National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

U. S. Government
Biometric Verification Mode Protection Profile
for Medium Robustness Environments,
Version 1.0

Report Number:	**CCEVS-VR-03-0050**
Dated:	**20 November 2003**
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

Kathy Cunningham
National Security Agency
Ft. Meade, MD

Common Criteria Testing Laboratory

Evaluation Team

COACT, Inc
Rivers Ninety Five
9140 Guilford Road, Suite G
Columbia, MD 21046-2587

Table of Contents

1. Executive Summary

The evaluation of the U. S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments, Version 1.0 was performed by COACT, Inc., CAFÉ Lab CCTL in the United States and was completed on 17 November 2003. The Protection Profile (PP) identified in this Validation Report has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the APE requirements of the Common Criteria for IT Security Evaluation (Version 2.1).

This Validation Report applies only to the specific version of the PP as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced.

The information contained in this Validation Report is not an endorsement of the Biometric Verification Mode Protection Profile for Medium Robustness Environments, version 1.0 by any agency of the US Government and no warranty of the PP is either expressed or implied.

The COACT, Inc., CAFÉ Lab evaluation team concluded that the Common Criteria requirements for a PP Evaluation have been met.

The technical information included in this report was obtained from the U. S. Government Biometric Verification Mode Protection Profile (PP) for Medium Robustness Environments, Version 1.0, Dated November 15, 2003 produced by U.S Government and the Biometric Verification Mode Protection Profile for Medium Robustness Environments Evaluation Technical Report (ETR), Dated November 19, 2003, Document No. F4-1103-001(2), produced by COACT, Inc., CAFÉ Lab.

1.1 Evaluation Details

Dates of Evaluation: April 2003 through November 2003
Evaluated Product: U. S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments, Version 1.0, Dated November 15, 2003
Developer: Aerospace, Biometrics Management Office (BMO) and National Security Agency (NSA),
CCTL: COACT, Inc., CAFÉ Lab, Columbia, MD
Validation Team: Kathy Cunningham, National Security Agency,
Ft. Meade, MD
Evaluation Class: None
PP Conformance: None

1.2 Interpretations

National Interpretations

I-0405	American English Is An Acceptable Refinement, 2000-12-20
I-0406	Automated Or Manual Recovery Is Acceptable, 2003-07-17
I-0407	Empty Selections Or Assignments, 2003-08-21
I-0410	Auditing of Subject Identity For Unsuccessful Logins, 2002-01-04
I-0414	Site Configurable Prevention of Audit Loss, 2003-07-17
I-0421	Application Notes In Protection Profiles Are Informative Only, 2001-06-22
I-0425	Settable Failure Limits Are Permitted, 2002-12-05
I-0427	Identification Of Standards, 2001-06-22
I-0429	Selecting One Or More, 2003-08-12

International Interpretations

003	Unique identification of configuration items in the configuration list, 2002-02-11
004	ACM_SCP.*.1C requirements unclear, 2001-11-12
019	Assurance Iterations, 2002-03-11
049	Threats met by environment, 2001-02-16
051	Use of ‘documentation’ without C&P elements, 2002-10-05
064	Apparent higher standard for explicitly stated requirements, 2001-02-16
084	Separate objectives for TOE and environment, 2001-02-16
085	SOF Claims additional to the overall claim, 2002-02-11
138	Iteration and narrowing of scope, 2002-06-05

1.3 Threats to Security

The Protection Profile identified the following Threats:

T.ADMIN_ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.ADMIN_ROGUE	An administrator’s intentions may become malicious resulting in user or TSF data being compromised.
T.AUDIT_COMPROMISE	A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user’s action.
T.BYPASS	An attacker may bypass any component of the biometric product and gain unauthorized authentication.
T.CRYPT_ATTACK	An attacker may defeat security functions through a cryptographic attack against the algorithm, through cryptanalysis on encrypted data, or through a brute-force attack and thereby gaining unauthorized authentication.
T.CRYPTO_COMPROMISE	A malicious user or process may cause key, data or executable code associated with the cryptographic

functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromise the cryptographic mechanisms and the data protected by those mechanisms.

T.HIGH_QUALITY_ARTIFACT An attacker may use a high quality artifact (e.g., artificial hand/fingerprint, life-size photograph, or other synthetic means) to gain unauthorized authentication.

T.MIMIC An attacker may masquerade as an enrolled user by presenting their biometric characteristic that is similar, or by reproducing the biometric characteristics of the enrolled user (e.g., changing his/her voice, forging a signature, or other mean of mimicry) to gain unauthorized authentication.

T.FLAWED_DESIGN Unintentional or intentional errors in requirement's specification or design of the TOE may occur, leading to flaws that may be exploited by a malicious user or program.

T.CORRUPTED_IMPLEMENTATION Unintentional or intentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a malicious user or program.

T.POOR_TEST Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being undiscovered thereby causing potential security vulnerabilities.

T.REPLAY_RESIDUAL_IMAGE An attacker may attempt to "reuse" an authorized user's biometric residual characteristic (e.g., finger print left on capture device) to gain unauthorized access.

T.RESIDUAL_DATA Residual biometric authentication data from a previous valid user if not cleared from memory may allow an attacker to gain unauthorized authentication.

T. REFERENCE_TEMPLATE An attacker modifies or creates a biometric reference template in storage or transmission to/from storage to gain unauthorized authentication.

T.POOR_ENROLLMENT An attacker may direct an attack against a low quality reference template and gain unauthorized authentication.

T.TAMPER An attacker may modify or otherwise alter the software or hardware components, the connections between them thereby gaining unauthorized authentication.

T.MALICIOUS_TSF_ COMPROMISE A malicious user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).

T.UNATTENDED_SESSION An attacker may gain unauthorized access to an administrator's unattended session.

T.UNAUTHORIZED_ACCESS A user may gain access to administrative functions for which they are not authorized according to the TOE security policy

	they are not authorized according to the TOE security policy.
T.UNIDENTIFIED_ACTIONS	The administrator may fail to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.
T.UNKNOWN_STATE	When the TOE is initially started or restarted after a failure, design flaws, or improper configurations may cause the security state of the TOE to be unknown.

2. Identification

2.1 PP and TOE Identification

PP: U. S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments, Version 1.0, Dated November 15, 2003.

CC Identification – *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999, ISO/IEC 15408.

CEM Identification – *Common Evaluation Methodology for Information Technology Security*, Part 1: Introduction and General Model, Version 0.6, January 1997; *Common Methodology for Information Technology Security Evaluation*, Part 2: Evaluation Methodology, Version 1.0, August 1999.

2.2 PP Overview

This Protection Profile (PP) specifies the minimum functional and assurance security requirements for biometric products operating in verification mode to provide authentication allowing physical and logical access control to facilities as well as to information systems in medium robustness environments (see Section 3.0 for a characterization of medium robustness environments). Biometric systems are enabling technologies designed to augment existing security measures by positively authenticating individuals based on measurable physical features or behaviors. 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 was a great deal of refinement of the CC requirements.

The requirements section of this PP specifies a need to protect biometric templates, to provide confidentially, and integrity. Since the biometric package (which includes the user identifier and their associated reference template(s)) may be stored in a device outside the control of the TOE, the biometrics TOE encrypts biometric packages for confidentiality reasons, and an enrolling TOE cryptographically signs a biometrics package so that modification of the package can be detected.

This PP defines:

- assumptions about the security aspects of the environment in which the TOE will be used;
- security objectives of the TOE and its environment;
- functional and assurance requirements to meet those security objectives; and
- rationale demonstrating how the requirements meet the security objectives, and how the security objectives address the threats.

A TOE conformant to this PP satisfies the specified functional requirements, as well as the Medium Robustness assurance requirements that are expressed in Section 5.2 TOE Security Assurance Requirements. The assurance requirements were originally based upon Evaluated Assurance Level (EAL) 4. In order to gain the necessary level of assurance for medium robustness environments explicit requirements have been created for some families in the ADV class both to remove ambiguity in the existing ADV requirements as well as to provide greater assurance than that associated with EAL4. The explicit assurance requirements are summarized in the Table below.

Assurance Class	Assurance Components	
Development	**ADV_ARC_EXP.1**	**Architectural Design**
	ADV_FSP_EXP.1	**Functional Specification with Complete Summary**
	ADV_HLD_EXP.1	**Security-Enforcing High-Level design**
	ADV_INT_EXP.1	**Modular Decomposition**
	ADV_LLD_EXP.1	**Security-Enforcing Low-Level design**
Vulnerability assessment	**AVA_CCA_EXP.2**	**Systematic cryptographic module covert channel analysis**

These explicit assurance requirements were deemed necessary by NSA to reduce the ambiguity in the associated CC assurance families and to provide the level of assurance appropriate for medium robustness environments. For more detail information on the assurance requirements, reference Section 5.2 of this PP.

2.3 IT Security Environment

In trying to specify the environments in which TOEs with various levels of robustness are appropriate, it is useful to first discuss the two defining factors that characterize that environment: ***value of the resources*** and ***authorization of the entities*** to those resources.

In general terms, the environment for the TOE can be characterized by the authorization (or lack of authorization) the least trustworthy entity has with respect to the highest value of TOE resources (i.e. the TOE itself and all of the data processed by the TOE).

3. Security Policy

The Operational Security Policies defined for the TOE:

P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.CRYPTOGRAPHIC_ FUNCTIONS	The TOE shall provide cryptographic functions (i.e., encryption/decryption and digital signature operations) to maintain the confidentiality and allow for detection of modification of TSF data that is transmitted between

physically separated portions of the TOE, or stored outside the TOE.

P.CRYPTOGRAPHY_ VALIDATED Where the TOE requires FIPS-approved security functions, only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key distribution, and random number generation services).

P.VULNERABILITY_ANALYSIS_TEST The TOE must undergo appropriate independent vulnerability analysis and penetration testing to demonstrate that the TOE is resistant to an attacker possessing a medium attack potential.

4. Assumptions

Personnel and Physical Assumptions

The specific conditions below are assumed to exist in a PP-compliant TOE environment.

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

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

A.OPERATING_RANGE The TOE is placed in an environment that does not exceed its normal operating range (e.g., temperature, humidity) as defined by the vendor.

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 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 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 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 could also have multiple capture devices that transmit the live template 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 template, capture device's 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 the TOE includes all the hardware and software that play a role in the TOE being able to satisfy the security requirements specified in this PP. When the TOE is physically separated, cryptography is used to maintain confidentiality and to detect modification of the transmitted data. It is also important to note that none of the TOE's software is executing on a platform other than the trusted platform provided by the TOE. This means that the comparison software or any capture controller function is not running on an IT product other than the TOE. Figure 1 illustrates an example of a distributed TOE. 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 IT product is connected to a network. The capture device transmits the live template, and possibly other data (e.g., unique device id), to the comparator through a path that is not trusted with respect to the TOE. This is acceptable, since the capture device signs and encrypts the data being transmitted. The comparator retrieves the reference template from storage. The reference template is included in the biometric package, which is encrypted and cryptographically signed by the TOE (or another authorized entity). The comparator compares the templates and generates a match/no match decision, whcih is then sent to the IT product in the clear. Sending the decision in the clear is permitted, since once the decision leaves the TOE's scope of control, it is left to the IT environment, including the IT product, to handle the decision appropriately.

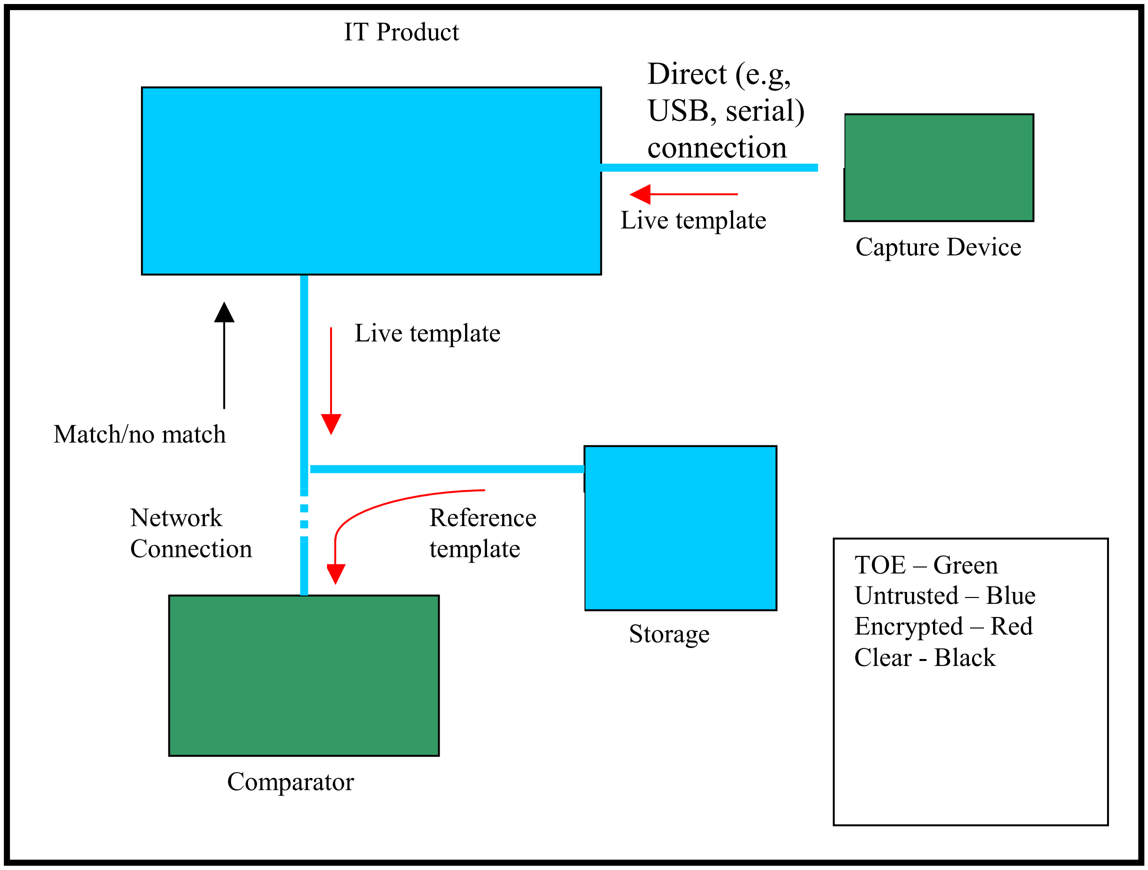

Figure 1. Example of a distributed TOE.

Another important aspect of the TOE, as defined by this PP, is that the storage of the biometric reference template is outside the scope of the TOE. This was done to allow flexibility in the deployment of the TOE and the scenarios under which the TOE or instantiations of the TOE may be used. The requirements in this PP were written to allow the storage of reference templates to take place at a single repository, be distributed across database servers, to allow single reference templates to be stored on a smart card, or other ways in which a developer wishes to handle storage. This is secure, since the biometrics package that contains the reference template is signed and encrypted by the TOE that performs the enrollment. However, the enrolling TOE must be a trusted signing authority for any instantiation of TOEs that are to use the biometric package when performing the authentication process.

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

Biometric Verification Mode Protection Profile for Medium Robustness Environments, Version 1.0, Dated November 15, 2003.

7. Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the APE section of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of the APE assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., APE) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone, electronic mail, and meetings. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. No constraints or assumptions were identified in performing this evaluation.

Chapter 3, Evaluation Results, in the Evaluation Team's ETR, states:

"The *U.S. Government Biometric Verification Mode Protection Profile (PP) for Medium Robustness Environments* was successfully evaluated."

Chapter 4, Conclusions, in the Evaluation Team's ETR, states:

"The *U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments* has satisfied the requirements of the *APE Assurance Requirement*s. The PP was assessed against the requirements as stated in the *Common Methodology for Information Technology Security Evaluation Part 2, Version 1*.0."

8. Validation Comments/Recommendations

The validation team had no recommendations concerning the U. S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments, Version 1.0.

Comments

The explicit cryptographic security functional requirements may seem long and complex as stated by the evaluators in the ETR. The purpose of these requirements is to guide the product developer in choices that are required for the FIPS 140-2 options. These requirements have specifics to tighten the cryptographic functions and bring the security level up to meet the medium robustness requirements.

The refinement for FPT_SEP.2-3 reflects the intent of the PP author, that the cryptographic portion of the TOE is maintained within its own address space.

Some of the Threats are not addressed by the TOE described herein: This arises from a misunderstanding of what threat statements are and has been propagated into this PP from other PPs.

This PP evaluation precedes the publication of the Consistency Manual for Medium Robustness Environment Profiles, which at the time of certification was under development.

In total agreement with the evaluation team's following comment found in the APE_DES.1-1 section of the ETR.
"It is not until the end of the 5th page in the TOE Description that the PP author clearly states that this PP is for a biometric TOE operating only in the verification mode. This occurs just before section 2.1.1 (5 pages later) and then the final section 2.1.2 provides more detail about this process. The PP Introduction, section 1.2 states the verification mode (as opposed to the identification mode which is separate PP) but does not explain what this is. The TOE Description describes Biometric functionality in general and includes both identification mode and verification mode, (for example, see Section 2.1) and then explains briefly what the difference between the two is. It would be much more clear to the reader if the concept of verification mode was made very clear in the opening paragraph, as it is done in the PP Introduction or more clearly explained in the PP Introduction."

9. Abbreviations

Abbreviations	Long Form
ASE	Advanced Encryption Standard
ATM	Asynchronous Transfer Method
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CEM	Common Evaluation Methodology
CM	Configuration Management
DES	Data Encryption Standard
DMZ	Demilitarized Zone
DoD	Department of Defense
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Patrol
ETR	Evaluation Technical Report
FIPS PUB	Federal Information Processing Standard Publication
FTP	File Transfer Protocol
GIG	Global Information Grid
HTTP	Hypertext Transfer Protocol
IATF	Information Assurance Technical Framework
ICMP	Internet Control Message Protocol
ID	Identification
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPSEC ESP	Internet Protocol Security Encapsulating Security Payload
IT	Information Technology
I&A	Identification and Authentication
MRE	Medium Robustness Environment
NBIAT&S	Network Boundary Information Assurance Technologies and Solutions Support
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
OR	Observation Report
PC	Personal Computer
PKI	Public Key Infrastructure
PP	Protection Profile
QA	Quality Assurance
RNG	Random Number Generator
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol

Abbreviations	**Long Form**
SOF	Strength of Function
ST	Security Target
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSE	TOE Security Environment
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy
TSS	TOE Summary Specification
UDP	User Datagram Protocol
URL	Uniform Research Locator
VPN	Virtual Private Network

10. Bibliography

The evaluation and validation methodology was drawn from the following:

[CC_PART1] Common Criteria for Information Technology Security Evaluation-Part 1: Introduction and general model, dated August 1999, version 2.1.

[CC_PART2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, dated August 1999, version 2.1.

[CC_PART2A] Common Criteria for Information Technology Security Evaluation Part 2: Annexes, dated August 1999, version 2.1.

[CC_PART3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, dated August 1999, version 2.1.

[CEM_PART 1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1997, version 0.6.

[CEM_PART2] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[CCEVS_PUB1] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Organization, Management and Concept of Operations, Scheme Publication #1, Version 2.0 May 1999.

[CCEVS_PUB2] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Validation Body Standard Operating Procedures, Scheme Publication #2, Version 1.5, May 2000.

[CCEVS_PUB3] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Technical Oversight and Validation Procedures, Scheme Publication #3, Version 0.5, February 2001

[CCEVS_PUB 4] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to CCEVS Approved Common Criteria Testing Laboratories, Scheme

Publication #4, Version 1, March 20, 2001

[CCEVS_PUB 5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Sponsors of IT Security Evaluations, Scheme Publication #5, Version 1.0, August 2000.

[GIG] Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510, Guidance and Policy for the Department of Defense Global Information Grid Information Assurance (GIG), June 2000.