CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Security Target

Version 1.7

March 24, 2008

CREDANT Technologies, Inc.
15303 Dallas Parkway
Suite 1420
Addison, Texas 75001

DOCUMENT INTRODUCTION

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 Service Pack (SP) 4. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1

1 SECURITY TARGET INTRODUCTION

This chapter presents security target (ST) identification information and an overview of the ST. An ST contains the information technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by that TOE to meet stated requirements. An ST principally defines:

A) A security problem expressed as a set of assumptions about the security aspects of the environment, a list of threats that the product is intended to counter, and any known rules with which the product must comply (Chapter 3, Security Environment).

B) A set of security objectives and a set of security requirements to address the security problem (Chapters 4 and 5, Security Objectives and Security Requirements, respectively).

C) The security functions provided by the TOE that meet the set of requirements (Chapter 6, TOE Summary Specification).

1.1 TOE Overview

The CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 is a scalable mobile security and management software platform that enables organizations to secure and manage mobile and wireless devices from a single management console.

1.2 ST and TOE Identification

This section provides information needed to identify and control this ST and its TOE.

ST Title	CREDANT Mobile Guardian Enterprise Edition Version 5.2.1 SP4 Security Target
ST Version	Version 1.7
Publication Date	March 24, 2008
Vendor	CREDANT Technologies, Inc.
ST Author	COACT, Inc.
TOE Identification	CREDANT Mobile Guardian Enterprise Edition Version 5.2.1 SP4 Target of Evaluation
CC Identification	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
Common Criteria Conformance	The ST is compliant with the Common Criteria (CC) Version 2.3 assurance requirements conformant for EAL3.
Protection Profile Conformance	The TOE does not claim conformance to any Protection Profile.
Keywords	File Encryption, access control

1.3 References

The following documentation was used to prepare this ST:

[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, August 2005, Version 2.3, CCMB-2005-08-001.
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, August 2005, Version 2.3, CCMB-2005-08-002.
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, August 2005, Version 2.3, CCMB-2005-08-003.
[CEM]	Common Methodology for Information Technology Security Evaluation - Evaluation Methodology, August 2005, Version 2.3, CCMB-2005-08-004.

1.4 Acronyms and Abbreviations

The following acronyms and abbreviations are used in this Security Target:

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CC	Common Criteria
CEM	Common Evaluation Methodology
DBMS	Database Management System
EAL	Evaluation Assurance Level
FSP	Functional Specification
GUI	Graphical User Interface
HLD	High Level Design
Inc.	Incorporated
Interps	Interpretations
I&A	Identification and Authentication
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NIAP	National Information Assurance Partnership
OS	Operating System
PP	Protection Profile

RAM	Random Access Memory
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Functional Policy
SFR	Security Functional Requirements
SOF	Strength of Function
SP	Service Pack
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy

Chapter 2

2 TOE DESCRIPTION

This chapter provides an overview of the CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Target of Evaluation (TOE).

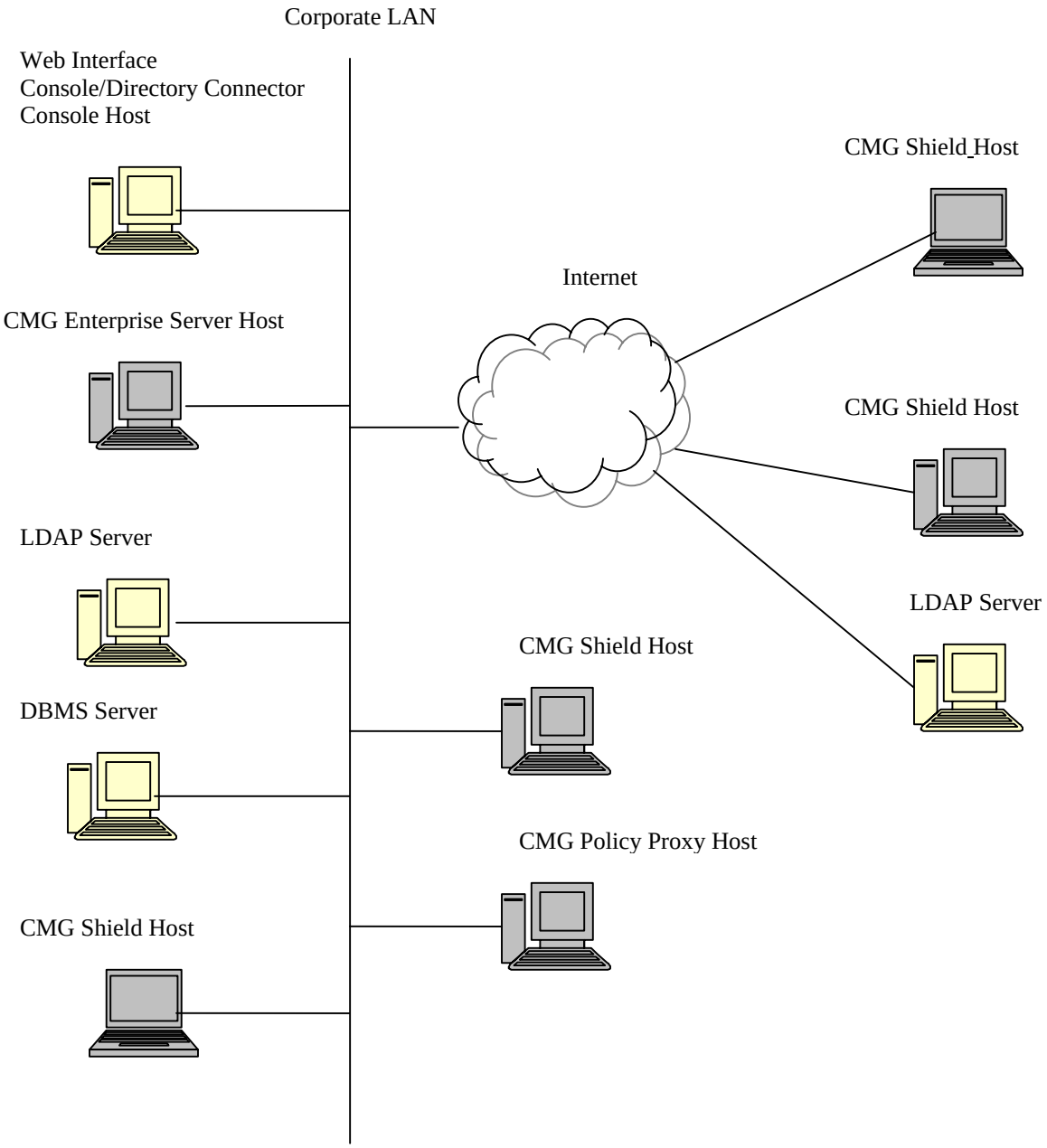
2.1 TOE Overview

The CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Target of Evaluation (TOE) (hereafter referred to as the TOE or CMG) is a distributed security solution designed to control enterprise-wise 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.

2.2 TOE Components

The TOE includes three software components: the CREDANT Mobile Guardian Enterprise Server (hereafter referred to as the CMG Enterprise Server); the CREDANT Mobile Guardian Policy Proxy (hereafter referred to as the CMG Policy Proxy); and the CREDANT Mobile Guardian Shield (hereafter referred to as the CMG Shield). Figure 1 depicts the TOE components' typical site placement. Shaded hosts are hosts running TOE components (software). The following sections describe the individual components and their roles in implementing the security functionality claimed.

Figure 1 - Typical CMG Enterprise Edition Deployment



2.2.1 CMG Enterprise Server

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.

2.2.2 CMG Policy Proxy

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.

2.2.3 CMG Shield

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.

2.3 TOE Interfaces

Administrators interface to the TOE is via the web interface of the CMG Enterprise Server. Users transparently interface to the TOE when they make system calls on an end user device which are intercepted by the TOE.

End Users are further identified as managed users or unmanaged users. A managed user is an end user with a Windows domain account who successfully authenticates and successfully receives a policy that specifies enabled encryption rules. An unmanaged user is an end user with a local machine account or a user for which an encryption policy is not available on the CMG Shield host because the userid is not defined in the CMG database.

2.3.1 Management

Management of the TOE includes modification of policies used to enforce the security functionality, publishing the policies to the appropriate TOE component, and creation/modification of users and roles used to enforce secure management. All management of the TOE is via the CMG Enterprise Server Administrator interface.

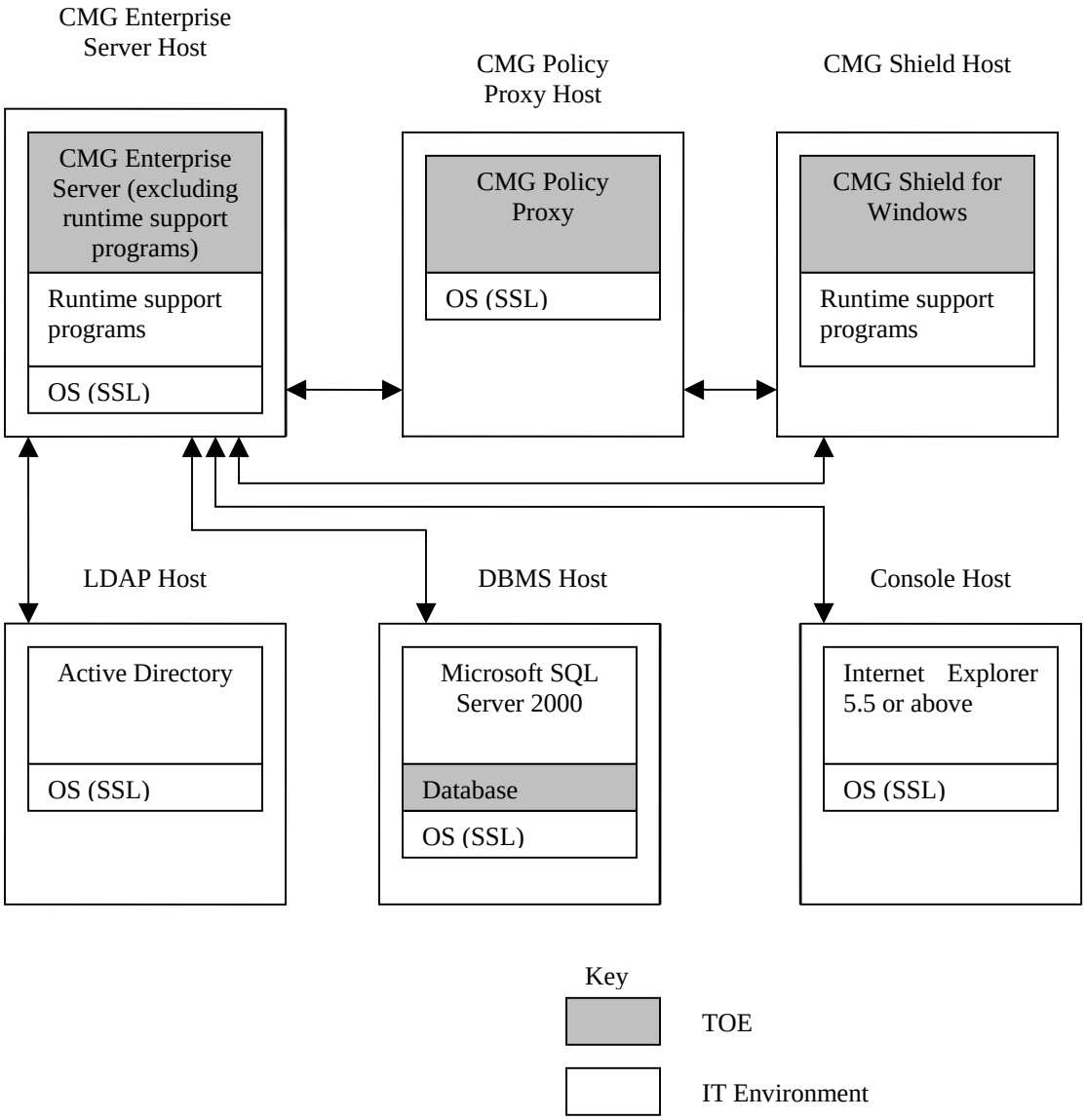
2.3.2 Monitoring (Audit)

The TOE's CMG Enterprise Server generates audit records that record security relevant events. CMG Enterprise Server audit records are viewed from the CMG Enterprise Server management interface.

2.4 Physical Boundary

Figure 2 depicts the TOE software components, TSF Data, and the software and hardware components relied upon by the TOE and provided by the IT Environment. The TOE detail is further explained in the following sections.

Figure 2 - TOE Physical Boundary



The Database on the DBMS Host stores TSF data used by the TOE.

2.4.1 CMG Enterprise Server TOE Components

The following table identifies and describes the CMG Enterprise Server TOE components.

Table 1 - CMG Enterprise Server TOE Components

CMG Enterprise Server Components	Description
Web Interface	A CMG Enterprise Server process that processes the interface to the web browser.
Device Server	The Device Server software module is an optionally installed software component. The Device Server component is required to support CMG Shield installed without the CREDANT GINA replacement (as required by the evaluated configuration). It processes initial connections from shields and processes password changes. The Device Server component is included in the TOE's evaluated configuration.
Enterprise Server	The Enterprise Server is the core CMG ES component that interacts with all other components.
Directory Connector	The Directory Connector component of the CMG Enterprise Server is a process used to access the IT Environment supplied LDAP implementation. Once accessed, the Directory Connector produces an XML file containing LDAP information.
Gatekeeper Connector	The Gatekeeper Connector component of the CMG Enterprise Server is an optionally installed software component. It coordinates policy updates with Policy Proxies. The TOE's evaluated configuration requires this software component.
CREDANT Cryptographic Kernel (CCK)	The CREDANT Cryptographic Kernel (CCK) is a library of cryptographic functions. The CCK is a software library (shared or dynamic link), which provides an API to cryptographic functions including AES, Triple DES, SHA-1, HMAC (SHA-1), and an ANSI X9.31 compliant pseudorandom number generator.

2.4.2 CMG Policy Proxy TOE Components

The following table identifies and describes the CMG Policy Proxy TOE components.

Table 2 - CMG Policy Proxy Components

CMG Policy Proxy Components	Description
Policy Proxy	The 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.

2.4.3 CMG Shield TOE Components

The following table identifies and describes the CMG Shield TOE components.

Table 3 - CMG Shield Components

CMG Shield Components	Description
CMG Shield for Windows Core	The CMG Shield for Windows core is a software module that coordinates all interactions between the other CMG Shield components.
CMG Shield Login Hook	The CMG Shield Login Hook is a software module that interfaces to the Windows OS login module. The IT Environment (OS) is responsible

CMG Shield Components	Description
	for identification and authentication of the End User. Once successfully authenticated, the CMG Shield Login Hook attempts to obtain a CMG Shield Initial Policy Distribution from the CMG Enterprise Server. If the End User had already obtained a CMG Shield Initial Policy Distribution, the CMG Shield Login Hook scans the folders and disks specified in the managed user's policy and encrypts/decrypts data as specified in the policy file (used primarily if files where created by another user while the managed user was logged off).
CMG Shield OS Hook	The CMG Shield OS Hook is a software module that interfaces to the Windows OS. OS data management calls (create, open, save, copy, rename) are intercepted by the CMG Shield OS Hook and encryption/decryption is performed according to the managed user's policies.
CREDANT Cryptographic Kernel (CCK)	The CREDANT Cryptographic Kernel (CCK) is a library of cryptographic functions. The CCK is a software library (shared or dynamic link), which provides an API to cryptographic functions including AES, Triple DES, SHA-1, HMAC (SHA-1), and an ANSI X9.31 compliant pseudorandom number generator.

2.5 Logical Boundary

The TOE's logical boundary is described below.

Windows End User's Data Protection

The TOE protects data on CMG Shield hosts from unauthorized access. This data includes CMG Shield administrator-configured host resident data. The TOE enables administrators to define central policies that define what file types and directories should be encrypted, what encryption standard to use, and whether to encrypt data copied to removable storage media. Administrators may also specify that all data created by specific applications should be encrypted, regardless of the file type or location.

Policies controlling encryption and Windows Service Invocation may be specified on a per-user basis (default policies apply if no user-specific policy has been defined). Identification and Authentication (required in order to associate the correct user policy) is performed by Windows (IT Environment).

TOE Management

The TOE supports management functionality that enables an administrator to define policies for protection (encryption) of data resident on end user workstations. Policies may be defined for specific users on specific workstations.

TOE Monitoring (Audit)

The TOE provides audit logs that track administrator activity and system events. Audit logs are stored in the Database via the IT Environment supplied DBMS. The TOE provides functionality for CMG Enterprise Server Administrators to view information and search logs based on a variety of criteria.

TOE Self Protection

The TOE protects itself from interference or bypass as much as possible. Since the TOE consists of a set of applications and Windows hooks, the TOE relies on the hardware and operating systems (IT Environment) to provide significant protection as well. TSF data is encrypted for protection.

2.6 Functionality Not Included in the Evaluation

The following functionality is not included in this evaluation:

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.

2.7 TOE Data

2.7.1 TSF Data

The TSF Data is described in the following table.

Table 4 - TSF Data

	Description
Security Attributes	
User Accounts	Unique userids are defined for all end users and administrators. The userid is used to bind the appropriate information to users when they authenticate.
Administrator Role	One of Help Desk Administrator, System Administrator, Security Administrator, Log Administrator, and Account Administrator. The role determines the administrator privileges.
Cryptographic Keys	
Authentication Key	The Authentication Key is used by the CMG Policy Proxy to

	Description
	authenticate a CMG Shield device. The Authentication Key is generated by the CMG Enterprise Server when a CMG Policy Proxy is installed, unique for each CMG Policy Proxy, and sent to the CMG Shield in the CMG Shield Initial Policy Distribution. The CMG Enterprise Server also sends the Authentication Key to the CMG Policy Proxy at initial CMG Policy Proxy/CMG Enterprise Server communication.
CMG Enterprise Server DBMS Key	The CMG Enterprise Server DBMS Key is used to encrypt data stored in the database. It is generated at CMG Enterprise Server installation.
Password Key	The Password Key is a derived key that is used to encrypt/decrypt the Root Key. The Password Key is derived by each the CMG Server and the CMG Shield by a SHA-1 hash of the user password. The Password Key unique to each managed user.
Policy Key	The Policy Key is used to encrypt/decrypt policies that are passed from the CMG Enterprise Server to the CMG Shield and used to encrypt the CMG Shield resident policies.
Root Key	Each managed user is assigned a unique Root Key. The Root Key is generated by the CMG Enterprise Server at End User initial login and sent to the End User in the CMG Shield Initial Policy Distribution. Once received, the CMG Shield uses the Root Key to decrypt all keys sent (except the Root Key), authenticate End Users on subsequent logins and to decrypt new keys sent from the CMG Enterprise Server in CMG Shield Policy Updates.
User Data Encryption Keys	
CMG Shield Application Encryption Key	Each CMG Shield User is assigned a CMG Shield Encryption Policy that defines the encryption policies for that user. Included in the Encryption Policy is a list of Application Data. The data generated or modified by the applications listed in the Application Data List will be encrypted with the CMG Shield Application Data Encryption Key. The CMG Shield enables an administrator to specify one of three privilege levels for the CMG Shield Application Data Key and a specific key is associated with each privilege level. Available privilege level options are Common, User, and User Roaming.
CMG Shield Common Encryption Key	Each CMG Shield User is assigned a CMG Shield Encryption Policy that defines the encryption policies for that user. Included in the Encryption Policy is a list of Common Files. Common Files define a list of folders, files and/or file-types on the CMG Shield resident host's hard drive(s) to be encrypted or excluded from encryption. Common Files can be accessed by all managed users who have access to the device.
CMG Shield User Data Encryption Key	Each CMG Shield User is assigned a CMG Shield Encryption Policy that defines the encryption policies for that user. Included in the Encryption Policy is a list of User Data. User Data define a list of folders, files and/or file-types on the CMG Shield resident host's hard drive(s) to be encrypted or excluded from encryption. User Data can only be accessed by the managed user whose policies specify encryption of the files. The CMG Shield enables an administrator to specify one of three privilege levels for the CMG Shield User Data Encryption Key and a specific key is associated with each privilege

	Description
	level. Available privilege level options are Common, User, and User Roaming.
Log Data	
Administrator Action Log	The Administrator Action Log is a table in the Database that records administrator logins, role modifications, policy modifications, policy publishing and LDAP communication.
Policies (Specific to a user)	
Encryption Enabled	True enables all encryption policies, and False disables all encryption policies. If this policy is False, no encryption takes place, regardless of other policy values.
Common Encrypted Folders	A list of folders on the device's hard drive(s) to be encrypted or excluded from encryption, which can then be accessed by all managed users who have access to the device.
Common Encryption Algorithm	Encryption algorithm used to encrypt data at the device (all users) level.
Application Data Encryption List	A list of process names of applications whose new files are to be encrypted.
Encrypt "My Documents"	True encrypts the My Documents folder with the User Data Encryption Key and the \All Users\Documents (or for Windows XP, \All Users\Shared Documents), which can then be decrypted by all managed users on the device, regardless of their policy settings.
Encrypt Outlook Personal Folders	True encrypts Outlook Personal Folders with the User Data Encryption Key.
Encrypt Removable Media	True encrypts all files (regardless of process ownership) created by the logged-on user on removable media/drives such that a user who activated against an Enterprise Server 5.0 or higher can work with them when logged on to any Shielded Windows device associated with the same Enterprise Server (and the same domain) the user activated against.
Encrypt Temporary Files	True encrypts all Windows OS temporary folders, which can then be decrypted by all managed users who have access to the device.
Encrypt Temporary Internet Files	True encrypts temporary Internet files cached on the Windows device with the User Data Encryption Key.
Encrypt Windows Paging File	True encrypts the Windows paging file.
User Encryption Algorithm	Encryption algorithm used to encrypt data at the individual user level. You can specify different values for different users of the same device.
Encrypt Executables on Removable Media	True encrypts files with .exe extensions on removable media when Encrypt Removable Media is True.
Scan Removable Media	True scans removable media on insertion, and encrypts or decrypts its contents based on the Encrypt Removable Media policy value.
Scan Workstation on Logon	True scans all current and previous encrypted folders on the Shielded workstation's local hard drives each time a managed user logs on.
User Encrypted Folders	A list of folders on the device's hard drive(s) to be encrypted with the User Data Encryption Key or excluded from encryption.

	Description
Workstation Scan Priority	Specifies the relative Windows priority of encrypted folder scanning. High and Highest prioritize scanning speed over system responsiveness, Low and Lowest prioritize system responsiveness over scanning speed and favor other resource-intensive activities, and Normal balances the two.
Gatekeeper Connections	If the Windows Shield cannot connect to the Policy Proxy specified during Shield installation, it attempts to connect to the alternate Policy Proxies listed here in the order specified.
Gatekeeper Polling Interval	The interval at which the Windows Shield attempts to poll the Policy Proxy for policy updates.
Length of Each Encryption Processing Delay	Defines the number of minutes an end user can defer applying the encryption/decryption related policies.
Number of Encryption Processing Delays Allowed	Defines the number of times an end user can defer the encryption/decryption delay period specified in the Length of Each Encryption Processing Delay.
Policy Distributions	
CMG Shield Initial Policy Distribution	The CMG Shield Initial Policy Distribution is created by the CMG Enterprise Server and sent to the CMG Shield at initial CMG Shield managed user login. The CMG Shield Initial Policy Distribution contains the following information: 1. Policies 2. User Data Encryption Keys 3. Root Key 4. Authentication Key 5. Policy Key
CMG Shield Policy Update Distribution	The CMG Shield Policy File Update Distribution is created by the CMG Enterprise Server and retrieved by the CMG Policy Proxy and then sent to the CMG Shield. The distribution contains the updated Policies

2.7.2 User Data

User Data is represented by the files on the end user device. Data files that have been encrypted cannot be read by unauthorized users.

2.8 Evaluated Configuration

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.

2.8.1 Deployment Options

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.

2.8.2 Configuration Parameters

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

2.8.3 IT Environment Detail

The following tables identify the IT Environment supplied details.

Table 5 - IT Environment Supplied Software Specifics

	DMBS host	LDAP host	Console host(s)	CMG Enterprise Server host	CMG Policy Proxy host	CMG Shield host
DBMS						
Microsoft SQL Server 2000 SP4	X					
Internet Browser						
Internet Explorer 5.5 SP2 and above			X			
LDAP						
Microsoft Active Directory®		X				
TOE Component Host OSs						
Microsoft Windows 2000 Advanced Server SP3 or SP4 (US English)				X	X	
Microsoft Windows 2000 Professional SP3 or SP4					X	X
Microsoft Windows 2000 Server SP3 or SP4 (US English)				X	X	
Microsoft Windows 2003 Server SP1 (US English)				X	X	
Microsoft Windows 2003 Server SP2 (US English)						X
Microsoft Windows XP Professional SP1 or SP2					X	
Support Software						
Apache Tomcat 5.5.9				X		
Java 2 Runtime Environment SE V5.0				X		
J2SE Runtime Environment (JRE) 5.0 Update 4				X		
Java 2 SDK SE V5.0				X		

	DMBS host	**LDAP host**	**Console host(s)**	**CMG Enterprise Server host**	**CMG Policy Proxy host**	**CMG Shield host**
OctetString VDE Server 2.0				X		
Apache Log4J				X		
SSL						
Supplied by OS	X	X	X	X	X	X
Smart card software (optional)						
Axalto Cyberflex E-Gate 32						X

Table 6 - IT Environment Supplied Hardware Specifics

	DMBS host	CMG Enterprise Server host	CMG Policy Proxy host	CMG Shield host
Hardware				
2+ GHz Intel class process (or dual processors)		X		X
Intel Pentium-class processor			X	
RAM				
2 GB RAM		X		
64 MB RAM				
Free Disk Space				
73.5 MB for Java				
2.5 GB for SQL database and logs	X			
6 MB for Directory Connector		X		
100 MB for logs				
13.2 MB minimum free disk space			X	
40 MB for free disk space				

2.9 Rationale for Non-Bypassability and Separation

The TOE is a set of applications that execute on top of an underlying system that includes hardware and software required for operation. Therefore responsibility for non-bypassability and separation are split between the TOE and IT Environment.

The TOE provides strictly controlled functionality to the users within the TSC. By limiting the functionality, the TSF is protected from corruption or compromise from users

within the TSC. The TOE interfaces are separated into 2 categories – security enforcing and security supporting. Security enforcing interfaces invoke the TSF and ensure that all enforcement functions complete successfully before allowing the user invoked action to proceed. Security supporting interfaces ensure that the TSF cannot be interfered with via those interfaces (i.e., they are isolated from the TSF).

The CMG Enterprise Server and CMG Policy Proxy components, as well as the LDAP Host and DBMS Host execute on Windows platforms dedicated to those applications. General purpose users should not have access to those systems for any purposes other than execution and support of the TOE. Multiple simultaneous administrator sessions via the CMG Enterprise Server web interfaces are supported, and the TOE associates distinct attributes and privileges with each to restrict their access appropriately.

On the end user devices executing the CMG Shield, the TOE operates via hooks to the OS. Users with Administrator privilege must be trusted to not interfere with the TOE. Non-Administrator users are unable to interfere with the TOE because of Windows protection mechanisms.

The OS and hardware support non-bypassability by ensuring access to protected resources passes through the TOE. On the end user devices executing the CMG Shield, the OS ensures that the TOE is invoked via the OS hooks. The hardware and OS provide separate process spaces in which the TOE executes; these process spaces are protected from interference from other processes except through the defined TOE interfaces.

Chapter 3

3 SECURITY ENVIRONMENT

This chapter identifies the following:

A) Significant assumptions about the TOE's operational environment.

B) IT related threats to the organisation countered by the TOE.

C) Environmental threats requiring controls to provide sufficient protection.

D) Organisational security policies for the TOE as appropriate.

This document identifies assumptions as A.*assumption* with *assumption* specifying a unique name. Threats are identified as T.*threat* with *threat* specifying a unique name.

3.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Environment.

Table 7 - Assumptions

A.Type	Description
A.INSTALL	The authorized administrator will install and configure the TOE and the IT Environment supplied hardware and software required by the TOE in a manner that maintains IT security policies and procedures described in the delivery and operation documentation and the administrator and user guidance documentation.
A.LOCATE	The processing resources of the TOE CMG Enterprise Server will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The administrators are non-hostile, appropriately trained and follow all administrator guidance.
A.RESTRICTDB	The administrator will configure access controls in the DBMS such that access to data in the database is as restrictive through the DBMS interfaces as it is through the TOE interfaces.

3.2 Threats

The following are threats addressed by the TOE and the IT Environment.

Table 8 - Threats

Threat	Threat Descriptions
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

Threat	Threat Descriptions
	devices through accidental means or unsophisticated attacks.

3.3 Organizational Security Policies

There are no security policies applicable to the TOE.

Chapter 4

4 SECURITY OBJECTIVES

Chapter 4 identifies the security objectives of the TOE and the IT Environment. The security objectives identify the responsibilities of the TOE and the TOE's IT environment in meeting the security needs.

This document identifies objectives of the TOE as O.*objective* with *objective* specifying a unique name. Objectives that apply to the IT environment are designated as O.E.*objective* with *objective* specifying a unique name. Objectives that apply to the Non-IT environment are designated as O.N.*objective* with *objective* specifying a unique name.

4.1 Security Objectives for the TOE

Table 9 - Security Objectives for the TOE

Security Objective for the TOE	Security Objectives for the TOE Descriptions
O.AUDIT	The TOE will provide the capability to create records of security-relevant events associated with administrators and provide the capability to view the audit records.
O.MANAGE	The TOE must include a set of functions that allow effective management of its security functionality and TSF data.
O.SFTSELFPROT	The TOE must protect itself from unauthorized modifications and access to its security functions.
O.TSFDATAPROT	The TOE must protect TSF Data from unauthorized access.
O.UDATAPROT	The TOE must protect end user data according to explicitly configured policies.

4.2 Security Objectives for the Environment

Table 10 - Security Objectives for the IT Environment

Security Objectives (IT Environment)	Security Objectives (IT Environment) Rationale
O.E.I&A	The IT Environment must provide a means to insure secure access to the hosts running TOE components and storing TSF Data.
O.E.ITSELFPROT	The IT Environment must provide a means to protect itself and the TOE from interference or bypass from interfaces and users outside the TSC.
O.E.SECMANACC	The IT Environment must provide a means to insure secure management access.
O.E.SECTRANS	The IT Environment must provide a means to insure secure transfer of TSF data sent between different hosts supporting TOE components and to/from hosts supporting IT Environment supplied software.
O.E.TIMESTAMP	The IT Environment must provide a reliable time stamp.

Table 11 - Security Objectives for the Non-IT Environment

Security Objectives (Non-IT Environment)	Security Objectives (Non-IT Environment) Rationale
O.N.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
O.N.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
O.N.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
O.N.RESTRICTDB	Those responsible for the TOE must ensure that access controls in the DBMS are configured such that access to data in the database is as restrictive through the DBMS interfaces as it is through the TOE interfaces.

Chapter 5

5 SECURITY REQUIREMENTS

Chapter 5 identifies the Security Functional Requirements for the TOE and for the IT Environment. The Security Functional Requirements included in this section are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.3* and all National Information Assurance Partnership (NIAP) and international interpretations with the exception of the items listed below.

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC.

Assignments: *indicated in italics.*

Selections: indicated in underlined text.

Assignments within selections*: indicated in italics and underlined text*.

Refinements: indicated in **bold text** with the addition of details and ~~**bold text strikeout**~~ when details are deleted.

Multiple Security Functional Requirement instances (iterations) are identified by the Security Functional Requirement component identification followed by the instance number in parenthesis (e.g. FDP_ACC.1(1)) and the Security Functional Requirement element name followed by the instance number in parenthesis (e.g. FDP_ACC.1.1(1)). This document continues the iteration numbering for Security Functional Requirements that apply to both the TOE and the IT Environment to provide a unique identifier for each SFR.

NIAP Interps (explicitly stated SFRs) used in this ST are identified by the NIAP Interp's SFR component identification and the NIAP Interp's SFR element name. Other explicitly stated SFRs component identification and SFR element name are identified by a name followed by _EXP. These explicitly stated SFRs are based on SFRs defined in [CC_PART2] and are therefore included in this ST in existing SFR's classes and SFR functional families.

5.1 TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear in Table 12 are described in more detail in the following subsections.

Table 12 - TOE Security Functional Requirements

Functional Component Class	Functional Component ID	Functional Component Name
Class FAU: Security Audit	FAU_GEN.1-NIAP-0347	Audit Data Generation
	FAU_SAR.1	Audit Review

Functional Component Class	Functional Component ID	Functional Component Name
Class FCS: Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.2	Cryptographic Key Distribution
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1	Cryptographic Operation
Class FDP: User Data Protection	FDP_ACC.1(1)	Subset Access Control
	FDP_ACC.1(2)	Subset Access Control
	FDP_ACF.1-NIAP-0407(1)	Security Attribute Based Access Control
	FDP_ACF.1-NIAP-0407(2)	Security Attribute Based Access Control
Class FMT: Security Management	FMT_MOF.1	Management of Security Functions Behaviour
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1(1)	Security Roles
Class FPT: Protection of the TSF	FPT_RVM_SFT_EXP.1	Non-Bypassability of the TSP for Software TOEs
	FPT_SEP_SFT_EXP.1	TSF Domain Separation for Software TOEs

5.1.1 Class FAU: Security audit

5.1.1.1 Security audit data generation (FAU_GEN.1-NIAP-0347)

5.1.1.1.1 FAU_GEN.1-NIAP-0347 Audit Data Generation

FAU_GEN.1.1-NIAP-0347 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the minimum level of audit; and

c) *additional auditable events identified in Table 13, column one, below.*.

FAU_GEN.1.2-NIAP-0347 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *audit information identified in Table 13, column three, below*.

Table 13 - FAU_GEN.1-NIAP-0347 Detail

Event Type	Description	Details
CMG Enterprise Server Administrator Login	Logging into and out of the CMG Enterprise Server	Userid
CMG Enterprise Server Administrator account management	Adding, modifying, and deleting CMG Enterprise Server Administrator accounts.	Userid of the administrator making the change, userid of the account changed, administrator role added, success or failure
LDAP synchronization	Synchronization of LDAP data	Success or failure
DBMS host communication	DBMS synchronization.	Success or failure
Modifying policies	Modifying policies.	Userid of the administrator making the change, serid of the account changed, field modified, previous value and new value
Publishing policies.	Publishing policies.	Userid of the administrator, userid of the policy published

5.1.1.2 Security audit review (FAU_SAR)

5.1.1.2.1 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *CMG Enterprise Server Administrators with the role of System Administrator, or Log Administrator* with the capability to read *all of the audit information identified in Table 13, column three, above* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.2 Class FCS: Cryptographic Support

5.1.2.1 Cryptographic key management (FCS_CKM)

5.1.2.1.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *random number generator* and specified cryptographic key sizes *specified in column 2 below* that meet the following: *X9.31 A.2.4 (TDES) with a modified seed (CAVP cert #229).*

Table 14 - FCS_CKM.1 Detail

Cryptographic Key	Cryptographic Key Sizes
Authentication Keys	

Cryptographic Key	Cryptographic Key Sizes
Authentication Key	128 bits
TSF Data Protection keys	
CMG Enterprise Server DBMS Key	128 bits
Policy Key	128 bits
Root Key	128 bits
CMG Shield User Data Protection Keys	
Common (for 3DES algorithm)	168 bits
Common (for AES 128 algorithm)	128 bits
Common (for AES 256 algorithm)	256 bits
User (for 3DES algorithm)	168 bits
User (for AES 128 algorithm)	128 bits
User (for AES 256 algorithm)	256 bits
User Roaming (for 3DES algorithm)	168 bits
User Roaming (for AES 128 algorithm)	128 bits
User Roaming (for AES 256 algorithm)	256 bits

Application Note: The Common keys are device-specific. The User keys are user-device-specific and User Roaming keys are user-specific.

5.1.2.1.2 FCS_CKM.2 Cryptographic Key Distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *key wrapping* that meets the following: *FIPS 197 (AES, CAVP Cert #117).*

5.1.2.1.3 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroization* that meets the following: *FIPS 140-2 (vendor affirmed).*

5.1.2.2 Cryptographic operation (FCS_COP)

5.1.2.2.1 FCS_COP.1 Cryptographic Operation

FCS_COP.1.1 The TSF shall perform *the cryptographic operation identified in column 1 below* in accordance with a specified cryptographic algorithm *specified in column two below* and cryptographic key sizes *specified in column three below* that meet the following: *standard specified in column four below.*

Table 15 - FCS_COP.1 Detail

Cryptographic Operation	Cryptographic algorithm	Cryptographic key sizes	Standard
Encryption/Decryption	AES (ECB and CBC modes)	128 and 256	FIPS 197 (CAVP Cert #117)
	Triple DES (ECB and CBC modes)	168	FIPS 46-3 (CAVP Cert #229)
Hashing	SHA-1	n/a	FIPS (CAVP Cert #206)
Random number	X9.31 A.2.4 (TDES) with a	n/a	X9.31 A.2.4

Cryptographic Operation	Cryptographic algorithm	Cryptographic key sizes	Standard
generation	modified seed		(TDES) (CAVP cert #229)

5.1.3 User Data Protection (FDP)

5.1.3.1 Access control policy (FDP_ACC)

5.1.3.1.1 FDP_ACC.1(1) Subset Access Control

FDP_ACC.1.1(1) The TSF shall enforce the *CMG Shield Open Access Control SFP* on

Subjects: CMG Shield OS Hook software component acting on behalf of an end user;

Objects: File on the end user device;

Operations: open, decrypt.

5.1.3.1.2 FDP_ACC.1(2) Subset Access Control

FDP_ACC.1.1(2) The TSF shall enforce the *CMG Shield Encrypt Access Control SFP* on

Subjects: CMG Shield OS Hook software component acting on behalf of an end user;

Objects: File on the end user device;

Operations: encrypt.

5.1.3.2 Access control functions (FDP_ACF-NIAP-0407)

5.1.3.2.1 FDP_ACF.1-NIAP-0407(1) Security Attribute Based Access Control

FDP_ACF.1.1-NIAP-0407(1) The TSF shall enforce the *CMG Shield Open Access Control SFP* to objects based on the following:

Subjects: CMG Shield OS hook software component acting on behalf of an end user;

Subject security attributes: managed or unmanaged, encryption policies (if managed).

Objects: File on the end user device;

Object Security attributes:

Whether or not the file was encrypted by the TOE,

Key reference of the key used to encrypt the file if it is encrypted.

FDP_ACF.1.2-NIAP-0407(1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) *If the file was not encrypted by the TOE, it may be opened (subject to any other access control constraints implemented by the IT Environment).*

b) *If the user is unmanaged, keys are not opened and access to encrypted data is denied.*

c) *If the key used to encrypt the file is open as the result of a successful domain user authentication, the file may be opened.*

d) *Otherwise access is denied.*

e) *If an encrypted file is allowed to be opened, the contents are decrypted using the same key and algorithm that were used to encrypt the file.*

Application Note: The purpose of this SFR is to ensure that an appropriate key is available to decrypt the file contents if the file is allowed to be opened. If no appropriate key is available to the end user, then access is denied on the open.

Application Note: Other common file operations are not restricted. For example, an unmanaged user is allowed to delete an encrypted file.

FDP_ACF.1.3-NIAP-0407(1) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *no additional rules.*

FDP_ACF.1.4-NIAP-0407(1) The TSF shall explicitly deny access of subjects to objects based on the following rules: *no additional explicit denial rules.*

5.1.3.2.2 FDP_ACF.1-NIAP-0407(2) Security Attribute Based Access Control

FDP_ACF.1.1-NIAP-0407(2) The TSF shall enforce the *CMG Shield Encrypt Access Control SFP* to objects based on the following:

Subjects: CMG Shield OS hook software component acting on behalf of an end user;

Subject security attributes:

managed or unmanaged,

application executing on behalf of the end user.

Objects: File on the end user device;

Object Security attributes:

File location and type and creating application.

FDP_ACF.1.2-NIAP-0407(2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) *If the end user is unmanaged, the file is not encrypted.*

b) *If the end user's policy has non-zero values for the deferred encryption parameters (Length of Each Encryption Processing Delay and Number of Encryption Processing Delays Allowed), encryption/decryption will be delayed per the parameters and end user input.*

c) *If the file location and name match an entry in the Common Encrypted Folder List for the end user, the file is encrypted using the configured Common Encryption Algorithm and the common key.*

If the file location and type match an entry in the User Encrypted Folder List for the end user, the file is encrypted using the configured User Data Encryption Key and the corresponding algorithm (either the User Encryption Algorithm for the user and user roaming keys or the Common Encryption Algorithm for the common key).

If the file location is on removable media and Encrypt Removable Media is active for the end user, the file is encrypted using the configured User Encryption Algorithm and the user roaming key.

If the application executing on behalf of the end user matches an entry in the Application Data Encryption List, the file is encrypted using the Application Data Encryption Key and the corresponding algorithm (either the User Encryption Algorithm for the user and user roaming keys or the Common Encryption Algorithm for the common key).

If the file location is under the Outlook Personal Folders and Encrypt Outlook Personal Folders is active for the end user, the file is encrypted using the configured User Data Encryption Key and the corresponding algorithm (either the User Encryption Algorithm for the user and user roaming keys or the Common Encryption Algorithm for the common key).

If the file location is under My Documents and Encrypt "My Documents" is active for the end user, the file is encrypted using the configured User Data Encryption Key and the corresponding algorithm (either the User Encryption Algorithm for the user and user roaming keys or the Common Encryption Algorithm for the common key).

If the file is a temporary file and Encrypt Temporary Files is active for the end user, the file is encrypted using the configured Common Encryption Key and the corresponding algorithm (either the User Encryption Algorithm for the user and user roaming keys or the Common Encryption Algorithm for the common key).

If the file is a temporary Internet file and Encrypt Temporary Internet Files is active for the end user, the file is encrypted using the configured User Data Encryption Key and the corresponding algorithm (either the User Encryption Algorithm for the user and user roaming keys or the Common Encryption Algorithm for the common key).

If the file is the Windows paging file and Encrypt Windows Paging File is active for the end user, the file is encrypted using AES-128 and the configured User Data Encryption Key.

Otherwise the file is not encrypted.

Application Note: This SFP references items contained within the encryption policies for the managed user. Since these items are described previously (see TSF Data in chapter 2), and for the sake of brevity, they are not enumerated in the subject security attributes for this SFR.

FDP_ACF.1.3-NIAP-0407(2) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *no additional rules*.

FDP_ACF.1.4-NIAP-0407(2) The TSF shall explicitly deny access of subjects to objects based on the following rules: *no additional explicit denial rules*.

5.1.4 Class FMT: Security management

5.1.4.1 Management of functions in TSF (FMT_MOF)

5.1.4.1.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to determine the behavior of, disable, enable, modify the behavior of the functions *encryption of data on end user devices, scanning of files on end user devices* to *administrator roles as defined in the following table*.

Table 16 - FMT_MOF.1 Detail

	Help Desk Administrator	System Administrator	Security Administrator	Log Administrator	Account Administrator
Encryption of data on end user devices			V, D, E, M		
Scanning of files on end user devices			V, D, E, M		
Deferring applying encryption/decryption on end user devices.			V,D, E,M		

Legend: V = determine behavior, D = Disable, E = Enable, M = Modify behavior

5.1.4.2 Management of TSF data (FMT_MTD)

5.1.4.2.1 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to *operation identified in Table 17, column two, below* the *list of TSF data identified in Table 17, column one, below* to *the role identified in Table 17, column three, below*.

Table 17 - FMT_MTD.1 Detail

TSF Data	Operation	Authorized Roles
User Accounts	query	Account Administrator, Help Desk Administrator, Security Administrator, System

TSF Data	Operation	Authorized Roles
		Administrator
Administrator Role	query, modify, delete	Account Administrator
Administrator Action Log	query	System Administrator, Log Administrator,
Encryption Enabled	modify	Security Administrator,
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
Common Encrypted Folders	modify	Security Administrator
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
Common Encryption Algorithm	modify	Security Administrator
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
Application Data Encryption List	modify	Security Administrator
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
Application Data Encryption Key	modify	Security Administrator
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
Encrypt “My Documents”	modify	Security Administrator
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
Encrypt Outlook Personal Folders	modify	Security Administrator
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
Encrypt Removable Media	modify	Security Administrator
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
Encrypt Temporary Files	modify	Security Administrator
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
Encrypt Temporary Internet Files	modify	Security Administrator

TSF Data	Operation	Authorized Roles
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
Encrypt Windows Paging File	modify	Security Administrator
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
User Encryption Algorithm	modify	Security Administrator
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
User Data Encryption Key	modify	Security Administrator
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
Secure Windows Password Hash	modify	Security Administrator
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
Encrypt Executables on Removable Media	modify	Security Administrator
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
Scan Removable Media	modify	Security Administrator
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
Scan Workstation on Logon	modify	Security Administrator
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
User Encrypted Folders	modify	Security Administrator
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
Workstation Scan Priority	modify	Security Administrator
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
Gatekeeper Connections	modify	Security Administrator

TSF Data	Operation	Authorized Roles
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
Gatekeeper Polling Interval	modify	Security Administrator
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
Length of Each Encryption Processing Delay	modify	Security Administrator
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator
Number of Encryption Processing Delays Allowed	modify	Security Administrator
	query	Account Administrator, Help Desk Administrator, Security Administrator, System Administrator

5.1.4.3 Specification of Management Functions (FMT_SMF)

5.1.4.3.1 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

A) Configure system parameters;

B) Configure end user encryption policies;

C) Review logs;

D) Manage administrator accounts

E) Sync with LDAP.

5.1.4.4 Security management roles (FMT_SMR)

5.1.4.4.1 FMT_SMR.1(1) Security Roles

FMT_SMR.1.1(1) The TSF shall maintain the roles *CMG Enterprise Server Help Desk Administrator, System Administrator, Security Administrator, Log Administrator, Account Administrator, CMG Shield Unmanaged User, and CMG Shield Managed User.*

FMT_SMR.1.2(1) The TSF shall be able to associate users with roles.

5.1.5 Class FPT: Protection of the TSF

5.1.5.1 Reference mediation for software TOEs (FPT_RVM_SFT_EXP)

5.1.5.1.1 FPT_RVM_SFT_EXP.1 Non-Bypassability of the TSP for Software TOEs

FPT_RVM_SFT_EXP.1.1: The TSF, when invoked shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed

5.1.5.2 Domain separation for software TOEs (FPT_SEP_SFT_EXP)

5.1.5.2.1 FPT_SEP_SFT_EXP.1 TSF Domain Separation for Software TOEs

FPT_SEP_SFT_EXP.1.1: The TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects in the TSC.

FPT_SEP_SFT_EXP.1.2: The TSF shall enforce separation between the security domains of subjects in the TSC.

5.2 Security Functional Requirements for the IT Environment

This section describes the security functional requirements for the IT Environment. The security functional requirements are identified in Table 18 and are described in more detail in the following subsections.

Table 18 - IT Environment Security Functional Requirements

Functional Component Class	Functional Component ID	Functional Component Name
Class FIA: Identification and Authentication	FIA_UAU.2	User Authentication Before any Action
	FIA_UID.2	User Identification Before any Action
Class FPT: Protection of the TSF	FPT_ITC.1	Inter-TSF Confidentiality During Transmission
	FPT_ITT.1	Basic Internal TSF Data Transfer Protection
	FPT_RVM_OS_EXP.1	Non-Bypassability of the TSP for Oss
	FPT_SEP_OS_EXP.1	TSF Domain Separation for Oss
	FPT_STM.1	Reliable Time Stamps

5.2.1 Class FIA: Identification and Authentication

5.2.1.1 FIA_UAU – User authentication

5.2.1.1.1 FIA_UAU.2 User Authentication Before any Action

FIA_UAU.2.1 The ~~TSF~~ **IT Environment** shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.1.2 User identification (FIA_UID)

5.2.1.2.1 FIA_UID.2 User Identification Before any Action

FIA_UID.2.1 The ~~TSF~~ **IT Environment** shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.2.2 Class FMT: Security management

5.2.2.1 Security management roles (FMT_SMR)

5.2.2.1.1 FMT_SMR.1(2) Security Roles

FMT_SMR.1.1(2) The ~~TSF~~ **IT Environment** shall maintain the roles *IT Administrator*.

FMT_SMR.1.2(2) The TSF shall be able to associate users with roles.

5.2.3 Class FPT: Protection of the TSF

5.2.3.1 Confidentiality of exported TSF data (FPT_ITC)

5.2.3.1.1 FPT_ITC.1 Inter-TSF Confidentiality During Transmission

FPT_ITC.1.1 The ~~TSF~~ **IT Environment** shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

5.2.3.2 Internal TOE TSF data transfer (FPT_ITT)

5.2.3.2.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 The ~~TSF~~ **IT Environment** shall protect TSF data from <u>disclosure</u> when it is transmitted between separate parts of the TOE.

5.2.3.3 Reference mediation for Oss (FPT_RVM_OS_EXP)

5.2.3.3.1 FPT_RVM_OS_EXP.1 Non-Bypassability of the TSP for Oss

FPT_RVM_OS.1.1 The security functions of the host OS shall ensure that host OS security policy enforcement functions are invoked and succeed before each function within the scope of control of the host OS is allowed to proceed.

5.2.3.4 Domain separation for Oss (FPT_SEP_OS_EXP)

5.2.3.4.1 FPT_SEP_OS_EXP.1 TSF Domain Separation for Oss

FPT_SEP_OS_EXP.1.1 The security functions of the host OS shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects in the scope of control of the host OS.

FPT_SEP_OS_EXP.1.2 The security functions of the host OS shall enforce separation between the security domains of subjects in the scope of control of the host OS.

5.2.3.5 Time stamps (FPT_STM)

5.2.3.5.1 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The ~~TSF~~ **IT Environment** shall be able to provide reliable time-stamps for its own use.

5.3 TOE Security Assurance Requirements

Table 19 identifies the security assurance components drawn from CC Part 3 Security Assurance Requirements EAL3. The SARs are not iterated or refined from Part 3.

Table 19 - Security Assurance Requirements

Assurance Class	Component ID	Component Description
Configuration Management	ACM_CAP.3	Configuration items
	ACM_SCP.1	CM Scope
Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.2	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support activity	ALC_DVS.1	Description of development security
Test activity	ATE_COV.2	Evidence of coverage
	ATE_DPT.1	Evidence of depth
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability Assessment	AVA_MSU.1	Misuse analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

5.4 SOF Declaration

The ST does not contain any TOE functional requirements that deal with computational and permutational mechanisms, so an SOF declaration is not needed for this ST. The minimum strength of function claim for the ST is SOF-Basic. This SOF claim is consistent with the intended threat environment for the TOE (low attack threat potential) and is consistent with EAL3.

Chapter 6

6 TOE SUMMARY SPECIFICATION

Chapter 6 identifies and describes the security functions implemented by the TOE and the assurance measures applied to ensure their correct implementation.

6.1 TOE Security Functions Detail

The TOE supports the following security functions:

1. Audit Data Generation Security Function
2. Audit Data Viewing Security Function
3. Management Security Function
4. Self Protection Security Function
5. User Data Protection Security Function

6.1.1 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

6.1.2 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.

6.1.3 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).

TSF Data is identified in the following table.

Table 20 - TSF Data

	Description
Security Attributes	
User Accounts	Unique userids are defined for all end users and administrators. The userid is used to bind the appropriate information to users when they authenticate.
Administrator Role	One of Help Desk, System, Security, Log, or Account. The role determines the administrator privileges.
Cryptographic Keys	
Authentication Key	The Authentication Key is used by the CMG Policy Proxy to authenticate a CMG Shield device. The Authentication Key is generated by the CMG Enterprise Server when a CMG Policy Proxy is installed, unique for each CMG Policy Proxy, and sent to the CMG Shield in the CMG Shield Initial Policy Distribution. The CMG Enterprise Server also sends the Authentication Key to the CMG Policy Proxy at initial CMG Policy Proxy/CMG Enterprise Server communication.
CMG Enterprise Server DBMS Key	The CMG Enterprise Server DBMS Key is used to encrypt data stored in the database. It is generated at CMG Enterprise Server installation.

	Description
Password Key	The Password Key is a derived key that is used to encrypt/decrypt the Root Key. The Password Key is derived by each the CMG Server and the CMG Shield by a SHA-1 hash of the user password. The Password Key unique to each managed user.
Policy Key	The Policy Key is used to encrypt/decrypt policies that are passed from the CMG Enterprise Server to the CMG Shield and used to encrypt the CMG Shield resident policies.
Root Key	Each managed user is assigned a unique Root Key. The Root Key is generated by the CMG Enterprise Server at End User initial login and sent to the End User in the CMG Shield Initial Policy Distribution. Once received, the CMG Shield uses the Root Key to decrypt all keys sent (except the Root Key), authenticate End Users on subsequent logins and to decrypt new keys sent from the CMG Enterprise Server in CMG Shield Policy Updates.
User Data Encryption Keys	
CMG Shield Application Encryption Key	Each CMG Shield User is assigned a CMG Shield Encryption Policy that defines the encryption policies for that user. Included in the Encryption Policy is a list of Application Data. The data generated or modified by the applications listed in the Application Data List will be encrypted with the CMG Shield Application Data Encryption Key. The CMG Shield enables an administrator to specify one of three privilege levels for the CMG Shield Application Data Key and a specific key is associated with each privilege level. Available privilege level options are Common, User, and User Roaming.
CMG Shield Common Encryption Key	Each CMG Shield User is assigned a CMG Shield Encryption Policy that defines the encryption policies for that user. Included in the Encryption Policy is a list of Common Files. Common Files define a list of folders, files and/or file-types on the CMG Shield resident host's hard drive(s) to be encrypted or excluded from encryption. Common Files can be accessed by all managed users who have access to the device.
CMG Shield User Data Encryption Key	Each CMG Shield User is assigned a CMG Shield Encryption Policy that defines the encryption policies for that user. Included in the Encryption Policy is a list of User Data. User Data define a list of folders, files and/or file-types on the CMG Shield resident host's hard drive(s) to be encrypted or excluded from encryption. User Data can only be accessed by the managed user whose policies specify encryption of the files. The CMG Shield enables an administrator to specify one of three privilege levels for the CMG Shield User Data Encryption Key and a specific key is associated with each privilege level. Available privilege level options are Common, User, and User Roaming.
Log Data	
Administrator Action Log	The Administrator Action Log is a table in the Database that records administrator logins, role modifications, policy modifications, policy publishing and LDAP communication.

	Description
Policies (Specific to a user)	
Encryption Enabled	True enables all encryption policies, and False disables all encryption policies. If this policy is False, no encryption takes place, regardless of other policy values.
Common Encrypted Folders	A list of folders on the device's hard drive(s) to be encrypted or excluded from encryption, which can then be accessed by all managed users who have access to the device.
Common Encryption Algorithm	Encryption algorithm used to encrypt data at the device (all users) level.
Application Data Encryption List	A list of process names of applications whose new files are to be encrypted.
Encrypt "My Documents"	True encrypts the My Documents folder with the User Data Encryption Key and the \All Users\Documents (or for Windows XP, \All Users\Shared Documents), which can then be decrypted by all managed users on the device, regardless of their policy settings.
Encrypt Outlook Personal Folders	True encrypts Outlook Personal Folders with the User Data Encryption Key.
Encrypt Removable Media	True encrypts all files (regardless of process ownership) created by the logged-on user on removable media/drives such that a user who activated against an Enterprise Server 5.0 or higher can work with them when logged on to any Shielded Windows device associated with the same Enterprise Server (and the same domain) the user activated against.
Encrypt Temporary Files	True encrypts all Windows OS temporary folders, which can then be decrypted by all managed users who have access to the device.
Encrypt Temporary Internet Files	True encrypts temporary Internet files cached on the Windows device with the User Data Encryption Key.
Encrypt Windows Paging File	True encrypts the Windows paging file.
User Encryption Algorithm	Encryption algorithm used to encrypt data at the individual user level. You can specify different values for different users of the same device.
Encrypt Executables on Removable Media	True encrypts files with .exe extensions on removable media when Encrypt Removable Media is True.
Scan Removable Media	True scans removable media on insertion, and encrypts or decrypts its contents based on the Encrypt Removable Media policy value.
Scan Workstation on Logon	True scans all current and previous encrypted folders on the Shielded workstation's local hard drives each time a managed user logs on.
User Encrypted Folders	A list of folders on the device's hard drive(s) to be encrypted with the User Data Encryption Key or excluded from encryption.
Workstation Scan Priority	Specifies the relative Windows priority of encrypted folder scanning. High and Highest prioritize scanning speed over system responsiveness, Low and Lowest prioritize system responsiveness over scanning speed and favor other resource-intensive activities, and Normal balances the two.
Gatekeeper Connections	If the Windows Shield cannot connect to the Policy Proxy specified during Shield installation, it attempts to connect to the alternate Policy Proxies listed here in the order specified.
Gatekeeper Polling Interval	The interval at which the Windows Shield attempts to poll Policy Proxy for policy updates.

	Description
Length of Each Encryption Processing Delay	Defines the number of minutes an end user can defer applying the encryption/decryption related policies.
Number of Encryption Processing Delays Allowed	Defines the number of times an end user can defer the encryption/decryption delay period specified in the Length of Each Encryption Processing Delay.
Policy Distributions	
CMG Shield Initial Policy Distribution	The CMG Shield Initial Policy Distribution is created by the CMG Enterprise Server and sent to the CMG Shield at initial CMG Shield managed user login. The CMG Shield Initial Policy Distribution contains the following information: 1. Policies 2. User Data Encryption Keys 3. Root Key 4. Authentication Key 5. Policy Key
CMG Shield Policy Update Distribution	The CMG Shield Policy File Update Distribution is created by the CMG Enterprise Server and retrieved by the CMG Policy Proxy and then sent to the CMG Shield. The distribution contains the updated Policies.

End user policies are organized in a hierarchical structure in the database and inherit policy settings from the parent node if no specific values are set for the end user. The following table summarizes the TSF data that can be modified by an authorized administrator by role.

Table 21 - Administrator Role Permissions

	Help Desk	System	Security	Log	Account
Viewing, modifying, deleting Encryption Policy entries			X		
Publishing policies			X		
Viewing and modifying Proxy Policy system parameters			X		
Analyzing logs		X		X	
Viewing, Creating, changing, deleting administrator accounts					X
Viewing end user accounts	X	X	X		X

6.1.4 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 22 - 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 23 - 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

6.1.5 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 24 - Encryption Summary

Data To Be Protected	Key Determination	Algorithm Determination
Common Encrypted Folders	Always uses the common key	Common Encryption Algorithm

Data To Be Protected	Key Determination	Algorithm Determination
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 25 - 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

Data To Be Protected	Special Considerations
	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.

6.2 Assurance Measures

The TOE satisfies CC EAL3 assurance requirements. This section identifies the Configuration Management, Delivery and Operation, Development, Guidance Documents, Test, Life Cycle support, and Vulnerability Assessment Assurance Measures applied by CREDANT to satisfy the CC EAL3 assurance requirements. All dependencies are satisfied.

Table 26 - Assurance Measures

Component ID	Documentation Satisfying Component	Rationale
ACM_CAP.3	CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Configuration Management Plan, Version 1.4	CREDANT performs configuration management on configuration items of the TOE. Configuration management is performed on the TOE and the implementation representation of the TOE. The configuration items are uniquely identified and each release of the TOE has a unique reference.
ACM_SCP.1	Bill of Materials for CmgEnterpriseEdition, Build 244	CREDANT includes all TOE components and relevant documents (including evidence generated for the CC evaluation) within their configuration management system.
ADO_DEL.1	CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Delivery Procedures, Version 1.2	CREDANT documents the delivery procedure for the TOE to include the procedure on how to download certain components of the TOE from the CREDANT website and how certain components of the TOE are physically delivered to the user. The delivery procedure detail how the end-user may determine if they have the TOE and if the integrity of the TOE has been maintained. Further, the delivery documentation describes how to acquire the proper license keys to use the TOE components.
ADO_IGS.1	CREDANT Mobile Guardian (CMG) Enterprise Edition Installation Supplement CREDANT Mobile Guardian (CMG) Enterprise Edition Custom Server Installation and Configuration Guide	CREDANT documents the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ADV_FSP.1	CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Functional Specification (FSP), Version 1.5	The externally visible interfaces of the TOE used by the users of the TOE along with the description of the security functions and a correspondence between the interfaces and the security functions from the ST are documented by CREDANT development evidence.

Component ID	Documentation Satisfying Component	Rationale
ADV_HLD.2	CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 High Level Design (HLD), Version 1.3	The subsystems and the communication between the subsystems of the TOE are documented in CREDANT development evidence.
ADV_RCR.1	CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Functional Specification (FSP), Version 1.5 CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 High Level Design (HLD), Version 1.3	The correspondence is contained in the documents used for ADV_FSP.1 and ADV_HLD.2.
AGD_ADM.1	AdminHelp.chm	The administrative guidance is detailed to provide descriptions of how administrative users of the TOE can securely administer the TOE using those functions and interfaces detailed in the guidance.
AGD_USR.1	WindowsShieldHelp.chm	User guidance is provided for those roles defined in the TOE that do not have all the authorizations as the administrative role.
ALC_DVS.1	CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Development Security Plan, Version 1.2	CREDANT implements processes and procedures for the development environment that provide security for the development process.
ATE_COV.2	CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Test Plan, Version 1.2	CREDANT demonstrates the external interfaces tested during functional testing using a coverage analysis.
ATE_DPT.1	CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Test Plan, Version 1.2	CREDANT demonstrates the subsystem interfaces tested during functional testing using a depth analysis.

Component ID	Documentation Satisfying Component	Rationale
ATE_FUN.1	CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Test Plan, Version 1.2 CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Test Procedures, Version 1.1 CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Test Results, Version 1.0	CREDANT functional testing documentation contains a test plan, a description of the tests, along with the expected and actual results of the test conducted against the functions specified in the ST.
ATE_IND.2	CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Test Plan, Version 1.2 CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Test Procedures, Version 1.1 CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Test Results, Version 1.0	CREDANT will help meet the independent testing by providing the TOE to the evaluation facility.
AVA_MSU.1	AdminHelp.chm WindowsShieldHelp.chm	The administrative and user guidance referenced for AGD_ADM.1 and AGD_USR.1 satisfy the requirements for this component also.
AVA_SOF.1	CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Strength of Function Analysis, Version 1.1	CREDANT documents the strength of function associated with any permutational or probabilistic mechanisms satisfies the minimum strength of function claimed in the ST.

Component ID	Documentation Satisfying Component	Rationale
AVA_VLA.1	CREDANT Mobile Guardian (CMG) Enterprise Edition Version 5.2.1 SP4 Vulnerability Analysis, Version 1.2	CREDANT documents their vulnerability analysis search for obvious flaws and weaknesses in the TOE.

Chapter 7

7 PROTECTION PROFILE CLAIMS

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Chapter 1, Section 1.1 Protection Profile Conformance.

7.1 Protection Profile Reference

This Security Target does not claim conformance to any registered Protection Profile.

7.2 Protection Profile Refinements

This Security Target does not claim conformance to any registered Protection Profile.

7.3 Protection Profile Additions

This Security Target does not claim conformance to any registered Protection Profile.

7.4 Protection Profile Rationale

This Security Target does not claim conformance to any registered Protection Profile.

Chapter 8

8 RATIONALE

8.1 Security Objective Rationale

This section demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective. Table 27 demonstrates the correspondence between the security objectives identified in Chapter 4 to the assumptions and threats identified in Chapter 3. Table 28 provides the rationale proving that each threat and assumption is addressed.

Table 27 - Threats, Policies and Assumptions to Security Objectives Mappings

	O.AUDIT	O.MANAGE	O.SFTSELFPROT	O.TSFDATAPROT	O.UDATAPROT	O.E.I&A	O.E.ITSELFPROT	O.E.SECMANACC	O.E.SECTRANS	O.E.TIMESTAMP	O.N.INSTALL	O.N.PERSON	O.N.PHYSICAL	O.N.RESTRICTDB
A.INSTALL											X			
A.LOCATE													X	
A.MANAGE												X		
A.NOEVIL												X		
A.RESTRICTDB														X
T.ACCIDENTAL	X									X		X		
T.TSF_COMP			X	X		X	X	X	X					
T.USERDATA		X			X									

Table 28 - Threats and Assumptions to Security Objectives Rationale

Threat/ Assumption	Security Objective Rationale
A.INSTALL	O.N.INSTALL addresses this assumption by requiring that the TOE be installed in an appropriate manner.
A.LOCATE	O.N.PHYSICAL addresses this assumption by requiring the CMG Enterprise Server to be located in an area that precludes unauthorized physical access.
A.MANAGE	O.N.PERSON addresses this assumption by requiring administrators to be trained.

Threat/ Assumption	Security Objective Rationale
A.NOEVIL	O.N.PERSON addresses this assumption by requiring administrators to be screened.
A.RESTRICTDB	O.N.RESTRICTDB addresses this assumption by requiring the administrators to limit access to data in the database via the DBMS to the privileges available through the TOE.
T.ACCIDENTAL	O.AUDIT ensures that all configuration changes made by administrators are audited in case those actions need to be reviewed at a later time. O.E.TIMESTAMP – helps to mitigate this threat by ensuring that audit records have correct timestamps. O.N.PERSON addresses this assumption by requiring administrators to be trained.
T.TSF_COMP	O.SFTSELFPROT – contributes to countering this threat by ensuring that the TSF can protect itself from users within the TSC. If the TSF could not maintain and control its domain of execution, it could not be trusted to control access to the resources under its control, which includes the audit trail. Ensuring that the TSF is always invoked is also critical to the mitigation of this threat. O.TSFDATAPROT – contributes to countering this threat by ensuring the TSF data cannot be modified or deleted by unauthorized users via interfaces within the TSC. O.E.I&A – contributes to countering this threat by providing a mechanism to identify and authenticate users so that appropriate permissions may be associated with them, thereby enabling their actions to be appropriately limited. O.E.ITSELFPROT – contributes to countering this threat by ensuring that the OS can protect itself from users within its control. In turn, this permits the OS (when properly configured) to protect the TSF and TSF data from unauthorized modifications or bypass from users or interfaces outside the TSC. O.E.SECMANGACC – this object helps to mitigate this threat by ensuring that all remote management access is protected by SSL. O.E.SECTRANS – this objective helps to mitigate this threat by ensuring that all TSF Data transmitted between hosts is protected by SSL.
T.USERDATA	O.MANAGE – this objective addresses this threat by providing a mechanism for the administrator to specify what data on the end user devices is sensitive. O.UDATAPROT – this objective address this threat by ensuring that data files (User Data) is protected (encrypted) according to explicitly stated configured policies.

8.2 Rationale for Security Functional Requirements

8.2.1 Rationale for SFRs of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the Security Functional Requirements are suitable to address the security objectives.

Table 29 identifies for each Security Functional Requirement identified in Section 5.1, the TOE security objective(s) identified in Section 4.1 that address it. Table 30 provides the rationale proving that each security objective is addressed by a Security Functional Requirement.

Table 29 - TOE SFRs to TOE Security Objectives Mapping

	O.AUDIT	O.MANAGE	O.SFTSELFPROT	O.TSFDATAPROT	O.UDATAPROT
FAU_GEN.1-NIAP-0347	X				
FAU_SAR.1	X				
FCS_CKM.1				X	X
FCS_CKM.2				X	
FCS_CKM.4				X	
FCS_COP.1				X	X
FDP_ACC.1(1)					X
FDP_ACC.1(2)					X
FDP_ACF.1-NIAP-0407(1)					X
FDP_ACF.1-NIAP-0407(2)					X
FMT_MOF.1		X			
FMT_MTD.1		X			
FMT_SMF.1		X			
FMT_SMR.1(1)	X	X			X
FPT_RVM_SFT_EXP.1			X		
FPT_SEP_SFT_EXP.1			X		

Table 30 - TOE SFRs to TOE Security Objectives Rationale

Security Objective (TOE)	Security Objectives Rationale
O.AUDIT	The TOE must record audit records that record security-relevant events associated with users and administrators. FAU_GEN.1.1-NIAP-0347 defines the set of events that the TOE records. This requirement ensures that the Administrator has the ability to audit any security

Security Objective (TOE)	Security Objectives Rationale
	relevant event that takes place in the TOE. This requirement also defines the information that is contained in the audit record for each auditable event. FAU_SAR.1.1 identifies the subset of administrator roles (FMT_SMR.1(1)) supported by the TOE that have access to CMG Enterprise Server resident audit records and by exclusion, identifies the roles that do not have access to the audit records.
O.MANAGE	The TOE must provide a means to effectively manage TOE functionality and TSF data used by the TOE. The TOE provides a management interface and management functionality that enables an administrator to define encryption policies enforced by the CMG Shield, review audit records that report the operation of the TOE, and to assign administrator users roles used to configure and monitor the TOE (FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1(1)).
O.SFTSELFPROT	The TOE must protect itself from unauthorized modifications and access to its security functions and TSF data. FPT_RVM_SW_EXP.1 – The TOE must ensure that its security functions cannot be bypassed via its own interfaces in order to protect itself from unauthorized disclosure and tampering. The TOE is composed of multiple software components. The software components of the TOE are not able to provide complete non-bypassability (FPT_RVM) by themselves. The TOE relies on IT environment supplied Oss, hardware and a DBMS to help in completely implementing non-bypassability. This SFR states the portion of the FPT_RVM (non-bypassability of the TSP) requirement that is addressed by the TOE. FPT_SEP_SW_EXP.1 – The TOE utilizes separate domains of execution in order to protect itself from tampering and interference. The TOE is composed of multiple software components. The software components of the TOE are not able to provide complete domain separation (FPT_SEP) by themselves. The TOE relies on IT environment supplied Oss and hardware to help in completely implementing domain separation. This SFR states the portion of the FPT_SEP (domain separation) requirement that is addressed by the TOE.
O.TSFDATAPROT	The TOE must protect TSF Data from unauthorized access. TSF data (keys and policies) at rest and in transit is always encrypted, thereby protecting the data from unauthorized access. FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, and FCS_COP.1 identify how cryptographic keys are generated or derived, how the keys are transmitted, how they are destructed after use, and the cryptographic operations used to generate the keys thereby identifying the protective mechanisms provided by the TOE that insures protective storage and transmission of the keys. The requirements also define the cryptographic protective mechanism provided by the TOE used in conjunction with the cryptographic keys and encryption/decryption algorithms identified in FCS_COP.1 to protect non-keying material TSF Data at rest and in transit.

Security Objective (TOE)	Security Objectives Rationale
O.UDATAPROT	The TOE must protect CMG Shield host resident user data from unauthorized access according to explicitly defined encryption rules. The TOE protects CMG Shield resident data files (user data) according to configured policies. FDP_ACC.1(1), FDP_ACC.1(2), FDP_ACF.1-NIAP-0407(1), and FDP_ACF.1-NIAP-0407(2) describe the rules enforced by the CMG Shield to protect CMG Shield resident data files from disclosure. FCS_CKM.1 defines the key generation algorithm used to generate the keys used to encrypt the User Data as specified in the algorithms identified in FCS_COP.1. FMT_SMR.1(1) is used to support this objective by defining CMG Shield resident user roles (managed users and unmanaged users) that are used by the TOE to enforce the user data protection rules.

8.2.2 Rationale for SFRs of the IT Environment

This section provides rationale for the IT Environment's Security Functional Requirements demonstrating that the IT Environment's Security Functional Requirements are suitable to address the IT Environment's security objectives. Table 31 identifies for each IT Environment Security Functional Requirement identified in Section 5.2, the IT Environment's security objective(s) identified in Section 4.2 that address it. Table 32 provides the rationale proving that each IT Environment security objective is addressed by an IT Environment Security Functional Requirement.

Table 31 - IT Environment SFRs to IT Environment Security Objectives Mapping

	O.E.I&A	O.E.ITSELFPROT	O.E.SECMANACC	O.E.SECTRANS	O.E.TIMESTAMP
FIA_UAU.2	X				
FIA_UID.2	X				
FMT_SMR.1(2)	X				
FPT_ITC.1			X	X	
FPT_ITT.1				X	
FPT_RVM_OS_EXP.1		X			
FPT_SEP_OS_EXP.1		X			

	O.E.I&A	O.E.ITSELFPROT	O.E.SECMANACC	O.E.SECTRANS	O.E.TIMESTAMP
FPT_STM.1					X

Table 32 - IT Environment SFRs to IT Environment Security Objectives Rationale

Security Objectives (IT Environment)	Security Objectives (IT Environment) Rationale
O.E.I&A	The IT Environment must provide a means to insure secure access to the hosts running TOE components and storing TSF Data. The IT Environment accomplishes this by requiring all users accessing any host running a TOE component (CMG Enterprise Server host, any CMG Policy Proxy host, any CMG Shield host) and any host running TOE relied upon IT Environment supplied software (any CMG console host, any LDAP host, and the DBMS host) to identify and authenticate themselves before allowing the user to invoke any action that will effect the TOE's security functionality or access TSF Data (FIA_UAU.2, FIA_UID.2, FMT_SMR.1(2)).
O.E.ITSELFPROT	The IT Environment, combined with the TOE, must provide a means to protect the TOE from unauthorized modifications and unauthorized access to the TOE's security functions and TSS data (FPT_RVM_OS_EXP.1, FPT_SEP_OS_EXP.1).
O.E.SECMANACC	The IT Environment must provide a means to insure secure management access. The IT Environment accomplishes this by requiring administrators accessing the CMG Enterprise Server via a remote system console host supporting remote administration from the console access point (Web Interface Console) using SSL only (FPT_ITC.1).
O.E.SECTRANS	The IT Environment must provide a means to insure secure transfer of TSF data sent between different hosts supporting TOE components and to/from hosts supporting IT Environment supplied software. The IT Environment accomplishes this by supporting intra-TOE communication between the CMG Enterprise Server host, the CMG Policy Proxy host, and the CMG Shielded host using SSL only (FPT_ITT.1). The IT Environment accomplishes this by supporting inter-TOE communication between the CMG Enterprise Server host and the LDAP host, the DBMS host, the Console host and the CMG Shield host and the LDAP host using SSL only (FPT_ITC.1).

Security Objectives (IT Environment)	Security Objectives (IT Environment) Rationale
O.E.TIMESTAMP	The IT Environment must provide a reliable time stamp. Each host relied upon by the TOE and supplied by the IT Environment provides a reliable time stamp (FPT_STM.1). The time stamp is supplied by both the IT Environment OS and hardware.

8.3 TOE Security Functions Rationale

This section demonstrates the suitability of the security functions defined in section 6.1 of meeting the TOE's Security Functional Requirements identified in Section 5.1 and that the security functional requirements are completely and accurately met by the TOE's Security Functions.

Table 33 demonstrates the correspondence between the Security Functions and the TOE Security Functional Requirements. Table 34 provides the rationale proving that each SFR addresses a Security Function. The following sections provide the rationale proving that each Security Function is addressed by a TOE Security Functional Requirement.

Table 33 - TOE SFRs to TOE Security Function Mapping

	Audit Data Generation Security Function	Audit Data Viewing Security Function	Management Security Function	Self Protection Security Function	User Data Protection Security Function
FAU_GEN.1.1-NIAP-0347(1)	X				
FAU_SAR.1		X			
FCS_CKM.1				X	X
FCS_CKM.2				X	

	Audit Data Generation Security Function	Audit Data Viewing Security Function	Management Security Function	Self Protection Security Function	User Data Protection Security Function
FCS_CKM.4				X	
FCS_COP.1				X	X
FDP_ACC.1(1)					X
FDP_ACC.1(2)					X
FDP_ACF.1-NIAP-0407(1)					X
FDP_ACF.1-NIAP-0407(2)					X
FMT_MOF.1			X		
FMT_MTD.1			X		
FMT_SMF.1			X		
FMT_SMR.1(1)		X	X		
FPT_RVM_SFT_EXP.1				X	
FPT_SEP_SFT_EXP.1				X	

Table 34 - TOE SFRs to TOE Security Functions Rationale

Security Functional Requirement (TOE)	Security Function Rationale
FAU_GEN.1.1-NIAP-0347	Audit Data Generation Security Function – The TOE generates audit records recording all TSF Data accesses and use of system functionality.

Security Functional Requirement (TOE)	Security Function Rationale
FAU_SAR.1	Audit Data Viewing Security Function - The TOE provides an administrator interface that enables administrators to view audit records generated by the TOE.
FCS_CKM.1	All cryptographic keys (except the Password Key) used by the TOE are generated according to a Credant FIPS approved algorithm (X9.31 A.2.4 (TDES)) with a modified seed. The keys generated by the TOE are classified in three categories: Authentication Keys, TSF Data Protection Keys, and CMG Shield User Data Protection Keys. Self Protection Security Function – Authentication Keys and TSF Data Protection Keys are used to support the Self Protection Security Function. User Data Protection Security Function – CMG Shield User Data Protection Keys are used to protect CMG Shield resident user data.
FCS_CKM.2	Self Protection Security Function – All cryptographic keys required by the CMG Shield are generated by the CMG Enterprise Server and sent to the CMG Shield protected (encrypted) by Credant's FIPS approved AES algorithm. The Authentication Key is also sent by the CMG Enterprise Server to the CMG Policy Proxy protected by Credant's FIPS approved AES algorithm.
FCS_CKM.4	Self Protection Security Function – All cryptographic keys used by the TOE are zeroed when no longer used. Specifically, when a user logs out the user's keys are zeroed out.
FCS_COP.1	The TOE uses FIPS approved algorithms for key generation, key distribution and user data protection. Self Protection Security Function – All cryptographic keys (except the Password Key) are generated using the Credant FIPS approved algorithm (X9.31 A.2.4 (TDES) with a modified seed. The RNG used for this algorithm is Credant's FIPS approved RNG. Self Protection Security Function – All distributed cryptographic keys are sent protected using the Credant FIPS approved AES algorithm. Self Protection Security Function – The password key is derived by hashing the key using a CREDENT FIPS approved algorithm. User Data Protection Security Function – CMG Shield resident User Data is encrypted/decrypted using either AES 128, AES 256, or 3DES algorithms FIPS approved algorithms.

Security Functional Requirement (TOE)	Security Function Rationale
FDP_ACC.1(1)	User Data Protection Security Function – The TOE decrypts CMG Shield resident User Data according to policy files received from the CMG Enterprise Server and updates received from the CMG Policy Proxy. The TOE uses the policy files to enforce decryption rules based on the files included in the folders identified or files excluded in the policy file's Common Encrypted Folders field, the User Encrypted Folders field, and if configured, on removable media. Decryption rules apply when a managed user creates, views, modifies, copies, moves, or renames User Data identified in the managed user's policy file Common Encrypted Folders field, the User Encrypted Folders field, and if configured, on removable media.
FDP_ACC.1(2)	User Data Protection Security Function – The TOE encrypts CMG Shield resident User Data according to policy files received from the CMG Enterprise Server and updates received from the CMG Policy Proxy. The TOE uses the policy files to enforce encryption rules based on the folders identified or excluded in the policy file's Common Encrypted Folders field, the User Encrypted Folders field, and if configured, on removable media. Encryption rules apply when a managed user creates, views, modifies, copies, moves, or renames User Data identified in the managed user's policy file Common Encrypted Folders field, the User Encrypted Folders field, and if configured, on removable media.
FDP_ACF.1-NIAP-0407(1)	User Data Protection Security Function – The TOE decrypts CMG Shield resident User Data according to policy files received from the CMG Enterprise Server and updates received from the CMG Policy Proxy. The TOE uses the policy files to enforce decryption rules based on the files folders identified or excluded in the policy file's Common Encrypted Folders field, the User Encrypted Folders field, and if configured, on removable media. FDP_ACF.1-NIAP-0407(1) defines the rules used to enforce encryption and decryption and defines the rules enforced that allow multiple users to access data and the rules that enforce whether data can be read on the resident CMG Shield host only or can be transferred to another CMG Shield host.
FDP_ACF.1-NIAP-0407(2)	User Data Protection Security Function – The TOE encrypts CMG Shield resident User Data according to policy files received from the CMG Enterprise Server and updates received from the CMG Policy Proxy. The TOE uses the policy files to enforce encryption rules based on the folders identified or excluded in the policy file's Common Encrypted Folders field, the User Encrypted Folders field, and if configured, on removable media. Encryption rules apply when a managed user creates, views, modifies, copies, moves, or renames User Data identified in the managed user's policy file Common Encrypted Folders field, the User Encrypted Folders field, and if configured, on removable media.
FMT_MOF.1	Management Security Function – The TOE enables administrators to modify security functionality. This security functionality includes whether end user's files should be encrypted and when the encryption rules are applied.

Security Functional Requirement (TOE)	Security Function Rationale
FMT_MTD.1	Management Security Function – The TOE enables administrators to query and modify all end user policies including policies that define CMG Shield system parameters that define polling and Policy Proxy communication and end user encryption policies. The TOE additionally enables administrators to define CMG Enterprise System administrators and their roles.
FMT_SMF.1	Management Security Function – the TOE provides Administrator accessible management functions that enable users to view audit records, modify and publish policies that define a CMG Shield Access Managed User's encryption/decryption policies, assign administrators the TOE supported roles, and modify system parameters that include (polling intervals, whether unmanaged users are supported).
FMT_SMR.1(1)	Audit Data Viewing Security Function – The TOE implements CMG Enterprise Server Administrator roles and defines a subset of these roles as CMG Enterprise Server Administrators who are allowed to view audit records. Management Security Function – the TOE implements CMG Enterprise Server Administrator roles and defines a subset of these roles as CMG Enterprise Server Administrators who are allowed to perform specific management operations.
FPT_RVM_SFT_EXP.1	Self Protection Security Function – Security functions of the TSF may not be bypassed by activities within the TSC. Interfaces to the TSF ensure that security policies are enforced. TOE interfaces that do not invoke the TSF can not be used to bypass the TSF.
FPT_SEP_SFT_EXP.1	Self Protection Security Function – Untrusted subjects within the TSC have strictly limited functionality that prevents interference or tampering with the TSF.

8.4 Rationale for Assurance Requirements

EAL3 was chosen because it is consistent with current best commercial practice for IT product development and is appropriate for the intended threat environment of the TOE (low attack threat potential).

8.5 TOE Security Functional Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified TOE and IT Security Functional Requirements include the appropriate hierarchical SFRs and dependent SFRs. Table 35 lists the TOE Security Functional Components and the Security Functional Components each are hierarchical to and dependent upon and any necessary rationale. Table 36 lists the IT Environment Security Functional Components and the Security Functional Components each are hierarchical to and dependent upon and any necessary rationale.

N/A in the rationale column means the Security Functional Requirement has no dependencies and therefore, no dependency rationale is required.

Table 35 - TOE SFR Dependency Rationale

Security Functional Requirement (TOE)	Hierarchical To	Dependency	Rationale
FAU_GEN.1.-NIAP-0347	Nothing	FPT_STM.1	Satisfied by the IT Environment.
FAU_SAR.1	Nothing	FAU_GEN.1	Satisfied by FAU_GEN.1-NIAP-0347.
FCS_CKM.1	Nothing	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	FCS_COP.1 is satisfied. FCS_CKM.4 is satisfied. FMT_MSA.2 is not satisfied. However, it is not applicable because there is no management configuration options of security attributes used to generate the keys identified in FCS_CKM.1.
FCS_CKM.2	Nothing	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1 is satisfied. FCS_CKM.4 is satisfied. FMT_MSA.2 is not satisfied. However, it is not applicable because there are no management configuration options of security attributes used for cryptographic key distribution identified in FCS_CKM.2.
FCS_CKM.4	Nothing	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FMT_MSA.2	FCS_CKM.1 is satisfied. FMT_MSA.2 is not satisfied. However, it is not applicable because there are no management configuration options of security attributes used for cryptographic key destruction identified in FCS_CKM.4.
FCS_COP.1	Nothing	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1 is satisfied. FCS_CKM.4 is satisfied. FMT_MSA.2 is not satisfied. However, it is not applicable because there are no management configuration options of security attributes used for cryptographic operations.

Security Functional Requirement (TOE)	Hierarchical To	Dependency	Rationale
FDP_ACC.1(1)	Nothing	FDP_ACF.1	FDP_ACF.1 is satisfied by FDP_ACF.1-NIAP-0407(1)
FDP_ACC.1(2)	Nothing	FDP_ACF.1	FDP_ACF.1 is satisfied by FDP_ACF.1-NIAP-0407(2)
FDP_ACF.1-NIAP-0407(1)	Nothing	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1 is satisfied by FDP_ACC.1(1). FMT_MSA.3 is not satisfied. However, if it not applicable because all of the security attributes are dynamically determined by the TSF.
FDP_ACF.1-NIAP-0407(2)	Nothing	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1 is satisfied by FDP_ACC.1(2). FMT_MSA.3 is not satisfied. However, if it not applicable because all of the security attributes are dynamically determined by the TSF.
FMT_MOF.1	Nothing	FMT_SMF.1, FMT_SMR.1(1)	Satisfied by the TOE. Satisfied by the TOE.
FMT_MTD.1	Nothing	FMT_SMF.1 FMT_SMR.1(1)	Satisfied by the TOE. Satisfied by the TOE.
FMT_SMF.1	Nothing	None	N/A
FMT_SMR.1(1)	Nothing	FIA_UID.1	Satisfied by the IT Environment.
FPT_RVM_SFT_EXP.1	Nothing	None	N/A
FPT_SEP_SFT_EXP.1	Nothing	None	N/A

Table 36 - IT Environment SFRs Dependency Rationale

Security Functional Requirement (IT Environment)	Hierarchical To	Dependency	Rationale
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	FIA_UID.1 is satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1.
FIA_UID.2	FIA_UID.1	None	N/A
FMT_SMR.1(2)	Nothing	FIA_UID.1	Satisfied by the IT Environment.
FPT_ITC.1	Nothing	None	N/A
FPT_ITT.1	Nothing	None	N/A
FPT_RVM_OS_EXP.1	Nothing	None	N/A
FPT_SEP_OS_EXP.1	Nothing	None	N/A
FPT_STM.1	Nothing	None	N/A

8.6 Rationale for Explicitly Stated SFRs

8.6.1 NIAP Interpretations

NIAP interpretations (FAU_GEN.1-NIAP-0347 and FDP_ACF.1-NIAP-0407 were used to provide the most recent interpretation of SFRs.

8.6.2 Explicitly Stated SFRs

8.6.2.1 FPT_RVM_SFT_EXP.1 and FPT_RVM_OS_EXP.1

Application TOEs are unable to fully satisfy FPT_SEP by themselves. These explicitly stated SFRs state the portion of FPT_SEP supplied by the TOE and the portion supplied by the OS and hardware in support of the overall FPT_SEP functionality.

8.6.2.2 FPT_SEP_SFT_EXP.1 and FPT_SEP_OS_EXP.1

Application TOEs are unable to fully satisfy FPT_SEP by themselves. These explicitly stated SFRs state the portion of FPT_SEP supplied by the TOE and the portion supplied by the OS and hardware in support of the overall FPT_SEP functionality.

8.7 Rationale for SFR Refinement

The SFRs levied on the TOE where not refined. The IT Environment SFRs (with the exception of the explicitly stated SFRs), where modified as follows: “TSF” was replaced with “IT Environment” to reflect that the SFR was levied on the IT Environment.