National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme

Validation Report

CREDANT

Mobile Guardian Enterprise Edition

Version 5.2.1 SP4

Report Number: CCEVS-VR-VID10240-2008

Dated: 05 May 2008

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

Shaun Gilmore (Lead Validator)

NSA

Dr. Jerome F. Myers (Senior Validator)

Aerospace Corporation

Columbia, Maryland

Common Criteria Testing Laboratory

COACT CAFÉ Laboratory

Columbia, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated. Prospective users should read the Validator Comments in Section 10 carefully.

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the CREDANT Mobile Guardian Enterprise Edition Version 5.2.1 SP4, the target of evaluation (TOE), conducted by the CAFÉ Laboratory of COACT Incorporated, the Common Criteria Testing Laboratory (CCTL). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation by COACT was performed in accordance with the United States evaluation scheme and was completed on March 24th, 2008. The information in this report is largely derived from the ST, Evaluation Technical Report (ETR) and the functional testing report. The ST was written by COACT, Inc. The evaluation was performed to conform with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.3, August 2005 Evaluation Assurance Level 3 (EAL 3) and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 2.3, August 2005.

The CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Target of Evaluation (TOE) is a distributed security solution designed to control enterprise-wide security for Windows-based PCs. CMG enforces data encryption and access control security policies designed to protect data at rest on Window-based PCs. Security policy protection is intended to provide data access protection from unauthorized users accessing a PC in the event of a lost or stolen PC and implementing hierarchical data access controls for authorized PC users. The CMG is a single base management control system enabling administrators to secure the Windows-based PCs from a single management console.

The CREDANT Mobile Guardian Enterprise consists of three software components:

A) The CMG Enterprise Server is a software component that runs on a workstation dedicated to this purpose. The CMG Enterprise Server provides centralized security policy administration of the three TOE components: the CMG Enterprise Server, the CMG Policy Proxy, and the CMG Shield; all TOE management is performed from the CMG Enterprise Server. The CMG Enterprise Server provides policy management, policy distribution, key generation, key distribution, TOE component access control management, and system audit generation and viewing.

B) The CMG Policy Proxy is a software component that provides distributed communications between the CMG Shield and the CMG Enterprise Server for transparent delivery of policy updates to the CMG Shields. The CMG Policy Proxy runs on a workstation or dedicated server and enforces ongoing compliance to security policies. Multiple CMG Policy Proxies may be deployed (communicating with a common CMG Enterprise Server) for scalability.

CMG Policy Proxies connect to their installation time configured CMG Server at CMG Policy Proxy start-up. The CMG Policy Proxy authenticates to the CMG Server using the IT Environment supplied Realm authentication method. During run-time the CMG Policy Proxy periodically probes the CMG Enterprise Server for CMG Shield end user policies. Policies are forwarded to the appropriate CMG Shield when the CMG Shield contacts the CMG Policy Proxy and successfully authenticates to the CMG Policy Proxy.

The Policy Proxy TOE component is implemented in two optionally installed software variants: Gatekeeper and Policy Proxy. The Policy Proxy communicates with devices such as workstations, laptops or tablet PCs. The Gatekeeper manages CMG Shield devices such as PDAs and Smartphones. For this evaluation, only the Policy Proxy is included.

C) The CMG Shield is software that runs on the end user's devices (not dedicated). The device may be a workstation or a laptop. The CMG Shield is the on-device component that enforces security policies whether a mobile device is connected to the network or not. The CMG Shield provides on-device policy enforcement for access control and user data encryption. Policies are user and device specific.

The CMG Shield encrypts and decrypts CMG Shield host resident data files (user data) according to the CMG Shield users' policies. These encryption policies may be shared policies (multiple CMG Shield users may have access to user data), or may be user specific (only the specific user may access data). Encryption and decryption of the data is transparent to the end user.

At initial end user login, the CMG Shield communicates with the CMG Enterprise Server. If the end user's credentials are verified by the CMG Enterprise Server, the CMG Enterprise Server returns a user policy to the end user. While the end user is logged in, the CMG Shield probes the end user's configured CMG Policy Proxy for updated user policies.

CMG supports variants of shields for a variety of platforms. The security functionality provided varies somewhat according to the shield in use. For this evaluation, only the CMG Shield for Windows is included. Therefore, the security functionality described in this document describes the security functionality pertinent to the CMG Shield for Windows.

1.1. Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that no international interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation. The TOE is also compliant with all International interpretations with effective dates on or before January 26, 2007.

The Evaluation Team determined that the following NIAP interpretations applied at the time of the start of the evaluation:

I-0418 – Evaluation of the TOE Summary Specification: Part 1 Vs Part 3

I-0426 – Content of PP Claims Rationale

I-0427 – Identification of Standards

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 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 IT products 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 product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	CREDANT Mobile Guardian Enterprise Edition Version 5.2.1 SP4 Target of Evaluation
Protection Profile	None
Security Target	CREDANT Mobile Guardian Enterprise Edition Version 5.2.1 SP4 Security Target
Dates of evaluation	September 2006 through February 2008
Evaluation Technical Report	Evaluation Technical Report for CREDANT Mobile Guardian (CMG) Enterprise Edition, Version 5.2.1 SP4. Document No. E3-0208-001, Dated 29 April 2008.
Conformance Result	Part 2 and Part 3 conformant, EAL 3
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 2.3, August 2005 and all applicable NIAP and International Interpretations effective on January 26, 2007
Common Evaluation Methodology (CEM) version	CEM version 2.3, August 2005 and all applicable NIAP and International Interpretations effective on January 26, 2007
Sponsor	CREDANT Technologies, Inc., 15303 Dallas Parkway, Suite 1420, Addison, Texas 75001
Developer	CREDANT Technologies, Inc., 15303 Dallas Parkway, Suite 1420, Addison, Texas 75001

Evaluators	Bob Roland, Greg Beaver and Ching Lee of COACT Incorporated
Validation Team	Shaun Gilmore (NSA), Dr. Jerome F. Myers (Aerospace Corporation)

3. SECURITY POLICY

The CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 consists of three software components:

A) The CMG Enterprise Server is a software component that runs on a workstation dedicated to this purpose. The CMG Enterprise Server provides centralized security policy administration of the three TOE components: the CMG Enterprise Server, the CMG Policy Proxy, and the CMG Shield; all TOE management is performed from the CMG Enterprise Server. The CMG Enterprise Server provides policy management, policy distribution, key generation, key distribution, TOE component access control management, and system audit generation and viewing.

B) The CMG Policy Proxy is a software component that provides distributed communications between the CMG Shield and the CMG Enterprise Server for transparent delivery of policy updates to the CMG Shields. The CMG Policy Proxy runs on a workstation or dedicated server and enforces ongoing compliance to security policies. Multiple CMG Policy Proxies may be deployed (communicating with a common CMG Enterprise Server) for scalability.

   CMG Policy Proxies connect to their installation time configured CMG Server at CMG Policy Proxy start-up. The CMG Policy Proxy authenticates to the CMG Server using the IT Environment supplied Realm authentication method. During run-time the CMG Policy Proxy periodically probes the CMG Enterprise Server for CMG Shield end user policies. Policies are forwarded to the appropriate CMG Shield when the CMG Shield contacts the CMG Policy Proxy and successfully authenticates to the CMG Policy Proxy.

C) The CMG Shield is software that runs on the end user's devices (not dedicated). The device may be a workstation or a laptop. The CMG Shield is the on-device component that enforces security policies whether a mobile device is connected to the network or not. The CMG Shield provides on-device policy enforcement for access control and user data encryption. Policies are user and device specific.

   The CMG Shield encrypts and decrypts CMG Shield host resident data files (user data) according to the CMG Shield users' policies. These encryption policies may be shared policies (multiple CMG Shield users may have access to user data), or may be user specific (only the specific user may access data). Encryption and decryption of the data is transparent to the end user.

   At initial end user login, the CMG Shield communicates with the CMG Enterprise Server. If the end user's credentials are verified by the CMG Enterprise Server, the CMG Enterprise Server returns a user policy to the end user. While the end user is logged in, the CMG Shield probes the end user's configured CMG Policy Proxy for updated user policies.

   CMG supports variants of shields for a variety of platforms. The security functionality provided varies somewhat according to the shield in use. For this evaluation, only the CMG Shield for Windows is included. Therefore, the security functionality described in this document describes the security functionality pertinent to the CMG Shield for Windows.

The security functions provided by the TOE and are described in the following sections.

3.1.1. Audit Data Generation Security Function

The TOE's Audit Data Generation Security Function creates audit records recording security-relevant events. Audit records are generated by the CMG Enterprise Server.

The CMG Enterprise Server provides audit logs that track administrator activity and host communications. The CMG Enterprise Server creates one audit log: the Administrator Actions Log. The log is stored in the Database via the IT Environment supplied DBMS. The following events are logged in the identified tables:

Administrative Actions Log:

1. Logging into and logging out of the CMG Enterprise Server
2. Adding, changing, or deleting CMG Enterprise Server Administrator roles
3. LDAP communication
4. Modifying and publishing CMG Shield Policies

3.1.2. Audit Data Viewing Security Function

The TOE's Audit Data Viewing Security Function enables a CMG Enterprise Server Administrator with System or Log role privileges to view audit records.

3.1.3. Management Security Function

The TOE's Security Management Security Function provides administrator support functionality that enables authorized administrators to configure and manage the TOE. The TOE maintains the following roles for administrators, with distinct privileges defined for each: Help Desk, System, Security, Log, and Account. Management functionality includes invocation of TOE management functions that effect security functionality behavior. Configuration functionality includes enabling authorized administrators to modify TSF Data used by the TOE's security functions.

The TOE's modification of security behavior functionality includes the ability to control the following security management functions:

1. enable or disable encryption for an end user;
2. scanning of all hard disk files after each logon;
3. scanning of removable media when first detected;
4. change the priority of the TOE's execution on end user devices;
5. change the encryption algorithm used on end user devices;
6. defining the parameters determining how long encryption/decryption can be deferred on an end user system;
7. modify system parameters (Policy Proxy related parameters);

8. manage administrator accounts;
9. manage end user accounts (sync with LDAP); and
10. view administrator logs.

The TOE's modification of TSF data functionality includes the ability to modify the following data:

1. administrator roles; and
2. policies stored in the database; and
3. policies on the end user devices (publishing policies).

3.1.4. Self Protection Security Function

The TOE provides for self protection and non-bypassability of functions within the TOE's scope of control (TSC). The TOE controls actions carried out by a user by controlling a user session and the actions carried out during a user session. By maintaining and controlling a user session a user has with the TOE, the TOE ensures that no security functions within the TSC are bypassed and that there is a separate domain for the TOE that prevents the TOE from being interfered with or tampered with for those users that are within the TSC.

The TOE protects (encrypts) all TSF Data in transit and at rest, with the exception of the administrator action logs stored in the database. Specifically, the TSF Data Protection Security Function includes the following functionality:

1. Protection of DBMS host resident TSF Data;
2. Protection of TSF Data in transit (CMG Shield Initial Policy Distribution and CMG Shield Policy Update);
3. Protection of CMG Policy Proxy host resident TSF Data; and
4. Protection of CMG Shield host resident TSF Data.

Note that access to the administrator action log through the TOE is limited to view only, and the administrator is required to limit access via the DBMS interfaces to these same privileges.

Policies managed by the CMG Enterprise Server are stored encrypted in the IT Environment supplied DBMS. The CMG Enterprise Server encrypts this data (AES-128). The key (CMG Enterprise Server DBMS Encryption Key) used to encrypt the data is generated with the X9.31 RNG with a modified seed algorithm. The encrypted data in the DBMS is thereby protected from unauthorized access.

On initial End User login, the CMG Shield sends the End User's username and password to the CMG Enterprise Server across the IT Environment provided SSL connection. If the CMG Enterprise Server successfully verifies the End User's credentials by performing an LDAP Bind against the LDAP directory with the End User's credentials, the CMG Enterprise Server builds a CMG Shield Initial Policy Distribution and sends this information to the End User across the same SSL link. All keys and data in the CMG Shield Initial Policy Distribution are encrypted (AES-128) according to the following table.

Table 1 - CMG Shield Initial Policy Distribution

CMG Shield Initial Policy Distribution Data	Protection Operation	Key used for Protection
Policies	Encryption	Policy Key
User Data Encryption Keys	Key wrapping	Root Key
Authentication Key	Key wrapping	Root Key
Policy Key	Key wrapping	Root Key
Root Key	Key wrapping	Password Key

Once the CMG End User receives the CMG Shield Initial Policy Distribution, the TOE derives the Password Key, decrypts the Root Key and then decrypts the remaining keys. A CRC covering the keys is calculated and compared to a stored value sent with the keys. If the calculated and stored values match, processing continues. The policies are next decrypted and applied.

The TOE stores the information from the CMG Shield Initial Policy Distribution (for subsequent logins) encrypted as received, in a CMG Shield host resident flat file. The Password Key is zeroized ensuring only the successfully authenticated Managed User can access the CMG Shield resident TSF Data.

At subsequent managed user logins and while a managed user is logged in, the CMG Shield periodically polls the CMG Policy Proxy for policy updates. Authentication is used between these devices to ensure the end user devices are authorized to access the CMG Policy Proxy. CMG Shield Policy Updates are protected according to the following table. On receipt of a CMG Shield Policy Update, the CMG decrypts the information, validates it by comparing a calculated CRC against a CRC stored with the data, and applies the new policies.

Table 2 - CMG Shield Initial Policy Distribution

Data	Protection Operation	Key used for Protection
Policies	Encryption	Policy Key
Any New User Data Encryption Keys	Key wrapping	Root Key

3.1.5. User Data Protection Security Function

The TOE encrypts data on the end user device according to the policies supplied by the CMG Enterprise Server. User-specific policies are retrieved from the CMG Enterprise Server when an end user successfully authenticates on the end user device. A policy may specify that all encryption is disabled, in which case no encryption or decryption takes place and the TOE behaves the same as for an unmanaged user.

The encryption and decryption operations are transparent to the end user. Encrypting data does not restrict Shield users' ability to view, create, change, rename, copy, move, share, or delete their files and/or folders as usual. Encrypting data also does not restrict administrators' ability to rename

and delete files and/or folders as usual. Deleted encrypted files and folders remain encrypted, whether they are in the Recycle Bin or "permanently deleted."

If an end user attempts to access an encrypted file for which they do not have the appropriate key to decrypt the data, they receive an "access denied" message when they try to open to file.

The data to be protected may be specified in multiple ways. Policies may designate data to be protected by a list of folders, a list of file names or types, or as all output from a list of applications. Individual configuration is provided for encryption of "My Documents," Outlook Personal Folders, Temporary Files, Temporary Internet Files, and Windows Paging Files. Configuration is also provided for encryption of all files on removable media or all executables on removable media.

Two categories may be used to specify a list of folders and/or file types to be protected: Common Encrypted Folders and User Encrypted Folders.

Data encryption policies involve one of three keys:

1. Common – all users logging into each device share a common key. Therefore data encrypted by one user with this key may be decrypted by any other defined user. This key is generated the first time any managed user logs on to each device with CMG Shield.

2. User – this key is user-device-specific. Data encrypted with this key may not be decrypted by any other users and can only be decrypted on the host it was encrypted on by the user who caused it to be encrypted. This key is generated the first time the specific managed user logs on to each device with CMG Shield.

3. User roaming – this key is user-specific but not user-device-specific. It is typically used when encrypting data on removable media and ensures that the data may be decrypted on a different system (also with CMG Shield installed and communicating with the same CMG Enterprise Server). Data encrypted with this key may not be decrypted by any other users. This key is generated the first time the specific managed user logs on to any device with CMG Shield.

All keys (except the Password Key) are generated on the CMG Enterprise Server using the X9.31 random number generator. Since multiple algorithms with different key sizes are supported, keys of the appropriate size for each algorithm for each key type are generated. All keys are generated by the CMG Enterprise Server.

Keys are associated with protected areas via the Application Data Encryption Key and User Encryption Key parameters. Each one may designate the common, user, or user roaming as the key to be used. These parameters are configured for the system as a whole and may not be specified on a per-user basis.

Administrators may configure one of AES-256, AES-128 or 3DES as the algorithm to be used for the following protection areas:

1. Common Encryption Algorithm – applies to all data encrypted with the common key

2. User Encryption Algorithm – applies to all data encrypted with the user or user roaming key

The following table summarizes the various methods of specifying data to be protected. It also describes the determination of the algorithm and key to be associated with that protection.

Table 3 - Encryption Summary

Data To Be Protected	Key Determination	Algorithm Determination
Common Encrypted Folders	Always uses the common key	Common Encryption Algorithm
Application Data Encryption List	Application Data Encryption Key	User Encryption Algorithm if the user or user roaming key is configured; Common Encryption Algorithm if the common key is configured
Encrypt “My Documents”	User Data Encryption Key	User Encryption Algorithm if the user or user roaming key is configured; Common Encryption Algorithm if the common key is configured
Encrypt Outlook Personal Folders	User Data Encryption Key	User Encryption Algorithm if the user or user roaming key is configured; Common Encryption Algorithm if the common key is configured
Encrypt Removable Media	Always uses the user roaming key	User Encryption Algorithm
Encrypt Temporary Files	Common Encryption Key	Common Encryption Algorithm
Encrypt Temporary Internet Files	User Data Encryption Key	User Encryption Algorithm if the user or user roaming key is configured; Common Encryption Algorithm if the common key is configured
Encrypt Windows Paging File	User Data Encryption Key	Always uses AES-128
Encrypt Executables on Removable Media	Always uses the user roaming key	User Encryption Algorithm
User Encrypted Folders	User Data Encryption Key	User Encryption Algorithm if the user or user roaming key is configured; Common Encryption Algorithm if the common key is configured

Special considerations apply to some of the protection areas. These considerations are summarized in the following table.

Table 4 - Encryption Summary

Data To Be Protected	Special Considerations
Common Encrypted Folders	This policy applies to all drives classified by Windows as Hard Disk Drives (see My Computer). This policy can't be used to encrypt drives or media classified by Windows as Devices with Removable Storage. If the same folder is specified in both this policy and the User Encrypted Folders policy, this policy prevails.
Application Data Encryption List	Changes to this policy do not affect files already encrypted because of this policy.
Encrypt Removable Media	This policy applies to all drives classified by Windows as Devices with Removable Storage (see My Computer).
Encrypt Temporary Files	When this policy first takes effect or its value changes, the Shield deletes all current temporary files.
Encrypt Temporary Internet Files	When this policy first takes effect or its value changes, the Shield deletes all current temporary Internet files.
Encrypt Windows Paging File	A change to this policy requires a reboot of the Windows device.
User Encrypted Folders	This policy applies to all drives classified by Windows as Hard Disk Drives (see My Computer). This policy can't be used to encrypt drives or media classified by Windows as Devices with Removable Storage. If the same folder is specified in this policy for multiple users of the same Windows device, each file in that folder is encrypted for the file's first owner after the policy takes effect, and can be decrypted only by that owner.

Scanning of all protected locations may be configured by an administrator. If this option is enabled for a user, then all protected locations are scanned when a managed user logs on to an end user device. Files that are not protected according to the policy (e.g., they were created in the protected area by an unmanaged user) are encrypted as a result of the scan.

Scanning may also be configured by an administrator for removable media whenever such media is made accessible to the end user device.

Because this scanning occurs in the background, the administrator may configure a priority to be used for both logon and removable media scanning. The possible settings are for the scanning are Highest, High, Normal, Low and Lowest. Normal is the default value.

When a CMG Shield Initial Policy Distribution or CMG Shield Policy Update is received, policy changes may require that some files previously encrypted be decrypted or some files not previously encrypted be encrypted at this time. The TOE scans the file system to effect these changes.

During runtime, when a file or files are created, the TOE enables an Administrator to allow deferring encryption. If these policy fields are non-zero the TOE Shield will prompt the end user and ask if they would like to defer encryption. Administrators define how many times an end user may defer encryption and the length of the time between each query.

4. ASSUMPTIONS AND CLARIFICATION OF SCOPE

4.1. Physical Security Assumptions

A key environmental assumption is physical security, for it is assumed appropriate physical security protection will be applied to the TOE hardware and software commensurate with the value of the IT assets. Specifically, the TOE is assumed to be located in a secure location providing physical protection and limited access to administrators only.

4.2. Personnel Security Assumptions

It is assumed that all authorized administrators are properly trained, not careless, not willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation.

4.3. Operational Security Assumptions

It is assumed that the CREDANT Mobile Guardian Enterprise Edition Version 5.2.1 SP4 system is dedicated to its primary function and is not intended to provide any general purpose computing or storage capabilities.

4.4. Threats Countered and Not Countered

The TOE and Operating IT Environment are designed to fully or partially counter the following threats:

T.ACCIDENTAL	Administrators may accidentally expose sensitive user data on the end user devices via inappropriate configuration of the TOE or TSF data.
T.TSF_COMP	A user or process may cause, through an unsophisticated attack, TSF data or executable code to be modified, thereby enabling unauthorised access to sensitive data.
T.USERDATA	Users may gain unauthorised access to sensitive data on the end user devices through accidental means or unsophisticated attacks.

4.5. Organizational Security Policies

There are no applicable organizational security policies

4.6. Clarification of Scope

The following functionality of CREDANT Mobile Guardian Enterprise Edition Version 5.2.1 SP4 is not included in the evaluation and should not be used by customers desiring the evaluated configuration:

1) CMG Shields for hand-held devices (the security functionality differs from that provided for Windows devices).

2) CMG Gatekeeper for synchronization with hand-held devices.

3) CredActivate (used to download CMG Shield on PDAs if an administrator chooses to not install CMG Gatekeeper).

4) CredEncrypt (allows users to create a password-protected, compressed, encrypted, and self-extracting archive of one or more files that can be decrypted on any host)

5) CREDANT GINA Replacement (optional replacement for the Windows GINA)

6) TOE generation of certificates used with SSL (the IT Environment must supply these certificates)

7) Secure Post-Encryption Cleanup (disk sanitization of the clear-text versions of files) is excluded because the operating system and hard drive are not within the TOE boundary.

It is also important to note that for this evaluation only the CMG Shield for Windows is included. Therefore, the security functionality described in this document describes the security functionality pertinent to the CMG Shield for Windows.

Additionally, access to the administrator action log through the TOE is limited to view only, and the administrator is required to limit access via the DBMS interfaces to these same privileges.

architectural information

The evaluated configuration consists of one instance of the CMG Enterprise Server; one or more instances of the CMG Policy Proxy; and one or more instances of the CMG Shield for Windows.

1) The CMG Enterprise Server components will be installed on one host. That host will be dedicated to CMG Enterprise Server functions.

2) The CMG Policy Proxy, DBMS, and LDAP server will be installed on separate hosts.

3) The CMG Shield will support CMG Shield for Windows on desktops and laptops.

4) The CMG Shield will support protection of user data on removable medium.

5) The CMG Shield integrates with smart card implementations on the end user devices that do not utilize one-time passwords or biometrics (a multiple use password is required). Support for authentication via Smart Cards is optional functionality in the IT Environment.

6) SSL provided by the IT Environment is used for communication between all systems.

7) Certificates used by the TOE will be generated by a third-party Certificate Authority provided by the IT Environment.

All unnecessary services listening on TCP/UDP ports on the CMG Enterprise Server and CMG Policy Proxy will be disabled.

The evaluated configuration is illustrated in the following figure.

4.7. Evaluated Configuration

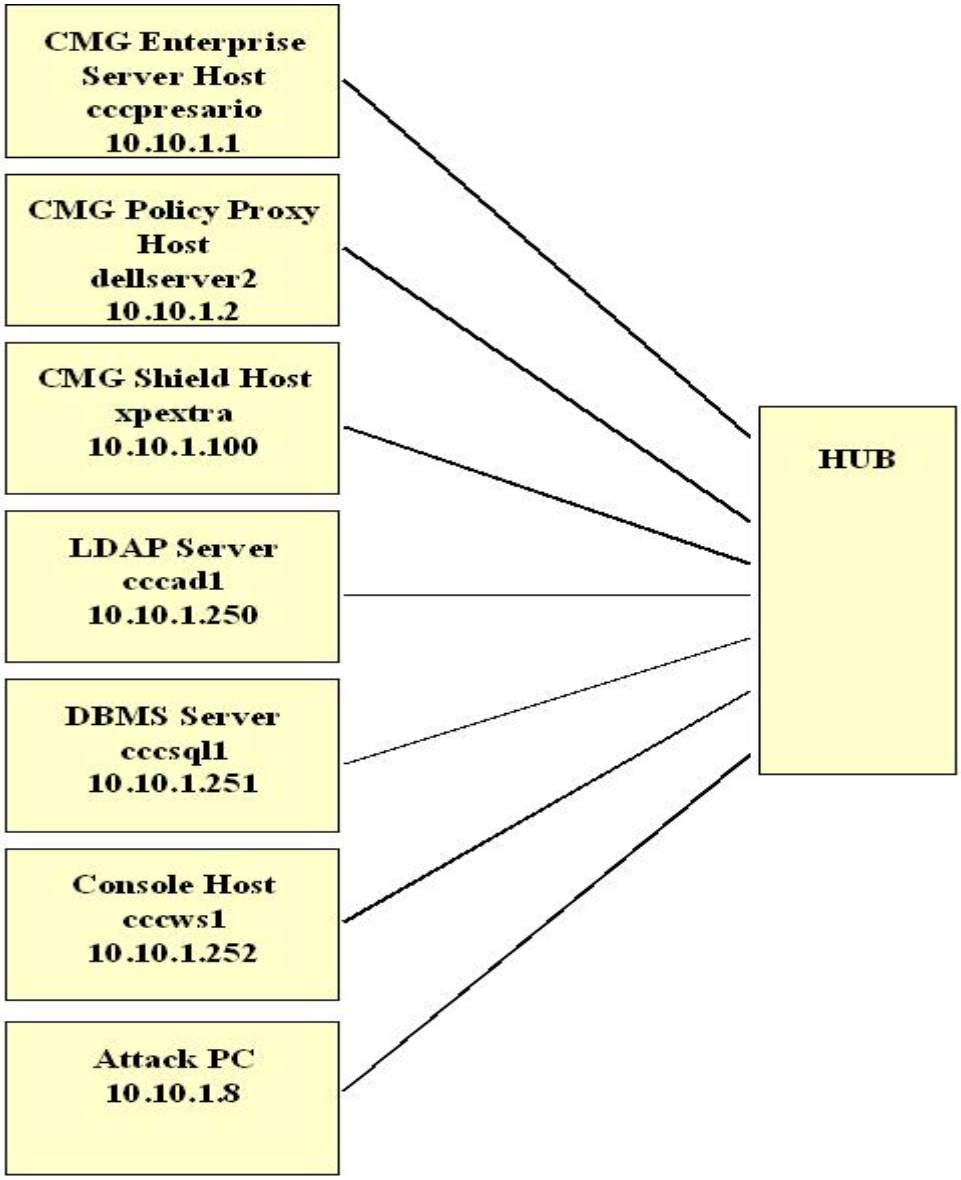


Figure 1 - Evaluated Configuration

An overview of the purpose of each of these systems is provided in the following table.

Table 5 - Test Configuration Overview

System	Purpose
cccpresario	The system running all of the CMG Enterprise Server (sub)-components.
dellserver2	The system running the CMG Policy Proxy.
xpextra	A system running the CMG Shield for Windows.
cccad1	The system acting as the Active Directory Primary Domain

System	Purpose
	Controller and DNS Server.
cccsql1	The system running the DBMS and hosting the TOE database.
cccws1	A system used to open a browser to the CMG Enterprise Server.
Attack	System used to launch penetration tests.

Specific configuration details for each of the systems are provided in the tables below.

Table 6 - cccpresario Details

Item	Purpose
Installed software	Microsoft Windows 2000 Server SP4 Microsoft Installer (MSI) Version 3.1 Microsoft Data Access Components (MDAC) Vresion 2.8 Microsoft Internet Explorer 6.0 SP1 Java Runtime Environment Version 1.5.0_06 (build 1.5.0_06_b05) Adobe Reader Version 8.0 WinZip Version 10.0 or later CMG Enterprise Edition Version 5.2.1 SP4 Enterprise Server Apache Tomcat 5.5.9
Configuration	Static IP address 10.10.1.1 DNS Server 10.10.1.250 FQDN cccpresario.domain1.credant.com

Table 7 - dellserver2 Details

Item	Purpose
Installed software	Microsoft Windows 2000 Server SP4 Microsoft Installer (MSI) Version 3.1 Microsoft Data Access Components (MDAC) Version 2.8 Microsoft Internet Explorer 6.0 SP1 Java Runtime Environment Version 1.5.0_06 (build 1.5.0_06_b05) Adobe Reader Version 8.0 WinZip Version 10.0 or later CMG Enterprise Edition Version 5.2.1 SP4 Policy Proxy
Configuration	Static IP address 10.10.1.2 DNS Server 10.10.1.250 FQDN dellserver2.domain1.credant.com

Table 8 - xpextra Details

Item	Purpose
Installed software	Microsoft Windows XP Professional SP2 Microsoft Internet Explorer 6.0 SP1 Java Runtime Environment Version 1.5.0_06 (build 1.5.0_06_b05) Adobe Reader Version 8.0 WinZip Version 10.0 or later CMG Enterprise Edition Version 5.2.1 SP4 Shield for Windows
Configuration	Static IP address 10.10.1.100 DNS Server 10.10.1.250 FQDN xpextra.domain1.credant.com

Table 9 - cccad1 Details

Item	Purpose
Installed software	Microsoft Windows 2000 Server SP4
Configuration	Static IP address 10.10.1.250 DNS Server 10.10.1.250 FQDN cccad1.domain1.credant.com Primary Domain Controller for domain1.credant.com DNS server with address records for all the test systems

Table 10 - cccsql1 Details

Item	Purpose
Installed software	Microsoft Windows 2000 Server SP4 Microsoft Installer (MSI) Version 3.1 Microsoft Data Access Components (MDAC) Vresion 2.8 Microsoft SQL Server 2000 SP4
Configuration	Static IP address 10.10.1.251 DNS Server 10.10.1.250 FQDN cccsql1.domain1.credant.com

Table 11 - cccws1 Details

Item	Purpose
Installed software	Microsoft Windows XP Professional SP2 Microsoft Internet Explorer 6.0 SP1 Java Runtime Environment Version 1.5.0_06 (build 1.5.0_06_b05) Adobe Reader Version 8.0 WinZip Version 10.0 or later Snag It Version 8.0.0 MS Word
Configuration	Static IP address 10.10.1.252 DNS Server 10.10.1.250

Item	Purpose
	FQDN cccws1.domain1.credant.com

Table 12 - Attack Details

Item	Purpose
Installed software	Microsoft Windows XP Professional SP2 Microsoft Internet Explorer 6.0 SP1 Java Runtime Environment Version 1.5.0_06 (build 1.5.0_06_b05) Adobe Reader Version 8.0 WinZip Version 10.0 or later NmapGUI Version 0.2Beta Snag It Version 8.0.0 WireShark Version 0.99.6a Nessus Version 3.0.6.1 Paros Proxy
Configuration	Static IP address 10.10.1.8 DNS Server 10.10.1.250 FQDN attack.domain1.credant.com

5. DOCUMENTATION

This section details the documentation that is delivered to the customer or was used as evidence for the evaluation of the CREDANT Mobile Guardian Enterprise Edition Version 5.2.1 SP4 Product.

1. CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Security Target, Version 1.6, January 7, 2008;

2. CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Configuration Management Plan, Version 1.4, December 14, 2007;

3. Bill of Materials for CmgEnterpriseEdition, Build 244, 1/4/2008;

4. CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Delivery Procedures, Version 1.2, December 14, 2007;

5. Enterprise Edition Installation Supplement Release 5.2.1 SP4, January 2008;

6. Custom Server Installation and Configuration Guide Release 5.2, Service Pack 3, June 2007, Document Revision 1;

7. CMG Online Help System, Version: 5.2.1 SP4, September 5, 2007;

8. Windows Shield Online Help System, Version: 5.2.1, February 13, 2007;

9. CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Functional Specification (FSP), Version 1.3, October 5, 2007;

10. CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 High Level Design (HLD), Version 1.3, December 7, 2007;

11. Credant Mobile Guardian (CMG) Enterprise Edition Version 5.1.5 Development Security Plan, Version 1.0;

12. CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Test Plan, Version 1.2, December 16, 2007;

13. Enterprise Edition Version 5.2.1 SP4 Test Procedures, Version 1.1, December 18, 2007;

14. CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Test Results, Version 1.0, December 18, 2007.

The files listed below are documentation files that were included in the CMG CC download from the website and used in the evaluation:

CMG Administrator Help File - Version: 5.2.1 SP4, Creation Date: September 5, 2007;

CMG Windows Shield Help File - Version: 5.2.1, Creation Date: February 13, 2007;

Enterprise Edition Installation Supplement Release 5.2.1 SP4, January 2008;

Custom Server Installation and Configuration Guide Release 5.2.1 Service Pack 4, September 2007, Document Revision 1.

The files listed below are documentation files that were included in the CMG CC download from the website but were not used in the evaluation:

Express Server Installation and Configuration Guide Release 5.2.1 SP4, September 2007,

Document Revision 1;

Gatekeeper and Windows Shield Deployment Guide Release 5.2.1 SP4, September 2007;

Migration Guide Release 5.2.1 Service Pack 4, September 2007, Document Revision 1;

Over-the-Air (OTA) Sync Control Installation Guide Release 5.2.1 SP4, September 2007;

Enterprise Edition Release Notes Release 5.2.1 Service Pack 4, January 2008;

Wireless Deployment Server Installation Guide Release 5.2.1 SP4, September 2007.

6. IT PRODUCT TESTING

This section describes the testing efforts of the Developer and the evaluation team.

6.1. Developer testing

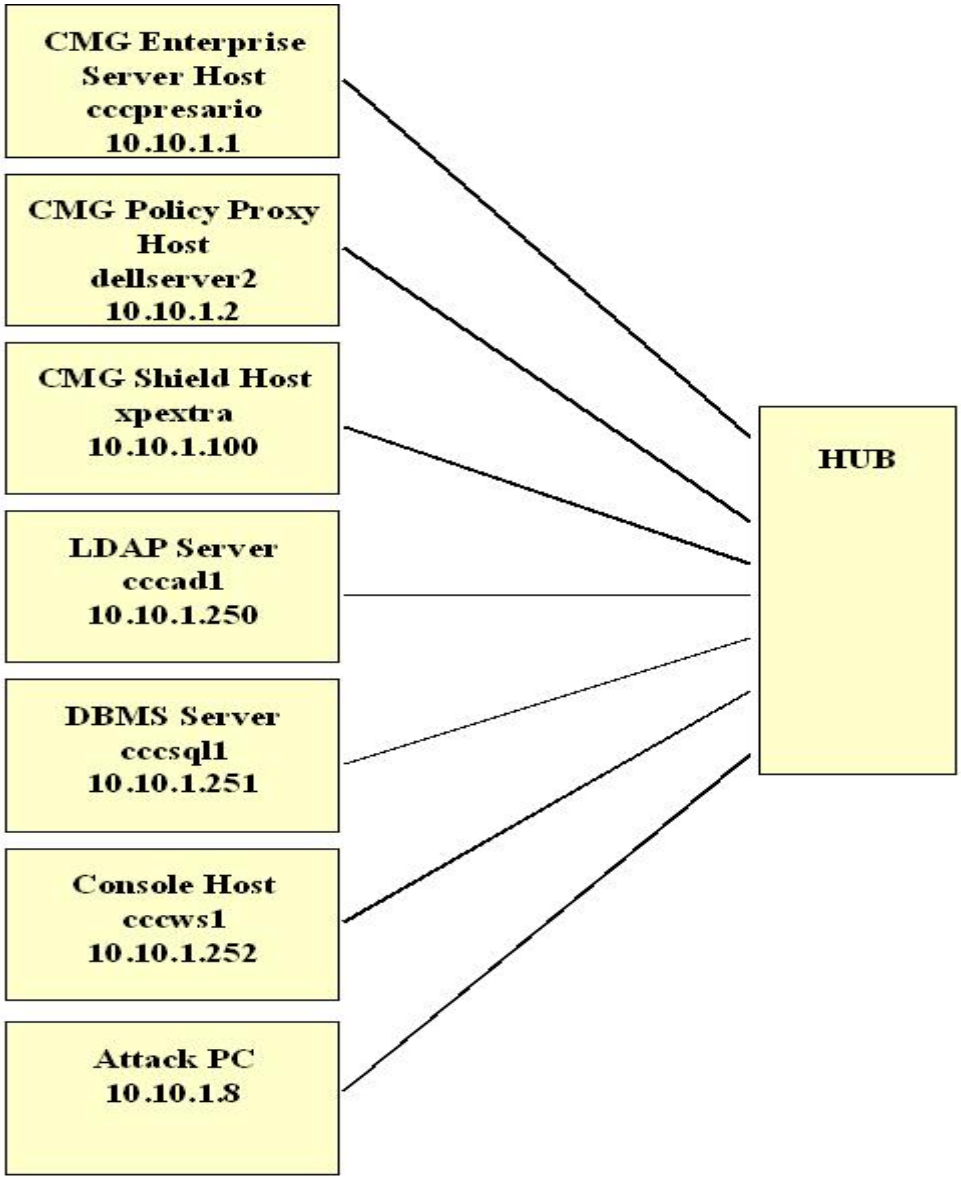
Since the Evaluation team repeated all of the security testing accomplished by the developer, the test descriptions presented below under the Evaluation Team testing provide the documentation of the developer's effort.

The Developer and evaluation team tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. Each test case was identified by a number that correlates to the expected test results in the TOE Test Plan.

The evaluation team analyzed the Developer's testing to ensure adequate coverage for EAL 3. The evaluation team determined that the Developer's actual test results matched the Developer's expected test results.

The following diagrams depict the test environment that was used by the Developers and the Evaluators. The Evaluators assessed that the test environment used by the Developers was appropriate and mirrored the test configuration during Independent testing.

Figure 2 - Test Configuration/Setup



An overview of the purpose of each of these systems is provided in the following table.

Table 5: Test Configuration Overview

System	Purpose
cccpresario	The system running all of the CMG Enterprise Server (sub)-components.
dellserver2	The system running the CMG Policy Proxy.
xpxtra	A system running the CMG Shield for Windows.
cccad1	The system acting as the Active Directory Primary Domain Controller and DNS Server.

System	Purpose
cccsql1	The system running the DBMS and hosting the TOE database.
cccws1	A system used to open a browser to the CMG Enterprise Server.
attack	System used to launch penetration tests.

Specific configuration details for each of the systems are provided in the tables below.

Table 6: cccpresario Details

System	Installed Components
Installed software	Microsoft Windows 2000 Server SP4 Microsoft Installer (MSI) Version 3.1 Microsoft Data Access Components (MDAC) Vresion 2.8 Microsoft Internet Explorer 6.0 SP1 Java Runtime Environment Version 1.5.0_06 (build 1.5.0_06_b05) Adobe Reader Version 8.0 WinZip Version 10.0 or later CMG Enterprise Edition Version 5.2.1 SP4 Enterprise Server Apache Tomcat 5.5.9
Configuration	Static IP address 10.10.1.1 DNS Server 10.10.1.250 FQDN cccpresario.domain1.credant.com

Table 7: dellserver2 Details

System	Installed Components
Installed software	Microsoft Windows 2000 Server SP4 Microsoft Installer (MSI) Version 3.1 Microsoft Data Access Components (MDAC) Version 2.8 Microsoft Internet Explorer 6.0 SP1 Java Runtime Environment Version 1.5.0_06 (build 1.5.0_06_b05) Adobe Reader Version 8.0 WinZip Version 10.0 or later CMG Enterprise Edition Version 5.2.1 SP4 Policy ProxyNessus Version 3 WireShark Version 0.99.4
Configuration	Static IP address 10.10.1.2 DNS Server 10.10.1.250 FQDN dellserver2.domain1.credant.com

Table 8: xpextra Details

System	Installed Components
Installed software	Microsoft Windows XP Professional SP2 Microsoft Internet Explorer 6.0 SP1 Java Runtime Environment Version 1.5.0_06 (build 1.5.0_06_b05) Adobe Reader Version 8.0 WinZip Version 10.0 or later CMG Enterprise Edition Version 5.2.1 SP4 Shield for Windows
Configuration	Static IP address 10.10.1.100 DNS Server 10.10.1.250 FQDN xpextra.domain1.credant.com

Table 9: cccad1 Details

System	Installed Components
Installed software	Microsoft Windows 2000 Server SP4
Configuration	Static IP address 10.10.1.250 DNS Server 10.10.1.250 FQDN cccad1.domain1.credant.com Primary Domain Controller for domain1.credant.com DNS server with address records for all the test systems

Table 10: cccsql1 Details

System	Installed Components
Installed software	Microsoft Windows 2000 Server SP4 Microsoft Installer (MSI) Version 3.1 Microsoft Data Access Components (MDAC) Version 2.8 Microsoft SQL Server 2000 SP4
Configuration	Static IP address 10.10.1.251 DNS Server 10.10.1.250 FQDN cccsql1.domain1.credant.com

6.2. Functional Test Results

The repeated developer test suite includes the developer functional tests. Additionally, each of the Security Functions and developer tested TSFIs are included in the CCTL test suite. The results are found in the Credant Functional Test Report, Document No. F3-0408-004, dated 29 April 2008.

6.3. Evaluator Independent Testing

The tests chosen for independent testing allow the evaluation team to exercise the TOE in a different manner than that of the developer's testing. The intent of the independent tests is to give the evaluation team confidence that the TOE operates correctly in a wider range of conditions than would be possible purely using the developer's own efforts, given a fixed level of resource. The selected independent tests allow for a finer level of granularity of testing compared to the developer's testing, or provide additional testing of functions that were not exhaustively tested by the developer. The tests allow specific functions and functionality to be tested. The tests reflect knowledge of the TOE gained from performing other work units in the evaluation. The test environment used for the evaluation team's independent tests was identical with the test configuration used to execute the vendor tests.

6.4. Evaluator Penetration Tests

The evaluators examined each of the obvious vulnerabilities identified during the developer's vulnerability analysis. After consulting the sources identified by the developer used during the initial vulnerability analysis, the evaluator consulted other vulnerability relevant sources of information to verify that the developer considered all available information when developing the non-exploitation rationale. These additional sources include:

Table 11: Internet Web Site Vulnerability Searches

Site	Keywords Used for the Searches
http://xforce.iss.net/	Credant, Mobile Guardian, CMG, 1.5.0_06, Apache 5.5.9, 5.5.9, SQL Server 2000
http://cve.mitre.org	Credant, Mobile Guardian, CMG, 1.5.0_06, Apache 5.5.9, 5.5.9, SQL Server 2000

Site	Keywords Used for the Searches
http://www.ciac.org/	Credant, Mobile Guardian, CMG, 1.5.0_06, Apache 5.5.9, 5.5.9, SQL Server 2000
http://www.cert.org/	Credant, Mobile Guardian, CMG, 1.5.0_06, Apache 5.5.9, 5.5.9, SQL Server 2000
http://www.securityfocus.com	Credant, Mobile Guardian, CMG, 1.5.0_06, Apache 5.5.9, 5.5.9, SQL Server 2000
http://tomcat.apache.org/security.html	Credant, Mobile Guardian, CMG, 1.5.0_06, Apache 5.5.9, 5.5.9, SQL Server 2000

After verifying that the developer's analysis approach sufficiently included all of the necessary available information regarding the identified vulnerabilities, the evaluator made an assessment of the rationales provided by the developer indicting that the vulnerability is non-exploitable in the intended environment of the TOE.

While verifying the information found in the developer's vulnerability assessment the evaluators conducted a search to verify if additional obvious vulnerabilities exist for the TOE. Additionally, the evaluator examined the provided design documentation and procedures to attempt to identify any additional vulnerability.

The evaluator determined that the rationales provided by the developer indicate that the vulnerabilities identified are non-exploitable in the intended environment of the TOE.

6.5. Test Results

The end result of the testing activities was that all tests gave expected (correct) results. The successful completion of the evaluator penetration tests demonstrated that the TOE was properly resistant to all the potential vulnerabilities identified by the evaluator. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities in the final evaluated version. The evaluation team tests and vulnerability tests substantiated the security functional requirements in the ST.

7. EVALUATED CONFIGURATION

The evaluated configuration of the CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Product, as defined in the Security Target, consists of the components as described in the testing section.

8. RESULTS OF THE EVALUATION

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 2.3. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.3.

COACT CAFÉ Laboratory has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 3. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished on March 11, 2008. A final Validation Oversight Review (VOR) was held on 22 April 2008 and final changes to the ST, ETR and VR were completed on 05 May 2008.

9. VALIDATOR COMMENTS

The TOE developer and sponsor, and the Evaluation Team are commended for their effort in developing tests for the CREDANT Mobile Guardian Enterprise Edition Version 5.2.1 SP4. All test plans were clear, complete, and comprehensible.

The validation team has no comments other than to state that the product should be used in accordance with all evaluated guidance documented in this report.

Annexes

None

10. SECURITY TARGET

CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Security Target, Version 1.7 dated March 24, 2008

11. GLOSSARY

- **Authentication:** Verification of the identity of a user.
- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

12. ACRONYM LIST:

AES ……Advanced Encryption Standard

CC ……Common Criteria

CCIMB……Common Criteria Interpretation Management Board

CMG ……Credant Mobile Guardian

DBMS ……Database Management System

EAL3 ……Evaluation Assurance Level 3

EAL3 ……Evaluation Assurance Level 3

IT……Information Technology

NIAP……National Information Assurance Partnership

NVLAP……National Voluntary Laboratory Accreditation Program

PDA……Personal Digital Assistant

PP……Protection Profile

SF……Security Function

SFP……Security Function Policy

SOF ……Strength of Function

ST……Security Target

TOE ……Target of Evaluation

TSC ……TSF Scope of Control

TSF……TOE Security Functions

TSFI ……TSF Interface

TSP ……TOE Security Policy

13. BIBLIOGRAPHY

1.) *Common Criteria for Information Technology Security Evaluation, Part 1 Introduction and General Model*, Version 2.3, dated August 2005, CCMB-2005-08-001

2.) *Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements*, Version 2.3, dated August 2005, CCMB-2005-08-002

3.) *Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements*, Version 2.3, dated August 2005, CCMB-2005-08-003

4.) *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, Version 2.3, dated August 2005, CCMB-2005-08-004

5.) *Guide for the Production of PPs and STs*, Version 0.9, dated January 2000

6.) *CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Security Target*, Version 1.6, January 7, 2008

7.) CAFÉ Laboratory of COACT Incorporated, *Evaluation Technical Report for CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4*, April 29, 2008, Document No. E3-0208-001