National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

U.S. Government
Biometric Verification Mode Protection Profile
For Basic Robustness Environments

Report Number: CCEVS-VR-06-0004

Dated: 15 February 2006

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Mike Allen

Jerome Myers

Aerospace Corporation

Columbia, Maryland

Common Criteria Testing Laboratory

COACT, Incorporated

Columbia, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

This report documents the NIAP validation team's assessment of the evaluation of the U.S. Government Biometric Verification Mode Protection Profile for Basic Robustness Environments. It presents the evaluation results, their justifications, and the conformance results. It acknowledges that the requirements listed in the Protection Profile (PP) are comprehensive and consistent and may be used to develop products whose security targets, which conform to this profile, will satisfy the needs of the sponsoring Government Agency, the Biometrics Management Office (BMO) of the National Security Agency (NSA).

The evaluation was performed by COACT Incorporated, an accredited Common Criteria Testing Laboratory (CCTL), and was completed during January 2006. The information in this report is largely derived from the PP, provided by BMO, and the Evaluation Technical Report (ETR) written by COACT. All security functional requirements are derived from Part 2 of the Common Criteria or special explicitly stated requirements using the format of the CC.

Products, that is, Targets of Evaluation (TOE),that conform to this PP will provide "Biometric Authentication", the automatic identification or identity authentication (verification) of living individuals based on physiological or behavioral characteristics. Examples of physiological characteristics include hand or finger images, facial characteristics, speaker verification and eye patterns. Biometric authentication is the "automatic", "real-time", "non-forensic" subset of the broader field of human identification. The focus to this PP is on the "verification mode" which means a subject claims an identity and the product will confirm or deny that claim based on biometric information. This is distinguished from "identification mode" products that accept a biometric sample and try to return an identity based solely on that sample and its database of known subjects without the subject claiming an identity.

Due to the unique nature of a biometrics TOE and the desire of the PP authors to attempt to accommodate the wide range of biometric technologies, explicit requirements were necessary, as were a great number of refinements to existing CC requirements.

In Addition, the requirements section of the PP levies requirements on the Information Technology (IT) environment that are necessary to address critical functionality that must be provided by the IT environment. In some instances the TOE only partially addresses a threat, and relies on the IT environment to play a role in completely addressing a threat. One critical aspect in these IT environment requirements is the protection of the biometrics package (i.e., trusted subject identifier, subject's reference template(s), and possibly other information). Unlike the medium robustness biometrics PP, there is no protection afforded to the biometrics package by the TOE. The acceptable degree of protection (e.g., encryption, access control provided by a database or operating system) provided by the IT environment is a determination that is made by the end-users of the TOE. It is important for integrators and certifiers to ensure that the IT environment satisfies these IT environment requirements, since they are necessary for the TOE to enforce its security policies.

One issue remains with this PP, namely the establishment of methodologies to determine the metrics for measuring the efficacy of biometric technologies. The PP authors need to assist CCEVS in the establishment of these metrics and methodologies which define the strength of function measurement and testing techniques to be used during evaluation.

The validation team monitored the activities of the COACT evaluation team, participated in team meetings, provided guidance on technical issues and the evaluation processes, reviewed successive versions of the Protection Profile, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and customer responses. The validation team determined that the evaluation showed that the PP satisfies all of the APE security assurance requirements according to the Common Criteria for Information Technology Security Evaluation, Version 2.2 and Part 2 of the Common Methodology for Information Technology Security Evaluation, Version 2.2. Therefore, the validation team concludes that the COACT findings are accurate, the conclusions justified, and the conformance claims correct.

The following interpretations applied to this evaluation:

National Interpretations:

I-0407 – Empty Selections Or Assignments, 2003-08-21

I-0410 – Auditing Of Subject Identity For Unsuccessful Logins, 2002-01-04

I-0427 – Identification of Standards, 2001-06-22

International Interpretations:

RI #137 – Rules governing binding should be specifiable, 2004-01-30

The information contained in this Validation Report is not an endorsement of the PP by any agency of the U.S. Government and no warranty of the PP is either expressed or implied.

2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product and protection profile evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products or protection profiles desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the protection profile, including:

- The Protection Profile (PP): the fully qualified identifier of the PP as evaluated;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Protection Profile	*Biometrics Verification Mode Protection Profile for Basic Robustness Environments*, Version 1.0, January 12, 2006
Evaluation Technical Report	*Evaluation Technical Report for the U.S. Government Biometric Verification Mode Protection Profile for Basic Robustness Environments*, January 20, 2006
Sponsor	Biometrics Management Office (BMO) National Security Agency (NSA)
Developer	Biometrics Management Office (BMO) National Security Agency (NSA)
Evaluators	COACT Incorporated
Validation Team	The Aerospace Corporation

3. SECURITY POLICY

The following security requirements listed in the PP make up the required security policies:

3.1. Audit Policy

The general Audit security policy calls for the capability to log and review all administrative activity as well as the presentation of claimed identity by subjects submitting biometric samples. Both success and failures are to be recorded. To support this policy the following FAU requirements are included, refined or explicitly stated as indicated.

In a refinement of the typical FAU_GEN requirements, the PP requires a TOE to generate audit events at the basic level including those events introduced by refinements and explicit requirements as determined by the ST author. Also in another refinement, additional details about what information is contained in an audit record are provided in Table 5.4 of the PP. It is possible that a user identifier may not be associated with a biometrics package (e.g., an invalid user identifier was presented), however the supplied user identifier should be captured in the audit record. This requirement applies somewhat differently depending on the type of user (i.e., untrusted user, administrator). For untrusted users, the TOE should associate auditable events to a user identifier that is supplied when a user attempts to authenticate. This case is different from an administrative user, because the TOE may have no knowledge of the human user associated with the supplied user identifier.

In a refinement of FAU_SAA, the PP requires that an alarm be generated (FAU_ARP.1) once the threshold for the audit event is met. Once the alarm has been generated it is assumed that the "count" for that event is reset to zero. The administrator settable number of authentication failures is intended to be the same value as specified in FIA_AFL. Also added are any failures of the TSF self-test and any indications of physical tampering with the TOE.

In a refinement of FAU_SEL, the PP requires "event type" to be defined by the ST author. The intent is to be able to include or exclude classes of audit events. While the administrator has the capability to "pre-select" audit events, this does not mean that this capability implicitly disables alarm events. If the administrator de-selects an audit event that is listed in FAU_SAA.1 that event will still generate an alarm if an administrator has enabled it to generate an alarm.

In a refinement of the typical FAU_ARP.1 requirement, the PP requires a TOE to generate a signal indicating an alarm condition to the environment by a method determined by the ST Author. Acceptable methods may include sending an interrupt or message to the IT environment. The TOE could satisfy this requirement by indicating an alarm without interaction with the environment, for example, an LED or audible indication that indicates an alarm condition. The intent of this requirement is to alert an administrator that the TOE has encountered a potential security violation. While some implementations may provide an alarm that communicates an alarm condition more effectively to an administrator than other implementations, the PP does not want to exclude devices that may not be able to "immediately alert" an administrator (e.g., stand alone TOEs with no connectivity).

3.2. Data Protection Policy

There is a requirement to protect the data (sample) presented for verification from being used again. In a refinement of FDP_RIP, the PP requires that the TOE ensures residual biometric data (e.g., biometric samples stored temporarily in the capture device) are not available after use in the functional identification component. This requirement was refined, since the resources may not be released or reallocated (e.g., memory may be allocated to a function and never released). The intent of the completion of an identification function is that once the TSF has completed the processing of data, that data is no longer accessible. For example, clearing a biometric sample from the capture device memory after its operation or from the "Matching and Comparison" component after a match/no match decision is made.

3.3. Identification and Authentication Policy

There are two types of Identification discussed in the PP; authorized administrators and subjects supplying a biometric sample claiming an identity. Three iterations of FIA_AFL with refinements are used to address these two types of users as follows:

- A single Biometric subject (Refined to include the terms "Biometric and consecutive")
- Consecutive failure limitations on multiple subjects (Refined to also include the term "consecutive")
- Administrative user (Also refined to include "consecutive")

Security attributes defined in FIA_ATD also contain a refinement indicating that security attributes are only associated with administrative users.

An explicit requirement is added to establish the details needed for enrollment of subjects presenting biometric samples.

Two types of identification are cited in the PP; biometric and non-biometric. FIA_SOS is used to establish the metrics to be used to ensure the strength of the mechanism is adequate for each type of user. The PP authors need to assist CCEVS in the establishment of these metrics and methodologies to define the strength of function measurement and testing techniques for the various biometric technologies.

FIA_UAU is refined as necessary to again differentiate between a subject submitting a biometric sample and an authorized administrator. It is noted that subjects submitting biometric samples against a claimed identity are not true users of the TOE since they have no direct interaction with the TOE after authentication and are never granted any privileges on the TOE.

FIA_USB is refined to again limit these requirements to the administrative user.

3.4. Security Management

The PP calls for TOE developers to limit the ability to determine the behavior of, enable, disable, or modify the behavior of various security functions to an authorized administrator. This is accomplished with seven different iterations of FMT_MOF, some of which involve refinements. The following is a list of the functions identified for security management in the PP.

- Audit
- Alarms and audit analysis
- Self-test (Refined to add the term "Invoke")
- Changing Modes
- Enrollment (Refined to add the concept of "Perform")
- Non-biometric Authentication
- Biometric Authentication

FMT_MTD is used in the PP to identify the parameters that may be queried and set by an authorized administrator. In addition, FMT_REV is refined to limit the revocation of security attributes to the administrative users. Finally, FMT_SMR is used to define the sole administrator role for products developed using this PP.

3.5. Self Protection Policy

Several self protection requirements are levied on the TOE as well as the environment. The following is a summary of those that are list, refined or explicitly stated.

An explicit requirement called "Detection of Physical Attack" was added to detect physical tampering with the TOE because the existing CC requirements do not allow for identifying the specific scenarios the TOE must detect. This requirement includes all components of the TOE (e.g., capture device, enrollment device). The intent of this requirement is to detect if someone has "opened" the TOE's physical housing. Exposing the internal components by "cutting" through the housing or other means of disturbing the integrity of the housing are not addressed by the loss of continuity aspect of this requirement. The ST author is free to address this type of physical tampering by filling in the open assignment. One method of detecting physical tampering could be an interlock switch. When detection of physical tampering occurs an audit record and alarm are generated.

In addition to the above explicit requirement, the typical FPT_RVM requirement and an explicit FPT_SEP requirement are included to ensure the TOE is always invoked and operates in a protected domain. The explicit FPT_SEP requirement is necessary, since the TOE may rely on the IT environment to provide some protection of the TSF. A CC requirement does not exist that addresses the required functionality.

Also an explicit testing requirement was added since some TOE data are dynamic (e.g., data in the audit trail, passwords) and so interpretation of "integrity" for FPT_TST.1.2 is required, leading to potential inconsistencies. The intention is that any parameter that only an administrator can control is verified to ensure its integrity is maintained. It is not necessary for the TOE to verify the integrity of audit data or user's passwords. If the TOE verifies the integrity of these, the ST author may fill in the assignment to include them. The ST author fills in the selection with any TSF data that is pertinent to their TOE (e.g., if the TOE provides more that one mode of operation, such as verification mode and identification mode, the mode of operation would go in the assignment).

Since candidate TOEs are not required to include all of the hardware necessary for the operation of the TOE, the element FPT_TST_EXP.2.1 ensures that the hardware portions included in the TOE (e.g., capture device, comparator) are tested prior to or during operations. It is not necessary to test the software portions of the TSF, since the evaluation ensures the correct operation of the software, software does not degrade or suffer intermittent faults, as does hardware, and integrity of the software portions of the TSF are addressed by FPT_TST_EXP.2.3.

3.6. TOE Access Policy

In a refinement of FTA_TAB, the PP requires that an access banner is displayed whenever the TOE will provide a prompt for identification and authentication of an administrator. The intent of this requirement is to advise administrators of warnings regarding the unauthorized use of the TOE. For untrusted users, the environment (IT or non-IT) would be responsible for displaying the appropriate banner. FTA_SSL is also included to ensure an administrative session is terminated after a settable time period of inactivity.

4. ASSUMPTIONS

Unlike the Medium Robustness Biometrics PP, the Basic robustness PP relies more heavily on the environment to ensure its security policies are satisfied. The follow assumptions concerning usage and the environment are cited in the PP.

4.1. Usage Assumptions

Administrators and authorized users are assumed to be trusted (i.e., non-malicious) and competent to carry out their responsibilities.

There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.

4.2. Environmental Assumptions

The communication paths between physically separate parts of the TOE and between the TOE and environment (IT and non-IT) are protected (e.g., physically, encrypted, etc.).

The biometrics package (i.e., reference template, and binding to a user identifier) is protected from disclosure and modification while in storage and during transmission between the IT environment and the TOE.

It is assumed that sites follow appropriate procedures for validating the identity of enrolled individuals.

The TOE is placed in an environment that does not exceed its normal operating range as defined by the vendor.

4.3. Clarification of Scope

The PP addresses a fairly comprehensive list of threats. There are, however, some threats the PP does not address, including a malicious developer inserting a backdoor into the TOE, emissions occurring during enrollment that would allow an eavesdropper to reconstruct either the biometric sample or the generated template. It is up to a certifier to determine how these types of threats apply in the target environment.

5. ARCHITECTURAL INFORMATION

This section describes biometric authentication devices as the Target of Evaluation (TOE) for this protection profile.

Biometric TOEs are unlike other information-technology-related TOEs. Untrusted users who interact with the TOE (known as "subjects" in the biometrics community, but not in the Common Criteria community) are not really *users* of the TOE. Their only role is to present a claimed identity and a fresh biometric sample, and the biometric TOE decides whether the biometric sample comes from a live individual and whether the biometric sample matches the biometric sample previously enrolled by the user with the claimed identity. The TOE does not contain any user data and does not provide a logical interface to untrusted users. The TOE only contains Trusted Security Function (TSF) data and the logical interface presented is only for administrative functions.

The physical and logical boundaries of the TOE will differ depending upon a vendor's implementation and the intended use of the product. There are many permutations of how and where these components can be hosted.

For controlling physical access (e.g., a building or room), a TOE could be comprised of components that are physically and logically housed in a single unit. An example is a device whose ultimate purpose is to control access to a door, which performs the capture and comparison functions within a single unit and is stand-alone. A TOE can also have multiple capture devices that transmit the live sample to a server that then performs the comparison function, which then generates the match/no match decision.

For controlling local logical access to an IT product (e.g., a workstation), the TOE's physical boundary could take different forms as well. As with the example above, the TOE could be contained in a single unit and provide a match/no match decision to the IT product, or the TOE could be physically separated. If the TOE is physically separated it could use the IT product to transmit data (e.g., the live sample, subject's claimed identity) through the IT product to another component of the TOE that performs the comparison function, which then in turn provides the match/no match decision to the IT product. It is important to note that unlike the TOE defined for medium robustness environments, the TOE for basic robustness environments excludes some security relevant functionality (e.g., audit storage, audit review) and may rely on another IT entity to provide logical protection to components of the TOE (e.g., an underlying OS may provide protection from tampering of software components of the TOE). This means that the comparison software or any capture controller function could execute on an IT product other than the TOE. Figure 1 illustrates an example of a TOE that is integrated into an IT product. In this example, the capture device is connected to an IT product (e.g., workstation) via a direct connection (e.g., USB connection) and the storage, comparator function, and any other TOE software resides in the IT product. The capture device transmits the live sample, and possibly other data (e.g., unique device id), to the comparator through a path that is not trusted with respect to the TOE. There is a reliance on the environment to protect this communication path (e.g., physical protection of the communication line, encryption).

The comparator retrieves the reference template from storage (in Figure 1, the storage is depicted as residing in the IT product, but the storage could be located elsewhere), which is also protected by the environment. The reference template is included in the biometric package. The comparator compares the templates and generates a match/no match decision, which is then provided to the IT product.

When the TOE is physically separated, the environment is required to maintain confidentiality and to detect modification of the transmitted data. This could be achieved by physically protecting the communication lines, or some form of logical protection (e.g., encryption).

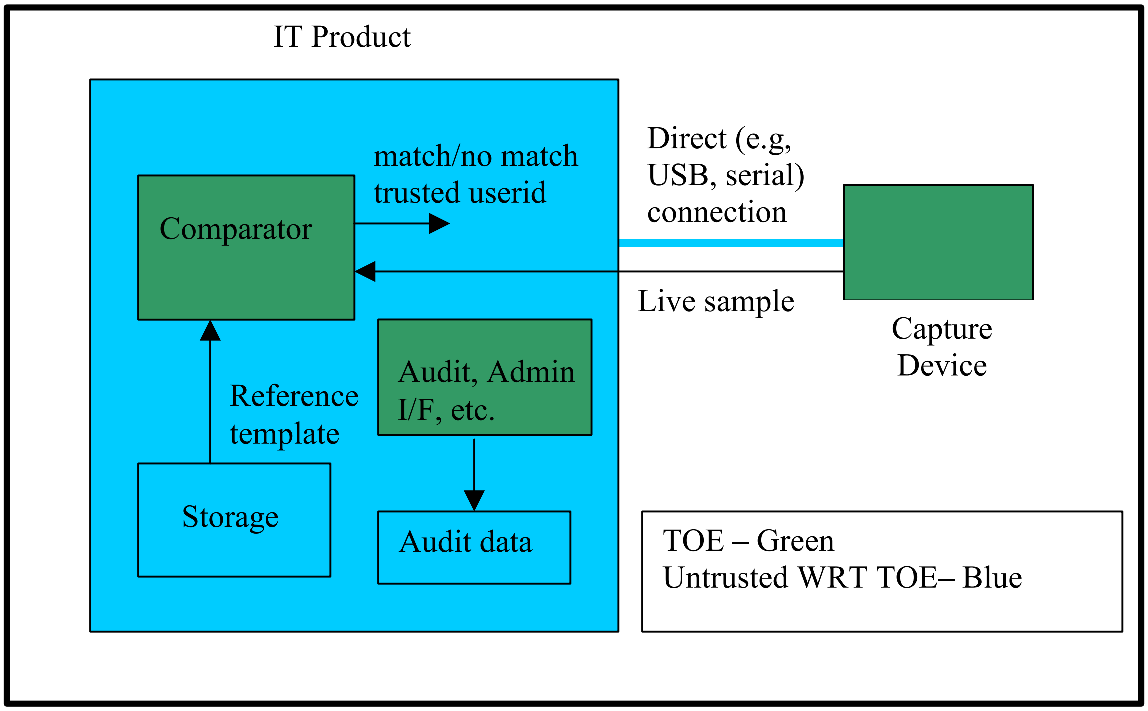

Figure 1. Example of TOE architecture with reliance on the IT environment for protection.

This TOE requires that a second, non-biometric authentication mechanism (e.g., password, PIN) be available to end-users for administrative purposes. This was done to provide end-users with the flexibility of requiring more rigorous authentication for an administrator if they choose, or to allow administrators to solely use the non-biometric authentication mechanism. The latter may be useful if the capture device became unusable.

6. DOCUMENTATION

1. Biometrics Verification Mode Protection Profile for Basic Robustness Environments, Version 1.0, January 12, 2006

7. RESULTS OF THE EVALUATION

The U.S. Government Biometric Verification Mode Protection Profile for Basic Robustness Environments has satisfied the evaluation requirements of the APE section of the CEM. The PP was assessed against the protection profile requirements as stated in the Common Criteria for Information Technology Security Evaluation Version 2.2.

8. VALIDATOR COMMENTS

The validation team's observations support the evaluation team's conclusion that the U.S. Government Biometric Verification Mode Protection Profile for Basic Robustness Environments has satisfied the evaluation requirements of the CEM.

9. GLOSSARY

BMO	Biometrics Management Office
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

10. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated January 2004, Version 2.2 Revision 256.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated January 2004, Version 2.2 Revision 256.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated January 2004, Version 2.2 Revision 256.

[4] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated January 2004, Version 2.2 Revision 256.

[5] U.S. Government Biometric Verification Mode Protection Profile for Basic Robustness Environments, Version 1.0, dated January 12, 2006.

[6] Evaluation Technical Report for the U.S. Government Biometric Verification Mode Protection Profile for Basic Robustness Environments, dated January 20, 2006.