	Store Reference Template/BIR.....	11
5.2.11	Retrieve Reference Template/BIR.....	12
5.2.12	Release User Data.....	12
5.2.13	Encrypt / Decrypt.....	12
5.3	ENVIRONMENT FUNCTIONS.....	12
5.4	SECURITY CONSIDERATIONS FOR TEMPLATES AND BIR.....	12
5.5	TRUSTED PATH.....	13
6	APPLICABLE SECURITY FUNCTIONAL REQUIREMENTS.....	13
6.1	GENERAL.....	13
6.2	SECURITY AUDIT.....	14
6.3	COMMUNICATION.....	15
6.4	CRYPTOGRAPHIC SUPPORT.....	15
6.5	USER DATA PROTECTION.....	16
6.6	IDENTIFICATION AND AUTHENTICATION.....	17
6.7	SECURITY MANAGEMENT.....	19
6.8	PRIVACY.....	20
6.9	PROTECTION OF TOE SECURITY FUNCTIONS.....	21

6.10	RESOURCE UTILISATION	22
6.11	TOE ACCESS	22
6.12	TRUSTED PATH / CHANNELS	23
7	APPLICABLE SECURITY ASSURANCE REQUIREMENTS	23
7.1	GENERAL	23
7.2	DISCUSSION OF ASSURANCE REQUIREMENTS.....	24
7.2.1	AGD - Guidance Documents	24
7.2.2	ATE - Tests	24
7.2.3	AVA - Vulnerability Assessment	25
7.2.4	ALC – Life Cycle Support.....	26
7.3	EVALUATION ASSURANCE LEVELS	27
8	TEST AND ANALYSIS - ISSUES AND GUIDELINES	27
8.1	PERFORMANCE- VERSUS SECURITY-ORIENTED EVALUATIONS.....	27
8.2	MODES OF OPERATION	29
8.3	UNIQUENESS AND ROBUSTNESS OF A BIOMETRIC.....	30
8.4	ENVIRONMENT FACTORS.....	32
8.5	FALSE-MATCH AND FALSE NON-MATCH.....	33
8.6	DETERMINATION OF BIOMETRIC SOF	35
8.7	THRESHOLD SETTINGS	38
9	PROPOSED EVALUATION METHODOLOGIES AND GUIDELINES.....	40
9.1	GENERAL	40
9.2	EAL1 EVALUATIONS	41
9.3	EAL2 EVALUATIONS	41
9.4	EAL3 EVALUATIONS	42
9.5	EAL4 EVALUATIONS	42
9.6	FM AND FNM RATE CALCULATION GUIDELINES	42
10	CONCLUSIONS AND RECOMMENDATIONS	44
10.1	CONCLUSIONS	44
10.2	RECOMMENDATIONS	45

LIST OF FIGURES

Figure 1 – Study Approach.....	5
Figure 2 - Generic Biometric Functional Model - Context Representation.....	8
Figure 3 - Generic Biometric Functional Model – Level 0 Representation	9
Figure 4 - Example of FM and FNM Rate Comparison [Wayman 1].....	34
Figure 5 - Distance Distributions.....	39
Figure 6 - Sample Distance Distribution for an Iris-Based Biometric System.....	40

LIST OF TABLES

Table 1 - Biometric Functions and Security Functional Requirements.....	14
Table 2 - Biometrics Overview.....	31

BIOMETRIC TECHNOLOGY SECURITY EVALUATION UNDER THE COMMON CRITERIA

1 INTRODUCTION

1.1 BACKGROUND

The Common Criteria (CC) is used as the basis for evaluation of security properties of Information Technology (IT) products and systems. The CC provides a common set of functional requirements for IT products and systems as well as assurance requirements that permit the establishment of levels of confidence that security functions and assurance measures applied to them meet these requirements. An important goal of CC-based evaluations is to help consumers determine whether an IT product is secure enough for its intended use and whether implicit risks are tolerable.

Biometric devices are relatively new in the security industry. Their promising potential in identification- and verification-based applications has been widely published and acclaimed. However, their breakthrough in terms of market sales and wide-spread use has been “on the verge” for longer than expected. It has been suggested that consumer confidence and understanding have been factors in holding back this breakthrough. Consequently, biometric product vendors are looking for ways to gain advantages in terms of capability, price and consumer confidence. Some are looking to CC evaluations as a means of gaining advantages through consumer confidence.

However, the proper and complete evaluation of biometric technology products is not explicitly catered for under the current version of the CC. Successful implementation of biometric products is highly dependent on both the application and the environment. These application and environment dependencies as well as technical issues (i.e., biometric-specific security functions and assurance requirements) are not adequately covered under the CC and must therefore be defined before any comprehensive evaluations can occur. To further complicate matters, biometric testing is problematic and still a developing discipline. Performance of any biometric technology is dependent on the nature of the application. Location, environmental factors, demographics of user population and many other variables impact test results and must therefore be carefully evaluated and stated. The testing methodology implicit in the CCs Common Evaluation Methodology must be carefully assessed in light of these biometric testing issues and requirements.

In support of the continuing development of the Canadian evaluation scheme, the requirement to maintain currency with technologies targeted for CC evaluations and to improve the application and appropriateness of the CC, development work is required to specifically address biometric technology evaluation requirements under the CC. The results of this work will benefit both Canadian CC evaluation laboratories and the international CC Mutual Recognition community.

1.2 PURPOSE

The purpose of this work is to clarify, modify or define appropriate security functions and assurance requirements for evaluations of biometric products under the Common Criteria. In addition, appropriate evaluation methodologies are defined. For the purposes of this study, a mature biometric technology (fingerprint) is used as a basis. However, other technologies are also considered.

1.3 REFERENCES

- [Ashbourn] Ashbourn, J. Series on Biometric Papers, www.biometric.freemove.co.uk/, 1999.
- [BioAPI] BioAPI Consortium, *BioAPI - H-Layer Specification Version 0.52*, December 21, 1999.
- [Campbell] Campbell, J., Communique – Biometric Testing Factors, (available at www.biometrics.org/biotesting.html).
- [CESG] Communications Electronic Security Group, *Biometrics Testing – Business Case*, November, 1999.
- [CESG2] Communications Electronic Security Group, *Best Practices in Testing and Reporting Performance of Biometric Devices*, Version 1.0, 12 January, 2000.
- [Domus] Domus Security Division, LGS Group Inc., *Communications Security Establishment Biometrics Research*, Version 1.0, March 1999.
- [Hustinx] Hustinx, P.J. (Chairman, Registratiekamer), *At Face Value – on Biometrical Identification and Privacy*, available at www.registratiekamer.nl/bis/top_1_5_35_1.html .
- [Intel] Intel Corporation, *User Authentication Services, Application Programming Interface*, Draft Release 1.0, May 1999.
- [Negen] Negen, M. et al, *An Iris Biometric System for Public and Private Use*, Computer Magazine, February 2000.
- [Phillips] Phillips, P.J., Martin, A. Wilson, C.L. Przybocki, M., *An Introduction to Evaluating Biometric Systems*, Computer Magazine, February 2000.
- [Roethenbaugh1] Roethenbaugh, G., *Biometric Buyer's Guide and Certification Findings*, ICSA, May 1998.
- [Roethenbaugh2] Roethenbaugh, G., *Biometric's Survey*, Information Security Magazine, February, 1999.

[SAEGM] SAEGM Morpho, Inc. *Fingerprint Identification Technology in Civil Applications*, 1998.

[Shen] Shen, W., Surette, M., Khanna R., *Evaluation of Automated Biometrics-Based Identification and Verification Systems*, IEEE, Vol 85, No. 9, September 1997.

[Strassberg] Strassberg, D. *Biometrics: You are your password*, EDN Access, May 1998 (available at www.ednmag.com/ednmag/reg/1998/050798/10cs.htm).

[Wayman1] Wayman, J.L., *Biometric Identification Standards Research, Final Report Volume 1*, December 1997.

[Wayman2] Wayman, J.L., *Biometric Technology – Testing, Evaluation, Results*, CardTech/SecurTech’99, May 1999.
(see also: www.engr.sjsu.edu/biometrics/publications_technology.html .)

[Wayman3] Wayman, J.L., *Fundamentals of Biometric Technologies*, Proceedings of CardTech/SecurTech’99, May 1999.

[Wayman 4] Wayman, J.L., *Technical Testing and Evaluation of Biometric Identification Devices*, in Jain, et al, eds. *Biometrics: Personal Identification in Networked Society*, Norwell, MA: Kluwer, 1999.

1.4 ACRONYMS AND DEFINITIONS

AFIS	Automated Fingerprint Identification System
API	Application Program Interface
BIR	Biometric Identification Record
CC	Common Criteria
CEM	Common Evaluation Methodology
DNA	Deoxyribonucleic Acid
EAL	Evaluation Assurance Level
FM	False Match
FNM	False Non-Match
HD	Hamming Distance
I&A	Identification And Authentication
ID	Identification
IT	Information Technology
NBTC	National Biometric Test Centre
ROC	Receiver Operating Curves
PDF	Probability Distribution Function
SOF	Strength Of Function
TOE	Target Of Evaluation
TSF	Target Of Evaluation Security Function
TSP	Target Of Evaluation Security Policy

Biometric: A measurable, unique physiological feature or behavioural trait used to recognise the identity or verify the claimed identity of an individual.

Verification and Identification: For the purposes of this study, a distinction is made between verification and identification. For verification, the user is required to claim an identity (by either entering a PIN, presenting a token or some other user input) and then verifying this claim by providing a live biometric sample. The resulting match or non-match depends on the predefined parameters. It is a one-to-one comparison. For identification, a particular template is not called up; the system compares the live sample against all database templates – a one to many comparison. Comparisons are listed in order of similarity.

Security Target: A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

TOE (Target of Evaluation): An information technology product or system and its associated administrator and user guidance documentation that is the subject of a CC evaluation.

TSF (TOE Security Function): A set consisting of all hardware, software and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TSP (TOE Security Policy): A set of rules that regulate how assets are managed, protected and distributed within a TOE.

2 CC EVALUATION OBJECTIVES

There are two primary objectives in a CC evaluation: to provide assurance that a product, as designed (and as claimed by the developer), meets security functional requirements appropriate to a given threat; and to provide assurance that the developer has followed an appropriate process for design and development of their product. The term assurance can be defined in many ways depending upon the specific aspect being examined or the viewpoint being adopted. However, in the majority of cases it can be said that it includes the notion of trust and also that of confidence. Information technology security refers to assurance in many contexts. At the very highest level it can be characterised as the confidence or trust that a customer can have that an organisation, system, product or service will perform as expected.

A more refined version of the notion expressed above, and one that is more specific to security, is the confidence that an organisation's product or system will fulfil its security objectives. From the customer's point of view this may be expressed as "the organisation, product, system or service will comply with their security needs."

Security evaluation objectives are as follows:

- a. Does the target of evaluation (TOE) meet the user's trust and confidence expectations?

- b. Does the TOE meet the security functions specified in Security Target?
- c. Does the TOE meet the assurance requirements specified in the Security Target?
- d. Does the TOE provide the claimed level of assurance and is the claimed level of assurance appropriate?
- e. Is the evaluation repeatable?
- f. Is the evaluation objective?

A security evaluation is neither a measure of system performance nor a determination of which biometric technology is best. It is a measure against technology-independent security requirements.

3 STUDY METHODOLOGY

The approach used in identifying new or modifications to functional and assurance requirements and evaluation methodologies is illustrated in Figure 1. A generic biometric functional model is proposed and used to highlight the “challenges” in security evaluations of a biometric TOE both in terms of function (i.e., security functional requirements) and development process (i.e., assurance requirements). Test and analysis issues identified in industry and academia related to biometric devices are considered in the proposed new or modified requirements and evaluation methodologies. The analysis with respect to the suitability of current security functional and assurance requirements is conducted at the family and component level for each class of requirements. As well, an assessment of the stated dependencies for each of the functional and assurance requirements is also made. If required, modifications or clarifications are proposed. In addition, guidelines are proposed to assist CC evaluators.

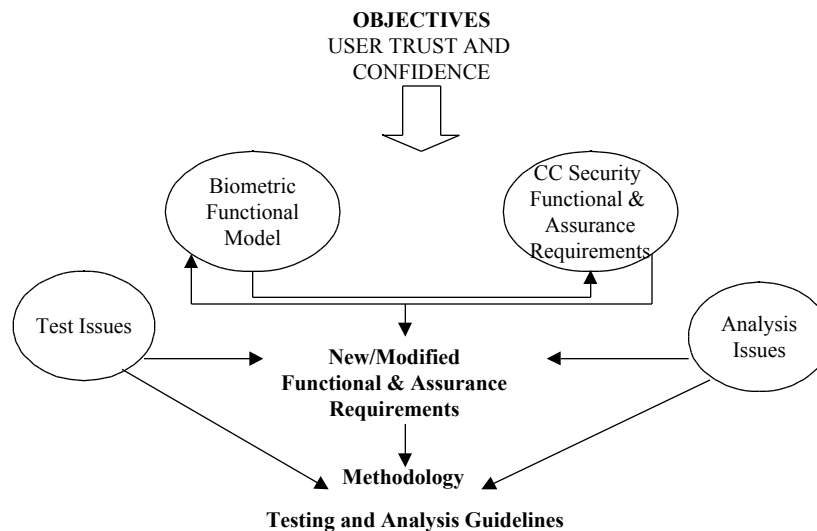


Figure 1 – Study Approach

4 SCOPE

Biometric function is defined as ...“automatic methods for the identification or identity verification of individuals based on physiological or behavioural characteristics” [Wayman 1]. Therefore, for the purposes of this study, methods using DNA are not considered, since as yet, this method is not considered “automatic”.

Identification and verification alone conveys no privileges, unless these privileges are somehow “appended” to the successful identification or verification. A resource manager (e.g., access control application to a network or system) on whose behalf the identification or verification is performed by the biometric TOE may use the positive ID to verify a set of credentials, e.g.:

- a. unlock a set of secrets, or a single secret associated with that identity that can be used for further verification and acquisition of privileges; or
- b. activate a specific account (e.g., local operating system, network operating system, bank account) and convey its privileges on the verified user for a session.

Therefore, for the purposes of this study, a biometric TOE is always associated with a Resource Manager and is intended to identify or verify for authorisation purposes.

5 BIOMETRIC SYSTEM FUNCTIONS

5.1 GENERAL

At a high-level, several biometric system functional models have been proposed [Wayman 1 and Wayman 3]. The major functions of a biometric TOE are defined as follows:

- a. **Data Collection** – A biometric TOE samples the raw biometric data and outputs a one- or multi-dimensional signal. The pattern is presented to the TOE (in a pre-determined standard manner) and then transduced into an electronic signal. In some cases, quality control is exercised to determine if the signal is acceptable or not.
- b. **Signal Processing** – A biometric TOE takes the signal and creates a template using a proprietary algorithm. This template maintains the uniqueness features of the raw sample. The template created may be used either as a reference against which other collected templates will be compared, or one that will be compared against a previously constructed reference template.
- c. **Decision** – A biometric TOE compares a collected template with a stored template. If the comparison measurement is close (as determined by some threshold) than a match is declared; if not a non-match is declared.
- d. **Transmission** – A biometric TOE can collect data in one location and process it in another.

- e. Store - A biometric TOE can store the created templates either in the TOE or in some external storage medium.

This description is used as a basis for further defining biometric TOE functions in order to highlight the “challenges” with respect to CC evaluations. In this vein, the primary purpose of the proposed functional model representation of a biometric TOE is to assist in the identification of security evaluation issues. It serves as a focal point by which each of the CC functional and assurance requirements are considered against each of the major functions of a biometric TOE and to assist in the determination for the need to add, modify or clarify functional and assurance requirements.

5.2 BIOMETRIC FUNCTIONAL MODELS

5.2.1 General

The functional model is defined in two ways: a *context* representation, which highlights the external entities that interface with a TOE and a *level 0* representation, which highlights the main functions of a TOE, the interfaces among them and with the external entities.

The diagram below (Figure 2) is a context representation. The external entities are defined as follows:

- a. Resource Manager – relies on the biometric TOE to verify the identity of a potential user of the resource. It may also determine the acceptable threshold for determining a match or non-match between a sample and reference biometric template (Note: In some configurations, this is done by the biometric device). It determines the appropriate security policy that governs the acceptance and rejection criteria for the presented biometric sample. The Resource Manager also provides the user’s rights and privileges (part of the User Data flow) that are bound to the reference biometric template.
- b. User Registry (optional; may be contained within the Biometric function) – contains the biometric reference templates against which all samples are compared. Could be distributed among other servers, databases or other devices.
- c. User – a person wishing access to the resource through the Resource Manager. The user provides the biometric to the TOE. In the case of a biometric identification system, the user provides no claim of identity and their biometric sample is compared against all those in the User Registry in search of a match. A biometric authentication system requires the user to claim a specific identity by some means (ex. typing a user ID, smartcard) and the biometric sample serves as their means of authentication to this identity.

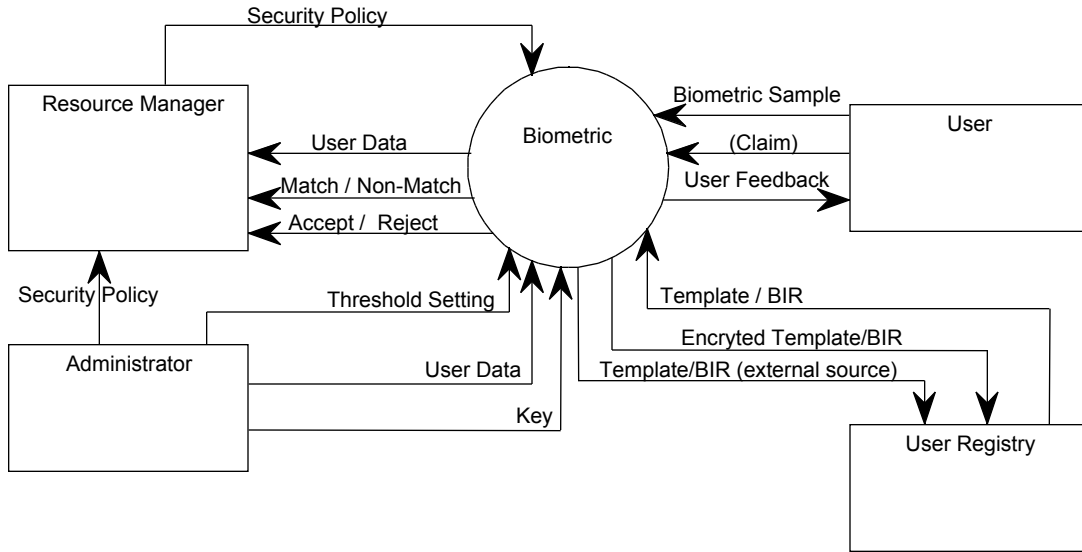


Figure 2 - Generic Biometric Functional Model - Context Representation

What is important to highlight from the context representation is that the biometric function informs the Resource Manager as to whether the User has been successfully identified or authenticated (depending on whether the system is used for identification or authentication). Once a match has occurred, then the pre-defined rights and privileges are granted to the user.

Furthermore, the context diagram supports the identification of the functional and assurance requirements that are most relevant to biometric evaluations. It would not be practical for the purposes of this study to consider every conceivable scenario in the use and evaluation of biometric TOEs and thus comment on each possible security functional and assurance requirement. What is conceivable is using the major capabilities of biometric TOEs as a basis for identifying which of the currently defined functional and assurance requirements are the **important** biometric evaluation requirements. The major capabilities are defined as follows:

- a. how accurately and consistently can the biometric TOE determine whether a user is who he/she is or claims to be to be in a given environment;
- b. how is the binding between template and user used to control and protect Resource access by the user; and
- c. how does the biometric TOE protect the user biometric (in terms of confidentiality, integrity and availability).

These criteria are used to select from among the functional and assurance classes, families and components those requirements that are most relevant to biometric security evaluations.

Detailed analysis of the functional and assurance requirements is based on a further definition of the biometric functions. This is illustrated by a level 0 diagram (see Figure 3), which defines in more detail the functions that provide the inputs to the external entities and how the outputs from these entities are managed. Functional models have been defined in the BioAPI Standard – H-Layer Specification Version 0.52, dated 21 December 1999 and User Authentication Services Application Program Interface, Version 2.0, May 1999. Although these models serve their purpose well for illustrating a generic biometric model, more detail is required to highlight and address security issues. Hence, the following is defined:

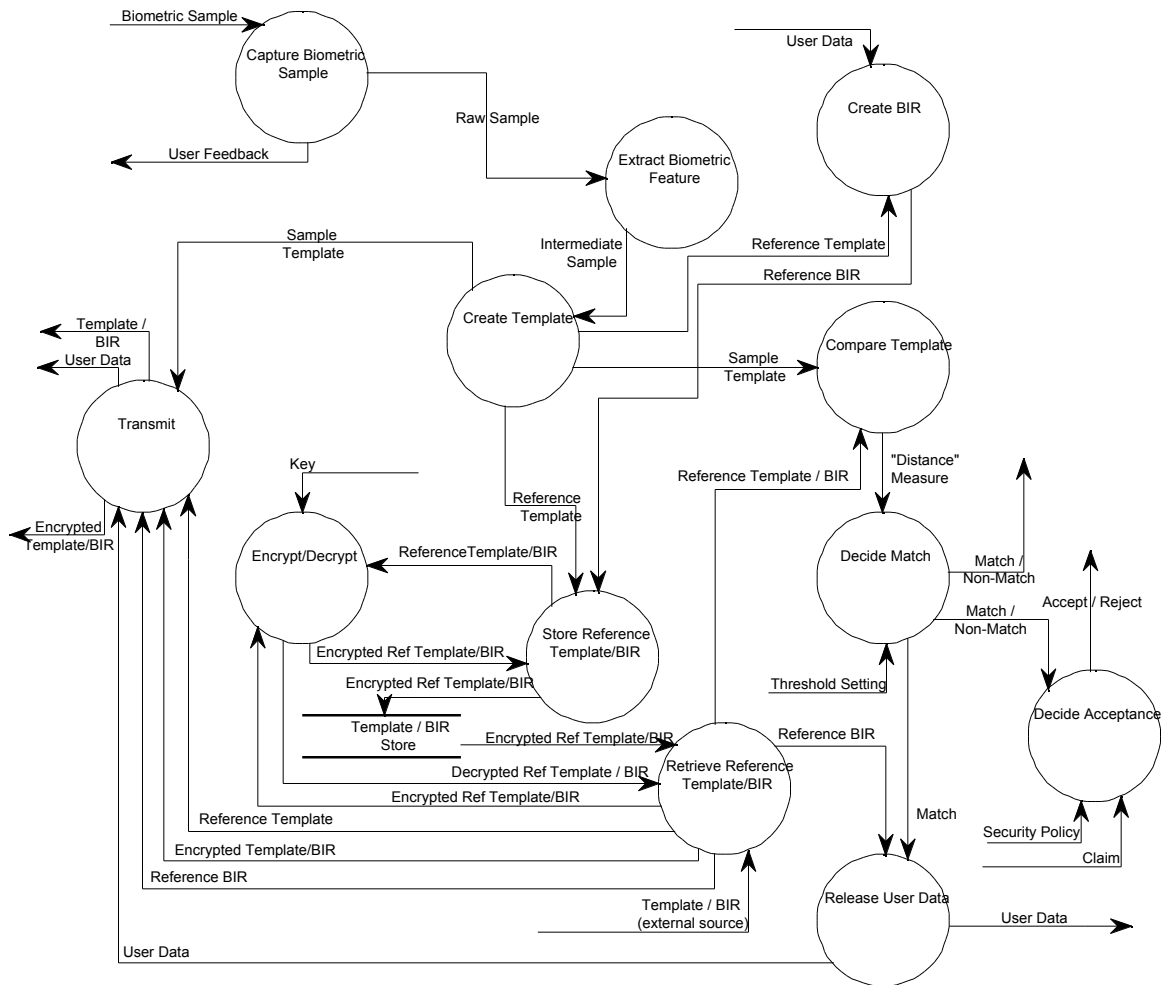


Figure 3 - Generic Biometric Functional Model – Level 0 Representation

5.2.2 Capture Biometric Sample

This functions includes:

- a. Enrolment-type capture; and

b. Verification-type capture

This function is defined as the automatic capture or measurement of the physiological or behavioural characteristic(s) of a person. The characteristics of this function depend on the TOE mode: enrolment or verification. In enrolment, the initial capture of the biometric is done and the link between the biometric and the individual is established. Thus, an important relationship exists in this critical phase with the environment (see Section 5.3), since the linking can only be done with proper identification references as witnessed by some administrator who assigns the captured biometric to an individual. With respect to the TOE, quality standards of the captured biometric are expected to be high during enrolment, since this forms the basis against which all further biometric comparisons are made. Multiple captures are typically required in enrolment so that the “best” biometric is used as the reference. During verification, typically a single capture is required for basis of comparison. However, in both cases, each device type will have certain criteria and procedures defined for the capture function. For example, in a fingerprint device, the capture must include the centre part of the fingerprint to ensure the maximum number of characteristic features of the print (i.e., ridges, bridges, bifurcations, and enclosures that make up the minutia markers). Tips or sides of fingertips are not accepted. For facial recognition devices, some require the person to be in a standard position directly facing the capture device. For other devices, other criteria and procedures must be clearly defined to ensure a standard (repeatable) capture process. These must be clearly defined in the evaluation process.

5.2.3 Extract Biometric Feature

This function extracts and preserves the distinct and repeatable biometric features from the “system” capture-representation of the sample. This function is critical from a security evaluation point-of-view, since the uniqueness characteristic of the biometric must be maintained after extraction (and later in the creation of a template).

5.2.4 Create Template

The template is defined as a device-specific representation of the biometric sample. It may be produced by the digital compression of analogue information. It represents the measured distinct and repeatable features of the biometric.

For the purposes of this study, a template can be a sample template (type used for verification process) or a reference template (one captured during the enrolment process and typically stored).

This function creates the template from the biometric feature through a usually proprietary algorithm or process. Inherent in this function is quality control, wherein through some mechanism, the sample is rated for quality. If the quality is not acceptable, the process is repeated. It should be noted that eliminating poor images used to create a template during enrolment by increasing the failure to enrol rate can decrease the false match and false non-match rates (see Section 8.5).

5.2.5 Create BIR

This function creates the Biometric Identification Record (BIR). A BIR includes the reference template and other data associated with the user. The data is appended in some way to the reference template.

5.2.6 Compare Template

This function includes the comparison of sample and reference templates. It may include the determination of “distance” measures between templates, which is a mathematical representation of the likeness or similarity between two templates. This function also includes the extraction of the reference template from the BIR.

5.2.7 Decide Match

This function includes the determination if templates match or not, based on data provided by the Compare Template function. Since templates are not accurate representations of the original raw sample and may be different among separate collections, this function also includes a threshold setting function. This includes the establishment of threshold “distances” below which a template does not match the reference. Threshold settings are discussed further in Section 8.7. Note that in some configurations, this function is done by the Resource Manager.

5.2.8 Decide Acceptance

This function includes the implementation of security policy that defines the rules for the acceptance or rejection of template against a reference template. The decision is then made using the match / non-match data from the Decide Match function. The decision may also be based on other corroborating evidence such as a claim to identity (username, PIN, etc.).

5.2.9 Transmit

This function includes the passing of system specific data from one location (or device) to another. Depending on the size of the biometric template, some compression and expansion functions may be required. Security issues related to this function include a determination of susceptibility to replay attacks and data capture during transmission.

5.2.10 Store Reference Template/BIR

This function includes the storage of reference templates and BIRs for comparison. Template storage options are summarised as follows:

- a. template within the biometric TOE;
- b. template remotely stored in a central repository; and
- c. template stored on a portable token (e.g., smart card).

Some systems may encrypt any templates or user data that are stored. Security issues related to this function include a determination of accessibility of the stored templates from unauthorised sources and the integrity and availability of the template.

5.2.11 Retrieve Reference Template/BIR

This function includes the extraction of BIRs and reference templates from external sources (external repository, smartcard, or some other token). Security issues related to this function include a determination of susceptibility to replay attacks and data capture.

5.2.12 Release User Data

This function separates user data from the template only if a MATCH is determined by the TOE. User data may then be provided to the Resource Manager or transmitted to an external system.

5.2.13 Encrypt / Decrypt

This function encrypts and decrypts data using a known encryption/decryption algorithm. A key is required for both encryption and decryption. This function is used to protect the template when stored in or transmitted through an unprotected environment. This function is considered optional, but is used in many biometric device architectures.

5.3 ENVIRONMENT FUNCTIONS

For any biometric system, it is assumed that, during enrolment, the true identity of an individual is verified outside the biometric system's context. The sample presented by the individual and linked to an identity is accomplished in a secure environment by trusted individuals.

The registration/enrolment process is key to the success of the use of any biometric TOE. It is analogous to the issuance of certificates for PKI – there is an implicit trust in the process that proper verification of the enrolled person has taken place before the identity is “assigned” to the biometric.

5.4 SECURITY CONSIDERATIONS FOR TEMPLATES AND BIR

Templates and other biometric samples are considered to be very sensitive information – they identify and are bound to people. It is the template that is used to determine the necessary credentials of a potential user of a resource and the user's rights and privileges to access a resource. Prior to the template being bound to the credentials, privileges, rights, etc., and thus forming a BIR, it is at its most vulnerable state. An attacker may try to substitute his/her own template to masquerade as the intended user.

Any time a template is disassociated from its binding with the user for the purpose of verification or identification, there is the possibility of a substitution attack. An appropriate means of protecting the unbound template, while transported or transmitted through an accessible, unprotected medium, must be considered. The possibility of somehow duplicating the device-specific format of the biometric must also be considered in an evaluation (higher levels of assurance; EAL4 and up). This must be done through the analysis of the proprietary algorithms that transform the biometric into the template used by the device for matching, determining the output of the algorithm and then determining the likelihood of duplicating the output through some means (e.g., brute force).

5.5 TRUSTED PATH

The path that templates and user credentials take within the biometric TOE and between the biometric TOE and a Resource Manager or some other external (e.g., storage device) must be trusted to behave in a manner that it is impossible (or at least prohibitively expensive) for an attacker to “sniff” or inject at any point in the path. This design feature is critical whenever the TOE concept includes storage or transmission of biometric templates outside a protected environment. The approach taken by a developer to provide a trusted path must be considered.

6 APPLICABLE SECURITY FUNCTIONAL REQUIREMENTS

6.1 GENERAL

The following section documents the assessments of security functional requirements (as defined in the CC, Part II) that: apply to the generic biometric system functions as written; require some modification; do not necessarily apply; and require new security functional requirements be defined. Table 1 below identifies which of the currently defined security functions (by class) apply to the biometric system functions; however, with the caveat that the recommended guidelines and explanations defined for some of the functions are considered. The analysis of security functional requirements is based on the more important (and relevant) classes, families and components (see discussion in Section 5.2.1). The paragraphs that follow discuss some of the issues related to these requirements.

BIOMETRIC SYSTEM FUNCTIONS	SECURITY FUNCTIONAL REQUIREMENTS										
	Security Audit	Communication	Cryptographic Support	User Data Protection	Identification and Authentication	Security Management	Privacy	Protection of TOE Security Functions	Resource Utilisation	TOE Access	Trusted Path / Channels
Capture Biometric Sample					x	x	x	x	x	x	
Extract Biometric Sample					x	x	x	x	x	x	
Create Template	x		x	x	x	x	x	x	x	x	
Create BIR	x		x	x	x	x	x	x	x	x	
Compare Template					x		x	x	x	x	
Store Reference Template/BIR	x		x	x			x	x		x	x
Decide Match	x				x	x	x	x	x	x	
Decide Acceptance					x	x	x	x	x	x	
Encrypt/Decrypt			x				x	x	x	x	
Transmit			x	x			x	x		x	x
Release User Data	x			x		x	x	x		x	
Retrieve Reference Template / BIR	x			x			x	x		x	x

Table 1 - Biometric Functions and Security Functional Requirements

6.2 SECURITY AUDIT

This class defines requirements for monitoring user activities, detecting violations of security policies. These functions are defined to help monitor security-relevant events and act as a deterrent against security violations.

Biometric TOEs depend on a protected environment and trusted administrator during the enrolment phase. In the case of a distributed architecture (where the reference templates are stored and retrieved from an external data store), the verification process assumes that the reference template comes from the “trusted” (known) source with the correct user identifier appended to the template. Therefore, processes involved in the enrolment phase (i.e., initial user enrolment, user re-enrolment (due to modified biometric or use of additional biometrics), and user deletion) or verification phase (verification acceptance or rejection, template retrieval) may be subject to security audit requirements. In particular, the security functional families related to recognising (FAU_ARP), recording (FAU_GEN) and storing (FAU_STG) are considered relevant to certain architectures for biometric applications. These would be defined in the TOE security target, using the FAU_SEL (Security Audit Event Selection) family.

This Security Audit class may be relevant to the following system functions:

- a. Create Template;
- b. Create BIR;
- c. Store;
- d. Decide Match;
- e. Release User Data; and
- f. Retrieve Reference Template/BIR.

Security policy in a biometric system is defined, in part, to determine conditions for acceptance and rejection of a biometric sample presented to the system. The decision is based on threshold levels set in the biometric product and may be audited. Violations may include re-setting threshold levels, spoofing, re-play, emulating decision result and changing decision result.

The current definition of the FAU class of requirements can be suitably interpreted to accommodate the definitions of security audit requirements as they relate to biometrics.

6.3 COMMUNICATION

This class defines requirements for non-repudiation of origin and receipt. It is of interest to systems that are used for the transportation of information.

Non-repudiation of origin or receipt of biometric data is not considered relevant to biometric TOEs. Establishing that an originator cannot deny having sent a biometric template or that the TOE cannot deny having received it does not provide assurance with respect to a biometric TOE.

6.4 CRYPTOGRAPHIC SUPPORT

This class defines requirements for the use of cryptographic support to satisfy high-level security objectives, including, but not limited to, identification and authentication, non-repudiation, trusted path, trusted channel and data separation. It is used when a system implements cryptographic functions through hardware, firmware, software or a combination. The class is composed of two families: cryptographic key management and cryptographic operation (i.e. operational use of the keys). FSC_CKM defines requirements for key generation, distribution, access and destruction and FSC_COP defines requirements for cryptographic operations.

This class is relevant to biometric systems. In general, biometric systems can either store the reference template (against which comparisons of sample templates are made) in the device itself, on a chip card (e.g. smart card) that is always kept by the user or in a centralised database (which in some cases may be publicly accessible) of templates. In the first two cases, this design can be such that template protection can be ensured. However, whenever the architecture concept includes retrieving a template from a centralised database or transporting the template across a public domain, a means of ensuring the protection of the template is required. Cryptography is a means used in some biometric systems to ensure trusted paths and channels, and privacy and protection

of the biometric template. In some cases it is also used for application-specific user data. In order to protect the template from modification or replacement when it resides outside a protected environment, some systems encrypt the template with internally-generated encryption keys and decrypt when inside a protected environment. This ensures the privacy of the user's biometric template, a critical factor in the social acceptance of the technology.

These functions are applicable to the following generic biometric functions:

- a. Create Template;
- b. Create BIR;
- c. Store;
- d. Encrypt/Decrypt; and
- e. Transmit.

The current definition of the FCS class of requirements can be suitably interpreted to accommodate the definitions of cryptographic support requirements as they relate to biometrics.

6.5 USER DATA PROTECTION

This class defines a significant set of functional requirements for a biometric system in terms of protecting user data within the biometric TOE, during import, export and storage, as well as security attributes directly related to user data.

User data can take several forms with respect to biometric systems; two forms are considered in this report. The first is the actual biometric itself, whether it is the reference or a sample used for comparison. It is understood that without any direct association between the biometric sample and an individual, a biometric TOE can not establish true or real identity. This must be done during the time of enrolment with documentation outside the biometric TOE, through confirmation of records, identity papers, affidavits, etc. However, due to the socially sensitive nature of these samples (see Section 6.8), these templates must be afforded the protection associated with "user data" and therefore subject to all the protective measures defined by this class of security functions. At issue is the threat of:

- a. reversing the template creation process and re-constructing the original image of the fingerprint, retinal pattern, etc;
- b. somehow fraudulently modifying the template;
- c. copying the template for malicious use outside the TOE; and/or
- d. replacing a template within the TOE with an attacker's.

As well, once templates are deleted, it is also reasonable to expect that they are no longer accessible to another user.

The second form of user data is the data appended to a template in order to define the individual's access rights and privileges to a system which is dependent on the

biometric TOE for identification or verification. This second form is prevalent in systems that “release” user data once the individual has been verified.

For both definitions of user data, the following families of User Data Protection may be applied to biometric TOEs:

- a. FDP_ACC – Access Control Policy;
- b. FDP_ACF – Access Control Functions;
- c. FDP_DAU – Data Authentication;
- d. FDP_ETC – Export to Outside TSF Control;
- e. FDP_ITC – Import from Outside TSF Control;
- f. FDP_IFC – Information Flow Control Policy;
- g. FDP_IFF – Information Flow Control Functions;
- h. FDP_ITT – Internal TOE Transfer;
- i. FDP_RIP – Residual Information Protection;
- j. FDP_ROL - Rollback
- k. FDP_SDI – Stored Data Integrity;
- l. FDP_UCT – Inter TSF User Data Confidentiality Transfer Protection; and
- m. FDP_UIT – Inter TSF User Data Integrity Transfer Protection.

This class may apply to the following generic biometric functions:

- a. Create Template;
- b. Create BIR;
- c. Store;
- d. Transmit;
- e. Release User Data; and
- f. Retrieve Reference Template / BIR.

The current definition of the FDP class of requirements can be suitably interpreted to accommodate the definitions of user data protection requirements as they relate to biometrics.

6.6 IDENTIFICATION AND AUTHENTICATION

This functional requirement includes unambiguous identification of a person (or entity) performing functions in a TOE. It represents requirements to establish the claimed identity of each user and verify that each user is indeed who he/she is claimed to be. For most applications, the biometric TOE provides the “password” that another system or application relies on for unambiguous identification. However, in this case, how the biometric system performs the unambiguous identification may come under evaluation – in other words, how unambiguous is the biometric characteristic that is measured (behavioural or physiological).

Biometric standards and vendors differentiate between identification and verification/authentication. Identification is the process of recognising a person without any claim to identity. Verification/authentication is the process of verifying the claimed

identity of a person. With respect to biometric products, identification means a match determination must be made against each of the stored reference templates (i.e., a one-to-many comparison). On the other hand, verification means that a claim is provided (e.g., username, userID) along with the sample template. This claim points to the reference template that is to be used in the match determination (i.e., a one-to-one comparison).

Some components of the FIA class address the requirements to establish and verify “claimed” identity of the user. An interpretation of “claimed” identity can be made as follows. A biometric TOE has been used to collect and store the biometrics of a large population for purposes of controlling access to information. A user, wishing to gain access to the information, is prompted by the biometric TOE to provide a sample biometric. No claim to identity is provided - i.e., the TOE must perform a one-to-many search and determine if a suitable match exists. However, the user’s “claim” in this case can be interpreted to mean that the user claims to exist in the database of biometric samples. The claim in this case is not a username or identifier of any type. Therefore, the “claimed identity” as defined in the CC is appropriate for biometric TOE applications.

The issue of “unambiguous identification” requires further discussion. Biometrics are implicitly not 100% unambiguous; they are close. Even though human characteristics may be unique, the technology and techniques used for measuring these characteristics have a built-in tolerance. This is due to the inaccuracies of the applied techniques and the different circumstances under which the characteristics are presented and measured. This tolerance results in false match rates and false non-match rates (see a discussion in sections 8.3 and 8.5). These two rates are inversely related – a lower false match rate (related to how many unauthorised persons will be falsely matched to a reference template) will result a higher false non-match rate (related to authorised persons not being matched to the reference template) and vice versa. Therefore, an acceptable balance between these two rates is required (see discussion in section 8.7) to approximate the “unambiguous identification” requirement for this security function.

Based on the above discussion, the following families (and their components) may be applied to biometric TOEs:

- a. FIA_AFL – Authentication Failures;
- b. FIA_ATD – User Attribute Definitions;
- c. FIA_UAU – User Authentication;
- d. FIA_UID – User Identification; and
- e. FIA_USB – User Subject Binding.

FIA_SOS, Specification of Secrets, is a family that may be applied in a generic sense to biometrics. The generation of the template can be interpreted to be the generation of the password that is defined in this family and therefore mechanisms that support this generation may be specified in terms of metrics. However, the secret, in terms of biometrics, is defined by something that you are, and not by something that you know.

This class may apply to the following generic biometric functions:

- a. Capture Biometric Sample;
- b. Extract Biometric Sample;
- c. Create Template;
- d. Create BIR;
- e. Compare Template;
- f. Decide Match; and
- g. Decide Acceptance.

With these recommendations, the current definition of the FIA class of requirements can be suitably interpreted to accommodate the definitions of identification and authentication as they relate to biometrics.

6.7 SECURITY MANAGEMENT

This requirement defines the management of security attributes, and TSF data and functions. With respect to biometric TOEs, the management of security functions and attributes are especially relevant to the establishment of threshold levels. These levels determine the “closeness” or score required between a sample and reference template in order to declare them a match. This setting in turn determines the rates of false matches and false non-matches, and acceptance or rejection by the TOE. Threshold levels also determine the similarity required among the samples collected during enrolment, which make up the reference template (see discussion in Sections 8.5 and 8.7). These are unique considerations for biometric evaluations. Furthermore, it is suggested that these security functions apply for TOEs that also include capabilities of (for example) appending user rights and privileges related to an application. In particular, the following families apply:

- a. FMT_MOF – Management of Functions in TSF (especially security functions behaviour);
- b. FMT_MSA – Management of Security Attributes;
- c. FMT_MTD – Management of TSF Data; and
- d. FMT_SMR – Security Management Roles.

With respect to FMT_SAE, Security Attribute Expiration, the evaluator must consider the robustness attribute of the biometric. Some biometrics are intrinsically robust over the lifetime of a person (e.g., fingerprints do not change over the life of a person) however are easily prone to damage (e.g., cut on a finger). This must be considered in the determination of expiration requirements.

This class may apply to the following generic biometric functions:

- a. Capture Biometric Sample;
- b. Extract Biometric Sample;
- c. Create Template;
- d. Create BIR;

- e. Decide Match;
- f. Decide Acceptance; and
- g. Release User Data.

With these recommendations, the current definition of the FMT class of requirements can be suitably interpreted to accommodate the definitions of security management requirements as they relate to biometrics.

6.8 PRIVACY

The use of biometrics and biometric products has created much discussion as to whether or not biometrics enhance or detract from privacy [Woodward]. With respect to the CC, privacy is a fundamental security function to be considered in an evaluation of a biometric TOE. However, it is suggested that the current definition of Privacy requirements in the CC is insufficient for the evaluation of biometric TOEs. This section highlights some of the major privacy concerns with respect to biometrics and suggests policy and legislation solutions as opposed to technological solutions for some of the concerns. It also discusses how the current definition of the Privacy requirements in the CC does not address concerns.

Society readily accepts that using a unique physical characteristic or personal trait can be used to recognise an individual. The measurement and storing of this powerful characteristic raises society's concern over its privacy. As stated by [Woodward], "...control over information about ourselves...lies at the very heart of the privacy concerns raised by this technology". Individuals have a concern and interest in determining how, when, why and to whom information about themselves, in this case in the form of biometrics, would be disclosed.

Some of the more significant privacy issues with respect to biometrics are defined as follows:

- a. *Giving up a biometric identifier.* The issue here is an individual is asked to give up truly unique information about identity when scanned by a biometric TOE. Therefore, what protection measures have been instituted to safeguard this unique identifier.
- b. *Disclosure to third parties.* Once the biometric information is obtained, the issue of replicating, copying or otherwise sharing among public and private sources is of concern, especially if conducted without the user's knowledge or consent.
- c. *Disclosure of invasive information.* The issue here is that some biometrics can be used for extracting medical or health information about an individual. It has been reported that there is a possibility of gleaning medical or health information from such biometrics as iris scans (eye diseases, diabetes) and fingerprints (Down's syndrome or other chromosomal disorders). Although these assertions are yet to be proven, the concern is now raised through documented possibilities by medical experts.

- d. *Regeneration.* The issue here is whether the device-specific representation of the biometric can be regenerated to the original (or close approximation of) biometric characteristics for identification / authentication purposes or identity theft.

Because of the direct link between the biometric and an individual's identity, privacy needs are considered very important and biometric templates should therefore be subject to protection. The implementation of appropriate policies concerning privacy issues "a" and "b" is considered to be an acceptable method of dealing with these issues. The *disclosure of invasive information*, although a valid concern, is outside the scope of a CC evaluation and assurance. An evaluation should not determine whether such disclosure is possible. However, the implementation of appropriate policies can prevent use of potential biometrics for these purposes.

The regeneration concern does fall under the CC evaluation. It is suggested that the current definition of Privacy as a security function is inadequate to address this issue. The issue is about identification and identification theft, which is far beyond the protection of user name. The current families of Privacy, namely Anonymity (FPR_ANO), Pseudonymity (FPR_PSE), Unlinkability (FPR_UNL), and Unobservability (FPR_UNO) can be applied to biometric TOEs; however they do not address the issue of regeneration for identification or theft identification. Either an extended requirement needs to be prepared in applicable situations or a new privacy family developed.

6.9 PROTECTION OF TOE SECURITY FUNCTIONS

As discussed previously (Section 5.2.1), a biometric TOE that simply identifies or verifies a user for a resource does not automatically convey rights or privileges for that resource. For a TOE to support this capability, the template must be bound to a resource in such a way that a successful match will convey privileges over that resource. It is this concept that makes the FPT class of functional requirement applicable to biometric TOEs.

Each aspect of this class of requirement – the TSF's abstract machine, implementation and data – is applicable to a biometric TOE. The major application of this class of requirements is highlighted by the following groups of families:

- a. FPT_ITA (Availability of Exported TSF Data), FPT_ITC (Confidentiality of Exported TSF Data), and FPT_ITI (Integrity of Exported TSF Data) for the protection and availability of BIRs that are transported between the biometric TOE and a remote data store of templates.
- b. FPT_RCV (Trusted Recovery), FPT_FLS (Fail Secure), FPT_TRC (Internal TOE TSF Data Replication Consistency) which addresses the expected safe behaviour of a biometric TOE when failure occurs and immediately after.

The current definition of the FPT class of requirements can be suitably interpreted to accommodate the definitions of TOE security function protection requirements as they relate to biometrics.

6.10 RESOURCE UTILISATION

This class of security functional requirements supports the availability of required resources such as processing capability and/or storage capacity. It provides for protection against unavailability of capabilities caused by failure of the TOE. It also ensures that resources will be allocated to the more important or time-critical tasks and cannot be monopolised by lower priority tasks.

An important aspect of Resource Utilisation may be considered with respect to false non-match rate determined for the biometric TOE. The FNM rate is a determination of the probability that an authorised and pre-enrolled user will not be verified and thus not allowed further access rights. It relates to availability and part of the list of security functions that define the availability service is Fault Tolerance (FRU_FLT)¹. Since it is a determination of the accessibility of a user to the TOE, it should therefore be an integral part of the TOE Access requirement and the security evaluation.

This class may apply to the following generic biometric functions:

- a. Capture Biometric Sample;
- b. Extract Biometric Sample;
- c. Create Template;
- d. Compare Template;
- e. Create BIR;
- f. Decide Match;
- g. Decide Acceptance; and
- h. Encrypt/Decrypt.

The current definition of the FRU class of requirements can be suitably interpreted to accommodate the definitions of resource utilisation requirements as they relate to biometrics.

6.11 TOE ACCESS

This class defines requirements for controlling the establishment of a user's session. A session is defined as the period starting at first interaction between user and TOE, up to the moment that all resources and attributes related to the session have been de-allocated.

A biometric TOE can be used in both an enrolment and verification mode. The enrolment mode implies specific conditions under which a user's identity is verified first by a trusted administrator with the support of identification documents and photos. Verification mode also implies some limitations with respect to access in terms of

¹ Issues related to failure of TOE components should also be considered as these can potentially result in false matches and/or false non-matches.

verification attempts allowed. Access should be limited and controlled differently in the enrolment mode than in the verification mode.

Another aspect of TOE Access that may be considered with respect to biometrics is the initial user interaction with the biometric TOE. The FNM rate is a determination of the probability that an authorised and pre-enrolled user will not be verified and thus not allowed further access rights. Although it is sometimes termed the “inconvenience” factor, it is a direct determination of the availability of a TOE to the user (similar to FRU), and therefore an integral part of the TOE Access requirement and the security evaluation.

Based on this scenario, each of the families of TOE Access requirements are deemed applicable to biometric TOEs. The current definition of the FTA class of requirements can be suitably interpreted to accommodate the definitions of TOE access requirements as they relate to biometrics.

6.12 TRUSTED PATH / CHANNELS

This class defines requirements for trusted communications path between users and the TOE and for the trusted communication between the TOE and other trusted IT products. Both families of requirements – FTP_ITC and FTP_TRP – are applicable to biometric TOEs in applications where a template is collected in part of the TOE and then processed or matched in another part or other trusted IT product.

Any time that a template is “unbound” (e.g., for matching), there is a possibility of substitution, altering or copying. Furthermore, if templates are not private, they can be easily copied for the purposes of masquerading, where an attacker might bind his template in place of another authorised user. Therefore, any path taken by the template must be trusted and protected. This path may include the connection between the sensing device and the host computer, within the sensing device itself, or between a storage device and the host or sensing device. Trusted path and channels and the implementation approach used by biometric TOE developers are subject to evaluation under both families of this class.

This class may apply to the following generic biometric functions:

- a. Store Reference Template/BIR;
- b. Transmit; and
- c. Retrieve Reference Template/BIR.

7 APPLICABLE SECURITY ASSURANCE REQUIREMENTS

7.1 GENERAL

The following section assesses the applicability of security assurance requirements (as defined in the CC, Part III). The assessment considers requirements

that: apply as written; require some modification; do not necessarily apply; and should be written as a new security assurance requirement.

Assurance requirements are not compared to individual biometric functions as in the case for functional requirements; they are considered in the context of the design, development and operation of a biometric system. The assurances to establish that the TOE's functional requirements and specifications are realised in its development and implementation are considered to be generally the same for any IT security system or component. In this context, it is determined that all classes of assurance requirements (including the respective families and components) are applicable to biometric TOEs. However, the following paragraphs provide additional information that should be considered in the evaluation of biometric TOEs.

7.2 DISCUSSION OF ASSURANCE REQUIREMENTS

7.2.1 AGD - Guidance Documents

This assurance class defines requirements directed at the clarity, coverage and completeness of the operational documentation provided by the developer for users and administrators.

The current definition of the AGD class of requirements can be suitably interpreted to accommodate the evaluation of biometric TOEs. However, in terms of providing evaluator guidance in assessing developer documents, the following is proposed for inclusion in these documents:

- a. Biometric Privacy. A discussion regarding the personal issues related to collecting and storing of biometrics, including the facts and myths of the biometric and its perceived invasiveness should be documented.
- b. Environmental Influences: Since it has been determined that biometric TOE operation is greatly affected by environment influences (e.g., dust, humidity, cleanliness of the biometric, users) and that these can affect accuracy of the enrolment and verification process, ways of minimising these influences should be documented.
- c. Setting of Thresholds. The importance of defining the effects of setting thresholds (see discussion in Section 8.7) should be documented.

7.2.2 ATE - Tests

This assurance defines the testing requirements to demonstrate that the TSF satisfies the security functional requirements. The concept of this class is to confirm, through developer and independent testing, that the TSF operates according to its specification. The general approach defined by each of the families and respective components of ATE makes them applicable to all IT security TOEs, including biometric ones.

The testing of biometric TOEs with respect to analysis of coverage (ATE_COV), depth (ATE_DPT), functional tests (ATE_FUN) and independent tests (ATE_IND) is conducted in much the same way as with other non-biometric TOEs. However, somewhat unique to biometric TOEs is the establishment of false match/non-match rate claims. Testing of these rates must include an appropriate and statistically representative data set that validates the rates. Sample space, sample size and sample type are critical in biometric tests. The problem in performing the testing is collecting the biometric database or having a representative test population available for enrolment and testing. Some databases of biometrics are available (National Biometrics Test Centre, San Jose California, National Institute of Standards and Technology); the conditions under which these samples were collected are important and must be defined. Another problem is ensuring that the collected data is of high quality (no excuses for high false [non] match rates due to poor quality images). This means that due care must be taken in configuring the equipment, verifying its correct functioning and consistency in collection procedures. The many test issues that must be considered are described in Section 8.

7.2.3 AVA - Vulnerability Assessment

This assurance class defines requirements directed at the identification of exploitable vulnerabilities. It addresses those vulnerabilities introduced in the construction, operation, misuse or incorrect configuration of the TOE.

The families of the AVA class of requirements include:

- a. Covert channel analysis (AVA_CCA). This analysis is carried out to determine the existence and potential capacity of unintended signalling channels that may be exploited. This is not considered applicable to biometric TOEs.
- b. Misuse (AVA_MSU). Misuse investigates whether the TOE can be configured or used in a manner that is insecure but that an administrator or user of the TOE would reasonably believe to be secure. With respect to biometric TOEs, this analysis would include the determination that complete and accurate guidance information is available to both the administrator and user regarding system modes and environmental impacts including the required security measures during enrolment. An example of enrolment misuse is where a user is trying to deceive a biometric TOE that is configured to determine who a user is NOT. For this scenario, a fingerprint device is used to determine if a person is an already registered applicant (i.e., licensed driver, recipient of government benefits, etc.). For an attacker who is already registered and is trying to register under another name, the attacker may try to deceive the system by temporarily altering a fingerprint (mutilation, coating with nail polish) or using a left instead of a right index fingerprint. The obvious protection against this misuse is proper developer guidance for the administrator related to the inherent weaknesses of the biometric in some of the more common applications.
- c. Strength of TOE Security (AVA_SOF). Strength of function investigates the strength of the underlying security mechanism of the TOE and its

vulnerability. With respect to biometric TOEs, the strength of function lies in the biometric's ability to unambiguously identify a user. This is measured through false match rates claimed by a developer. Although false non-match rate is considered to be a measure of "inconvenience", it is also a measure of availability and should therefore be considered part of the strength of function analysis. The strength of function for a biometric TOE is determined by the uniqueness of the biometric captured from a person and by the transformation of that biometric by the TOE into a measurable quantity. Further details for SOF are provided in Section 8.6.

- d. Vulnerability Analysis (AVA_VLA). Vulnerability analysis is an assessment to determine whether vulnerabilities identified (during the evaluation of the development, construction and anticipated operation of the TOE) could allow users to violate the TSP. Vulnerability analysis is not considered unique or different for biometric TOEs; therefore each of the families and the respective component requirements are appropriate for biometric TOEs as defined.

7.2.4 ALC – Life Cycle Support

This class of assurance requirements defines how discipline and control are established in the processes of refinement of the TOE during development and maintenance. In general, the approach defined by each of the families and respective components of ALC makes them applicable to all IT security TOEs, including biometric ones. However, the family dealing with Tools and Techniques (ALC_TAT) requires special consideration.

ALC_TAT, Tools and Techniques, deals with the appropriate selection and implementation of tools (including programming languages, documentation, implementation standards) that are used to develop, analyse and implement the TOE. In general, the selection and use of appropriate development tools is not unique to biometric TOEs. However, there are emerging development standards with respect to both the biometric and the interface between a biometric device and an application or operating system (e.g., NT operating system).

Standards related to a biometric (e.g., fingerprint, voice pattern, iris pattern) are not sufficiently developed to be considered as a requirement in the design and implementation of a biometric TOE. With the exception of fingerprint, work in developing or at least thinking about developing implementation standards for a particular biometric is considered to be work in progress. Advances have been made in establishing standards for facial analysis, handwriting and voice. Fingerprint standards are probably the most advanced (FBI Fingerprint Compression Standard based on WSQ Grey-Scale Fingerprint Compression Specification).

Standards related to application program interfaces (APIs) are also in development. The most significant work is being conducted by the BioAPI Consortium, whose three working groups are developing application, device and external standards for biometric applications. They have also consolidated earlier initiatives (Human

Authentication-API) into this one. The API standard has been released in draft form (Version 0.52) for public review (see www.bioapi.org).

At higher levels of assurance (EAL4 and higher), evaluations should consider how the developer has followed the intent of standards related to biometrics and API standards. However, none of these standards have been accepted and “approved” and therefore can not be specified as a requirement on the biometric TOE design.

7.3 EVALUATION ASSURANCE LEVELS

Evaluation assurance levels provide an increasing scale of assurance based on a model that balances the level of assurance with the effort and cost required to achieve that level of assurance (reference: CC Part 3 – Security Assurance Requirements). Each EAL is defined by the appropriated assurance requirements for that level, and is ordered hierarchically – i.e., each EAL represents more assurance than all lower EALs. The increase in assurance is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (increasing in rigour, depth and/or scope) and from the addition of assurance components from other assurance families (adding new assurances).

The selection of assurance requirements for each level as defined by the CC Part 3 Table 6.1 – Evaluation Assurance Level Summary is considered appropriate for biometric TOEs. Note that Section 9 provides additional guidance by evaluation assurance levels.

8 TEST AND ANALYSIS - ISSUES AND GUIDELINES

8.1 PERFORMANCE- VERSUS SECURITY-ORIENTED EVALUATIONS

Testing of biometric systems has been categorised as problematic. Testing to determine which system is “best” for a particular application, to help a perspective user select the most accurate and cost-effective system or to improve the performance of a device is expensive and effort- (data collection and analysis) intensive. The low error rates that typify biometric devices mean that massive amounts of data are required to achieve statistical relevance. This is usually achieved by frequent and repeated tests using many people of diverse characteristics (ethnic origin, gender, age, etc.) in order to collect a wide and accurate representation.

A primary premise of this study is the differentiation between performance- and security-oriented testing. Briefly, performance testing is defined as testing to determine which of two or more devices is “best”, or which is the most efficient, cost-effective device that meets application requirements. Security testing is testing to determine how the device meets security functional and assurance requirements. It is testing against a security target, and not against other devices, nor to determine which system is best for a particular application.

A survey of the various testing approaches used for biometric devices was conducted in preparing this report. Among the organisations and journals consulted were

the National Biometric Test Centre in San Jose, California, the Biometric Consortium, and the Central Information Technology Unit, United Kingdom. Typical performance measures are summarised as follows:

- a. Modes of operation: A device may be able to operate in distinct modes (e.g., enrolment, verification, training, degraded, etc.) A mode of operation may have a distinct set of requirements and functions from other modes within the device. Understanding and fully characterising all modes of operation is critical to defining the full functionality of the biometric device.
- b. Uniqueness or distinctiveness of a biometric (identification accuracy): Defined as a measure of how unique a person's biometric is amongst a population.
- c. Robustness of a biometric: Defined as the stability and repeatability of the biometric.
- d. Distance measure: Defined as the difference between closely matching templates of a biometric. With inherent differences between sample and reference template caused by biometric-, presentation-, sensor-, or transmission-related differences, distances will probably not ever be zero.
- e. False-match rates: Defined as the rate at which the device incorrectly matches a sample with a reference template.
- f. False non-match rates: Defined as the rate at which the device rejects a true match between a sample and the reference template.
- g. Receiver Operating Characteristic curves (ROC curves): A graphical representation of false match versus non-match rates, and associated confidence intervals:
- h. User acceptance: A subjective determination or assessment of how the device's measurement of the biometric is considered to be acceptable by an individual.
- i. Enrolment time: Defined as the time required by the device to enrol an individual.
- j. Enrolment requirements: Defined as requirements that must be met by the device to complete the enrolment operation.
- k. Learning rate: Defined as a qualitative measure of how quickly administrators and first-time users can consistently and accurately use the device.
- l. Throughput rate: Defined as the number of comparisons completed by the device during a unit of time.
- m. Bin-error rate: Probability that a search for a match between the sample and reference templates will be unsuccessful because of an incorrect categorisation of either the sample or reference template.
- n. Recognition time: Defined as the time required by the device to match a sample and template.
- o. Size of templates: Defined as the byte size for the biometric template.
- p. "Liveness" estimates: Defined as the ability of the device to determine whether the biometric sample is from a live person.

- q. Environmental influences: Defined as the effects on the device by such environmental factors as heat, humidity, vibration, etc.
- r. Level of invasiveness: A subjective measure defining perceived level of invasive behaviour of the device when capturing the biometric sample.
- s. Ease of integration: A subjective measure defining how easily the device integrates with other systems or devices.
- t. Sensor characteristics: Defined as the performance characteristics of the sensor within the device that captures and extracts the biometric. Characteristics include size, ruggedness, bandwidth, sensitivity, detectivity.
- u. Maintenance requirements: Defined as the maintenance overhead associated with the device, including calibration requirements and frequency, cleaning requirements, sparing, etc.
- v. Life cycle costs: Defined as the costs associated with operating the device over its expected lifetime.
- w. Public acceptability: This indicates how readily the biometric device will be accepted by those who use it.

At the very least, biometric devices are benchmarked (i.e., evaluated from a performance point of view) with the following measures: single or multiple comparison false match versus false non-match rates, bin error rate and throughput rate. These benchmarks are used to measure the performance of devices no matter what biometric they measure and thus provide an acceptable measure for selecting a type of biometric device over another. Bin error rates are more relevant to biometric devices used for identification, where a claim of identity is not available to select a biometric template for comparison. A biometric device used for identification must search and compare an entire database of templates, thus making it susceptible to bin errors. Enrolment time, throughput rate and recognition time are performance measures – from a security point of view, it does not matter if the device takes 10 milliseconds or 10 seconds to determine a match. Some of the remaining measures are considered under the FM and FNM determination such as liveness estimate, sensor characteristic, distance measure and ROC. The remainder are clearly performance measures that complete the benchmark evaluation.

However, it is proposed that only some of these measures are relevant to security evaluations. These are: modes of operation; uniqueness and robustness of a biometric; FM, FNM and ROCs; and environment influences. These are discussed in more detail in the following paragraphs. The remainder are not considered relevant to security evaluations and are therefore not discussed further.

8.2 MODES OF OPERATION

The following generic modes of operation are defined below:

- a. Enrol: Samples are collected, and reference template constructed and stored.

- b. Verify: Samples are collected, a sample template constructed, an identification claim is made and the sample is compared to the reference template associated with the claim. The results of the comparison are returned.
- c. Identify: Samples are collected, a template constructed, and compared against an input template list. No identification claim is required. A list is returned showing how close the template compares against the template in the list.
- d. Update: Samples are collected and a revised template constructed and stored. Allows the BIR to be updated, either as a specific operation or in conjunction with the VERIFY mode. It is useful to be able to update a biometric template, since the user's physiology has a tendency to change over time.

For a security evaluation, it is critical to identify and understand the device's modes. The ones defined above are generic in nature, and relevant to most biometrics. In the same way as a clear understanding of the design of any TOE is required to ensure an accurate security evaluation, a clear understanding of these modes is also important. The net effect is to identify the potential security issues that may differ between modes. Some devices have different environmental expectations during enrolment (versus verification), which may mean that administrator and user guidance may require specific instruction by mode to ensure that these expectations are clearly defined. For example, a developer may assume that the enrolment process is conducted in a secure, protected environment. The definition of protected needs to be made clear to the administrator and to the evaluator. Image quality requirements may differ between modes. For example, image capture during enrolment may require a high image quality because the product of this mode is a template which is then used as a master against which all comparisons are made; image capture during verification may not require as high of an image quality in order to compare it against a template.

8.3 UNIQUENESS AND ROBUSTNESS OF A BIOMETRIC

There are many parts of the human body and various human behaviours that have been suggested and used for biometric identification. However, the important questions are: Which part or behaviour is so different among a representative sample of people that it will uniquely identify one person from everyone else?; and, Which part or behaviour is sufficiently stable and repeatable so that the same part or behaviour can be used for identification over a long period of time?

Table 2 identifies key biometrics in use or in development today. The assessment of uniqueness and robustness is based on current evidence collected from various sources, including the Biometrics Report and ICSAs Biometric Technology Overview.

Biometric	Generic Technique	Robustness	Distinctiveness	Evidence	Biometric Potential
Fingerprint	Minutia or image	Medium-high	High	Very high	High
Hand Geometry	Combination of finger length, lines of palm print, vein patterns on back of hand, hand and/or finger geometry	Medium-high	High	Medium	Medium-high
Eye-iris	Combination of corona, crypts, filaments, freckles, pits, radial furrows and striations	High	Very high	High	High-Very high
Eye-retina	pattern of blood vessels on the fovea	High	Very high	High	High-Very high
Face	Complex combination using varying degrees of artificial intelligence	Medium	High	Low	Medium
Signature	dynamic signature verification - the way names are signed	Low – Medium	Medium	Low	Low-medium
Voice	voice signal dependent on vocal characteristics defined by vocal tract, mouth, nasal cavities and other speech processing mechanisms	Medium	Medium - high	Medium-high	Medium-high
Body Odour	chemical analysis of air sample	unknown	unknown	Low	unknown
Ear Shape	shape, size and contours	unknown	unknown	Low	unknown
Thermal Imaging	IR energy	unknown	unknown	Low	unknown
Keystroke	typing rhythm	unknown	unknown	Low	unknown

Table 2 - Biometrics Overview

From a security evaluation point-of-view, these characteristics are considered essential for an evaluation of a biometric device. A problem lies in the amount of evidence available that defines the degree to which a part or behaviour has been tested or observed for uniqueness and robustness. There are sufficient studies and databases that support the uniqueness characteristic of fingerprints, retinas, irises and voice recognition. However other parts or behaviours may not have subjected to such rigour. There is apparently little reliable data for the “world population” and therefore it cannot be said that any biometric is truly unique. However, the probability of finding identical fingerprints, irises, hands and retinas within a typical population is low enough for them to be regarded as a reliable identifier. Beware of claims of absolute uniqueness – some individuals are similar enough to cause false matches. The evaluator must be prepared to investigate current research in the biometric technology under evaluation for tests related to uniqueness and robustness.

With respect to robustness, the input biometric pattern must be stable over a specified period of time. Some targeted patterns are stable for life (e.g., fingerprint, iris patterns or retinal vasculature), but subject to injury or disease which may cause changes in the measured patterns. Others patterns such as voice, face or signature “drift” over time, although in some cases reversibly. The robustness of the biometric is an important consideration in determining an appropriate time period after which a re-enrolment must take place. In other words, the security offered by a biometric device may be time limited.

The last column in the table (Biometric Potential) is a qualitative assessment of the potential of how strong a biometric could be in recognising the identity or verifying the claimed identity of an individual, based only on the 3 parameters (uniqueness, robustness and evidence). This is proposed as a means of determining the *potential* SOF

of a biometric device, without actually considering how the technology converts the biometric into a technology/device-specific template. It is recommended that the next step could perhaps be to assign a scale to each of the parameters (e.g., 1 to 5 with 1 being very low and 5 being very high) in order to determine an SOF value for the biometric type. Determining the SOF of the biometric TOE on the other hand requires a more rigorous, quantitative approach, which is defined in Section 8.5.

8.4 ENVIRONMENT FACTORS

Environment factors help characterise the applications (i.e., how is it going to be used) for the biometric TOE. The factors are defined as follows [Wayman 4]:

- a. Co-operative versus Non-Co-operative. Is the user expected to co-operate with the system in order to be recognised (positive claim of identity) or is the user expected to deceive the system in an attempt NOT to be identified (negative claim of identity)?
- b. Overt versus Covert. Is the use of the biometric technology under overt (i.e., under full awareness by the user) or covert (i.e., hidden from the user)?
- c. Habituated versus Non-Habituated. Is the user familiar with and understands the use and operation of the biometric technology?
- d. Attended versus Not Attended. Is the use of the biometric technology observed and guided as required during its operation?
- e. Standard Environment. Is the operating environment under standard conditions – standard atmosphere, temperature and weather?
- f. Public versus Private. Will the users be customers (i.e., public) of the resource being protected by the biometric technology or employees (i.e., private)?
- g. Open versus Closed. Does the system now or will it in the future interface with other biometric devices? If the system is to be open, standards for capture, storing, transmission are probably required.

With respect to helping select which device is appropriate for an application, these factors are very important. From a security evaluation point of view, these factors also help to identify conditions of vulnerabilities related to the intended application.

Another important issue related to environment and biometric technology is that all test results must be interpreted in the context of the test application (environment) and cannot be translated directly to other applications [Wayman]. In security evaluations, an important consideration is the threat to and vulnerability of the biometric TOE. The environment in which the device is intended for use is characterised by not only the factors defined above, but also security related characteristics; i.e., the security environment. The security environment is defined by:

- a. the TOE physical environment which identifies all aspects of the TOE operating environment relevant to TOE security, including known physical and personnel security arrangements;

- b. the assets requiring protection by the element of the TOE to which security requirements will apply; and
- c. the TOE purpose, which addresses the product type and its intended use.

Items “a” and “b” are biometric technology independent; item “c” brings into question the appropriateness of the biometric technology for its intended use. In other words, are the requirements defined by the device’s environment adequately met by the technology?

The interpretation of the developer’s test results must be carefully executed especially with respect to the environment simulated in the test activities. All testing must be clearly defined with respect to the environment under which the tests were conducted. Only if the characteristics of the test environment are defined can a decision be made if it is appropriate to compare results from one application against another.

8.5 FALSE-MATCH AND FALSE NON-MATCH

An important and underlying service provided by a biometric TOE is the unambiguous identification of a user. However, due to the very nature of the biometric and the process to build a template (see Section 6.6), a biometric TOE is statistically ambiguous. An accepted measure of this ambiguity is the false match (FM) and false non-match (FNM) rates.

The FM rate is the percentage of comparisons in which the device determined that a biometric template matched another one in the database even though they were taken from two different people. The FNM rate is the percentage of comparisons in which the device determined that the biometric did not match another biometric in the database even though it was from the same person and should have been a match. Together, these rates are an estimation of how well the device can perform unambiguous identification.

The relationship between the threshold, FM and FNM rates is further examined in the following is an extract from [Wayman 1]:

“Single Comparison False Match Rate

A single comparison false match occurs when a sample print is incorrectly matched to a print in the database by the decision subsystem because the similarity score between the two exceeded a fixed threshold. The "impostor" probability distribution function, $f_1(s)$, is a function of the positive similarity measure s , which increases with increasing similarity between compared prints. Unlike other biometric systems, the impostor distribution function is closer to the origin ($s=0$) on the abscissa than the "genuine" distribution of similarity scores between truly matching prints.

The single comparison false match rate can be expressed as a function of decision threshold, τ , as

$$FMR(\tau) = \int_{\tau}^{\infty} f_1(s) ds = 1 - \int_0^{\tau} f_1(s) ds$$

which decreases with increasing decision threshold.

Single Comparison False Non-Match Rate

A single comparison false non-match occurs when a sample print is incorrectly not matched to a print from the same finger by the decision subsystem because the similarity score between the two is less than a fixed threshold. The single comparison false non-match rate, FNMR, can be given as a function of decision threshold, τ , as

$$FNMR(\tau) = \int_0^{\tau} g(s) ds$$

where $g(s)$ is the genuine probability distribution function. FNMR increases with increasing decision threshold. It is clear from equations (7) and (8) that false match and false non-match rate are competing factors based on the threshold.”

It is unlikely that the CC will specify FM and FNM rates as a requirement to be met by biometric systems. Each rate is dependent on the requirements specified by the application and will have to be determined by both the developers and users. For example, a representation of FM, FNM rates is shown below.

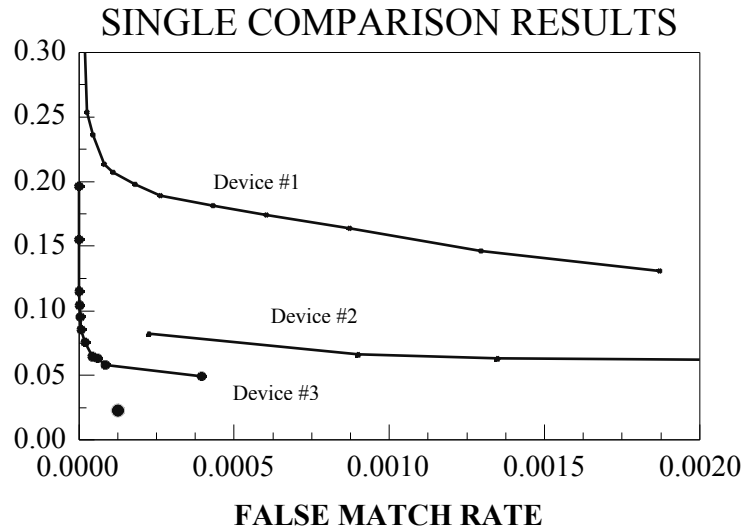


Figure 4 - Example of FM and FNM Rate Comparison [Wayman 1]

Although appropriate for comparison of rate behaviour among several systems, from the point of view of CC testing such comparisons may not be required for security evaluations. However, if a user has a specified FM / FNM rate requirement, then what is relevant to CC testing is an assessment of the manufacturer’s method for this rate determination, including test set-up, conditions, sampling rate, size and type, and repeatability.

A FM rate is a discriminator of a biometric TOE against an accidental misidentification or a “zero effort” [CESG] attack where an attacker hopes to fool and thus circumvent the system by providing their own biometric and hoping for a match. Therefore, it is clear that from a security evaluation perspective, a measure of the FM rate is appropriate.

However, what about the FNM rate? In some references, it is only termed an “inconvenience factor”. However, due to the inverse relationship between the FM and FNM rates (see Figure 4), it can be argued that the FNM rate should also be considered in a security evaluation. Specifically, the FNM rate relates directly to availability. Availability is considered to be an intrinsic service provided by an IT security system, along with confidentiality and integrity of information. The FNM rate is a clear measure of availability – will an authorised and enrolled user be able access to the information, resource, etc. protected by the biometric. It is unique in the case of biometric TOEs because of the uncertainty associated with the biometric. It is not like a password that is either correct or incorrect, and when it is correct, the user is always assured the availability (everything else being equal) of the information, resource, etc. The correct matching between the reference and sample templates of an authorised, enrolled user is a probability function. Therefore, the availability from the point of view of unambiguous identification, is NOT a given.

In some of the previous sections, it is proposed that the availability service of a TOE be defined by appropriate security functions. FNM rates are loosely related to the current definitions of User Data Protection (FDP), TOE Access (FTA) and Resource Utilisation (FRU_FLT specifically), but the applicability is not solid. It is proposed that with the recommendations and guidelines defined herein under these security functions, the FNM rate can be considered part of a security evaluation.

8.6 DETERMINATION OF BIOMETRIC SOF

The strength of function (SOF) rating is a qualification of the security behaviour of an underlying security mechanism that is fundamental and intrinsic to a TOE. For example, the security of a device might be dependent on a password mechanism or token, or in the case of biometrics, a fingerprint or iris scan. In the case of a biometric TOE, it is proposed that the underlying security mechanism supports the “unambiguous identification” service. An SOF rating, in accordance with guidelines provided in Annex B, Part 2 of the Evaluation Methodology, is currently defined in terms of “attack potential” (using Tables B-3 and B-4 of the CEM). However, it is proposed that for biometric TOEs, additional quantitative and statistical analysis is required to further assess the SOF rating.

Both the uniqueness characteristic of a biometric and the FM/FNM rates are proposed as major determining factors for SOFs. The uniqueness characteristic of a biometric (see Table 2) is based on evidence – at best a qualitative assessment of the ability to uniquely identify a person. However, a biometric TOE converts this biometric into a measurable quantity through proprietary algorithms that introduce inherent errors during the transformation of the biometric into a device-specific template as well as environmental errors (dirt, input variations, etc.). The only measures that ultimately take into account the uniqueness of the biometric in its original form (i.e., the potential SOF discussed in Section 8.3) as well as the errors introduced by the device and its environment are the false match (FM) and false non-match (FNM) rates of the device.

In order to estimate the FM/FNM probabilities of a biometric TOE, an appropriate set of test data is required. The important characteristics of the test data are:

- a. data is representative of the “normal” or expected operating conditions of the biometric TOE (environmental conditions including lighting, weather, movement, surroundings, etc);
- b. data is of sufficient size that an accurate estimate of the FM/FNM rate can be determined; and
- c. data is representative of the type of samples collected (e.g., gender, age, occupation and other biometric influences).

It should be noted that current references regarding performance testing of biometric TOEs state that it is difficult to predict even approximately how many tests will be required to have “statistical confidence” in the test results. There is currently no way of accurately estimating how large a test will be necessary to adequately characterise a biometric TOE in any application. However, for the purposes of this report and in the spirit of recommending viable guidelines for the Canadian Certification scheme, the following are considered.

[Wayman 2] describes an approach based on an assumption called “Dodgington’s Law”, which states that the required number of comparisons and test subjects is based on 30 errors – test until 30 errors have been observed. As stated by [Wayman 2], “...if the test is large enough to produce 30 errors, there is a 95% confidence level that the true value of the error rate lies within about 40% of that measured”. In practice, it seems that testers have to settle for as many users as practical, each giving several samples separated by as much time as possible. The collected data should closely resemble the intended application and target population.

The quality of the test data and the conditions under which the test data are collected influence the outcome of the FM/FNM rate estimations. Poor quality test data may not produce results that truly reflect the biometric TOE’s capabilities. Similarly, a very high quality data set may also not indicate the true performance of an automated system because it does not accurately reflect the intended operating environment.

Another approach to sampling is put forth by [Shen]. He states that the FM and FNM rate estimation is making a best guess of the value based on the collection of outcomes of an experiment and recognising the degree of confidence to be placed in the estimate. In a test or experiment, a sequence of identical and independent trials is repeated, each of which produces an outcome. If the outcome of each trial in the test depends on neither the outcomes of any of its predecessors nor those of any of its successors, then these are independent trials. As the number of independent trials increase, the outcomes of the test would convey more meaningful information. It has been suggested that the estimation of automated biometric-based identification and verification systems can be formulated as a parameter estimation based on the outcomes of repeated Bernoulli experiments. A thorough explanation of this methodology is presented at [Shen].

A third approach proposed is a trade-off between the qualitative biometric SOF (Table 2) and sample size/type used to generate FM / FNM rates. The FM rate inherently accounts for the uniqueness of the measured characteristic. However, a statistically representative sample size is required to substantiate all the variables in biometric device measurements. If the biometric is supported by significant evidence of uniqueness (i.e., outside of a biometric measurement), then it might be reasonable to accept a smaller sample size to calculate FM and FNM rates than for a biometric where there is little evidence of uniqueness (where a statistically representative size must be used to support the FM/FNM rates). However, such a qualitative approach would have no measure of confidence associated with the estimation.

A final proposed method that could be used to support biometric SOF calculations is simulation. Simulation is generally not acceptable from a performance test perspective since performance is very much dependent on the factors that may be difficult to accurately simulate. However, from a security evaluation perspective, this approach may be appropriate. It has been proposed to use test methods where templates previously captured are submitted, off-line, to the matching algorithm to compare each template with all others to check for correct matching (against the owner's template) and for false matching (against any other's template). This seems a practical way of achieving the very large number of cross comparisons necessary to verify low levels of error. Trying to evaluate the transformation effect (perhaps using a modulation transfer function approach) at each stage of the biometric transformation) and trying to assess how effectively distinctiveness is maintained (related to original qualitative SOF determination) may be another approach, albeit complicated and difficult. Simulation may allow the use of a machine-specific files instead of live samples. However, this approach would verify the matching algorithm only and not the biometric capture mechanism of the device. Therefore, additional testing of the capture mechanism would be required to augment and support the simulation testing.

Several organisations are currently involved in establishing test databases for a variety of biometrics. The AFIS Program (Automated Fingerprint Identification System) has long been a target for fingerprint standards. The American National Standard for Information Systems developed a data format for the interchange of fingerprint information – ANSI/NIST-CSL1-1993. This standard defines the content, format, and units of measurement for the exchange of information that may be used in the fingerprint identification of a subject. The ESPRIT project, an initiative by the National Physical Laboratory, Middlesex, UK, endeavours, as part of its mandate, to investigate current suitable databases, define procedures for collecting representative samples for certain biometric techniques and produce a design specification for such a database. The National Biometric Test Centre (NBTC) (San Jose University), California, US, is also involved in establishing test databases. Their work has begun in populating a database of fingerprints for use in standardised testing of FM and FNM rates. Other organisations include the National Institute of Standards and Technology (standard fingerprint formats and Facial Recognition Technology (FERET) for standardised facial images), American National Standards Institute (administers and co-ordinates standardisation efforts),

European Union BIOTEST (database of fingerprints, hand geometry and signatures) and others. Other than the NBTC database, most are in development.

For the purposes of a CC evaluation, FM and FNM rate claims made by the developer must be supported by developer test results. Without testing, these rates have no meaning and therefore, SOF can not be verified. Depending on the level of assurance to be evaluated, the most appropriate evaluator action is to evaluate the developer's FM/FNM analysis, with supporting independent evaluator testing, as required. The evaluator's analysis must determine if the developer's tests to determine these rates were conducted in accordance with some or all of the criteria described herein (i.e. sample size defined, collected under expected operating conditions, and samples representative of type to be collected). The evaluator's independent testing should include a portion of the developer tests, without repeating the total number of samples used by the developer. In other words, the objective of the independent test is to determine if the test procedures and associated results are repeatable, based on a subset of the sample biometrics used by the developer. It would not be practical nor cost effective for an evaluation lab to independently collect sample biometrics for use in the testing. Once standard test databases are developed and accepted, CC evaluations should consider their use as part of the independent tests. In the meantime, a portion of the developer's test samples would be the most practical and cost-effective, assuming the evaluator determined that the test samples are valid. The number or percentage to be used by the evaluator should be stated in the evaluator's procedure and report; the smaller the number the larger the uncertainty in the results.

In summary, there is no clear answer with respect to number of required samples to establish FM and FNM rates within a specified level of confidence. The number of samples used to determine FM/FNM rates impact the confidence in these calculated rates. Without clear recommendations for sample sizes, best engineering practices is the only guideline available to evaluators.

As a minimum, if rates are claimed, then some developer testing has to be expected to support the claims; if not, no claim should be made. In fact, the amount of developer testing that is available to support a CC evaluation must be determined during a feasibility stage prior to the CC certification scheme and a CC lab embarking on an evaluation of a biometric product. The Biometric Working Group [CESG] is working to develop "best practice" standards for performance testing of biometric products, which include the determination and presentation of FM and FNM rates. In the meantime, security evaluations will have to settle for as many test subjects as practical.

8.7 THRESHOLD SETTINGS

Thresholds determine matches or non-matches, depending on how close a sample is to a reference. Important security issues related to thresholds are: the appropriate determination of thresholds; the ability to set threshold settings for FM and FNM; and the control over these thresholds.

Thresholds can be determined through the appropriate measurement of verification, or sometimes referred to as “distance”, distributions. As discussed in [Wayman], three application-dependent probability distribution functions (PDF) can be determined based on distance measures: genuine (short hash curve), inter-template (longer hash curve) and impostor (solid line) distributions. The following figure illustrates the three distributions [Wayman 2].

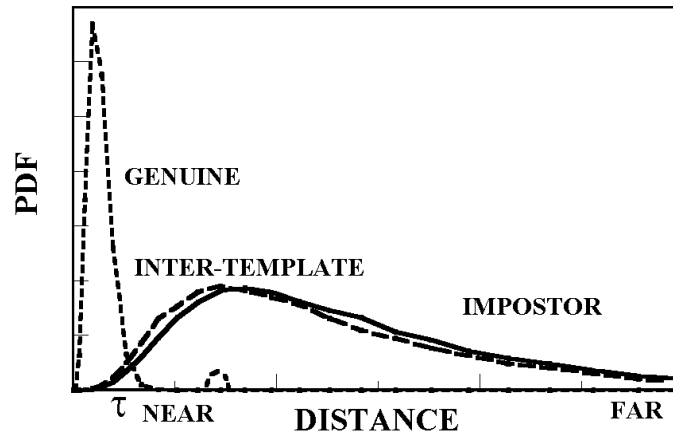


Figure 5 - Distance Distributions

The genuine distribution is created from distance measures resulting from comparison of samples to like templates (shows repeatability of measures from the same person). The inter-template distribution is created from the distance measures resulting from comparison of templates from different enrolled individuals. The third distribution is created from the distance between samples to non-like templates (showing the distinctiveness of measures from different individuals). This is called an impostor distribution.

From Figure 5, it can be seen that a threshold setting generally in between the genuine distribution and the inter-template and impostor distributions would result in an optimum compromise. However, it also shows that errors would inevitably still be made because of the overlap between the genuine and impostor distributions. There is a trade-off that must be considered between the acceptable FM and FNM rates (see Figure 4). Increasing the ability to reject an impostor increases the likelihood of rejecting an authorised user.

Another example of using this distribution measurement for threshold setting is explained in [Negin et al]. Here, the human iris is the biometric and the distance measure is called the Hamming Distance. This measure is determined from the comparison of computed iris codes. For two identical iris codes, the HD is zero; for two perfectly unmatched iris codes, the HD is 1.

A typical distribution for this particular application is illustrated in Figure 6.

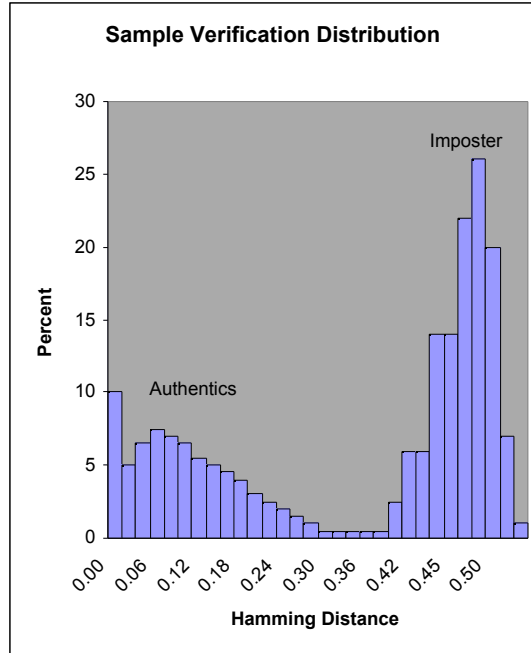


Figure 6 - Sample Distance Distribution for an Iris-Based Biometric System

For this particular system, the threshold setting was set at 0.32, where distances less than this value are declared a match, and distances above a non-match. The manufacturer claims that a false accept (or match, assuming that the security policy defines a match as accept) was never experienced at this threshold setting and that the false reject was experienced by 0.5 percent of all users.

Thresholds are usually set by the developer and in some cases available as an administrator function to modify the setting dependent on the application and/or environment.

9 PROPOSED EVALUATION METHODOLOGIES AND GUIDELINES

9.1 GENERAL

The Evaluation Methodology is defined in the Common Methodology for Information Technology Security Evaluation (CEM), which is a companion document to the CC. The current scope of the CEM is up to and including an EAL4 assurance level. The current version of the CEM recognises that not all questions regarding IT security evaluations are answered therein and that further interpretations are required. What follows in this section should be considered as interpretations as well. Further work and actual evaluations of biometric TOEs will be required before a significant number of biometric-related questions will be answered. However, in this section, CEM methodologies will be assessed in terms of the assurance requirements identified in Section 7.2 as being deserving of special attention with respect to biometric TOEs – namely, Guidance Documents (AGD), Tests (ATE), Life Cycle (ALC) and Vulnerability Assessment (AVA) requirements.

9.2 EAL1 EVALUATIONS

With respect to EAL1 evaluations, the following guidance is suggested:

- a. AVA_SOF. It is recommended that the requirements of EAL1 be augmented for biometric evaluations to include AVA_SOF.1, as strength of function is an intrinsic characteristic of all biometric devices. This analysis should take into consideration issues discussed in Sections 8.3, 8.5 and 8.6 in addition to the CC guidance already provided.
- b. AGD_ADM. In addition to the CC guidance already provided to evaluators, guidance (described in Section 7.2.1) regarding biometric privacy, environmental influences including conditions that increase and decrease the accuracy of the capture process of the biometric, and setting of thresholds is suggested as additional clarifications. Descriptions of the differences and requirements associated with the different capture modes (enrolment and verification) are also suggested.
- c. AGD_USR. In addition to the CC guidance already provided, myths and facts regarding biometric capture should be briefly discussed.
- d. ATE_IND. At this level of assurance, additional guidance is not required.

9.3 EAL2 EVALUATIONS

With respect to EAL2 evaluations, the following guidance is suggested:

- b. AGD_ADM: as per EAL1.
- c. AGD_USR: as per EAL1.
- d. ATE_COV: Additional guidance is not required.
- e. ATE_FUN: Refer to Sections 8.5 and 8.7 for suggested clarifications in addition to guidance already provided.
- f. ATE_IND: Independent testing conducted by the evaluator should take into consideration the issues discussed in Sections 8.5 and 8.7, in addition to the CC guidance already provided. In the evaluation of biometric TOEs that claim to have an identification capability (i.e., no claim required), testing must take into consideration such factors as bin errors (see section 8.1), effect of database size on accuracy, and matching criteria, to name a few. In addition, as part of the enrolment mode, an identification capability is based on no two templates being the same; therefore, a means of ensuring that two templates are not within the match criteria is probably required.
- g. AVA_SOF: SOF analysis should take into consideration issues discussed in Sections 8.3, 8.5 and 8.6 in addition to the CC guidance already provided.
- h. AVA_VLA: In addition to the CC guidance already provided, the evaluator should take into consideration the various TOE modes and environment characteristics as a means of analysing vulnerabilities

(Sections 8.2 and 8.4) as well as the trade-off between FM and FNM rates in determining thresholds (see Section 8.7).

9.4 EAL3 EVALUATIONS

With respect to EAL3 evaluations, the following guidance is suggested:

- a. AGD_ADM: as per EAL1.
- b. AGD_USR: as per EAL1.
- c. ATE_COV: Additional guidance is not required.
- d. ATE_FUN: Refer to Sections 8.5 and 8.7 for suggested clarifications in addition to CC guidance already provided.
- e. ATE_IND: as per EAL2.
- f. AVA_MSU: In addition to the CC guidance already provided, see Section 7.2.3 for additional clarification.
- g. AVA_SOF: as per EAL2.
- h. AVA_VLA: as per EAL2.

9.5 EAL4 EVALUATIONS

With respect to EAL4 evaluations, the following guidance is suggested:

- a. AGD_ADM: as per EAL1.
- b. AGD_USR: as per EAL1.
- c. ATE_COV: Additional guidance is not required.
- d. ATE_FUN: Refer to Sections 8.5 and 8.7 for suggested clarifications in addition to CC guidance already provided.
- e. ATE_IND: as per EAL2.
- f. AVA_MSU: In addition to the CC guidance already provided, see Section 7.2.3 for additional clarification.
- g. AVA_SOF: as per EAL2.
- h. AVA_VLA: Additional guidance is not required.
- i. ALC_TAT: Current draft standards can be considered and used to compare against developers design and implementation; however these standards are not “approved” therefore can not be specified as design or implementation requirements (see Section 7.2.4).

9.6 FM AND FNM RATE CALCULATION GUIDELINES

The following is presented as evaluator guidelines for the determination of FM and FNM rates in support of SOF assessments. These guidelines are based on current understanding and methodology in use by the biometric testing community (for example, methodology discussed in [CESG2]) and therefore are still very much in development. It is strongly recommended that evaluation labs re-assess the state-of-the-art methodology in use by the community on a continual basis.

Developer vs. Evaluator Testing. As previously stated, developer test results must be available to support any claims regarding FM and FNM rates. The procedures followed by the developer should be analysed by the evaluator to determine if:

- a. environmental conditions during sample collection is defined (see Section 8.4 for further guidance) so that comparisons to the target application can be assessed;
- b. population from which the samples are collected is defined;
- c. quality control implemented during sample collection is defined (see Section 8.7);
- d. number of attempts to enrol and verify is recorded;
- e. method of calculating FM and FNM rates is defined (see Sections 8.5 and 8.6); and
- f. size of sample base and number of comparisons made between sample and reference templates are defined.

Independent testing conducted by an evaluator should be based on a sample of the data used by the developer (for example, 20% of the data points used by the developer to calculate FM and FNM rates). A recommended sample size for independent testing can not be defined at this point. There are no standard test databases of biometrics available for evaluators and evaluator-sponsored collection of these samples is not considered cost-effective. It is assumed that some developer testing will have been conducted; independent testing will not be the only tests and calculations conducted to confirm claimed FM and FNM rates.

Transaction Types. Both developer and independent evaluator testing should use both genuine and impostor type transactions. Genuine transactions are attempts by a user made in good faith to match their own template stored in the system. An impostor transaction is one where an unknown user (to the system) attempts to match any sample already in the system as if they were attempting successful verification against their own template.

Number of Attempts. Both developer and independent testing should be based on one attempt to enrol and one attempt to verify.

Live vs Off-Line Samples. Live samples imply having the “bodies” available to enrol and verify, while off-line samples imply injecting the sample into the matching algorithm. For the purposes of this report, use of off-line samples very much depends on the ability to inject the samples into the matching algorithms. This may be beyond the scope of some test set-ups. Live samples may be easier to use, but offers less control than off-line samples (e.g., re-use of off-line samples after an extended period of time may be easier than re-calling an individual to enrol or verify).

Collecting Enrolment Data. In situations where the collection of enrolment data are required, the conditions under which enrolment takes place should be defined. The quality control used in the collection process should be defined and the reporting of any failures to enrol should be documented. Consistent enrolment conditions should be used.

Collecting Test (Verification) Data. For the collection of verification data, the conditions should approximate the target application.

FM and FNM Calculations. The method of calculating FM and FNM rates should be consistent with the techniques discussed in Sections 8.5 and 8.6. Some developers use “distance” measures while others use template matching scores (based on how close the match is between the reference and sample templates). In most cases, these methods require additional software modules (provided by the developer) to calculate “distance” or “score”, which can then be used by the evaluator in independent testing. All templates collected are compared against each other (i.e., if there are N templates, then N^2 comparisons are made). The results of the comparisons are plotted as FM versus FNM rates (x vs y) encountered at various threshold settings.

Reporting of Results. The results of independent testing should include the following:

- a. FM vs. FNM curves;
- b. failure to enrol and failure to acquire data;
- c. details of the sample population and test environment;
- d. size of the sample population and the number of comparisons made; and
- e. details of the test procedure, including all assumptions, constraints and conditions.

10 CONCLUSIONS AND RECOMMENDATIONS

10.1 CONCLUSIONS

The security evaluation of a biometric TOE must consider the following:

- a. how accurately and consistently can the biometric TOE determine if a user is who he/she claims to be in a given environment;
- b. how is the binding between template and user used to control and protect Resource access by user; and
- c. how does the biometric TOE protect the user biometric (in terms of confidentiality, integrity and availability).

Based on these criteria, the current definition of and guidelines to CC security and functional requirements do not fully support biometric TOE evaluations. The assignment of assurance requirements as listed in EAL1 through EAL4 is applicable to biometric TOE evaluations; however, additional guidelines are required for the CEM in order to execute appropriate evaluation methods and procedures. EAL5 through EAL7 are considered outside the scope of this study. Details of these findings are discussed below.

- a. Security evaluations of biometric TOEs are not the same as performance evaluations. However, key elements of accepted performance evaluation practices are applicable to security evaluations, namely: modes of

- operation; uniqueness and robustness; FM/FNM rates; and environment influences.
- b. The “context” and “level 0” representations of biometric functional models assist in the identification of applicable functional and assurance requirements.
 - c. The environment has a significant impact in the evaluation of a biometric TOE, in terms of supporting the identification of both function and vulnerabilities. The characterisation factors defined herein assist in the determination of TOE application as well as of associated vulnerabilities.
 - d. Most of the security functions require additional explanation and guidelines in their application to biometric TOEs; in particular: FAU - Security Audit; FCS - Cryptographic Support; FDP – User Data Protection; FIA – Identification and Authentication; FMT – Security Management; FPR – Privacy; FRU – Resource Utilisation; and FTA – TOE Access. FCO – Communication is not considered relevant to biometric TOE security evaluations.
 - e. Assurance requirements are generally applicable to biometric TOEs. However, AGD – Guidance, ATE-Tests, AVA - Vulnerability Assessment, and ALC - Life Cycle Support require significant explanation and guidelines in their application to biometric TOEs.
 - f. The assurance requirements assigned by EAL1 through 4 are applicable to biometric evaluations with the caveat that the recommended guidelines and recommendations be considered.
 - g. The potential SOF of a biometric can be determined in a qualitative fashion, based on the documented evidence of the uniqueness and robustness of the biometric. However, the SOF of the biometric device requires a more rigorous, quantitative approach.
 - h. FM and FNM rates can be used as means of determining SOF.
 - i. FM and FNM rate claims must be supported by appropriate testing that take into account the factors and criteria defined in this report.
 - j. Due to the probabilistic nature of FM and FNM rates, an associated factor is critical with respect to biometric TOE evaluations – threshold settings: their determination, setting and control.
 - k. Testing to determine SOF (through FM and FNM rates) is problematic in terms of sample size, type and quality. Different approaches are provided; in the short term, sample size required to determine FM and FNM should be based on current best practices guidance documents.
 - l. Many organisations are working to develop best practices in terms of performance evaluations of biometric products. These practices, as they are developed and used, should be reviewed for security evaluation purposes.

10.2 RECOMMENDATIONS

This study identifies the security functions and assurance requirements, and evaluation methodologies that are considered “weak” with respect to biometric TOE evaluations. The issues are identified and guidelines to address them are provided.

However, how best to implement them in the CC is left to the Canadian Scheme certifiers. It is recommended that:

- a. the “context” and “level 0” representations of biometric functional models be adopted for evaluations, especially to assist in the identification of applicable functional and assurance requirements;
- b. the environment characterisation factors defined herein be adopted to assist in the determination of TOE applications and associated vulnerabilities;
- c. the following security functions consider the recommended explanation and guidelines provided: FAU - Security Audit; FCS - Cryptographic Support; FDP – User Data Protection; FIA – Identification and Authentication; FMT – Security Management; FPR – Privacy; FRU – Resource Utilisation; and FTA – TOE Access, FPT – Protection of the TSF, FTP- Trusted Path/channels;
- d. the following assurance requirements adopt the recommended explanations and guidelines provided: AGD – Guidance, ATE-Tests, AVA - Vulnerability Assessment, and ALC - Life Cycle Support;
- e. the assurance requirements assigned by EAL1 through 4 be deemed applicable to biometric evaluations with the caveat that the recommended guidelines be considered;
- f. the potential SOF of a biometric be determined in a qualitative fashion, based on the documented evidence of the uniqueness and robustness of the biometric;
- g. FM and FNM rates be used as means of determining SOF;
- h. the concept of employing the statistical formula provided for determining appropriate sample size for the calculation of FM and FNM rates be adopted until further work in establishing best practices is conducted and accepted by the biometric community; and
- i. all of the presented conclusions and recommendations be verified during actual biometric TOE evaluations.