California Microwave Mail List Agent (MLA) and the Profiling User Agent (PUA) Security Target

Version 1.0
Aug 12, 2003

Prepared for:
Northrop Grumman, California Microwave Systems

21200 Burbank Ave.
Bldg. 30
Woodland Hills, CA 91367

Prepared By:
Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is provided by California Microwave Systems, an organization within the Northrop Grumman Corporation. The TOE is the CMS Mail List Agent and Profiling User Agent (MLA/PUA). The MLA/PUA enforces a security policy on e-mail exchanges.

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).

1.1 Security Target, TOE and CC Identification

ST Title – California Microwave Mail List Agent (MLA) and the Profiling User Agent (PUA) Security Target

ST Version – Version 1.0

ST Date – Aug 12, 2003

TOE Identification – CMS MLA/PUA Version 3.1.0 with Patch A.

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 MLA_DAC.1 and MLA_MAC.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
    - Evaluation Assurance Level 2 (EAL2)

1.3 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the Security Target.

1.3.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - 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.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - 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 …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

2. TOE Description

The TOE is the California Microwave CMS Mail List Agent and Profiling User Agent (MLA/PUA) mail distribution product, Version 3.1.0 with Patch A installed. The MLA/PUA is designed and manufactured by Northrop Grumman, California Microwave Systems Incorporated, located at 21200 Burbank Blvd., Building 30, Woodland Hills, CA 91367.

2.1 Product Type

The MLA/PUA is an application operating within Windows 2000 Server processes and utilizing the services of other services in the IT environment to perform its functions. The primary purpose of MLA/PAU is to profile and control the flow of electronic mail (e-mail) within an enterprise. The MLA/PUA is necessarily designed for large volume and flexibility. However, the MLA/PAU must be installed properly to ensure that all e-mail (intended to be profiled or controlled) must flow through it to ensure that its policies can always be enforced.

The MLA/PUA ***enforces*** a mandatory, label-based security policy as well as an administrator discretionary access control policy on messages created by a sender (also known as the originator) when the sender attempts to send the message to a recipient (i.e., user, mail-list, or port). While the MLA/PAU enforces the e-mail flow policies, it requires its IT environment to manage the acceptable access control specification as well as the to implement the policy decision functions.

2.2 Product Description

The MLA/PUA is composed of two subsystems, the MLA and the PUA. MLA and PUA are two logical grouping of functions that enforce security policies that are applied on messages created by a sender when the sender attempts to send the message to a recipient (user, mail-list, port). The TSF enforces a mandatory security policy decisions as well as ACL administrator discretionary access control access policy decisions after requesting such decisions and providing necessary identity and security label information to the policy decision maker.

The MLA/PUA interfaces with an Access Control Library (ACL) server – the *policy decision maker* – that stores access control information about the potential message senders and receivers, including their security labels, as well as access lists that identify allowed sender/receiver pairs. With the sender's identity, the security level of the sender, and the intended receiver's identity, the MLA/PUA calls the ACL server whenever an access decision is required.

When called by the MLA/PUA, the ACL server returns a binary decision to grant or refuse access and then the MLA/PUA enforces the access decision.

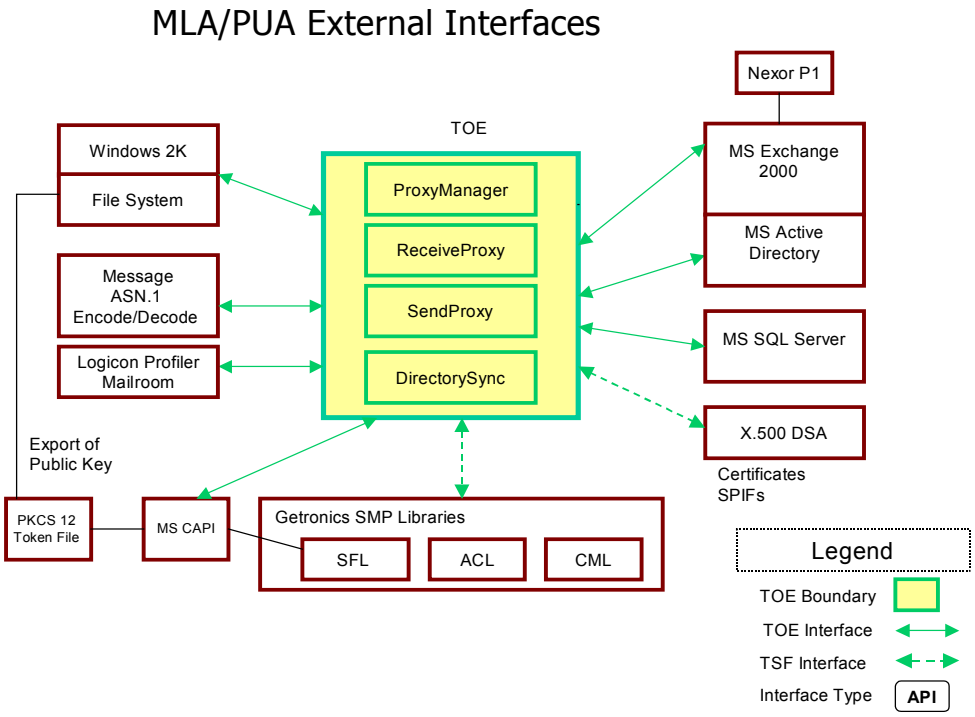
2.3 Product Features

The MLA/PUA plays an integrated role in enforcing security policies for sending mail messages among senders and receivers. To accomplish this, the MLA/PUA interacts with a number of environmental entities

2.4 Security Environment TOE Boundary

The MLA/PUA includes both physical and logical boundaries.

The physical boundary of the TOE are the external interfaces to environmental software that is not part of the



MLA/PUA but necessary to the overall function to provide secure e-mail services. The logical boundary of the MLA/PUA is the security functions that the MLA/PUA exports.

2.4.1 Physical Boundaries

The MLA and PUA are collocated (collectively referred to as MLA/PUA) and will function on a single Windows 2000 Server.
The MLA/PUA is but one of several products that are integrated to provide mandatory and administrative control for processing e-mail messages. Since many products are involved and interface to protect e-mail, MLA/PUA has many external interfaces. The interfaces between the MLA/PUA and the supporting IT environment components create the physical boundary of the TOE.

The following interfaces define the physical boundary of the TOE:

- Windows 2000 Server Operating System
- Windows 2000 File System
- MS Exchange 2000
- MS Active Directory (DIB/GAL)
- Microsft SQL Server 2000
- MMHS X.500 DSA (LDAP/ADSI)
- Message ASN.1 Encoder/Decoder (Bolden James)
- Microsoft CAPI
- Getronics SMP Libraries (ACL, CML, SFL)
- Profiler (Logicon Mailroom)
- NEXOR P1 Connector (indirectly through MS Exchange)

Of these interfaces, only the Microsoft Exchange 2000 Server interface represents an interface to external users since all mail exchanges will be processed using the exchange Server.

2.4.2 Logical Boundaries

The logical boundaries of the CMS MLA/PUA includes the following interfaces:

1. Access Control using the Getronics Access Control Library (ACL)
2. Identification using the Getronics S/MIME Freeware Library (SFL), Certificate Management Library (CML), and X.500 DSA.

2.4.2.1 Access Control

The MLA/PUA product interfaces with the ACL that provides access control information about the message recipient including the security label associated with the recipient, which is not necessarily a person, as well as access lists that identify appropriate sender/receiver pairs. With the level of the sender and the label of the recipient, a security policy engine that is outside the TOE is called that returns a binary decision to grant or refuse access. The TOE enforces the access decision. Therefore, the TSF enforces a mandatory security policy based upon the Bell and LaPadula model as well as administrator enforced access policy based upon sender and receiver identity. It is the identity security policy that is different between the two subsystems.

2.4.2.2 Identification

In addition to the ACL library, the SFL and CML libraries provide additional security functions. The CML provides the functions necessary for validating the certificates and their associated certification paths. The SFL provides the decryption and encryption services.

The TOE has the message parsed and decrypted so that TOE can see the *inside signedData*, to obtain the message and signed attributes. The inside signed attributes include the inside security label of the message, and the receipt request (if any).

The TOE verifies the outside-originator's signature and the validity of the message. If the signature is invalid, the TOE terminates processing the message. Therefore, through the senders certificate the TOE identifies the sender as well as the security label of the message, which is the security level at which the message was sent.

The X.500 DSA contains MMHS security objects such as public certificates, application certificates, CRLs, and SPIFs. These security objects are downloaded, verified and cached by the TOE to support the enforcement of its security policies.

3. Security Environment

The MLA/PUA (i.e., TOE) provides for a level of protection that is appropriate for IT environments that require strict control over the information flow across a network. The TOE is not designed to withstand physical attacks directed at disabling or bypassing its security features, however it is designed to withstand logical attacks originating from its attached network. The TOE is suitable for use in both commercial and government environments.

This section defines the security policies the TOE, in conjunction with its environment, is intended to fulfill as well as usage assumptions about the TOE's intended environment.

3.1 Threats to Security

All of the threats countered by the TOE are implicit in the organizational security policies described below.

3.2 Organization Security Policies

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

P.CONFIDENTIAL	All data must be protected from unauthorized disclosure.
P.INTEGRITY	All data must be protected from unauthorized modification.
P.LABELING	All messages must be labeled with an appropriate classification.
P.I&A	All subjects must be uniquely identified in concert with access control decisions and auditing.
P.ACCESS	Messages can be sent from an originator to a recipient only if the security label of the recipient is greater than or equal to that of the originator and the originator is authorized to send messages to the recipient.
P.REPUDIATION	Message origination and reception cannot be plausibly denied.
P.AUDIT	Support must be provided for the auditing of noteworthy events.

3.3 Secure Usage Assumptions

The following usage assumptions are made about the intended environment of the TOE.

3.3.1 Personnel Assumptions

A.NOTOEAC	Human users have no direct interface into the TOE. Rather, mail requests are delivered to the TOE from mail servers and administrators configure the TOE only during installation.
A.ADMIN	Administrators will be appropriately qualified and will appropriately follow applicable guidance related to the TOE.

3.3.2 Physical Assumptions

A.CHOKE The environment of the TOE will be configured such that all of the e-mail traffic that is required to be controlled using the access control policy implemented by the TOE will be directed through the TOE.

3.3.3 Logical Assumptions

A.GENPUR There are no general purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) or storage repository capabilities provided by the TOE.

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

A.PUBLIC The TOE does not host public data.

A.PHYSEC The TOE is physically protected from tampering.

A.ITSPRT The TOE operates in an IT environment where all of the IT components operate correctly, providing necessary support to the TOE, and securely, where the IT components are protected or protect themselves as necessary to ensure that they do not interfere with the TOE's security policy enforcement.

4. Security Objectives

This section defines the security objectives of the MLA/PUA (i.e., TOE) and its supporting environment. Security objectives, categorized as either IT security objectives for the TOE or its environment or non-IT security objectives for the environment of the TOE, reflect the stated intent to comply with the organizational security policies described previously. All of the identified organizational policies are addressed by the security objectives described below.

4.1 IT Security Objectives for the TOE

The following security objectives are intended to be satisfied by the TOE.

O.CERT	The TOE must ensure that message has a certificate that uniquely identifies the originator and the security label of the message.
O.DAC	The TOE must ensure that the ACL administrator discretionary access control policy checks made by the IT Environment are enforced.
O.MAC	The TOE must ensure that the security checks made by the IT Environment are enforced.
O.MEDIAT	The TOE must mediate access to mail lists, components, and addresses of individual recipients for all messages from originators on a connected network to recipients, components, or other e-mail systems on another connected network.
O.REPUDI8	The TOE must prevent individuals from plausibly denying their involvement in either the origination or the receipt of a specific message.

4.2 IT Security Objectives for the Environment

The following security objectives for the IT environment of the TOE must be satisfied in order for the TOE to fulfill its own security objectives.

OIE.DAC	The IT Environment provides a function that (when provided an originator identity, message security label, and recipient mail list identifier) will implement appropriate checks to determine whether the ACL administrator has allowed access to the intended recipient or mail list and respond with access decisions to be enforced by the TOE.
OIE.MAC	The IT Environment provides a function that (when provided an originator identity, message security label, and recipient mail list identifier) will implement appropriate Bell and LaPadula-based access checks and respond with access decisions to be enforced by the TOE.

4.3 Non-IT Security Objectives for the Environment

The following security objectives are intended tom be satisfied by the environment of the TOE. Note that while some of the objectives may appear to be IT security objectives, they are not treated as IT security objectives because the TOE has no direct IT dependency related to these objectives. As such, they could potentially be accomplished by any means available in the environment.

OE.AUDIT	The environment must have an available audit service that provides the storage capability when the IT environment sends audit information (e.g., based on access decisions).

OE.I&A	To perform the duties of an authorized administrator, the MLA/PUA administrator must be appropriately and uniquely identified within the environment of the TOE.
OE.ACCESS	All data within the environment must be protected from disclosure or modification at all times.
OE.NOTOEAC	Human users have no direct interface into the TOE. Rather, mail requests are delivered to the TOE from mail servers and administrators configure the TOE only during installation.
OE.ADMIN	Administrators will be appropriately qualified and will appropriately follow applicable guidance related to the TOE.
OE.CHOKE	The environment of the TOE will be configured such that all of the e-mail traffic that is required to be controlled using the access control policy implemented by the TOE will be directed through the TOE.
OE.GENPUR	There are no general purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) or storage repository capabilities provided by the TOE.
OE.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
OE.PUBLIC	The TOE does not host public data.
OE.PHYSEC	The TOE is physically protected from tampering.
OE.ITSPRT	The TOE operates in an IT environment where all of the IT components operate correctly, providing necessary support to the TOE, and securely, where the IT components are protected or protect themselves as necessary to ensure that they do not interfere with the TOE's security policy enforcement.

5. IT Security Requirements

5.1 TOE Security Functional Requirements

The following table describes the SFRs that are candidates to be satisfied by the MLA/PUA (i.e., TOE).

Security Functional Class	Security Functional Components
Non-repudiation of origin (FCO)	Enforced proof of origin (FCO_NRO.2)
	Enforced proof of receipt (FCO_NRR.2)
User Data Protection (FDP)	Complete access control (FDP_ACC.2)
	Security attribute access control (FDP_ACF.1)
Identification and authentication (FIA)	User attribute definition (FIA_ATD.1)
	User identification before any action (FIA_UID.2)

Table 1 Security Functional Components

5.1.1 Non-repudiation of origin (FCO)

5.1.1.1 Enforced proof of origin (FCO_NRO.2)

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 [**originator'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 a capability to verify the evidence of origin of information to [***recipient***] given

- [**the public key of the originator and**
- **the private key of the recipient**].

5.1.1.2 Enforced receipt (FCO_NRR.2)[1]

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 [**successful receipt**] of the recipient of the information, and the [**message identification**] of the information to which the evidence applies.

[1] Note that the TOE relies on the Getronics SFL functions to parse and generate signed e-mail receipts.

5.1.1.2.3 FCO_NRR.2.3

The TSF shall provide a 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 access control (FDP_ACC.2)

5.1.2.1.1 FDP_ACC.2.1(a)

The TSF shall enforce the [**mandatory access control SFP**] on
[

- **subjects: message originators and message recipients,**
- **objects: messages,]**

and all operations among subjects and objects covered by the SFP.

5.1.2.1.2 FDP_ACC.2.1(b)

The TSF shall enforce the [**ACL administrator discretionary access control SFP**] on
[

- **subjects: message originators and message recipients,**
- **objects: messages,**]

and all operations among subjects and objects covered by the SFP.

5.1.2.1.3 FDP_ACC.2.2

The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

5.1.2.2 Security attribute access control (FDP_ACF.1)

5.1.2.2.1 FDP_ACF.1.1(a)

The TSF shall enforce the [**mandatory access control SFP**] to objects based on
[

- **security labels of messages and**
- **security labels of recipients].**

5.1.2.2.2 FDP_ACF.1.1(b)

The TSF shall enforce the [**ACL administrator discretionary access control SFP**] to objects based on **the following**[2]
[

- **originator,**
- **recipient, and**
- **originator/recipient pairs allowed by the ACL Server**]

and all operations among subjects and objects covered by the SFP.

[2] This refinement (i.e., "the following") has been inserted to comply with U.S. Interpretation #416.

5.1.2.2.3 FDP_ACF.1.2 (a)

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**the IT Environment must provide a positive indication that the message security label is dominated by the security label of the recipient**[3]].

5.1.2.2.4 FDP_ACF.1.2 (b)

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**the IT Environment must provide a positive indication that the originator is allowed to send a message to the recipient based on the ACL**[4]].

5.1.2.2.5 FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [***no additional rules***].

5.1.2.2.6 FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the [***no additional explicit denial rules***].

5.1.2.3 User attribute definition (FIA_ATD.1)

5.1.2.3.1 FIA_ATD.1.1

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

- **[Identity;**
- **Level].**

5.1.2.4 User identification before any action (FIA_UID.2)

5.1.2.4.1 FIA_UID.2.1

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.2 Security Functional Requirements for the IT Environment

There are two security functional requirements for the IT environment. Each of these requirements has been explicitly defined to fulfill TOE dependencies on the IT environment originating from FDP_ACF.1.

5.2.1 Mail List Agent (MLA)

This class has been explicitly defined to support requirements, not available in the CC, designed to require that access checks be performed with the expectation that some other IT entity will enforce those decisions. This class has two families – one for discretionary and one for mandatory checks.

[3] This check is dependent on the IT environment requirement MLA_MAC.1.
[4] This check is dependent on the IT environment requirement MLA_DAC.1.

5.2.1.1 Mail List Agent Discretionary Access Check (MLA_DAC)

This family has been explicitly defined to support requirements, not available in the CC, designed to require that discretionary access checks be performed with the expectation that some other IT entity will enforce those decisions. This family has only a single component.

5.2.1.1.1 Message Mail List Agent Discretionary Access Check (MLA_DAC.1)

5.2.1.1.1.1 MLA_DAC.1.1

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 originator is allowed to send messages to the intended message recipient. An affirmative indication indicates that the send operation should be allowed relative to this check.

5.2.1.2 Mail List Agent Mandatory Access Check (MLA_MAC)

This family has been explicitly defined to support requirements, not available in the CC, designed to require that mandatory access checks be performed with the expectation that some other IT entity will enforce those decisions. This family has only a single component.

5.2.1.2.1 Message Mail List Agent Mandatory Access Check (MLA_MAC.1)

5.2.1.2.1.1 MLA_MAC.1.1

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 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. No operations are applied to the assurance components.

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

	AVA_VLA.1 Developer vulnerability analysis

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]

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 ACM_CAP.2.RI3

The configuration list shall uniquely identify all configuration items that comprise the TOE.[6]

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~~ **configuration list** shall uniquely identify all configuration items.[7]

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] This requirement has been removed to comply with U.S. Interpretation #412.
[6] This requirement element has been added to comply with International Interpretation #3.
[7] This requirement has been changed to comply with U.S. Interpretation #412.

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.[8]

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 Function Specification (ADV_FSP.1)

5.3.3.1.1 ADV_FSP.1.1D

The developer shall provide a functional specification.

[8] This requirement has been modified to comply with International Interpretation #51.

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 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 documents supplied for evaluation.

5.3.4.1.9 AGD_ADM.1.8C

The administrator guidance shall describe all security requirements on 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 on 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 Evidence 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 vulnerability analysis (AVA_VLA.1)

5.3.5.5.1 AVA_VLA.1.1D

~~The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.~~ **The developer shall perform a vulnerability analysis.**[9]

5.3.5.5.2 AVA_VLA.1.2D

~~The developer shall document the disposition of obvious vulnerabilities.~~ **The developer shall provide vulnerability analysis documentation.** [10]

5.3.5.5.3 AVA_VLA.1.1C

~~The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.~~ **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.**[11]

5.3.5.5.4 AVA_VLA.1.2C

The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.[12]

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. [13]

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.

---

[9] This requirement has been modified to comply with International Interpretation #51.
[10] This requirement has been modified to comply with International Interpretation #51.
[11] This requirement has been modified to comply with International Interpretation #51.
[12] This requirement has been added to comply with International Interpretation #51.
[13] This requirement has been added to comply with International Interpretation #51.

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

6.1.1 Access Control

The TOE ***enforces*** a mandatory, label-based security policy as well as an ACL administrator discretionary access control policy on messages created by a sender when the sender attempts to send the message to a recipient (user, mail-list, port). The MLA/PUA requires its environment to manage the acceptable access control specification as well as the to make the policy decision. The TOE calls the policy decision maker with the appropriate subject identity, subject security attributes, and the object identity for which access is being requested. The policy decision maker returns the grant access decision to the TOE. The TOE then enforces the policy decision and either provides access or returns an error to the subject.

The TOE does not support the administrator interface to implement either the object attributes by which a security policy decision is based. Nor does the TOE make the policy decision. Rather once the TOE receives an access decision concerning the user e-mail send request, the TOE enforces the decision.

The Access Control function is designed to satisfy the following security functional requirements:

- FDP_ACC.2
- FDP_ACF.1

6.1.2 Identification

Once a mail message send request arrives at the TOE, the user's certificate is parsed and the originator's digital signature uniquely identifies the user. If the user cannot be identified the TOE will perform no actions.

The TOE has the message parsed and decrypted, using services of Getronics (in the IT environment), so that TOE can see the *inside signedData*, to obtain the message and signed attributes. The inside signed attributes include the inside security label of the message, and the receipt request (if any).

The TOE verifies the outside-originator's signature and the validity of the message. If the signature is invalid, the TOE terminates processing the message. Therefore, through the senders certificate the TOE identifies the sender as well as the security label of the message, which is the security level at which the message was sent.

If the message includes a receipt request and the message was valid and passed on to its intended recipients, the TOE returns a digitally signed message to the originator identifying the message. Alternately, if the message includes a receipt request and the message was rejected for any reason, the TOE returns a digitally signed message to the originator indicating non-delivery. Note that the delivery receipt provides the originator assurance that the TOE received and processed the message appropriately. There is no assurance that the final intended recipient actually received the message once it left control of the TOE. Note also that the TOE utilizes Getronic SFL functions to generate the necessary signed receipts and then uses Exchange functions to return the receipt to the originator. In each case, it is assumed that each of these IT environment components performs correctly and securely.

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FCO_NRO.2
- FCO_NRR.2
- FIA_ATD.1

- FIA_UID.2

6.2 TOE Security Assurance Measures

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

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

6.2.1 Process Assurance

6.2.1.1 Configuration Management

The configuration management measures applied by California Microwave ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. California Microwave ensures changes to the implementation representation are controlled and that TOE associated configuration item modifications are properly controlled. California Microwave performs configuration management on the TOE implementation representation, design, tests, user and administrator guidance, and the CM documentation. These activities are documented in:

- Configuration Management Plan
- Software Configuration Management Work Instruction
- Software Version Identification
- Quality Manual

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

6.2.2 Delivery and Guidance

California Microwave provides delivery documentation that explains how the TOE is delivered and procedures to identify the TOE, allow detection of unauthorized modifications of the TOE and installation and generation instructions at start-up. California Microwave's delivery procedures describe the procedures to be used for the secure installation, generation, and start-up of the TOE. These procedures are documented in:

- Delivery and Operation
- Software CD Delivery Procedure
- Deliverable Software CD Identification

California Microwave provides administrator guidance in the installation and initialization procedures. The installation and generation procedures, included in the administrator guidance, describe the steps necessary to install California Microwave Appliances in accordance with the evaluated configuration. The TOE provides no administrator interface once it is operational. Similarly, the TOE provides only a simple mail exchange interface to users. Because there are no interfaces allowing users to manage security relevant data and there is no administrator interface the only applicable guidance is the installation manual.

The administrator guidance is documented in:

- MLA/PUA Installation Manual
- MLA/PUA Administrator Manual

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

The Design Documentation provided for MLA/PUA is provided in two documents: "MLA/PUA Functional Specification" and "MLA/PUA High Level Design." These documents serve to describe the security functions of the TOE, its interfaces both external and between subsystems, the architecture of the TOE (in terms of subsystems), and correspondence between the available design abstractions (including the ST). The Design Documentation security assurance measure satisfies the following security assurance requirement:

- ADV_FSP.1;
- ADV_HLD.1; and,
- ADV_RCR.1.

6.2.4 Tests

The Test Documentation provided for MLA/PUA is provided in two documents: "MLA/PUA EAL2 Software Test Plan" and "MLA/PUA EAL2 Software Test Description." These documents describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. In addition, these documents describe how the functional specification has been appropriately tested.

The Tests assurance measure satisfies the following assurance requirements:

- ATE_COV.1;
- ATE_FUN.1; and,
- ATE_IND.2.

6.2.5 Vulnerability Assessment

California Microwave performs vulnerability analyses of the TOE to identify weaknesses that can be exploited in the TOE. There are no SOF claims since the TOE provides no TOE security function where the strength of the function is based on the randomness of some numerical token. The vulnerability analyses are documented in "MLA/PUA EAL2 Vulnerability Analysis: Vulnerability Analysis and Strength of TOE Security Function".

The Vulnerability Assessment assurance measure satisfies the following assurance requirements:

- AVA_SOF.1; 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;
- TOE Summary Specification;
- Security Functional Requirement Dependencies; and
- Internal Consistency.

8.1 Security Objectives Rationale

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

8.1.1 Security Objectives Rationale for the TOE and Environment

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

Objectives	O.CERT	O.DAC	O.MAC	O.MEDIAT	O.REPUDI8	OIE.DAC	OIE.MAC	OE.AUDIT	OE.I&A	OE.ACCESS	OE.NOTOEAC	OE.ADMIN	OE.CHOKE	OE.GENPUR	OE.LOWEXP	OE.PUBLIC	OE.PHYSEC	OE.PHYSEC
P.CONFIDENTIAL		X	X	X		X	X			X								
P.INTEGRITY										X								
P.LABELING	X																	
P.I&A	X					X	X		X									
P.ACCESS		X	X	X		X	X			X								
P.REPUDIATION				X	X													
P.AUDIT						X	X	X										
A.NOTOEAC											X							
A.ADMIN												X						
A.CHOKE													X					
A.GENPUR														X				
A.LOWEXP															X			
A.PUBLIC																X		
A.PHYSEC																	X	
A.ITSPRT																		X

Table 3 Environment to Objective Correspondence

8.1.1.1 P.CONFIDENTIAL

All data must be protected from unauthorized disclosure.

This policy is satisfied by ensuring that:

- the message-related access control policies are always invoked (O.MEDIAT) and succeed before allowing messages to be successfully transmitted from originator to recipient (O.DAC, O.MAC, OIE.DAC, and OIE.MAC) and
- the TOE environment protects information from unauthorized disclosure or modification (OE.ACCESS).

8.1.1.2 P.INTEGRITY

All data must be protected from unauthorized modification.

This policy is satisfied by ensuring that:

- the TOE environment protects information from unauthorized disclosure or modification (OE.ACCESS).

8.1.1.3 P.LABELING

All messages must be labeled with an appropriate classification.

This policy is satisfied by ensuring that:

- each message has an associated unique originator identity and security label (O.CERT).

8.1.1.4 P.I&A

All subjects must be uniquely identified in concert with access control decisions and auditing.

This policy is satisfied by ensuring that:

- each message has an associated unique originator identity and security label (O.CERT);
- the originator identity is used in access decisions (OIE.DAC and OIE.MAC); and
- administrators are appropriately and uniquely identified within the TOE environment when allowing them to install and configure the TOE (OE.I&A).

8.1.1.5 P.ACCESS

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

This policy is satisfied by ensuring that:

- the message-related access control policies are always invoked (O.MEDIAT) and succeed before allowing messages to be successfully transmitted from originator to recipient (O.DAC, O.MAC, OIE.DAC, and OIE.MAC) and
- the TOE environment protects information from unauthorized disclosure or modification (OE.ACCESS).

8.1.1.6 P.REPUDIATION

Message origination and reception cannot be plausibly denied.

This policy is satisfied by ensuring that:

- the TOE will prevent individuals from plausibly denying their involvement in either the origination or the receipt of a specific message (O.REPUDI8) and
- all messages are processed through the TOE to prevent the possibility of bypassing the TOE with a message not subject to non-repudiation functions (O.MEDIAT).

8.1.1.7 P.AUDIT

Support must be provided for the auditing of noteworthy events.

This policy is satisfied by ensuring that:

- the TOE provides the necessary information to the IT environment for use in access decisions and potentially auditing (OIE.DAC and OIE.MAC) and
- the TOE environment has a suitable audit capability (OE.AUDIT).

8.1.1.8 A.NOTOEAC

Human users have no direct interface into the TOE. Rather, mail requests are delivered to the TOE from mail servers and administrators configure the TOE only during installation.

This assumption is addressed by the directly corresponding objective for the TOE environment (OE.NOTOEAC).

8.1.1.9 A.ADMIN

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

This assumption is addressed by the directly corresponding objective for the TOE environment (OE.ADMIN).

8.1.1.10 A.CHOKE

The environment of the TOE will be configured such that all of the e-mail traffic that is required to be controlled using the access control policy implemented by the TOE will be directed through the TOE.

This assumption is addressed by the directly corresponding objective for the TOE environment (OE.CHOKE).

8.1.1.11 A.GENPUR

There are no general purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) or storage repository capabilities provided by the TOE.

This assumption is addressed by the directly corresponding objective for the TOE environment (OE.GENPUR).

8.1.1.12 A.LOWEXP

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

This assumption is addressed by the directly corresponding objective for the TOE environment (OE.LOWEXP).

8.1.1.13 A.PUBLIC

The TOE does not host public data.

This assumption is addressed by the directly corresponding objective for the TOE environment (OE.PUBLIC).

8.1.1.14 A.PHYSEC

The TOE is physically protected from tampering.

This assumption is addressed by the directly corresponding objective for the TOE environment (OE.PHYSEC).

8.1.1.15 A.ITSPRT

The TOE operates in an IT environment where all of the IT components operate correctly, providing necessary support to the TOE, and securely, where the IT components are protected or protect themselves as necessary to ensure that they do not interfere with the TOE's security policy enforcement.

This assumption is addressed by the directly corresponding objective for the TOE environment (OE.ITSPRT).

8.2 Security 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.

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

Requirements / Objectives	FCO_NRO.2	FCO_NRR.2	FDP_ACC.2	FDP_ACF.1	FIA_ATD.1	FIA_UID.2	MLA_DAC.1	MLA_MAC.1
O.CERT	X				X	X		
O.DAC			X	X				
O.MAC			X	X				
O.MEDIAT			X	X	X	X		
O.REPUDI8	X	X				X		
OIE.DAC							X	
OIE.MAC								X

Table 4 Objective to Requirement Correspondence

8.2.1.1 O.CERT

The TOE must ensure that message has a certificate that uniquely identifies the originator and the security label of the message.

This objective is satisfied by requiring that user mail requests are accompanied by a certificate that identifies the user (FIA_UID.2), identifies the user attributes (FIA_ATD.1), and provides the origin for the transmitted mail request (FCO.NRO.2).

8.2.1.2 O.DAC

The TOE must ensure that the ACL administrator discretionary access control policy checks made by the IT Environment are enforced.

This objective is satisfied by requiring that all message are subjected to the ALC administrator discretionary access control policy (FDP_ACC.2) and by enforcing the decision made as a result of applying the policy (FDP_ACF.1).

8.2.1.3 O.MAC

The TOE must ensure that the security checks made by the IT Environment are enforced.

This objective is satisfied by requiring that all message are subjected to the mandatory access control policy (FDP_ACC.2) and by enforcing the decision made as a result of applying the policy (FDP_ACF.1).

8.2.1.4 O.MEDIAT

The TOE must mediate access to mail lists, components, and addresses of individual recipients for all messages from originators on a connected network to recipients, components, or other e-mail systems on another connected network.

This objective is satisfied by requiring that user mail requests are accompanied by a certificate that identifies the user (FIA_UID.2), and identifies the user security level (FIA_ATD.1) as well as the intended recipients. All message requests are sent to an environmental policy decision engine with the information from the certificate. The policy decision engine makes an access decision based on both the MAC policy and the administrator DAC policy (FDP_ACF.1). Upon receiving the decision from the policy decision engine, The TOE enforces the decision returned from the policy decision engine (FDP_ACC.2). There is no interface provided to bypass the policy decision engine check or the enforcement of the policy decision engine decision.

8.2.1.5 O.REPUDI8

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

This objective is satisfied by requiring that user mail requests are accompanied by a certificate that identifies the user (FIA_UID.2) and provides the origin for the transmitted mail request (FCO.NRO.2). For the recipient, this objective is satisfied by providing evidence of receipt for the originator's certificate, since the recipient is able to decrypt the certificate (FCO_NRR.2). Also, if a message cannot be delivered for any reason a "non-delivery" message is returned by the TOE (FCO_NRR.2).

8.2.1.6 OIE.DAC

The IT Environment provides a function that (when provided an originator identity, message security label, and recipient mail list identifier) will implement appropriate checks to determine whether the ACL administrator has allowed access to the intended recipient or mail list and respond with access decisions to be enforced by the TOE.

This objective is satisfied by requiring that the IT Environment perform an access check based on the ACL administrator discretionary access policy configuration in conjunction with the originator and recipient identifications provided by the TOE and respond with an access decision to be enforced by the TOE (MLA_DAC.1).

8.2.1.7 OIE.MAC

The IT Environment provides a function that (when provided an originator identity, message security label, and recipient mail list identifier) will implement appropriate Bell and LaPadula-based access checks and respond with access decisions to be enforced by the TOE.

This objective is satisfied by requiring that the IT Environment perform an access check based on the security labels of the message, the message originator, and the message recipient provided by the TOE and respond with an access decision to be enforced by the TOE (MLA_MAC.1).

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 medium level of risk to the assets. The security environment assumes physical protection and the TOE itself offers only a very limited interface and can only be configured during initialization, offering essentially no opportunity for an attacker to subvert the security policies without physical access. 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, except as noted below. Table 5 Requirement Dependency Rationale lists each requirement from Section 5.1 with a dependency and indicates which requirement was included to satisfy the dependency, if any. For each dependency not included, a justification is proved.

Functional Component	Dependency	Included
Enforced proof of origin (**FCO_NRO.2**)	FIA_UID.1	FIA_UID.2
Enforced receipt (**FCO_NRR.2**)	FIA_UID.1	FIA_UID.2
Complete information flow control (**FDP_ACC.2**)	FDP_ACF.1	FDP_ACF.1*
Complete information flow control (**FDP_ACF.1**)	FDP_ACC.1	FDP_ACC.2
	FMT_MSA.3	*
User attribute definition(**FIA_ATD.1**)	None	
Timing of identification (**FIA_UID.2**)	None	-

Table 5 Requirement Dependency Rationales

*Functional component FMT_MSA.3 does not apply since there is no administrative interface to the TOE once the TOE has been installed and initialized. Note that since the TOE is always fully initialized before it goes online all security attribute values are defined and no role can modify those values subsequently.

Based on the FDP_ACF.1 operation completed in this ST, a dependency (beyond those defined in the Common Criteria) on the IT environment has been introduced. This dependency is fulfilled by requirements specified for the IT environment, specifically MLA_MAC.1 and MLA_DAC.1.

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 are two explicitly stated requirements for the IT environment in this ST (MLA_DAC.1 and MLA_MAC.1). These requirements are designed to work in conjunction with FDP_ACF.1, where FDP_ACF.1 enforces decisions made by the security functions corresponding to MLA_DAC.1 and MLA_MAC.1. There is no comparable requirement in the CC that supports the notion of simply making, but not enforcing, an access decision and therefore explicit requirements have 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.

	ACCESS CONTROL	IDENTIFICATION
FCO_NRO.2		X
FCO.NRR.2		X
FDP_ACC.2	X	
FDP_ACF.1	X	
FIA_ATD.1		X
FIA_UID.2		X

Table 6 Security Functions vs. Requirements Mapping

FCO_NRO.2
The certificate provided with a *send* mail request provides the origin for the transmitted mail request.

The identification security function addresses this requirement.

FCO_NRR.2
When a delivery receipt is requested by a message originator, the TOE returns a receipt, signed using Getronic SFL functions, indicating whether the message was successfully forwarded. The receipt provides proof only that the TOE received the message and not whether any final recipient received the message.

The identification security function addresses this requirement.

FDP_ACC.2

All message requests are sent to an environmental policy decision engine with the information from the certificate. The policy decision engine makes an access decision based on both the MAC policy and the administrator DAC policy. The TSF, upon receiving the decision from the policy decision engine, The TOE enforces the decision returned from the policy decision engine

The access control function addresses this requirement.

FDP_ACF.1

From Section 6.2 of Part B of the Common Criteria, the requirement FDP_ACF is described as, "Security attribute based access control allows the TSF to enforce access based upon security attributes and named groups of attributes. Furthermore, the TSF **may** have the ability to explicitly authorize or deny access to an object based upon security

attributes." The TSF enforces security attribute based access control, however the TSF does not provide the optional ability to explicitly authorize or deny access to an object. Rather, all message requests are sent to an environmental policy decision engine. The TSF calls the policy engine with the subject identity the subject's security attributes necessary for an appropriate policy decision to be made, and the identity of the object for which access is requested. The environmental policy engine returns a binary decision is access should be granted. The TSF then grants access based on the decision received from the policy engine.

The access control function addresses this requirement.

FIA_ATD.1 User attribute Definition

The TSF receives user attributes in the certificate that is part of the initial send request. The TSF maintains the following attributes for individual users:

- Identification,
- Level.

The identification security function addresses this requirement

FIA_UID.2 User Identification Before any Action

The interface whereby the TOE receives a mail send requests contains a user certificate. This certificate identifies the user. There is no other user interface to the TOE presented.

The identification security function addresses this requirement.

8.7 PP Claims Rationale

This Security Target makes no claim of compliance to a Protection Profile.