Nexor MMHS Security

Security Target

ST Version 1.0

February 23rd, 2005

Prepared for:
Nexor Ltd.
Nottingham Science and Technology Park
University Boulevard
Nottingham NG7 2RL
United Kingdom

Prepared By:
Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

Table of Content

1 Security Target Introduction

This Security Target (ST) describes the IT security requirements for Nexor MMHS Security that enhances the security aspects of the Microsoft products: Outlook, Explorer, and Exchange.

The Nexor Target of Evaluation (TOE) is a set of software products developed by Nexor LTD. Nottingham Science and Technology Park, University Boulevard, Nottingham NG7 2RL, United Kingdom, herein called simply Nexor.

The Nexor TOE, Nexor MMHS Security, is comprised of three components and each component has an associated security component. The Nexor components generally enhance the functionality of existing Microsoft components.
Nexor Defender for Outlook with Nexor S/MIME Security provide additional messaging capabilities, including secure messaging capabilities for Microsoft Outlook 2000 installed upon Windows 2000 Professional. Nexor Directory Administrator provides additional X.500 directory browsing and secure access to the directory utilizing the capabilities of Windows Explorer installed upon Windows 2000 Professional. Nexor Overseer provides mailbox monitoring and secure alert messaging for Microsoft Exchange Server 2000 installed upon Windows 2000 Advanced Server.

1.1 Security Target, TOE and CC Identification

ST Title - Nexor MMHS Security Security Target

ST Version – 1.0

ST Date – February 23, 2005

TOE Identification – The Nexor MMHS Security TOE consists of the following components:

Component	Version	Version Label	Patch	Patch Label
Nexor Defender for Outlook	4.1	DEFO-410-N500-RC4	4	DEFO-410-N500-Z004
Nexor S/MIME Security	2.0	SMIME-410-N500-RC3	3	SMIME-200-N500-Z003
Nexor Directory Administrator	2.0	ADUA-200-N500-RC4	2	ADUA-200-N500-Z002
Nexor Mailer/Directory Support Maintenance Release	3.40	Included in Nexor Administrator 2.0	3.41	MDSP-341-N500-RC1
Nexor Strong Authentication	2.0	SA-200-N500-RC7	-	N/A
Nexor Overseer	2.0	NOFE-200-N500-RC3	2	NOFE-200-N500-Z002
Nexor Security Server	1.0	NOSS-200-N500-RC3	3	NOSS-410-N500-Z003

Evaluation Assurance Level — EAL2

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

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.1, August 1999, ISO/IEC 15408-2.
    - Part 2 Extended with DEC_SEND.1

- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.1, August 1999, ISO/IEC 15408-3.
    - Part 3 Conformant

1.3 Strength of Environment

The Nexor TOE includes a set of services that provide secure enhancements to email services of Microsoft Outlook 2000 and Exchange, and to the browsing capabilities of Windows Explorer. These features require a level protection that is subject to an information flow control policy, so that the data flow can remain protected and access is controlled. The assurance requirements, EAL2, and the minimum strength of function, SOF-basic, were chosen to be consistent with those environments.

1.4 Conventions

The following conventions have been applied in this document:

- All requirements in this ST are reproduced relative to the requirements defined in CC v2.1.
- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: assignment, selection, refinement, and iteration. See section 5 for a description of how these operations are highlighted in this ST. Also see section 5 for a description of how Interpreted requirements are highlighted in this ST.

Other sections of the ST use bolding and italics to highlight text of special interest, such as captions.

1.5 Security Target Overview and Organization

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Environment (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8)

2 TOE Description

The set of software products that form the TOE include: Nexor Defender for Outlook, with the support of Nexor S/MIME Security; Nexor Directory Administrator, with the support of Nexor Strong Authentication; and Nexor Overseer, with the support of Nexor Security Server.

The Nexor Defender for Outlook component is a user agent designed to extend the functionality of Microsoft Outlook 2000. The component enables users to send and receive X.400 military messages. It includes an LDAP Address Book provider to provide integrated directory services into Microsoft Outlook 2000, such as support for multiple servers to allow for redundancy and consolidation of searches across multiple directories providing access to email addresses and security objects, and directory browsing to allow the user to navigate through the directory information to find the appropriate recipient. In addition, the Nexor Defender for Outlook supports an X.400 transport provider which allows connections to an X.400 message store. Since this component has been built on the Microsoft Outlook Object Model, it has the look and feel of the standard Microsoft form. It closely integrates with Microsoft Office, works with and takes advantage of features available in the Windows 2000 operating system. Additionally, Nexor Defender for Outlook includes the S/MIME Security Plug-in to provide the ability to attach a label to a message and verify recipient and originator clearance before sending a message.

The Nexor Directory Administrator component is an administrative directory user agent (ADUA) designed to enhance the functionality of Windows 2000 Explorer. The component facilitates browsing and modification of an X.500 directory using the Directory Access Protocol (DAP). It introduces an "X.500 Neighborhood" that allows access to multiple directory servers and allows administrators to manage sensitive directory objects, such as objects that contain security information and role information. The Nexor Directory Administrator component is closely integrated into Windows Explorer and offers email integration, which enhances the functionality offered by the Nexor LDAP Address book; for example, users can use Nexor Directory Administrator to search and browse the directory to locate appropriate information, including address information, which can then be passed to Microsoft Outlook. Additionally, the Nexor Strong Authentication module allows the DAP operations used by the Nexor Directory Administrator to be signed and verified. This ensures both integrity and authentication services are enforced on both the operations and the results.

The Nexor Overseer component is an email manager. It handles the notification of arrival and the re-routing of email messages without the need for user intervention. Nexor Overseer works alongside Microsoft's Exchange Server 2000, monitoring mail as it is placed in mailboxes stored on the Exchange Server. The two main capabilities provided by this component are that it can send an automatic message alert to a designated individual if messages are received when the intended recipient is not logged in. And it can automatically forward messages to an alternate address if they have not been read within a pre-determined period of time. Additionally, the Nexor Security Server allows the Nexor Overseer to sign and label the alert and redirect messages that it generates.

2.1 TOE Boundary

The scope of the TOE is provided below in Figure 1 TOE Boundary. The figure identifies the actual TOE components and the components in the environment of the TOE. The components that are considered within the TOE are within the shaded area (Nexor Defender for Outlook with Nexor S/MIME Security, Nexor Directory Administrator with Nexor Strong Authentication, Nexor Overseer with Nexor Security Server).

The TOE components are add-on packages to the following products: Microsoft Outlook 2000, Windows Explorer, and Microsoft Exchange 2000. These products are not within the scope of the TOE.

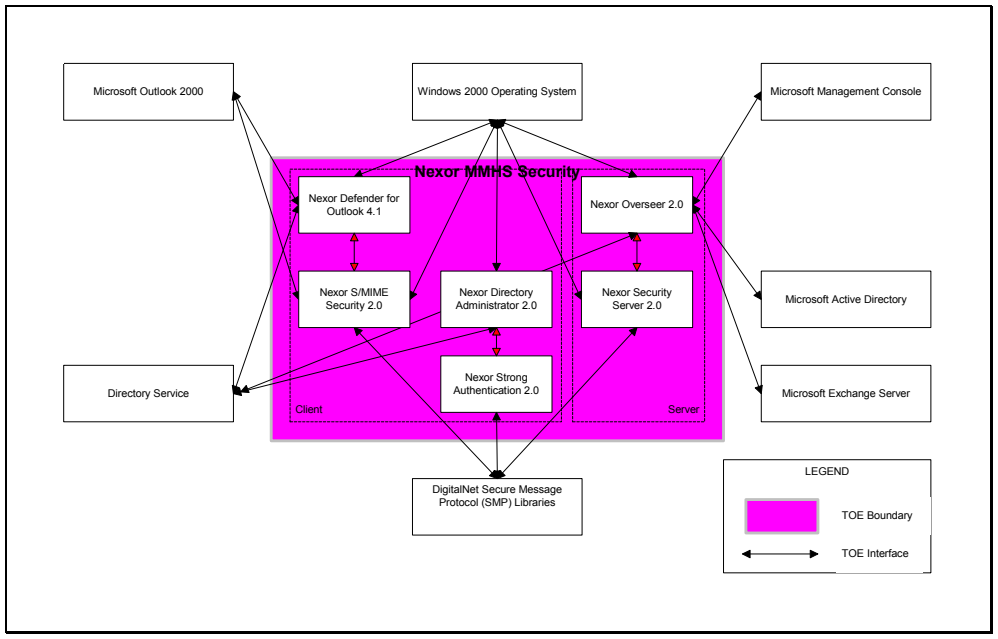
The TOE relies upon the following services in the IT environment to perform its security functions:

- Nexor Directory - used by all of the Nexor components primarily to obtain addressing and security information.

- Certificate Authority (CA) - is used to publish the security objects into the directory for use by the Nexor components to ensure the security of various pieces of data.

- DigitalNet Secure Message Protocol (SMP) Libraries – is used to provide the following services:
    - S/MIME Freeware Library – digital signatures, encryption, decryption, message labeling
    - Certificate Management Library – certificate validation, authentication of users
    - Access Control Library – provides an Access Control Decision Function (ACDF) that determines if a subject's clearance allows the subject to access data at a given label.

Figure 1 TOE Boundary



2.1.1 Physical Boundaries

The TOE is the set of Nexor Products that includes the Nexor Defender for Outlook component with the S/MIME Security component, the Nexor Directory Administrator with the Strong Authentication component and the Nexor Overseer with the Nexor Security Server component. The set of Nexor products that comprise the TOE are a set of software applications. The Nexor Overseer with the Nexor Security Server component is installed on a server node (the Microsoft Windows 2000 Advanced Server) where mailboxes will be monitored to ensure the timely processing of received messages. The Nexor Defender for Outlook with the S/MIME Security component and the Nexor Directory Administrator with the Strong Authentication components are installed on a workstation node (the Microsoft Windows 2000 Professional) where a user will send and receive messages, and browse and modify the directory. The requirements of the platform the TOE components are installed upon are summarized in the below table.

Component	Platform Requirements
Nexor Defender for Outlook with S/MIME Security	Windows 2000 Professional with Service Pack (SP) 2
Nexor Directory Administrator with Nexor Strong Authentication	Windows 2000 Professional with Service Pack (SP) 2
Nexor Overseer with Nexor Security Server	Windows 2000 Advanced Server with Service Pack (SP) 2 MMC (Microsoft Management Console) and the ADSI Edit snap-in must be installed

2.1.2 Logical Boundaries

The logical boundaries of the TOE can be described in terms of the security functions implemented in the TOE. The Nexor TOE is composed of a mix of client and server components that enhance the functionality of Microsoft Outlook 2000 and Microsoft Explorer. The TOE implements the following security functions:

Communication — The TOE ensures non-repudiation of messages with proof of origin and non-repudiation with proof of receipt.

User Data Protection — The TOE implements access control rules to ensure that only authorized users can access the addresses and security information stored in the available directories. Additionally, the TOE ensures that recipients are cleared to the appropriate security level to send and receive labeled messages.

Identification — All users must be identified by the TOE and authenticated by the IT environment before they are allowed to access the specific security services of the TOE.

Security Management — The TOE provides administrators with the capabilities to specify the labels that can be associated with messages.

3 Security Environment

The TOE security environment consists of the threats to the security of the TOE, organizational security policies, and usage assumptions as they relate to the set of Nexor Components. The Nexor Components provide for a level of protection that is appropriate for IT environments that require that messages sent and received through Microsoft Outlook are protected and secured, and secure access to multiple directory servers.

3.1 Threats to Security

T.NOAUTH An unauthorized person may gain access to modify security information stored in the protected directory managed by the Nexor Directory Administrator, therefore violating the access control policies of the TOE.

T.ACCESS An unauthorized person may gain access to resources for which that user is not authorized.

T.REPUDIATION A user may deny having sent a Message or having received a Message.

3.2 Organization Security Policies

The following policies apply to the TOE and the intended environment of the TOE.

P.INTEGRITY All critical data must be protected from unauthorized modification.

P.LABELING All messages must be labeled with an appropriate classification.

3.3 Secure Usage Assumptions

A.ADMIN Administrators will be appropriately qualified and will appropriately follow applicable guidance related to the TOE.

A.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

4 Security Objectives

This section defines the security objectives of Nexor products and its supporting environment. Security objectives, categorized as either IT security objectives or non-IT security objectives, reflect the stated intent to counter identified threats, and/or comply with any organizational security policies identified, and address assumptions. All of the identified threats, organizational policies, and assumptions are addressed under one of the categories below.

4.1 IT Security Objectives

O.IDENT	The TOE ensures that all subjects must be successfully uniquely identified to modify security information used by the TOE to make security relevant decisions.
O.ACCESS	The TOE ensures that messages can be sent from an originator to a recipient only if the clearance of the recipient is greater than or equal to the message security label and the originator is authorized to send messages to the recipient. Additionally, the TOE ensures that access to X.500 directories is restricted to authorized users.
O.SIG	The TOE must ensure that message has a signature that uniquely identifies the originator of the message.
O.REPUD	The TOE must prevent individuals from plausibly denying their involvement in either the origination or the receipt of a specific message.
O.LABEL	The TOE must ensure that each labeled message is labeled at a security level for which the originator is authorized to send messages at.

4.2 Security Objectives for the Environment

4.2.1 IT Security Objectives for the Environment

OE.AUTH	The IT environment provides an authentication mechanism to authenticate users.

4.2.2 Non-IT Security Objectives for the Environment

All of the assumptions, above, are considered to be security objectives for the environment. The following are the non-IT security objectives, which are to be satisfied without imposing technical requirements on the TOE. That is, they will be satisfied largely through application of procedural or administrative measures.

OE.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered to be low.
OE.ADMIN	Administrators will be appropriately qualified and will appropriately follow applicable guidance related to the TOE.

5 IT Security Requirements

5.1 TOE Security Functional Requirements

This section of the ST details the security functional requirements (SFR) for the TOE and the IT Environment that will support the TOE. The SFR were drawn from the CC Part 2.

CC defined operations for assignment; selection, refinement, and iteration were used to tailor the requirements to the level of detail necessary to meet the stated security objectives. The convention used in this section to highlight these operations is described below:

- Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that in cases where a selection operation is combined with an assignment operation and the assignment is null, the assignment operation is simply deleted leaving on the completed selection to identify the combination of operations.
- Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
- Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FDP_ACC.1(a) and FDP_ACC.1(b) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.

The appropriate International Interpretations have been applied to the requirements included in this ST. Note that no National Interpretations have been applied in this ST. The convention used in this section to identify those requirements to which International Interpretations have been applied is described below:

- Interpreted Requirements: Requirements that have been modified based upon an International Interpretation are identified by an italicized parenthetic comment following the requirement element that has been modified (e.g. *(per International Interpretation #51)*).

Security Functional Class	Security Functional Components
Communication (FCO)	Non-Repudiation of Origin (FCO_NRO.2)
	Non-Repudiation of Receipt (FCO_NRR.2)
User Data Protection (FDP)	Complete Information Flow Control (FDP_IFC.2)
	Simple Security Attributes (FDP_IFF.1)
Identification and Authentication (FIA)	User attribute definition (FIA_ATD.1)
	Timing of identification (FIA_UID.1)
Security management (FMT)	Management of object security attributes (FMT_MSA.1)
	Static attribute initialization (FMT_MSA.3)
	Specification of Management (FMT_SMF.1)
	Security roles (FMT_SMR.1)
Security Requirements for the IT Environment	

Identification and Authentication (FIA)	Timing of identification (FIA_UAU.1)
Information Flow	Decision to Send Information (DEC_SEND.1)

Table 1 Security Functional Components

5.1.1 Communication (FCO)

5.1.1.1 Non-repudiation of origin (FCO_NRO)

5.1.1.1.1 FCO_NRO.2.1

The TSF shall enforce the generation of evidence of origin for transmitted [**messages**] at all times.

5.1.1.1.2 FCO_NRO.2.2

The TSF shall be able to relate the [**sender's certificate**] of the originator of the information, and the [**entire message content**] of the information to which the evidence applies.

5.1.1.1.3 FCO_NRO.2.3

The TSF shall provide the capability to verify the evidence of origin of information to [***recipient***] given [**the public key of the originator.**]

5.1.1.2 Non-repudiation of Receipt (FCO_NRR)

5.1.1.2.1 FCO_NRR.2.1

The TSF shall enforce the generation of evidence of receipt for received [**messages**].

5.1.1.2.2 FCO_NRR.2.2

The TSF shall be able to relate the [**receipt**] of the recipient of the information, and the [**message identification**] of the information to which the evidence applies.

5.1.1.2.3 FCO_NRR.2.3

The TSF shall provide the capability to verify the evidence of receipt of information to [***originator***] given [**that a receipt was requested.**]

5.1.2 User Data Protection (FDP)

5.1.2.1 Complete Information Flow Control (FDP_IFC.)

5.1.2.1.1 FDP_IFC.2.1

The TSF shall enforce the [**Message Information Flow Control Policy SFP**] on [**subjects – senders, objects - messages**] and all operations that cause that information to flow to and from subjects covered by the SFP.

5.1.2.1.2 FDP_IFC.2.2

The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.

5.1.2.2 Simple Security Attributes (FDP_IFF.1)

5.1.2.2.1 FDP_IFF.1.1

The TSF shall enforce the [**Message Information Flow Control SFP**] based on the following types of subject and information security attributes:

[

subjects –

sender's clearance

recipient's clearance

objects –

message security label.] *(per International Interpretation #104)*

5.1.2.2.2 FDP_IFF.1.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if each of the following rules hold: [

- **The sender's clearance allows the user to send messages at the label of the message.**
- **The recipient's clearance allows the identified recipient to receive messages at the label of the message as determined by the IT environment SMP Libraries.**
- **And no other rules**.]

5.1.2.2.3 FDP_IFF.1.3

The TSF shall enforce the [**no additional information flow control SFP rules**.]

5.1.2.2.4 FDP_IFF.1.4

The TSF shall provide the following [**no list of additional information SFP capabilities.**]

5.1.2.2.5 FDP_IFF.1.5

The TSF shall explicitly authorize an information flow based on the following rules: [**no additional rules**.]

5.1.2.2.6 FDP_IFF.1.6

The TSF shall explicitly deny an information flow based on the following rules: [**no additional rules**.]

5.1.3 Identification and Authentication (FIA)

5.1.3.1 User Attribute Definition (FIA_ATD.1)

5.1.3.1.1 FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [

a) User Certificate (includes the user's Distinguished Name (DN) and clearance)]

5.1.3.2 Timing of Identification (FIA_UID.1)

5.1.3.2.1 FIA_UID.1.1

The TSF shall allow [**retrieval of X.500 address information**] on behalf of the user to be performed before the user is identified.

5.1.3.2.2 FIA_UID.1.2

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.4 Security Management (FMT)

5.1.4.1 Management of Object Security Attributes (FMT_MSA.1)

5.1.4.1.1 FMT_MSA.1.1

The TSF shall enforce the [**Message Information Flow Control Policy SFP**] to restrict the ability to [***modify***] the [**security label with an object**] to [**originator of the message**]. *(per International Interpretation #202)*

5.1.4.2 Static Attribute Initialization (FMT_MSA.3)

5.1.4.2.1 FMT_MSA.3.1

The TSF shall enforce the [**Message Information Flow Control Policy SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

5.1.4.2.2 FMT_MSA.3.2

The TSF shall allow the [**the authorized user that sent the message (originator of the message)**] to specify alternative initial values to override the default values when an object or information is created.

5.1.4.3 Specification of Management Functions FMT_SMF.1

5.1.4.3.1 FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: [**Message Information Flow Control SFP**]. *(per International Interpretation #65)*

5.1.4.4 Security Roles (FMT_SMR.1)

5.1.4.4.1 FMT_SMR.1.1

The TSF shall maintain the roles:
[
- **Authorized Administrator;**
- **Authorized user;**

]

5.1.4.4.2 FMT_SMR.1.2

The TSF shall be able to associate users with roles.

5.2 IT Environment Security Functional Requirements

5.2.1 Timing of Authentication (FIA_UAU.1)

5.2.1.1 FIA_UAU.1.1

The TSF shall allow [**retrieval of X.500 address information**] on behalf of the user to be performed before the user is authenticated.

5.2.1.2 FIA_UAU.1.2

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.2 Decision to Send Information (DEC_SEND.1)

The following requirement has been explicitly defined to fulfill a TOE dependency on the IT environment originating from FDP_IFF.1.2.

This requirement has been explicitly defined to support a requirement, not available in the CC, designed to require that checks be performed with the expectation that some other IT entity will enforce its decision.

5.2.2.1 DEC_SEND.1

Upon receipt of a request to check access, given the identification of a message originator , security label of the message, and identification of the intended message recipient, the IT Environment will respond with an indication of whether the message security label of the message is less than or equal to the security label of the intended message recipient. An affirmative indication indicates that the send operation should be allowed relative to this check.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level (EAL) 2 components as specified in Part 3 of the Common Criteria. The SARs have been changed, when necessary, to conform to National and International Interpretations.

Assurance Class	Assurance Components

Assurance Class	Assurance Components
Configuration Management (ACM)	Configuration items (ACM_CAP.2)
Delivery and Operation (ADO)	Delivery procedures (ADO_DEL.1)
	Installation, generation, and start-up procedures (ADO_IGS.1)
Development (ADV)	Informal functional specification (ADV_FSP.1)
	Descriptive high-level design (ADV_HLD.1)
	Informal correspondence demonstration (ADV_RCR.1)
Guidance Documents (AGD)	Administrator guidance (AGD_ADM.1)
	User Guidance (AGD_USR.1)
Tests (ATE)	Evidence of coverage (ATE_COV.1)
	Functional testing (ATE_FUN.1)
	Independent testing – sample (ATE_IND.2)
Vulnerability assessment (AVA)	Strength of TOE security function evaluation (AVA_SOF.1)
	Developer vulnerability analysis (AVA_VLA.1)

Table 2 EAL2 Assurance Components

5.3.1 Configuration Management (ACM)

5.3.1.1 Configuration Items (ACM_CAP.2)

5.3.1.1.1 ACM_CAP.2.1D

The developer shall provide a reference for the TOE.

5.3.1.1.2 ACM_CAP.2.2D

The developer shall use a CM system.

5.3.1.1.3 ACM_CAP.2.3D

The developer shall provide CM documentation.

5.3.1.1.4 ACM_CAP.2.1C

The reference for the TOE shall be unique to each version of the TOE.

5.3.1.1.5 ACM_CAP.2.2C

The TOE shall be labeled with its reference.

5.3.1.1.6 ACM_CAP.2.3C

The CM documentation shall include a configuration list.

5.3.1.1.7 International Interpretation RI #3

The configuration list shall uniquely identify all configuration items that comprise the TOE. *(per International interpretation #3)*

5.3.1.1.8 ACM_CAP.2.4C

The configuration list shall describe the configuration items that comprise the TOE.

5.3.1.1.9 ACM_CAP.2.5C

The CM documentation shall describe the method used to uniquely identify the configuration items.

5.3.1.1.10 ACM_CAP.2.6C

The CM system list shall uniquely identify all configuration items.

5.3.1.1.11 ACM_CAP.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and Operation (ADO)

5.3.2.1 Delivery Procedures (ADO_DEL.1)

5.3.2.1.1 ADO_DEL.1.1D

The developer shall document procedures for delivery of the TOE or parts of it to the user.

5.3.2.1.2 ADO_DEL.1.2D

The developer shall use the delivery procedures.

5.3.2.1.3 ADO_DEL.1.1C

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

5.3.2.1.4 ADO_DEL.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

5.3.2.2.1 ADO_IGS.1.1D

The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

5.3.2.2.2 ADO_IGS.1.1C

The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE. *(per International Interpretation #51)*

5.3.2.2.3 ADO_IGS.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2.4 ADO_IGS.1.2E

The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

5.3.3.1.1 ADV_FSP.1.1D

The developer shall provide a functional specification.

5.3.3.1.2 ADV_FSP.1.1C

The functional specification shall describe the TSF and its external interfaces using an informal style.

5.3.3.1.3 ADV_FSP.1.2C

The functional specification shall be internally consistent.

5.3.3.1.4 ADV_FSP.1.3C

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

5.3.3.1.5 ADV_FSP.1.4C

The functional specification shall completely represent the TSF.

5.3.3.1.6 ADV_FSP.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.1.7 ADV_FSP.1.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security requirements.

5.3.3.2 Descriptive high-level design (ADV_HLD.1)

5.3.3.2.1 ADV_HLD.1.1D

The developer shall provide the high level design of the TSF.

5.3.3.2.2 ADV_HLD.1.1C

The presentation of the high level design shall be informal.

5.3.3.2.3 ADV_HLD.1.2C

The high level design shall be internally consistent.

5.3.3.2.4 ADV_HLD.1.3C

The high level design shall describe the structure of the TSF in terms of subsystems.

5.3.3.2.5 ADV_HLD.1.4C

The high level design shall describe the security functionality provided by each subsystem of the TSF.

5.3.3.2.6 ADV_HLD.1.5C

The high level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

5.3.3.2.7 ADV_HLD.1.6C

The high level design shall identify all interfaces to the subsystems of the TSF.

5.3.3.2.8 ADV_HLD.1.7C

The high level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

5.3.3.2.9 ADV_HLD.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.2.10 ADV_HLD.1.2E

The evaluator shall determine that the high level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

5.3.3.3.1 ADV_RCR.1.1D

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

5.3.3.3.2 ADV_RCR.1.1C

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

5.3.3.3.3 ADV_RCR.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance Documents (AGD)

5.3.4.1 Administrator Guidance (AGD_ADM.1)

5.3.4.1.1 AGD_ADM.1.1D

The developer shall provide administrator guidance addressed to system administrative personnel.

5.3.4.1.2 AGD_ADM.1.1C

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

5.3.4.1.3 AGD_ADM.1.2C

The administrator guidance shall describe how to administer the TOE in a secure manner.

5.3.4.1.4 AGD_ADM.1.3C

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

5.3.4.1.5 AGD_ADM.1.4C

The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

5.3.4.1.6 AGD_ADM.1.5C

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

5.3.4.1.7 AGD_ADM.1.6C

The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

5.3.4.1.8 AGD_ADM.1.7C

The administrator guidance shall be consistent with all other documentation supplied for evaluation.

5.3.4.1.9 AGD_ADM.1.8C

The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

5.3.4.1.10 AGD_ADM.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence

5.3.4.2 User Guidance (AGD_USR.1)

5.3.4.2.1 AGD_USR.1.1D

The developer shall provide user guidance.

5.3.4.2.2 AGD_USR.1.1C

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

5.3.4.2.3 AGD_USR.1.2C

The user guidance shall describe the use of user-accessible security functions provided by the TOE.

5.3.4.2.4 AGD_USR.1.3C

The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

5.3.4.2.5 AGD_USR.1.4C

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

5.3.4.2.6 AGD_USR.1.5C

The user guidance shall be consistent with all other documentation supplied for evaluation.

5.3.4.2.7 AGD_USR.1.6C

The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

5.3.4.2.8 AGD_USR.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Security Testing (ATE)

5.3.5.1 Analysis of coverage (ATE_COV.1)

5.3.5.1.1 ATE_COV.1.1D

The developer shall provide evidence of the test coverage.

5.3.5.1.2 ATE_COV.1.1C

The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

5.3.5.1.3 ATE_COV.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.2 Functional testing (ATE_FUN.1)

5.3.5.2.1 ATE_FUN.1.1D

The developer shall test the TSF and document the results.

5.3.5.2.2 ATE_FUN.1.2D

The developer shall provide test documentation.

5.3.5.2.3 ATE_FUN.1.1C

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

5.3.5.2.4 ATE_FUN.1.2C

The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

5.3.5.2.5 ATE_FUN.1.3C

The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

5.3.5.2.6 ATE_FUN.1.4C

The expected test results shall show the anticipated outputs from a successful execution of the tests.

5.3.5.2.7 ATE_FUN.1.5C

The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

5.3.5.2.8 ATE_FUN.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.3 Independent testing – sample (ATE_IND.2)

5.3.5.3.1 ATE_IND.2.1D

The developer shall provide the TOE for testing.

5.3.5.3.2 ATE_IND.2.1C

The TOE shall be suitable for testing.

5.3.5.3.3 ATE_IND.2.2C

The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

5.3.5.3.4 ATE_IND.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.3.5 ATE_IND.2.2E

The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

5.3.5.3.6 ATE_IND.2.3E

The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.5.4 Strength of TOE security function evaluation (AVA_SOF.1)

5.3.5.4.1 AVA_SOF.1.1D

The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

5.3.5.4.2 AVA_SOF.1.1C

For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

5.3.5.4.3 AVA_SOF.1.2C

For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

5.3.5.4.4 AVA_SOF.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.4.5 AVA_SOF.1.2E

The evaluator shall confirm that the strength claims are correct.

5.3.5.5 Developer analysis (AVA_VLA.1)

5.3.5.5.1 AVA_VLA.1.1D

The developer shall perform a vulnerability analysis. *(per International Interpretation #51)*

5.3.5.5.2 AVA_VLA.1.2D

The developer shall provide vulnerability analysis documentation *(per International Interpretation #51)*

5.3.5.5.3 AVA_VLA.1.1C

The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP. *(per International Interpretation #51)*

5.3.5.5.4 AVA_VLA.1.2C

The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.[1]

5.3.5.5.5 AVA_VLA.1.3C

The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE. *(per International Interpretation #51)*

5.3.5.5.6 AVA_VLA.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.5.7 AVA_VLA.1.2E

The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6 TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

Each of the security function descriptions is organized by the security requirements corresponding to the security function. Hence, each function is described by describing how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions are suitable to satisfy the necessary requirements.

6.1.1 Communication

The TSF provides the capability to protect e-mail messages by ensuring messages are encrypted and digitally signed before they are sent. Digital signatures provide evidence that identifies the sender and ensures the message has not been modified during transmission. The TSF can identify the sender's certificate and uses the sender's public key to identify the sender of the message.

The TSF allows for the sender to request a signed receipt upon when the message has been opened. The TSF then ensures a receipt is signed using the private key of the message recipient and sent to the sender of the message.

The TSF uses external libraries to perform the cryptographic services such as message signing, message encryption, and receipt signing.

The TSF provides the TOE administrator the capability to define alert messages. An alert message is an automatic message that can be sent to a designated individual (which *may* be the same user as the recipient, using another email account) if messages are received when the intended recipient is not logged in to their mailbox.

Information from the original message will be included in the notification such as the sender or the recipient. The information to be included is defined during configuration and can be changed by the TOE Administrator.

Alerts can also be digitally signed, using the external libraries, to provide integrity of the alert message.

The communication function satisfies the following requirements:

> FCO_NRO.2 *Non-Repudiation of Origin* – The TOE fulfils this requirement by ensuring that the TSF digitally signs all messages before they are sent.
>
> FCO_NRR.2 *Non-Repudiation of Receipt* **-** The TOE fulfils this requirement by ensuring that the TSF provides digitally signed message receipts.

6.1.3 User Data Protection

Users must be authenticated by the IT environment using credentials that allow for the access requested to the X.500 directories, with the exception of retrieving address information upon which anonymous access is allowed.

The TSF ensures that messages can only be sent at a classification level the user is authorized to send messages at. The TSF ensures that messages can only be sent to users authorized to read messages of the classification being sent to them. The TSF ensures that messages can be sent from an originator to a recipient only if the clearance of the recipient is greater than or equal to the message security label and the originator is authorized to send messages to the recipient. The TSF uses external libraries (SMP Libraries) to perform label comparisons.

The available classification labels that can be used by the TSF are derived from the Security Policy Information Files (SPIFs) which can be defined and modified by TOE administrators.

SPIFs are ASN.1 encoded objects that are signed for integrity. The SPIF provides details about the security classifications and categories that are appropriate for the security policy. It also defines the relationship between classification and categories and between categories themselves e.g if EYES ONLY category is chosen, the classification must be RESTRICTED. The SPIF also holds information about how a security label should be displayed.

The user data function satisfies the following requirements:

> FDP_IFC.2 *Complete Information Flow Control* – The TOE fulfils this requirement by restricting the flow of messages based upon a check performed by the TSF.
>
> FDP_IFF.1 *Simple Security Attributes* – The TOE fulfils this requirement by only allowing messages to be sent when the sending and recipient users are appropriately cleared based upon the message label.

6.1.4 Identification

Users must be authenticated and identified before they are allowed to perform any of the following actions:

- Sending a message (which may initiate the signing a message and/or the encryption of the message)
- Defining alerts and forward messages
- Accessing X.500 directories (to perform task other than retrieving address information)

To exercise any of the TOE security functions, other than to retrieve address information, the TOE ensures the user must be logged on (i.e. authenticated). The TOE uses an external interface (Secure Message Protocol (SMP)) to authenticate the user through the use of a token and a password. If the user is successfully authenticated the user is identified by a distinguished name (DN) which is the subject DN from the user's certificate.

> FIA_ATD.1 *User Attribute Definition* – The TOE fulfils this requirement by maintaining the following security attributes for each user: user name (Distinguished Name (DN)) and user's clearance which are included in the user's certificate which is retrieved by the TOE from the Directory Service.
>
> FIA_UID.1 *Timing of Identification* – The TOE fulfils this requirement by requiring the user to be identified before performing all TSF-mediated actions, with the exception of retrieving X.500 address information.

6.1.5 Security Management

The TSF implements several roles and ensures that the below functionality is restricted to the following roles:

1) The authorized administrator is a user who can perform the administrative task of modifying security attributes upon which the following decision is made: sending of messages. An individual is identified as an authorized administrator by being configured as an Authorized Signer. An Authorized Signer is an individual having the authority to specify a security label for a message and sign messages upon submission.
2) The authorized user is an identified and authenticated user who has been granted authorization to read messages. An individual is identified as an authorized user by being configured as an Authorized Reader. An Authorized Reader is an individual having the authority to read signed and encrypted email messages sent to the role of which they are

an authorized reader. An individual can also be identified as an authorized user by being configured as an Alternate or a Role Occupant. An Alternate can be forwarded secure messages when the message is not read within a given time period. A Role Occupant can be sent an alert if a message is delivered into a mailbox that no-one is currently logged into.

The assignment of authorized administrator and authorized user roles are performed within the TOE environment (within the environment directory service) and not within the scope of the TOE. The TOE enforces the restrictions placed upon each role (within SPIFs and clearances held within the environment directory service) with regard to message composition, signing and reading. The restrictions include ensuring the list of possible security label values to the user are those allowed by the SPIF and clearance (held within the environment directory service). The default security label value is set to the lowest security classification available.

The Security Management function satisfies the following requirements:

FMT_SMF.1 *Specification of Management Functions* – The TOE fulfils this requirement by providing the administrator with a list of allowable label values that can be associated with messages.

FMT_MSA.1 - *Management of Object Security Attributes* – The TSF fulfils this requirement by restricting the ability to modify the label of a message to authorized administrators.

FMT_MSA.3 *Static Attribute Initialization* – The TOE fulfils this requirement by setting a default label value and allowing only the message sender the ability to change the label of a message to an alternative value.

FMT_SMR.1 *Security Roles* – The TOE fulfils this requirement by maintaining the ability to associate users with two roles: authorized administrator and the authorized user.

6.2 TOE Security Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL2 assurance requirements:

- Configuration Management Assurance;
- Delivery and Guidance;
- Design Documentation;
- Tests; and
- Vulnerability Assessment.

6.2.1 Configuration Management

The configuration management measures applied by Nexor to ensure that configuration items are uniquely identified and the TOE is uniquely labeled are documented in the following documents:

- Engineering Development and Maintenance Guide (NEX1214ENG02)
- Product and Maintenance Release Policy (NEX01369PDC01)
- Documentation Procedure (NEX0588COR08)
- Installation Design Document for Nexor Directory Administrator 2.0 (ADUA-Design Document-02)
- Installation Design Document for Defender For Outlook 4.1 (DEFO4.1-Design Document-03)

- Installation Design Document for NEXOR Overseer 2.0 (NOFE2.0-Design Document-01)
- Nexor Overseer Security Server 1.0 Installation Design Document (NOSS1.0 Design Document-1.0)
- Installation Design Document for S/MIME Security 2.0 (PCT2.0-Design Document-01)
- Strong Authentication 2.20 Installation Design Document (SA220 Design Document-01)

The Configuration Management assurance measure satisfies the ACM_CAP.2 assurance requirements

6.2.2 Delivery and Guidance

The Delivery procedures describe the procedures to identify the TOE and the appropriate instructions for installation, generation and start-up of the TOE. Additionally, delivery procedures are described that maintain security when distributed to the user's site. These procedures are documented in the following document:

- Product Despatch (NEX1423COR02)
- Nexor Release Engineering Procedure (NEX0618ENG07)

Nexor provides administrator and user guidance on how to utilize the TOE security functions and warnings to authorized administrators and users about actions that can compromise the security of the TOE. Administrator guidance is documented in:

- Release Notes (NEX1267MAN10-3)
- Installing and Configuring Nexor MMHS Security (NEX1653ENG03)
- Nexor Defender for Outlook 4.1 Administrator Guide (NEX0757MAN05)
- Nexor Defender for Outlook 4.1 Patches (NEX1248MAN05)
- Nexor S/MIME Security Administrator's Guide (NEX0647MAN04)
- Nexor S/MIME Security 2.00 Patches (NEX1304MAN04)
- Nexor Directory Administrator 2.0 (NEX0689MAN07)
- Nexor Directory Administrator 2.0 Patches (NEX1273MAN03)
- Maintenance Releases for Nexor Directory 5.00 (NEX1425MAN05)
- Nexor Overseer 2.0 Administrator Guide (NEX0840MAN08)
- Nexor Overseer 2.0 Patches (NEX1388MAN02)
- Nexor Security Server 1.0 Patches (NEX1372MAN02)

User guidance is documented in:

- Nexor Defender for Outlook 4.1 User Guide (NEX0758MAN04)
- Nexor Defender for Outlook 4.1 Patches (NEX1248MAN05)
- Nexor S/MIME Security User's Guide (NEX0648MAN05)
- Nexor S/MIME Security 2.00 Patches (NEX1304MAN04)
- Nexor Directory Administrator 2.0 (NEX0689MAN07)

- Nexor Directory Administrator 2.0 Patches (NEX1273MAN03)

The Delivery and Guidance assurance measure satisfies the following Assurance requirements:

- ADO_DEL.1;
- ADO_IGS.1;
- AGD_ADM.1; and,
- AGD_USR.1.

6.2.3 Development

Nexor provides design documentation that identifies and describes the external interfaces and the decomposition of the TOE into subsystems. The design documentation also includes a correspondence analysis between the various abstractions of the Nexor design. The design documentation consists of the following documents and various references from these documents:

- Nexor MMHS Security (NEX1506ENG10)

The Design Documentation security assurance measure satisfies the following security assurance requirements:

- ADV_FSP.1;
- ADV_HLD.1;
- ADV_RCR.1.

6.2.4 Tests

Nexor provides test documentation that describes how each of the TOE security functions is tested including a test plan, test procedures, expected results and the actual results of applying the tests. The test documentation consists of the following documents:

- Nexor MMHS Security Test Suites (Nexor MMHS Security Test Suites-v7)

The Tests assurance measure satisfies the following assurance requirements:

- ATE_COV.1
- ATE_FUN.1
- ATE_IND.2

6.2.5 Vulnerability Assessment

Nexor performs a systematic vulnerability analysis of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE. There are no probabilistic or permutational mechanisms included in the TOE. Therefore, a SOF analysis is not applicable to the TOE. The vulnerability analysis is documented in:

- Vulnerability Analysis of Nexor MMHS Security (NEX1424ENG07)

The Vulnerability Assessment assurance measure satisfies the following assurance requirements:

- AVA_SOF.1 (not applicable); and,
- AVA_VLA.1.

7 Protection Profile Claims

There are no Protection Profile conformance claims for the TOE.

8 Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements
- Requirements Dependency
- Explicitly Stated Requirements
- TOE Summary Specification;
- Strength of Function (SOF)

8.1 Security Objectives Rationale

This section shows that all threats, secure usage assumptions, and organizational security policies are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, threat, or organizational security policy.

This section provides evidence demonstrating the coverage of threats, organizational policies, and usage assumptions by the security objectives.

Objectives / Environment	O.IDENT	O.ACCESS	O.SIG	O.REPUD	O.LABEL	OE.AUTH	OE.LOWEXP	OE.ADMIN
T.NOAUTH	X					X		
T.ACCESS		X						
T.REPUDIATION			X	X				
P.INTEGRITY	X					X		
P.LABELING					X			
A.ADMIN								X
A.LOWEXP							X	

Table 3 Environment to Objective Correspondence

T.NOAUTH

An unauthorized person may gain access to modify security information stored in the protected directory managed by the Nexor Directory Administrator, therefore violating the access control policies of the TOE.

This threat is countered by O.IDENT and OE.AUTH that require identification and authentication of user before a user is allowed to modify any information used by the TOE to make security relevant decisions.

T.ACCESS

An unauthorized person may gain access to resources for which that user is not authorized.

This threat is countered by O.ACCESS that ensures that a recipient must have the appropriate clearance level to receive a labeled message and have the appropriate authority to have access to X.500 directories.

T.REPUDIATION

Message origination and reception may be denied.

This threat is countered by O.SIG and O.REPUD by ensuring that messages have a signature binding the identification of the originator to the message and that users are prevented from denying they sent messages and from denying they received messages.

P.INTEGRITY

All critical data must be protected from unauthorized modification.

This policy is realized by O.IDENT and OE.AUTH that requires identification and authentication of user before a user is allowed to modify any information used by the TOE to make security relevant decisions.

P.LABELING

All labeled messages must be labeled with an appropriate classification.

This policy is realized by O.LABEL that requires that a user cannot label and send a message at a level for which the user is not authorized to send messages at.

A.ADMIN

Administrators will be appropriately qualified and will appropriately follow applicable guidance related to the TOE.

This assumption is addressed by OE.ADMIN, which ensures that administrators will be appropriately qualified and follow the related TOE guidance.

A.LOWEXP

The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

This assumption is addressed by OE.LOWEXP, which ensures that the threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

8.2 Security Functional Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that **Table 4** indicates the requirements that effectively satisfy the individual objectives. Objectives for the IT environment are satisfied only by requirements for the IT environment; however some of those requirements also support, in some relatively small way, the TOE security objectives.

Additionally, this section demonstrates that the functional components selected for this Security Target provide complete coverage of the defined security objectives. The mapping of security functional components (SFRs) to security objectives is depicted in the table below followed by rationale that additionally demonstrates the coverage for each security objective.

Requirements / Objectives	FCO_NRO.2	FCO_NRR.2	FDP_IFC.2	FDP_IFF.1	FIA_ATD.1	FIA_UID.1	FIA_UAU.1	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1	DEC_SEND.1
O.IDENT					x	x					x	
O.ACCESS			x	x				x	x	x	x	x
O.SIG	x											
O.REPUD	x	x										
O.LABEL			x	x								
OE.AUTH							x					

Table 4 IT Objectives to Requirement Correspondence

O.IDENT

The TOE ensures that all subjects must be successfully uniquely identified to modify security information used by the TOE to make security relevant decisions.

Users must be identified (FIA_UID.1) to access TOE data and functions, with the exception of retrieval of address information. Access to TOE data and functions is based upon the attributes the TOE associates with users (FIA_ATD.1) and their role (FMT_SMR.1).

O.ACCESS

The TOE ensures that messages can be sent from an originator to a recipient only if the clearance of the recipient is greater than or equal to the message security label and the originator is authorized to send messages to the recipient.

The Message Information Flow Control SFP restricts access to messages (FDP_IFC.2). The rules of this SFP is defined (FDP_IFF.1) which enforce the decision received from the environment (DEC_SEND.1). The initialization and modification of the security attributes the SFPs are based upon are defined (FMT_MSA.1, FMT_MSA.3, FMT_SMF.1).

O.SIG

The TOE must ensure that message has a signature that uniquely identifies the originator of the message.

Messages can be signed which credibly identify the originator (FCO_NRO.2).

O.REPUD

The TOE must prevent individuals from plausibly denying their involvement in either the origination or the receipt of a specific message.

Evidence will be generated that identifies the sender of a message (FCO_NRO.2) and evidence of message receipt can be generated (FCO_NRR.2)

O.LABEL

The TOE must ensure that each labeled message is labeled at a label for which the originator is authorized to send messages at.

A user's clearance must be at an appropriate level with respect to the label assigned to a message by that user (FDP_IFF.1, FDP_IFC.2).

OE.AUTH

The IT environment provides an authentication mechanism to authenticate users

.

An authentication mechanism is provided for use by the TOE to ensure users are authenticated.

8.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL2 assurance package and is based on good commercial development practices. This ST has been developed for a generalized environment with a low level of risk to the assets. As such, it is believed that EAL 2 provides an appropriate level of assurance in the security functions offered by the TOE.

8.4 Requirement Dependency Rationale

The ST satisfies all the requirement dependencies of the Common Criteria. Table 5 Requirement Dependency Rationale lists each requirement from Section 5 with a dependency and indicates which requirement was included to satisfy the dependency, if any. As demonstrated in Table 5, all requirement dependencies are satisfied.

Functional Component	Dependency	Included
Enforced proof of origin (FCO_NRO.2)	FIA_UID.1	FIA_UID.1
Enforced receipt (FCO_NRR.2)	FIA_UID.1	FIA_UID.1
Complete Information Flow (FDP_IFC.2)	FDP_IFF.1	FDP_IFF.1
Simple Security Attributes (FDP_IFF.1)	FDP_IFC.1	FDP_IFC.2
	FMT_MSA.3	FMT_MSA.3
	DEC_SEND.1	DEC_SEND.1
User attribute definition(FIA_ATD.1)	None	
Timing of identification (FIA_UID.1)	None	
Timing of authentication (FIA_UAU.1)	FIA_UID.1	FIA_UID.1
Management of object security attributes (FMT_MSA.1)	FMT_SMR.1	FMT_SMR.1
	FDP_IFC.1	FDP_IFC.1
	FMT_SMF.1	FMT_SMF.1
Security Attribute Initialization (FMT_MSA.3)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
Specification of Management (FMT_SMF.1)	None	
Security Roles (FMT_SMR.1)	FIA_UID.1	FIA_UID.1
Decision to Send Information (DEC_SEND.1)	None	

Table 5 Requirement Dependency Rationales

8.5 Explicitly Stated Requirements Rationale

All Security Functional Requirements for the TOE in this ST are reproduced relative to the requirements defined in CC v2.1, using the conventions described in Section 1.3.1. There is one explicitly stated requirement for the IT environment in this ST (DEC_SEND.1). This requirement is designed to work in conjunction with FDP_IFF.1, where FDP_IFF.1.2 enforces decisions made by the security function corresponding to DEC_SEND.1. There is no comparable requirement in the CC that supports the notion of

simply making, but not enforcing, an information flow decision and therefore the explicit requirement has been constructed.

8.6 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 6 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	COMMUNICATION (FCO)	USER DATA PROTECTION (FDP)	IDENTIFICATION (FIA)	SECURITY MANAGEMENT (FMT)
FCO_NRO.2	X			
FCO_NRR.2	X			
FDP_IFC.2		X		
FDP_IFF.1		X		
FIA_ATD.1			X	
FIA_UID.1			X	
FMT_MSA.1				X
FMT_MSA.3				X
FMT_SMF.1				X
FMT_SMR.1				X

Table 6 Security Functions vs. Requirements Mapping

8.7 Strength of Function (SOF) Rationale

Section 1.3 identifies the minimum strength of function as SOF-basic. This level is sufficient, given the assumption (A.LOWEXP) that the threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

There are no mechanisms of a probabilistic or permutational nature included in the TOE. Therefore, a SOF analysis is not applicable to the TOE.