ISO/IEC JTC 1 N 9557

2009-04-01

ISO/IEC JTC 1
Information Technology

Document Type:	**Proposed NP**
Document Title:	**SC 37 Proposal for a New Work Item on Evaluation Methodology for Environmental Influence in Biometric Systems**
Document Source:	**SC 37 Secretariat**
Reference:	
Document Status:	**This document is circulated to JTC 1 National Bodies for concurrent review. If the JTC 1 Secretariat receives no objections to this proposal by the due date indicated, we will so inform the SC 37 Secretariat.**
Action ID:	**ACT**
Due Date:	**2009-07-01**
No. of Pages:	**32**

ISO/IEC JTC 1/SC 37 N 2946

2008-12-10

ISO/IEC JTC 1/SC 37
Biometrics

Document Type: Proposed New WorkItem

Document Title: Proposal for a New Work Item on Evaluation Methodology for Environmental Influence in Biometric Systems

Source: Project Editor

Document Status: This document is circulated to SC 37 National Bodies for ballot. Please submit votevia the online balloting system.

Action ID: VOTE

Due Date: 2009-03-31

No. of Pages: 31

A1 New Work Item Proposal

November 2008

PROPOSAL FOR A NEW WORK ITEM

Date of presentation of proposal: 30-01-2008	Proposer: AENOR
Secretariat of JTC1/SC37 and JTC1: ANSI National Body US	**ISO/IEC JTC 1 N** XXXX ISO/IEC JTC 1/SC 37 N2946

A proposal for a new work item shall be submitted to the secretariat of the ISO/IEC joint technical committee concerned with a copy to the ISO Central Secretariat.

Presentation of the proposal - to be completed by the proposer

Title (subject to be covered and type of standard, e.g. terminology, method of test, performance requirements, etc.) Evaluation Methodology for Environmental Influence in Biometric Systems

Scope (and field of application) - of the project:

This standard provides a generic methodology to evaluate the environmental influence in biometric systems. This evaluation is intended for testing biometric systems performance when these systems are working under different environments.

For this document environment must be understood as all atmosphere parameters (e.g. temperature, humidity, etc) and other physic and chemical phenomena (e. g. illumination, noise, vibration, dust, corrosion, etc) that could surround the biometric system and influence in its performance.

These evaluations consist of generating controlled scenarios for each environmental factor and monitoring both, scenarios and biometric systems, in order to determine error rates and throughput rates while the biometric system is operated under such conditions. It allows knowing whether biometric systems are influenced by any environmental parameter and provides repeatable and reproducible tests.

The targets of this kind of evaluations include:

- Analyse biometric systems performance into its operational environment. This environment involves the operational range for which biometric systems have been designed and/or the operational environment in which biometric systems is used.
- Test biometric systems outside its operational environment and/or under extreme conditions. This analysis allows knowing whether an attacker might modify operational environment in order to break biometric systems.

The purpose of these kind of evaluations are that suppliers and users may know which environmental conditions affect performance of a particular biometric system, to what extent and for which applications such biometric system could be suitable. Also this methodology could be used for examining environmental parameters for which biometric systems could be vulnerable.

This standard address:

- How to plan environmental evaluations for biometric system, and the performance metrics to consider
- Relevant scenarios to analyse specific parameters that could influence in the performance of different modalities. Such scenarios are defined both for operational environment as well as for analysis of extreme conditions
- Ranges for which to examine these parameters
- Requirements for the test equipment and how to control and monitor the overall evaluation
- How to select test population and guide them during tests
- Test pre-requirements and how to execute all test procedures
- Results to record, analyse and report

This standard does not :

- Determine which parameters must be analyzed for a specific biometric modality. This is somehow currently covered in 19795-3.
- How to perform a vulnerability analysis modifying environmental factors. This is expected to be covered by ISO/IEC JTC1/SC27 standards, although this methodology might be used for such analysis.
- Classify biometric systems depending of its performance against different ambient conditions.

Purpose and justification - attach a separate page as annex, if necessary

Many documents related to biometrics and their evaluation claim that the environmental conditions must be taking into account during performance testing but none of them establishes a specific method for measuring how much performance could be affected.

- ISO/IEC 19795-2, Biometric Performance Testing and Reporting — Part 2: Testing Methodologies for Technology and Scenario Evaluation addressed scenario evaluations. In relation with environment this standard define that environmental factors must be specified, measured and reported however it does not describe any approach.
- ISO/IEC 19795-3, Biometric Performance Testing and Reporting — Part 3: Modality Specific Testing defines which environmental factors can influence in performance testing but this technical report does not provide a specific methodology for doing it.
- Common Criteria for Information Technology Security Evaluation only considers environmental conditions as assumptions, not being evaluated ever.

According all these documents it is necessary an environmental evaluation of biometric system and a genetic methodology must be specified in order all tests are reproducible and repeatable.

Programme of work

If the proposed new work item is approved, which of the following document(s) is (are) expected to be developed?
_X_ a single International Standard

___ more than one International Standard (expected number: ....)
____ a multi-part International Standard consisting of .... parts
____ an amendment or amendments to the following International Standard(s) ....
____ a technical report , type ....

And which standard development track is recommended for the approved new work item?

____a. Default Timeframe

____b. Accelerated Timeframe

_X__c. Extended Timeframe

Relevant documents to be considered

Attached there is one paper showing previous works in this area, as to be considered for a preliminary WD.

Co-operation and liaison

None is proposed, although cooperation with ISO/IEC JTC1/SC27 experts is welcomed.

Preparatory work offered with target date(s)

Upon approval of this NWI, a WD will be offered based on the paper attached.

Spain will provide an Editor.

Signature: Miguel Angel Aranda, AENOR

Will the service of a maintenance agency or registration authority be required? ....NO.............
- If yes, have you identified a potential candidate? ....
- If yes, indicate name ....

Are there any known requirements for coding? ....NO.............
-If yes, please specify on a separate page

Does the proposed standard concern known patented items? .... NO.

- If yes, please provide full information in an annex

Comments and recommendations of the JTC 1 or SC 37 Secretariat - attach a separate page as an annex, if necessary

Comments with respect to the proposal in general, and recommendations thereon:
The proposer has suggested that this new work item be assigned to JTC 1/SC 37 WG5

Voting on the proposal - Each P-member of the ISO/IEC joint technical committee has an obligation to vote within the time limits laid down (normally three months after the date of circulation).

Date of circulation: 2008-12-12	**Closing date for voting:** 2008-03-31	**Signature of Secretary:** Lisa Rajchel

NEW WORK ITEM PROPOSAL - PROJECT ACCEPTANCE CRITERIA		
Criterion	**Validity**	**Explanation**
A. Business Requirement		
A.1 Market Requirement	Essential __X_ Desirable ___ Supportive ___	The business justification is to establish a common methodology for analyzing the influence in performance biometric systems. These tests allow that users and suppliers know applications for which a specific biometric system is suitable. The use of a standardized methodology provides that performance biometric testing will be repeatable and reproducible.
A.2 Regulatory Context	Essential ___ Desirable _X__ Supportive ___ Not Relevant __	
B. Related Work		
B.1 Completion/Maintenance of current standards	Yes _X__ No___	ISO/IEC 19795 Part 2
B.2 Commitment to other organisation	Yes ___ No__X_	
B.3 Other Source of standards	Yes _X__ No__	ISO/IEC 19795 Part 1, and 3
C. Technical Status		
C.1 Mature Technology	Yes __ No_X__	
C.2 Prospective Technology	Yes ___ No__X_	

C.3 Models/Tools	Yes __X_ No___	
D. Conformity Assessment and Interoperability		
D.1 Conformity Assessment	Yes _X__ No___	
D.2 Interoperability	Yes _X__ No___	
E. Cultural and Linguistic Adaptability	**Yes**____ **No**__ X ___	It seems unlikely that cultural or linguistic aspects will influence this work.
F. Other Justification		

Notes to Proforma

A. Business Relevance. That which identifies market place relevance in terms of what problem is being solved and or need being addressed.

A.1 Market Requirement. When submitting a NP, the proposer shall identify the nature of the Market Requirement, assessing the extent to which it is essential, desirable or merely supportive of some other project.

A.2 Technical Regulation. If a Regulatory requirement is deemed to exist - e.g. for an area of public concern e.g. Information Security, Data protection, potentially leading to regulatory/public interest action based on the use of this voluntary international standard - the proposer shall identify this here.

B. Related Work. Aspects of the relationship of this NP to other areas of standardisation work shall be identified in this section.

B.1 Competition/Maintenance. If this NP is concerned with completing or maintaining existing standards, those concerned shall be identified here.

B.2 External Commitment. Groups, bodies, or for a external to JTC 1 to which a commitment has been made by JTC for Co-operation and or collaboration on this NP shall be identified here.

B.3 External Std/Specification. If other activities creating standards or specifications in this topic area are known to exist or be planned, and which might be available to JTC 1 as PAS, they shall be identified here.

C. Technical Status. The proposer shall indicate here an assessment of the extent to which the proposed standard is supported by current technology.

C.1 Mature Technology. Indicate here the extent to which the technology is reasonably stable and ripe for standardisation.

C.2 Prospective Technology. If the NP is anticipatory in nature based on expected or forecasted need, this shall be indicated here.

C.3 Models/Tools. If the NP relates to the creation of supportive reference models or tools, this shall be indicated here.

D. Conformity Assessment and Interoperability Any other aspects of background information justifying this NP shall be indicated here.

D.1 Indicate here if Conformity Assessment is relevant to your project. If so, indicate how it is addressed in your project plan.

D.2 Indicate here if Interoperability is relevant to your project. If so, indicate how it is addressed in your project plan

E. **Cultural and Linguistic Adaptability** Indicate here if cultural and linguistic adaptability is applicable to your project. If so, indicate how it is addressed in your project plan.

F. Other Justification Any other aspects of background information justifying this NP shall be indicated here.

ISO/IEC JTC 1/SC 37 N XXXX

Date: 2008-10-8

ISO/IEC WD -zzz

ISO/IEC JTC 1/SC 37/WG 5

Secretariat: ANSI

Introductory element — Evaluation Methodology for Environmental Influence in Biometric Systems

Élément introductif — Élément central — Partie zzz: Titre de la partie

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage: (20) Preparatory
Document language: E

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC -zzz was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information Technology*, Subcommittee SC 37, *Biometrics*.

This second/third/... edition cancels and replaces the first/second/... edition (), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] been technically revised.

ISO/IEC consists of the following parts, under the general title *Introductory element — Evaluation Methodology for Environmental Influence in Biometric Systems*:

—

— *Part [n]:*

— *Part [n+1]:*

Introduction

This standard provides a generic methodology to evaluate the environmental influence in biometric systems. This evaluation is intended for testing biometric systems performance when these systems are working under different environments.

For this document environment must be understood as all atmosphere parameters (e.g. temperature, humidity, etc) and other physic and chemical phenomena (e. g. illumination, noise, vibration, dust, corrosion, etc) that could surround the biometric system and influence in its performance.

These evaluations consist of generating controlled scenarios for each environmental factor and monitoring both, scenarios and biometric systems, in order to determine error rates and throughput rates while the biometric system is operated under such conditions. It allows knowing whether biometric systems are influenced by any environmental parameter and provides repeatable and reproducible tests.

The targets of this kind of evaluations include:

— Analyse biometric systems performance into its operational environment. This environment involves the operational range for which biometric systems have been designed and/or the operational environment in which biometric systems is used.

— Test biometric systems outside its operational environment and/or under extreme conditions. This analysis allows knowing whether an attacker might modify operational environment in order to break biometric systems.

The purpose of these kind of evaluations are that suppliers and users may know which environmental conditions affect performance of a particular biometric system, to what extent and for which applications such biometric system could be suitable. Also this methodology could be used for examining environmental parameters for which biometric systems could be vulnerable.

Introductory element — Evaluation Methodology for Environmental Influence in Biometric Systems

1 Scope

This standard address:

- How to plan environmental evaluations for biometric system, and the performance metrics to consider
- Relevant scenarios to analyse specific parameters that could influence in the performance of different modalities. Such scenarios are defined both for operational environment as well as for analysis of extreme conditions
- Ranges for which to examine these parameters
- Requirements for the test equipment and how to control and monitor the overall evaluation
- How to select test population and guide them during tests
- Test pre-requirements and how to execute all test procedures
- Results to record, analyse and report

This standard does not :

- Determine which parameters must be analyzed for a specific biometric modality. This is somehow currently covered in 19795-3.
- How to perform a vulnerability analysis modifying environmental factors. This is expected to be covered by ISO/IEC JTC1/SC27 standards, although this methodology might be used for such analysis.
- Classify biometric systems depending of its performance against different ambient conditions

2 Conformance

A paragraph.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 19795-1, Biometric Performance Testing and Reporting — *Part 1: Principles and Framework*

ISO/IEC 19795-2, Biometric Performance Testing and Reporting — *Part 2: Testing Methodologies for Technology and Scenario Evaluation*

ISO/IEC 19795-3, Biometric Performance Testing and Reporting — *Part 3: Modality Specific Testing*

4 Terms and definitions

For the purposes of this document, the following terms and definitions apply / the terms and definitions given in … and the following apply.

4.1
Typical indoors conditions
text of the definition

5 Symbols (and abbreviated terms)

A paragraph.

6 Overview of environmental evaluation methodology

Before evaluation some statements have to be specified in order to focus the goal of the evaluation

6.1 Define evaluation objectives

Objectives have to be defined. These include the following issues:

- A description of biometric system to analyse. This consists on an explanation of components that compose the system to test.

- In which modality biometric system bases on. It is important in order to know which envoronmental factors must be assessed. ISO/IEC 19795-3 addresses all factors that shall be tested.

- A guide of how biometric system works. This guide will be used during the subsequent tests.

6.2 Define operational environment

The operational range in which biometric system works have to be defined. There must be a range for each environmental parameter to assess.

6.3 Define extreme conditions

Taking into account operational range, extreme conditions for each environmental parameter shall be defined. These conditions have been outside of operational range.

7 Relevant scenarios

Biometric systems have to be tested in different scenarios in order to analyse whether its performance is influenced by ambient conditions. These scenarios must to be selected according to environmental conditions to test during the evaluation.

In each scenario only one parameter shall be modified in order to note its influence. The rest of them have to be kept fixed and with the value of the typical indoor scenario.

7.1 Typical indoor scenario

This scenario has typical indoors ambient conditions. These conditions are:

- Temperature: between 22 to 25 ºC
- Relative humidity: between 40 to 60% RH
- Illumination:
  - Visible light (400 to 750 nm) with an intensity between 1,000 to 2,500 lux
  - Near infrared light (750 to 900 nm) with an intensity between 0 to 1,000 lux

EXAMPLE This is the typical conditions of an office.

7.2 Operational range scenarios

For each parameter, four measurements shall be made: two near both limits of the specified range and two within operational range at an equidistant distance from the boundaries.

7.2.1 Temperature scenarios

7.2.1.1 Minimun temperature into operational range

A paragraph.

7.2.1.2 Maximun temperature into operational range

A paragraph.

NOTE Note integrated in the text.

7.2.1.3 Temperature operational range variability

A paragraph.

EXAMPLE Example integrated in the text.

7.2.2 Humidity scenarios

7.2.2.1 Minimun relative humidity into operational range

A paragraph.

7.2.2.2 Maximun relative humidity into operational range

A paragraph.

NOTE Note integrated in the text.

7.2.2.3 Relative humidity operational range variability

A paragraph.

EXAMPLE Example integrated in the text.

7.2.3 Illumination scenarios

7.2.3.1 Minimun illumination into operational range

A paragraph.

7.2.3.2 Maximun illumination into operational range

A paragraph.

NOTE Note integrated in the text.

7.2.3.3 Illumination operational range variability

A paragraph.

EXAMPLE Example integrated in the text.

7.3 Extreme conditions scenarios

7.3.1 Extreme scenarios for temperature

7.3.2 Extreme scenarion for relative humidity

7.3.3 Extreme scenarios for illumination

8 Test population

A wide set of users shall be chosen to participate in performance evaluation. These users shall satisfy specific characteristic in order to obtain generic results. People have to be of different gender, age, ethnic origin and occupation. In addition, the number of users has to be significant regarding the target user population.

NOTE 1: Users should be informed about the possibility of having to take part many times during the evaluation. It is important that they know and accept a visit schedule and all related legal issues in order to avoid problems while evaluation is performed.

NOTE 2: Users must know how to use the biometric acquisition sensor within the test instruments (e.g. climatic chamber) to make their interactions easier and to achieve the OE.GUIDE objective.

9 Test equipment

Test instruments must cover two main functionalities at the evaluation: keep stable test scenario conditions and register all results both ambient conditions and biometric performance data.

All of these measuring instruments have to cover all operational range and it is recommended to exceed it. This over-requirement could avoid non-lineal conditions near the limits.

9.1 Scenario conditions

9.1.1 Test instruments for temperature

The equipment must produce controlled temperature environments. It shall have enough space to introduce a biometric sensor and the user's biometric reference (e.g. hands, arms, direct vision to the face or eyes, etc.)

EXAMPLE Climatic chamber. In the market there are a wide variety of climatic chambers with different volumes and parameters to control among several ranges. This specification requires that the climatic chamber has to be designed with special through-out holes to allow the users' interaction with biometric sensor, keeping the environmental conditions stable.

9.1.2 Test instruments for relative humidity

The equipment must produce controlled humidity environments. It shall have enough space to introduce a biometric sensor and the user's biometric reference (e.g. hands, arms, direct vision to the face or eyes, etc.)

EXAMPLE Climatic chamber. In the market there are a wide variety of climatic chambers with different volumes and parameters to control among several ranges. This specification requires that the climatic chamber has to be designed with special through-out holes to allow the users' interaction with biometric sensor, keeping the environmental conditions stable.

9.1.3 Test instruments for illumination

The equipment must produce a controlled illumination area taking into account type of light, intensity and orientation.

EXAMPLE Illumination Controlled Area: certain space or room where different bulbs and fluorescent have to be allocated. These lights must be laid out in a uniform way and shall illuminate capture sensor directly. Depending on scenario requirements and the power emitted from the light sources, the number of bulbs and/or fluorescent and their location will be changed to satisfy the specified ranges.

9.2 Measuring instruments

9.2.1 Measuring instruments for temperature

EXAMPLE A climatic chamber has the instruments to measure both the temperature and humidity. Therefore, no further instrument is needed, as long as such equipment do not have an uncertainity above 0.5 degrees for temperature, and 0.5% for humidity.

9.2.2 Measuring instruments for relative humidity

9.2.3 Measuring instruments for illumination

EXAMPLE Spectrometer. This instrument permits to analyze the intensity for a wide range of light spectrum. It is necessary to install a special instrument in the receptor to obtain omni-directional measurements. Such sensor has to be located as next as possible to the biometric capture device.

9.3 Register instruments

An automatic system for recording significant data generated during tests. This kind of system makes evaluator‘s work easier and it prevents from human mistakes. Evaluation ends up being more independent and reports will be generated more easily. This automatic system could have multiple configurations: for biometric related data it can be a part of biometric application, for ambient parameters it can belong to the measurement instruments or, in general, it can be an independent application and/or a mixture of them. Evaluator shall decide the better way to save all requested data.

10 Test results

During the evaluation several data are generated. From such data, evaluators must check that evaluation methods are applied properly and test equipments work correctly. All these data have to be saved.

Later, biometric data are used by evaluators to calculate performance statistics and these will be reported together with non-biometric data (e.g. user data and scenario data).

10.1 Performance metrics

Several rates are normally used to measure biometric system performance. Evaluators must report the same rates that ISO/IEC 19795 Part 1 and 2 specified for their evaluations.

10.1.1 Error rates

- FTA: Failure To Acquire. Proportion of verification attempts for which the system fails in capture or location phases.
- FNMR: False Non-Match Rate. Proportion of genuine attempt samples falsely declared not to match the template of the same characteristic from the same user supplying the sample.
- FMR: False Match Rate. Proportion of zero-effort impostor attempt samples falsely declared to match the compared non-self template.

10.1.2 Throughput rates

These are based on computational speed and human-machine interaction. Throughput rates show the number of users that can be processed per time unit.

10.2 Non-biometric data

Apart from biometric data, a lot of non-biometric information will be generated during evaluation. This information is important in order to allow the evaluator to understand and analyse results later. Some data to be saved are:

- Personal data of users*:* gender, age, ethnic origin, occupation, attitude against the system, etc.
- Scenario users: the number of users that have participated in each scenario*.*
- Environmental data: data collected during evaluations about atmosphere conditions. For each scenario it must record:
  - The average temperature and relative humidity.
  - The maximum and minimum temperature and relative humidity.
  - A graphic of the spectrum of light with the intensity for each wavelength, within the relevant range.

11 Evaluation methodology

11.1 Biometric system shall be suitable for testing

Evaluator must examine the biometric system, check if its configuration is consistent with configuration specified in the objectives of evaluation and whether biometric system includes all hardware and software to be tested.

In addition test equipments have to be calibrated and its operation shall be verified.

Operational environment objectives have to be applied.

NOTE 1: At this point it is suggested that evaluators contact with the set of users needed for perform the evaluation, and start programming their visits to the evaluation laboratory.

11.2 Examine biometric system

Biometric system shall be installed and started-up. Evaluator shall determine the state of the biometric system and analyse that it works properly.

NOTE 1: A simple proof to perform an enrolment and a further verification of one or two users is enough to check that the biometric system works correctly.

11.3 Devise a test subset

A set of tests have to be selected. Also a properly strategy to evaluate biometric system has to be planned.

EXAMPLE For an authentication system, a possible set of tests could be verify function.

11.4 Produce test documentation

Evaluator must describe in detail all test plans for the overall test set. This documentation shall specify all test procedures in order to guarantee that tests will be repeatable. Such documentation has to include at least:

- the approach that will be used
- the initial conditions and test scenarios that must be applied
- subjects and test equipments that will be needed

11.5 Conducting testing

Evaluator shall execute the entire set of tests specified for the evaluation. In any case, if the evaluator considers that new tests have to be done, those will be carried out too. This new test may be needed according to the behaviour of the biometric system in previous tests. All of them shall be justified and documented.

11.5.1 Approach to carry out testing

Evaluator must follow a set of steps in order to carry on the evaluation. In general two previous steps must be followed:

1. Explain genuine users how to use the biometric sensor under test.
2. From the complete set of users choose how many of them will behave as genuine users, and how many will be impostors.

3. Execute steps for enrollment and/or verification functions

4. Generate and report all data specified for the evaluation

11.5.1.1 Enrollment function

1. Introduce biometric system into the modeled scenario.

2. Generate the environmental conditions fixed for the enrolment scenario and wait till scenario conditions are reached. Biometric system will reach these conditions gradually. This prevents the system suffering from impacts derived from sudden changes in scenario conditions.

3. Check if the environmental parameters are stable and within the ranges stated for the enrolment scenario.

4. Run the biometric application and check if it is working properly.

   NOTE 1: One or two enrollments are enough.

5. Begin with the enrolment process. For all genuine users selected, the following actions shall be completed:

   a. Start function for a new enrolment.

   b. User must present his/her biometric reference to sensor when biometric application requests it. This action may be repeated several times depending on how enrolment function has been implemented. During enrolment, each user will be identified by means of name or number. Evaluator must make sure that it is unique for each user.

   c. Wait whereas biometric system generates the corresponding template and saves it. When enrolment has finished, biometric system will show the result. Typically this result is a message like “Enrolment successful” or “Enrolment failure”.

   d. If FTE error is returned, a new enrolment may be carried out. If not, this user has to be removed from the list for the remaining evaluation. Evaluator shall choose the best options according to the number of available users and the size o samples needed for test.

6. Performance rates and statistics specified for enrolment must be recorded.

NOTE 1: It is recommend that users are guided during this process and administrator controls that enrolment has been done correctly.

11.5.1.2 Verification function

1. Introduce biometric capture sensor into the modeled scenario.

2. Generate the environmental conditions fixed for this scenario and wait till scenario conditions are reached. Biometric sensor will reach these conditions gradually. This prevents the sensor suffering from impacts derived from sudden changes in scenario conditions.

3. Check if the environmental parameters are stable and within the ranges stated for the scenario.

4. Run the biometric application and check if it is working properly.

   NOTE 1: One or two verifications are enough.

5. Begin with verification process. For each user, both genuines and impostors, the following steps has to be followed:

e. Start function for authentication.

f. Introduce the identifier of the corresponding user. If it is an impostors choose randomly the identifier of a genuine user. Identifiers chosen have to be reported for traceability.

g. Present his/her biometric reference to the sensor when the application requires it. Maybe, this action will be required several times. Also sensor can indicate that user moves up or down his/her biometric reference or get it out. User must follow all of these instructions.

h. Wait while biometric system matches the sample with the corresponding template. The result return is usually a message like “Matching successful” or “Matching Failed”.

i. Record verification results, ambient factors of scenario and any other result that may be relevant to carry out the complete analysis.

j. Wait until scenario conditions are recovered after the user interaction.

6. Performance rates and all statistics specified for verification process shall be obtained.

7. Repeat these steps until biometric system has been checked in all scenarios.

11.6 Record information related to test

Some information must be saved during the test execution. It has to incorporate:

- instructions to connect and setup test equipments
- test pre-requirements
- how to interact with the interface
- the behaviour of the interface
- expected test results and actual test results

11.7 Analyze the consistence of results

Evaluator has to compare test results with the expected results. If there are differences, these shall be documented. Then evaluator must analyse the problems shown and perform all proper changes required.

11.8 Report results

Test results and testing information must be reported in order to know the results of the evaluation. Reports have to detail:

- test configurations
- interfaces tested
- the overall testing approach
- final results obtained

Annex A
(normative)

Annex title

A.1 General

A.2 Clause

A.2.1 Subclause (level 1)

A.2.1.1 Subclause (level 2)

A paragraph.

A.2.1.1.1 Subclause (level 3)

A paragraph.

Bibliography

[1] ISO/IEC Directives, Part 2, *Rules for the structure and drafting of International Standards*, 2001

[2] ISO/IEC TR 10000-1, *Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework*

Evaluation Methodology Based on CEM for Testing Environmental Influence in Biometric Devices

Belen Fernandez-Saavedra, Raul Sanchez-Reillo, Raul Alonso-Moreno
University Carlos III of Madrid
Electronics Technology Dpt. – University Group for Identification Technologies (GUTI)
Avda. Universidad, 30; 28911 – Leganes (Madrid); SPAIN
{mbfernan,rsreillo,ramoreno}@ing.uc3m.es

Abstract — **During these past years biometrics is becoming important as a technique to provide security. The number of biometric products and biometric applications on the market has increased significantly. Most of biometric suppliers claim excellent performance error rates for their products. Unfortunately such rates have not been tested by any independent body. Therefore consumers may not have any objective reference for comparing solutions. Independent evaluations are complex due to the dependence on multiple parameters. One of the most important is environmental conditions and how these conditions can affect the performance of capture sensors and so, the whole biometric system. In this paper authors propose a generic evaluation methodology for testing environmental influence in biometric devices. This methodology is based on the existing security evaluation for IT products (Common Criteria) and more specifically on certain methods defined on its Common Evaluation Methodology (CEM).**

***Keywords*—evaluation methodology, biometric system, environmental factors, repeatability tests.**

I. Introduction

Biometrics is nowadays being increasingly used for providing user authentication in current Information Systems. As more are more biometric products are introduced in the market and both, the privacy of the data handled and their use as a security mechanism, are very important, it is becoming a must to analyze their security properties.

As IT products, biometric devices can be evaluated by Common Criteria (CC). However, such products have special characteristics to be included in their security evaluation. Biometric is based on probabilistic functions and it is very dependent on several factors as environmental conditions, users and their attitude, or sample quality. This has been remarked by some previous works like BEM [1], Best Practices [2] and ISO/IEC 19795-1 International Standard [3]. As these factors are parameters that can influence in system performance, they also might affect the security level achieved. Currently there are some Protection Profiles [4] [5] [6] and [7] and Security Targets [8] for biometric devices, but none of them consider environmental factors as a variable parameter to evaluate the security level achieved. Previous studies by the authors [9] have shown that environmental conditions can change significantly the security level offered by biometric products.

In CC [10] environment conditions are only considered as assumptions and they are translated into security objectives for operational environment, not being evaluated ever. On the contrary, authors consider that biometric devices have to be evaluated against a set of significant environmental conditions and such conditions have to be generated in a controlled way in order to carry out repeatable, reproducible and objective tests.

In this work, authors propose a general methodology to test biometric products under different ambient conditions for its operational range. This methodology is based on CEM methodology [11], proposed for independent testing (ATE_IND) and is defined according to biometric products/devices of any biometric modality and their particular features. In addition, authors propose the same evaluation methodology to perform penetration test as part of the vulnerability analysis (AVA_VAN). Biometric systems must also be evaluated under extreme conditions and out of its operational range to assure that these systems always keep the security target.

As mentioned in the preceding paragraph, there will be two consecutive evaluations: one within the typical operational range and another under extreme conditions. Both will be illustrated through a characteristic example: a biometric system used for access control to particular resources in a company with typical indoor conditions.

Next section introduces the specifications and objectives for the evaluation of biometric systems and their acquisition sensors as well as ST (Security Target) in CC. In section III, the evaluation methodology based on ATE_IND actions specified at CEM will be described. The following sections will explain in detail the overall tests plan including the selection of relevant scenarios, test resources needed, initial conditions for each test, selection of target population, results to analyze and other important issues that should be considered in biometric performance testing. Later, in section IX relevant scenarios for vulnerability analysis and how to conduct penetration tests will be defined. Finally, in section X main conclusions will be presented.

II. Biometric Systems as TOE

In order to focus the proposed evaluation methodology, this section will detail only major parts defined at ST needed for better understanding. This includes TOE overview, security problem definition, security objectives and TOE summary specification. Some of these statements have been defined from biometric PPs [4] [5] [6] and [7], and ST [8] that have already been published.

A. TOE Overview

The target of evaluation is a general biometric system used to personal identification. This system consists of a capture sensor connected to a PC or token where biometric algorithms process the information received from the sensor. Also the system may have a database where biometric templates are stored and associated with the corresponding users. Such database can belong to the same PC or token or be an independent part which is connected to it.

Biometric system normally has three main functions:

1) Enrolment: this function involves a transaction in which user presents his/her biometric reference to sensor. It is processed to generate and store a template for that individual.

2) Verification: in this function users presents his/her biometric reference to sensor and it is processed to compare with his/her template and verify his/her identity previosly claimed.

3) Identification: in this case users presents his/her biometric reference to sensor and it is processed to compare with all templates in order to find his/her identifier.

B. Security Problem Definition

Considering major characteristics of the current evaluation, an outline of the security problem is defined as following:

1) Threats:

- T.ENVIRONMENT: Environmental conditions could be modified to get access to biometric system. Biometric system must provide security in its operational range in spite of the influence of these factors.
- T.IMPOSTOR: Impostors and attackers could try to access to the biometric system.

2) Organisational Security Policies:

- OP.FMRFNMR: Biometric system must meet a recognised national or international standard for false acceptance and false rejection rates.

3) Assumptions:

- A.VERIFICATION: Type of comparison mode of biometric system will be verification.
- A.SENSOR: Although performance rates are calculated within the whole biometric system, only capture sensor will be subjected to different ambient conditions.
- A.TYP_CONDITIONS: For the complete evaluation, we refer to typical ambient conditions as the next conditions:
  - Temperature: between 22 to 25 ºC.
  - Relative Humidity: between 40 to 60 % RH.
  - Illumination: Visible light between 400 to 750 nm with an intensity between 1,000 to 2,500 and near-infrared light (NIR) between 750 to 900 nm with an intensity between 0 to 1,000.
- A.USER: Biometric reference could change at different ambient conditions. But only biometric sensor will be tested in this evaluation. Therefore biometric reference will be kept at typical ambient conditions (A.TYP_CONDITIONS) until it will have to be presented to capture sensor.
- A.GUIDE: Biometric performance depends on the attitude of users and also his/her knowledge of the system. As well as it happens at the previous assumptions, only biometric sensor will be evaluated. Consequently users will be guided during all evaluation process.
- A.ENROL: Enrolment will be realized indoors and we suppose typical (A.TYP_CONDITIONS) ambient conditions.
- A.AMBIENT: There are several environmental parameters that can influence on a generic biometric system. In this paper, authors will only consider some of them (temperature, humidity and illumination) to explain this evaluation methodology. However, this methodology can be applied to other parameters related to environmental conditions (e.g. noise, vibration, corrosion, etc), defining their relevant scenarios and test equipments.

C. Security Objectives

1) TOE Security Objectives:

- O.FMRFNMR: Biometric system shall meet specified error rates.
- O.SENSOR: Biometric sensor has to perform correctly in its operational range.
- O.VERIFICATION: Biometric system must provide a biometric verification mechanism to authenticate users.

2) Operational Environment Security Objectives: Those operational objectives related to environmental factors, specify the operational range in which biometric sensor must work properly. These will be defined in a generic way. Then they will determined based on the example of an indoor biometric access control. These objectives do not include extreme conditions because its will be defined into the analysis on vulnerabilities later.

- OE.TEMP: Operational temperature range is between Tmin to Tmax. In our example: Tmin=0ºC and Tmax=50ºC.
- OE.HUM: Operational humidity range is between RHmin to RHmax. In our example: RHmin=20% and RHmax=80%.
- OE.LIGHT: Operational Illumination range is a wavelength band between 400-900nm. We define different intensity ranges for visible and near-infrared

light. For visible intensity has to be between IVmin and IVmax and for NIR shall be between INIRmin and INIRmax. In our example: IVmin=1,500 to IVmax=3,000 and INIRmin= 0 to INIR= 1000.

- OE.SYSTEM: Biometric system without capture sensor works in typical ambient conditions (A.TYP_CONDITIONS).
- OE.USER: Users are in typical ambient conditions (A.TYP_CONDITIONS). Only when they have to present their biometric reference to the capture sensor these conditions could be changed.
- OE.GUIDE: There is an administrator to control enrolment and to guide users all the time.
- OE.ENROL: Users' enrolment is carried out in typical ambient conditions (A.TYP_CONDITIONS).

D. Security Requirements

1) SFRs (Security Functional Requirements): The translation of the above security objectives to security functional requirements uses mainly components of identification and authentication class (Class FIA) with refinements for biometric systems. The most important of these are:

- FIA_SOS: Specification of secrets.
- FIA_UAU: User authentication.

2) SARs (Security Assurance Requirements): security assurance requirements are generally specified depending on the EAL selected for evaluation. In this case we comment on those families related to evaluation methodology offered in this paper.

- ATE_IND: Independent test. Evaluation methodology for addressing performance testing of biometric products into their operational range is based on this family. That is why their components should include specific refinements taken from BEM [1]. Such refinements are the following:
    - Performance testing is needed to determine the effectiveness of security mechanisms in biometrics. Major performance evaluation results to be considered are FMR and FNMR.
    - Testing of these rates must include appropriate and statistically representative data that validate such rates.
    - Test should also include checks on the environmental conditions.
- AVA_VAN: Analysis of vulnerabilities. On the contrary, this family addresses performance testing of biometric products outside their operational range. As the previous family these components must include the same refinements for biometric products.

E. TOE Summary Specification: TOE Security Functions

- F.ENROL: this function allows that users can gather into the biometric system. It asks the user to introduce a username or identifier and then it requires that he/she presents his/her biometric reference to sensor as many times as necessary. Biometric system generates a template and stores it into its database.
- F.VERIFY: this function provides the ability to authenticate a user. The biometric system requests the user to enter his/her username or identifier. Later it asks the user to presents his/her biometric reference to the capture sensor under test. Then it calculates the feature vector that is compared to the corresponding template. Finally, the biometric system shows the decision of such comparison.

III. Evaluation Methodology

From objectives, assumptions and considerations for operational environment above mentioned, authors suggest the following evaluation methodology based on ATE_IND work units detailed at CEM [11].

A. TOE shall be suitable for testing

Evaluator must examine the biometric system, check if its configuration is consistent with configuration specified in the ST and whether TOE includes all hardware and software to be tested.

In addition test equipments have to be calibrated and its operation shall be verified.

Operational environment objectives have to be applied. For this evaluation, this clause is not considered due to the fact that this is what is really going to be modified during the tests.

At this point authors suggest contacting with the set of users needed for perform the evaluation, and start programming their visits to the evaluation laboratory.

B. Examine the TOE

Biometric system shall be installed and started-up. Evaluator shall determine the state of the TOE and analyse that it works properly. A simple proof to perform an enrolment and a further verification of one or two users is enough to check that the biometric system works correctly.

C. Devise a test subset

A set of tests have to be selected. Also a properly strategy to evaluate the TOE has to be planned. In this case, the interface to evaluate is the F.VERIFY function. We will explain the approach to evaluate its performance at different environmental conditions in the next section.

F. ENROL function is not analysed because users enrol at standard ambient conditions (OE.ENROL) and the target of evaluation is testing the influence of environmental conditions.

D. Produce test documentation

Evaluator must describe in detail all test plans for the overall test set. This documentation shall specify all test procedures in order to guarantee that tests will be repeatable. Such documentation includes: the approach that will be used, the initial conditions and test scenarios that must be applied, subjects and test equipments that will be needed, etc. Such documentation is the basis of the evaluation to be carried out in the following sections.

E. Conduct testing

Evaluator shall execute the entire set of tests specified for the evaluation. In any case, if the evaluator considers that new tests have to be done, those will be carried out too. This new test may be needed according to the behaviour of the TOE in previous tests. All of them shall be justified and documented.

F. Record information related to test

Some information must be saved during the test execution. This has to include instructions to connect and setup test equipments, test pre-requirements, how to interact with the interface, the behaviour of the interface, expected test results and actual test results. Most of these instructions will be described when test plan is specified. Therefore only test results to record will be explained related to the evaluator action.

G. Analyze the consistence of results

Evaluator has to compare test results with the expected results. If there are differences, a fail is reported. He/She must analyse the problems shown and perform all proper changes required.

H. Report results

Test results and testing information must be reported in order to know the results of the evaluation. Reports have to include TOE test configurations, interfaces tested, the overall testing approach and final results obtained.

Once evaluation methodology has been defined, all documentation related to test plan for the set of scenarios will be described in detail.

IV. Relevant Scenarios to Evaluate

Biometric systems have to be tested in different scenarios in order to analyse whether its performance is influenced by ambient conditions. These scenarios are selected according to environmental conditions defined as operational environment objectives (OE.TEMP, OE.HUM and OE.LIGHT). In each scenario only one parameter is modified in order to note its influence. The rest of them are kept fixed and with the value of the typical scenario (A:TYP_CONDITIONS). For each parameter, four measurements shall be made: two near both limits of the specified range (e.g. Xmin and Xmax) and two within operational range at an equidistant distance from the boundaries (e.g. X_1 and X_2).All relevant scenarios are showed at Table I.

V. Test Equipment

A set of measuring instruments is necessary to perform this independent testing. These instruments must cover two main functionalities at the evaluation: keep stable test scenario conditions and register all results both ambient conditions and biometric performance data.

TABLE I
RELEVANT SCENARIOS FOR INDEPENDENT TESTING

	SCENARIO	**T (ºC)**	**RH(%)**	**ILLUMINA.**
STD.	Typical A.TYP_ CONDITIONS	22-25	40-60	Visible 1,000 to 2,500 NIR 0 to 1,000
TEMP.	Cool	Tmin (e.g. =0)	40-60	Visible 1,000 to 2,500 NIR 0 to 1,000
	High	Tmax (e.g. =50)		
	Temp. Range Variability	T_1 (e.g. = 23)		
		T_2 (e.g.= 36)		
HUM.	Low humidity	22-25	RHmin (e.g. =20)	Visible 1,000 to 2,500 NIR 0 to 1,000
	High humidity		RHmax (e.g. =80)	
	RH. Range Variable		RH_1 (e.g.=40)	
			RH_2 (e.g.= 60)	
LIGHT	Low light	22-25	40-60	Visible IVmin (e.g.1,500 to 1,600) NIR INIRmin (e.g. 0 to 100)
	High light			Visible IVmax (e.g.3,400 to 3,500) NIR INIRmax (e.g. 900 to 1,000)
	Light Range Variable			Visible IV_1 (e.g.1,600 to 2,500) NIR $INIR_1$ (e.g. 100 to 500)
				Visible IV_2 (e.g.2,500 to 3,400) NIR $INIR_2$ (e.g. 500 to 900)

A. Scenario conditions

1) Temperature and humidity: Climatic chamber. This equipment can produce controlled temperature and humidity environments. In the market there are a wide variety of climatic chambers with different volumes and parameters to control among several ranges. The climatic chamber for this evaluation shall have enough space to introduce a biometric sensor and the user's biometric reference (e.g. hands, arms, direct vision to the face or eyes, etc.). This specification requeires that the climatic chamber has to be designed with special through-out holes to allow the users' interaction with biometric sensor, keeping the environmental conditions stable.

2) Illumination Controlled Area: certain space or room where different bulbs and fluorescent have to be allocated. These lights must be laid out in a uniform way and shall illuminate capture sensor directly. Depending on scenario requirements and the power emitted from the light sources, the number of bulbs and/or fluorescent and their location will be changed to satisfy the specified ranges.

B. Measuring instruments

1) Temperature and humidity: typically the climatic chamber has the instruments to measure both the temperature and humidity. Therefore, no further instrument is needed, as long as such equipment do not have an uncertainity above 0.5 degrees for temperature, and 0.5% for humidity.

2) Illumination: Spectrometer. This instrument permits to analyze the intensity for a wide range of light spectrum. It is necessary to install an special instrument in the receptor to obtain omni-directional measurements. Such sensor has to be located as next as possible to the biometric capture device.

All of these measuring instruments have to cover all operational range and it is recommended to exceed it. This over-requirement could avoid non-lineal conditions near the limits.

C. Register instruments

Authors suggest an automatic system for recording significant data generated during tests. This kind of system makes evaluator‘s work easier and it prevents from human mistakes. Evaluation ends up being more independent and reports will be generated more easily. Depending on data to be saved, this automatic system could have multiple configurations: for biometric related data it can be a part of biometric application, for ambient parameters it can belong to the measurement instruments or, in general, it can be an independent application and/or a mixture of them. Evaluator shall decide the better way to save all requested data.

VI. Test Subjects

Due to the type of TOE and the evaluation that it will be done, a wide set of users shall be chosen to participate in it. These users shall satisfy specific characteristic in order to obtain generic results. Following considerations of Best Practise [2] people have to be of different gender, age, ethnic origin and occupation. In addition, the number of users has to be significant regarding the target user population.

Authors recommended that users should be informed about the possibility of having to take part many times during the evaluation. It is important that they know and accept a visit schedule and all related legal issues in order to avoid problems while evaluation is performed.

Furthermore, they must know how to use the biometric acquisition sensor within the test instruments (e.g. climatic chamber) to make their interactions easier and to achieve the OE.GUIDE objective.

VII. Test Results

During the evaluation several data are generated. From such data, evaluators must check that evaluation methods are applied properly and test equipments work correctly. All these data have to be saved.

Later, biometric data are used by evaluators to calculate performance statistics and these will be reported together with non-biometric data (e.g. user data and scenario data).

Authors suggest recording at least the following kind of information:

A. Performance metrics

Several rates are normally used to measure biometric system performance. Authors propose to employ the same rates that ISO/IEC 19795-1[3] analyse for their evaluations. These rates are:

1) Error rates:

- FTA: Failure To Acquire. Proportion of verification attempts for which the system fails in capture or location phases.
- FNMR: False Non-Match Rate. Proportion of genuine attempt samples falsely declared not to match the template of the same characteristic from the same user supplying the sample.
- FMR: False Match Rate. Proportion of zero-effort impostor attempt samples falsely declared to match the compared non-self template.

2) Throughput rates: these are based on computational speed and human-machine interaction. Throughput rates show the number of users that can be processed per time unit.

B. Data available

Apart from biometric data, a lot of non-biometric information will be generated during evaluation. This information is important in order to allow the evaluator to understand and analyse results later. Some data to be saved are:

1) Personal data of users: gender, age, ethnic origin, occupation, attitude against the system, etc.

2) Scenario users: the number of users that have participated in each scenario.

3) Environmental data: data collected during evaluations about atmosphere conditions. For each scenario it must record:

- The average temperature and relative humidity.
- The maximum and minimum temperature and relative humidity.
- A graphic of the spectrum of light with the intensity for each wavelength, within the relevant range.

VIII. TEST PROCEDURE

This section addresses the steps to follow in order to carry on the evaluation. There are three first steps common to all scenarios, which are related to the enrolment of users. Then the rest of steps are different for each scenario.

1. Explain users how to use the biometric sensor under test. (OE.GUIDE).

2. From the complete set of users choose how many of them will behave as genuine users, and how many will be impostors.

3. Begin with the enrolment process. For all genuine users selected, the following actions shall be completed:

    a. Start function for a new enrolment.
    b. Check whether the environmental conditions comply to those stated for the Office scenario.
    c. User must present his/her biometric reference to sensor when biometric application requests it. This action may be repeated several times depending on how F. ENROL function has been implemented. During enrolment, each user will be identified by means of name or number. Evaluator must make sure that it is unique for each user.
    d. Wait whereas biometric system generates the corresponding template and saves it. When enrolment has finished, biometric system will show the result. Typically this result is a message like "Enrolment successful" or "Enrolment failure".
    e. If FTE error is returned, a new enrolment may be carried out. If not, this user has to be removed from the list for the remaining evaluation. Evaluator shall choose the best options according to the number of available users and the size o samples needed for test.

    Authors recommend that users are guided during this process and administrator controls that enrolment has been done correctly (OE.GUIDE).

From here, the remaining process shall be done for each scenario.

4. Introduce biometric capture sensor into the modeled scenario.

5. Generate the environmental conditions: temperature, humidity and illumination fixed for this scenario and wait till scenario conditions are reached. Biometric sensor will reach these conditions gradually. This prevents the sensor suffering from impacts derived from sudden changes in scenario conditions.

6. Check if the environmental parameters are stable and within the ranges stated for the scenario.

7. Run the biometric application and check if it is working properly. One or two verifications are enough.

8. Begin with verification process. For each user, both genuines and impostors, the following steps has to be followed:

    a. Start function for authentication.
    b. Introduce the identifier of the corresponding user. If it is an impostors choose randomly the identifier of a genuine user. Identifiers chosen have to be reported for traceability.
    c. Present his/her biometric reference to the sensor when the application requires it. Maybe, this action will be required several times. Also sensor can indicate that user moves up or down his/her biometric reference or get it out. User must follow all of these instructions.
    d. Wait while biometric system matches the sample with the corresponding template. The result return is usually a message like "Matching successful" or "Matching Failed".
    e. Record verification results, ambient factors of scenario and any other result that may be relevant to carry out the complete analysis.
    f. Wait until scenario conditions are recovered after the user interaction.

9. Obtain performance rates and all statistics specified in the evaluation.

10. Repeat steps 4 to 9 until biometric system has been checked in all scenarios.

IX. VULNERABILITIES ANALYSIS

After all previous tests have been carried out, authors propose that TOE has to be evaluated in extreme conditions in order to check that threats as T.ENVIRONMENT do not affect TOE. Attackers can generate artificial ambient conditions to break biometric security mechanisms. From this kind of attacks, evaluators have to consider these extreme conditions as an exploitable vulnerability.

Taking into account this vulnerability penetration test shall be defined. Authors suggest specifying these penetration test, following the same evaluation methodology that the proposal for previous tests. However, other scenarios should be considered as to test TOE under extreme conditions. Such conditions are defined in Table II. Again we use biometric access control example to define such scenarios.

X. RESULTS

This methodology has been tested with different sensors of different biometric modalities. Unfortunately, due to confidentiality, detailed results for each of the sensors cannot be given. Also no results can be shown at modality level, due to heterogeneity of sensors.

What is can be said is that this methodology has been used, and results obtained have proved its viability for carrying on independent, traceable and repeatable tests. Although further improvements may be considered, such as parameter ranges, the methodology is viable and complete.

XI. Conclusions

A general evaluation methodology to perform independent tests of biometric systems has been defined. Such methodology has been specified based on Common Criteria and its Common Evaluation Methodology (CEM).

Biometric system, security problem definition and objectives of evaluation have been detailed in the same way as in a ST. Then all test plans have been described in detail following ATE_IND working units, including relevant test scenarios, test subjects, test equipments, test results and the whole test procedure to be carried out by evaluators. Finally how to perform vulnerability analysis and the proper scenarios for penetration tests have been explained.

TABLE II
RELEVANT SCENARIOS FOR ANALYSIS OF VULNERABILITIES

	SCENARIO	**T (ºC)**	**RH (%)**	**ILLUMINAT.**
TEMP.	Cold	−10- −5	40-60	Visible 1,000 to 2,500 NIR 0 to 1,000
	Very cold	−20- −10		
	Very high	50-60		
HUM.	Very low humidity	22-25	0-10	Visible 1,000 to 2,500 NIR 0 to 1,000
	Very high humidity		90-100	
LIGHT	Infrared	22-25	40-60	Visible 1,000 to 2,500 NIR 0 to 3,000
	Outdoor			Visible 1,000 to 35,000 NIR 0 to 10,000
	Darkness			Visible 0 to 100 NIR 0 to 100

Acknowledgment

This work has been partially funded by PIBES Project, which is funded by the Spanish Ministry of Science and Education (TEC2006-12365).

References

[1] Common Criteria - Common Methodology for Information Technology Security Evaluation – “Biometric Evaluation Methodology Supplement [BEM]”. v.1.0 – 2002.

http://www.cesg.gov.uk/site/ast/biometrics/media/BEM_10.pdf

[2] A. Mansfield, J. L. Wayman “Best Practices in Testing and Reporting Performance of Biometric Devices” v2.01. 2002.

[3] ISO/IEC International Standard 19795 Biometric Performance Testing and Reporting –Part 1: Principles and Framework, 2005.

[4] UK Government Biometrics Working Group, “Biometric Device Protection Profile (BDPP)”, Draft Issue 0.82, 2001.

[5] BSI, “Common Criteria Protection Profile: Biometric Verification Mechanisms”, BSI-PP-0016, v1.04. 2005.

[6] US Information Assurance Directorate, “Biometric Verification Mode Protection Profile for Basic Robustness Environments”, v1.0. 2006.

[7] US Information Assurance Directorate, “Biometric Verification Mode Protection Profile for Medium Robustness Environments”, v1.0. 2003.

[8] EWA Ltd, “Security Target for Bioscrypt^{TM} Inc. Bioscrypt^{TM} Enterprise for NT Logon”, v3.2 EWA-1360-013-350. 2001.

[9] R. Sanchez-Reillo, B. Fernandez-Saavedra, J. Liu-Jimenez and C. Sanchez-Avila, “Vascular Biometric Systems and Their Security Evaluation,” 41st Annual IEEE International Carnahan Conference on Security Technology (ICCST 2007), Proceedings, pp. 44–51, Otawa, Canada, 8-11 October, 2007.

[10] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, v.3.1 – 2006.

[11] Common Criteria - Common Methodology for Information Technology Security Evaluation – Evaluation Methodology [CEM]”. v.3.1 – 2006.