National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

The Northrop Grumman Systems Corporation,
California Microwave Systems
Mail List Agent and Profiling User Agent (MLA/PUA)
Version 3.1.0 with Patch A

Report Number: CCEVS-VR-03-0046

Dated: 13 August 2003

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Dr. Jerome Myers
The Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

Science Applications International Corporation
Columbia, Maryland 21046

Table of Contents

Table of Figures

1 Executive Summary

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the Northrop Grumman Systems Corporation, California Microwave Systems Mail List Agent and Profiling User Agent. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by Science Applications International Corporation (SAIC), and was completed 13 August 2003. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by SAIC and submitted to the Validators. The evaluation determined the product conforms to the CC Version 2.1, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level 2, resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The NGSC/CMS MLA/PUA is an enterprise profiling and mail list system. The MLA/PUA is used to automatically identify, filter and distribute Military Message Handling System (MMHS) messages to recipients based on interest profiles. The MLA/PUA is a software application that executes on a Windows 2000 based platform. The MLA/PUA integrates Microsoft Exchange 2000 and Microsoft Active Directory Services with the NGSC/CMS MailRoom message profiler. The MLA/PUA also has a mail list capability that uses Directory System Agent (DSA) input to generate a distribution list that can be used to send out mail to the various members of the mail list. The MLA/PUA is designed to operate in a distributed network environment. Figure 1: MLA/PUA External Interfaces illustrates the relationship between the TOE and its environment. The TOE is just the MLA/PUA software application. The other components in the diagram have not been evaluated because they are in the IT Environment.

The evaluated security features include:

- Access Control on messages based upon the security level of the message and the levels of the sender and recipient.
- Access Control on messages based upon an administrator defined policy for permissible (sender, receiver) pairs that can communicate.
- Identification of the originator of a message prior to providing services
- Proof of Origin for messages that are delivered by the TOE
- Non-Repudiation of Receipt of a message by the TOE when an originator requests that a proof of receipt be provided.

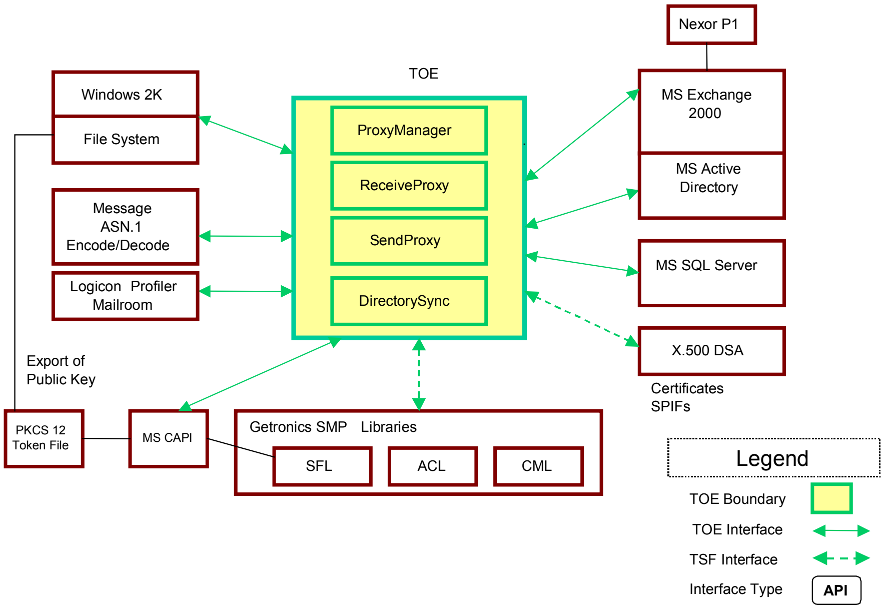
Nexor P1
TOE
Windows 2K
File System
ProxyManager
ReceiveProxy
SendProxy
DirectorySync
MS Exchange 2000
MS Active Directory
MS SQL Server
X.500 DSA
Certificates
SPIFs
Message ASN.1 Encode/Decode
Logicon Profiler Mailroom
Export of Public Key
PKCS 12 Token File
MS CAPI
Getronics SMP Libraries
SFL
ACL
CML
Legend
TOE Boundary
TOE Interface
TSF Interface
Interface Type
API

Figure 1: MLA/PUA External Interfaces

The MLA/PUA is intended to be used in a message handling system. There are many other components required to correctly handle the secure end-to-end delivery of messages. The correct security functionality of the overall message handling system environment is not directly addressed by this evaluation.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desire a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP CCEVS' Validated Products List. Table 1 provides information needed to completely identify the product, including:

- the Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated,
- the Security Target (ST), describing the security features, claims, and assurances of the product,
- the conformance result of the evaluation,
- the organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers Item Identifier

Evaluation Identifiers for Northrop Grumman Systems, California Microwave Systems MLA/PUA Version 3.1.0 with Patch A	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Northrop Grumman Systems, California Microwave Systems Mail List Agent and Profiling User Agent, Version 3.1.0 with Patch A
Protection Profile	N/A
Security Target	California Microwave Mail List Agent (MLA) and the Profiling User Agent (PUA) Security Target, Version 1.0, dated 12 August 2003 [10]
Evaluation Technical Report	Evaluation Technical Report (ETR) for the California Microwave Systems Mail List Agent and Profiling User Agent, Version 1.0, dated 13 August 2003 [9]

Evaluation Identifiers for Northrop Grumman Systems, California Microwave Systems MLA/PUA Version 3.1.0 with Patch A	
Conformance Result	Part 2 conformant, Part 3 conformant, and EAL2
Version of CC	CC Version 2.1 [1], [2], [3], [4] and all applicable NIAP CCEVS and International Interpretations effective on September 16, 2002
Version of CEM	CEM Version 1.0 [5], [6], and all applicable NIAP CCEVS and International Interpretations effective on September 16, 2002
Sponsor	Northrop Grumman, California Microwave Systems 21200 Burbank Ave. Bldg. 30 Woodland Hills, CA 91367
Developer	Northrop Grumman, California Microwave Systems 21200 Burbank Ave. Bldg. 30 Woodland Hills, CA 91367
Evaluator(s)	Science Applications International Incorporated Terrie Diaz Tammy Compton Sukrat Abbas
Validator(s)	NIAP CCEVS Dr. Jerome Myers

3 Security Policy

The TOE implements several security policies in conjunction with its role in the delivery of messages.

3.1 Access Control Policies

The MLA/PUA enforces a mandatory, label-based access control security policy and an IT environment administratively configured discretionary access control policy. Both of those policies are implemented by the TOE enforcing decisions that are made in the IT environment and communicated to the TOE through the interfaces with the ACL library. 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 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 and that security policy engine 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 security levels as well as an IT environment administrator defined discretionary access policy based upon sender and receiver identity.

3.1.1 Label-based Access Policy

The TOE enforces a mandatory label-based access policy on messages that are to be sent. Prior to sending a message on to its intended recipients, the TOE ensures that the security label of the intended recipients dominates the security label of the message

The dominance relation between labels that is used for making the decisions is specified in a SPIF that is externally defined and is never directly processed by the TOE. The TOE uses information that it obtains from the IT security environment to determine the security labels of the sender and intended recipients. The TOE uses its interfaces with the Getronics libraries to obtain the security labels of the messages from digitally signed data within the messages and then to request and access control decision based upon those labels and the SPIF that the ACL library uses.

3.1.2 Discretionary Access Policy

The TOE enforces a discretionary access control policy on messages that is based upon another access decision provided by the Getronics ACL. The MLA/PUA makes calls to the Getronics ACL to determine whether the originator is permitted to send messages to the intended recipients. The TOE will only process a message for release if it receives a positive response from the ACL stating that the operation is permitted.

3.2 Identification Policy

The TOE will only provide services for users that have been properly identified. The only user interface to the TOE is the mail message send request. Users are identified through information contained within signed data in submitted messages. The first action that the TOE takes when it receives a message is to check that the message contains a properly identified originator that is bound to the message with a valid digital signature. If the message does not pass this check then all processing of the message is terminated without a response to the originator.

3.3 Proof of Origin Policy

The TOE ensures that every message that it releases for delivery includes a digital signature that identifies the original sender of the message. When a mail message send request arrives at the TOE, the user's certificate is parsed and the originator's digital signature is checked to ensure that it is valid. The originators signature is maintained on messages that are then further processed and eventually sent out for delivery.

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.

3.4 Non-Repudiation of Receipt Policy

After a message is received by the TOE and checked for a valid originator, the TOE determines whether a return receipt has been requested by the originator. If the message includes a receipt request and the message was passed on to its intended recipients, then the TOE will return a digitally signed message to the originator indicating that the message was accepted by the TOE. If the message includes a receipt request and the message is rejected for any reason other than failure to have a properly identified originator the TOE will return 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 Getronics 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 for a proper return receipt to be delivered to the originator.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The evaluation made the following assumption concerning product usage:

4.1.1 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.

4.1.2 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. The only message path between originators and recipients must go through the TOE.

4.1.3 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.

4.2 Clarification of Scope

The CMS MLA/PUA is intended to be used in a message handling system. There are many other components required to correctly handle the secure end-to-end delivery of messages. The correct security functionality of the overall message handling system environment is not directly addressed by this evaluation. There are two important implications of the scope of the TOE evaluation that although stated in the basic description of the TOE and its usage assumptions warrant elaboration. Firstly, the TOE can only enforce its access control policies on messages that are directed through the TOE. Messages that have explicitly identified destinations rather than mail lists for destinations would not be directed through the TOE. Hence, the analogous send/receive access control policies on those messages would have to be handled by other components in an overall message handling architecture. Secondly, with regards to non-repudiation of receipt, the TOE only provides proof that it received and accepted a message for distribution. The TOE does not guarantee the delivery of that message to its ultimate destination nor does the non-repudiation receipt provide a necessary link in a chain of evidence for end-to-end proof of delivery.

This evaluation is based upon some assumptions and IT environmental requirements that the associated environment is appropriately configured and managed and the authorized users are properly trained. The configuration of a message handling system involves coordinated configuration of many components. Hence, the installation procedure for the TOE specifically states that it requires that the installer be trained to install the TOE.

Important architectural components of the environment in which the CMS MLA/PUA is installed include the base platform (hardware and operating system) for the MLA/PUA, the Getronic libraries as well as architectural components (Microsoft Exchange Server, the DSA, and compatible user agents) that reside on different platforms than the TOE. The evaluation of this TOE is not directly tied to possible evaluations of any of the other components in the message handling system. In particular, the evaluation of this TOE does not imply that all of the properties required of the MLA/PUA for the evaluation of those other products have been included in this evaluation. This is not necessarily a limitation upon the capabilities of this product or those other components of the messaging environment, but rather it is a statement of the limitations on the scope of the analysis that was performed for this evaluation.

5 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target.

The architectural relationship between the MLA/PUA and its IT environment is illustrated in Figure 1: MLA/PUA External Interfaces. The support provided by some of the external interfaces is further discussed in the Security Policy section and the Logical Boundaries section of this report.

5.1 Subsystems

The high level design of the MLA/PUA decomposes the TOE into 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). Further information about the decomposition of the TOE is considered proprietary.

.

6 Delivery and Documentation

The TOE is distributed on two CDs. One CD contains all components of TOE software and documentation except for Patch A. The second CD contains Patch A. Both CDs have identification labels and the CDs are enclosed in cases that are tamper sealed. The TOE must be purchased directly from the developer, California Microwave Systems. Each distribution is uniquely tagged and, at the time of purchase, the buyer is provided with the procedures for verifying that the CDs that are delivered contain the correct distribution for that specific purchaser.

There is no hardcopy documentation that is delivered with the CDs. The installation guidance and user documentation are provided in softcopy on the TOE CD. The installation procedures require that a trained administrator perform the actual installation.

7 IT Product Testing

7.1 Developer Testing

The developer maintains a suite of tests for confirming that the product meets its advertised functional requirements. Testing was performed at a developer facility in Woodland Hills, CA. However, the test network was distributed and included a DSA that was located in Scottsdale, AZ. 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.

The developer's tests were documented in a MLA/PUA EAL2 Software Test Plan and MLA/PUA EAL2 Software Test Description documents. The Test Cases provided a high level description of the functionality tested and test setup The Test Cases were mapped to one or more Test Procedures. The Test Procedures provided detailed instructions for the tester as well as expected and actual test results.

Test documentation including test plans, test procedures, a description of the test configuration, test coverage documentation, expected test results, and actual test results were provided to the CCTL for review. The evaluators reviewed the developers tests and test results to ensure that the developers testing and test results were appropriate for the evaluated configuration. An evaluation team review of all of the security functions and the mapping between security functions and tests confirmed that security functions were appropriately tested by the developer tests.

7.2 Evaluator Testing

Evaluation team testing was conducted from July 30 thru August 1, 2003 at the California Microwave Systems facility in Woodland Hills, CA. The evaluation team performed the following activities during testing:

1. Installation of the TOE in its evaluation configuration
2. Execution of a sample of the developer's functional tests
3. Independent Testing
4. Vulnerability Testing (AVA_VLA.1)

The TOE was tested in a network configuration that included three client hosts (two for confirming delivery of messages and one for sending messages), a host for Microsoft Exchange Server 2000, and a host for the TOE and the associated libraries that are required in its environment. In addition, the network was connected to a remote network in Scottsdale, AZ where additional message processing systems resided. However, the only host that was used on the remote network was the DSA mentioned in the discussion of the developer's testing.

The evaluators conducted testing using a sample of tests found in the developer test plan and procedures. The evaluators' tests were selected based upon a review of

CMS's test evidence and the evaluators' understanding of the TOE's design. The evaluator selected a set of tests that exercised each of the user interface options and tested each of the security functional requirements stated in the ST.

All of the tests that the evaluator selected used for testing were manual tests. Moreover, the test results involved visual observation and interpretation of information presented by GUI's and logs displayed in the test environment. Although test results were often observed through a GUI, the actual test results were also captured in the logs that were preserved. Hence, sufficient information was captured in the logs to reproduce any analysis of test results that was performed by visual inspection.

The evaluation team's independent testing included testing some of the security functionality with different input parameter combinations than were included in the vendor tests and some negative testing to confirm that additional functionality was not provided through the interfaces.

The evaluator performed some vulnerability testing. The heart of an evaluator team's contributions to conformance with AVA_VLA.1 is in the evaluators' analysis of the vendor's vulnerability analysis. The evaluation team determined that the vendor's vulnerability analysis was thorough and appropriately tested. Hence, the evaluators did not need to generate new tests based upon the vendor's vulnerability analysis. However, the evaluator team did include some testing that confirmed the absence of some hypothesized vulnerabilities that the vendor had already claimed to be eliminated through analysis.

A developer representative was available to facilitate the testing. The developer showed the evaluator how to use some of the test tools prior to the evaluator performing testing. The vendor also assisted the evaluator in obtaining appropriate data that could be injected into the TOE for testing. More precisely, some of the evaluation team's functional and vulnerability tests required the setting up of information at the remote DSA so it could be pulled into the MLA/PUA and used during the tests. The vendor coordinated with the administrator of that remote server to make the appropriate changes. An evaluator then used a combination of MLA/PUA logging capabilities and local tools to pull the configured data into the MLA/PUA and to confirm that the data contained the desired information as part of the performance of the tests.

The end result of the testing activities was that all tests gave expected (correct) results. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities.

The evaluation team tests and penetration tests substantiated the security functional requirements in the ST.

8 Evaluated Configuration

8.1 TOE

This section documents the configuration of the IT product during the evaluation. The administrator and installation guides provide the necessary details for the correct configuration of the IT product in its evaluated configuration.

It is important for potential users to realize that if the evaluated configuration differs from the intended operational use, the differences must be factored into the final risk assessment.

The MLA/PUA includes both physical and logical boundaries. Figure 1: MLA/PUA External Interfaces illustrates the external interfaces. The physical boundary of the TOE are the delineated by the external interfaces to environmental software that is not part of the MLA/PUA but is 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.

8.1.1 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)
- Microsoft 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.

8.1.2 Logical Boundaries

The logical boundary 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.

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.

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.

9 Results of the Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC, Version 2.1; CEM, Version 1.0, and all applicable NIAP CCEVS and International Interpretations in effect on September 16, 2002.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence.

In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Section 4, Results of Evaluation, from the document *Evaluation Technical*

Report (ETR) for the California Microwave Systems Mail List Agent and Profiling User Agent, Version 1.0, dated 13 August 2003, contains the verdicts of “PASS” for all the work units.

The evaluation determined the product to be Part 2 compliant and, as well, meeting the requirements for Part 3, and EAL 2. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by SAIC.

10 Validator Comments

The Security Target includes reference to a policy, P.AUDIT, requiring support for the auditing of significant events. However, the responsibility for addressing this policy was completely allocated to the IT environment. The MLA/PUA does log many events and those logs were quite useful during the testing of the product. However, it does not log some of the events (in particular start-up/shutdown) that are required to meet the auditing functional requirements in the Common Criteria. Hence, rather than crafting an explicitly stated requirement that captured the logging capabilities of the TOE, the ST authors chose to exclude any analysis of the logging capabilities from the evaluation.

All other validator comments regarding this evaluated product are already captured in the Clarification of Scope section of this report.

There were no evaluator comments for the validator to pass on in this section of the report.

11 Security Target

The Security Target, “California Microwave Mail List Agent (MLA) and the Profiling User Agent (PUA) Security Target, Version 1.0, dated August 12, 2003” is included here by reference.

12 Glossary

12.1 Definition of Acronyms

ACL	Access Control Library
CA	Certificate Authorities
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CI	Configuration Items
CLI	Command Line Interface
CM	Configuration Management
CMS	California Microwave Systems
CRL	Certificate Revocation List
DSA	Directory System Agent
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
I&A	Identification and Authentication

I/O	Input/Output
IT	Information Technology
MAC	Mandatory Access Control
MLA	Mail List Agent
MMHS	Military Message Handling System
NAT	Network Address Translation
NIAP	National Information Assurance Program
NIST	National Institute of Science & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OR	Observation Report
PUA	Profiling User Agent
PP	Protection Profile
SAIC	Science Applications International Corporation
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirements
SOF	Strength of Function
SPIF	Security Policy Information File
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

13 Bibliography

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

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

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

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

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

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

[7] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.

[8] Common Criteria Evaluation and Validation Scheme for Information Technology Security Guidance to Validators of IT Security Evaluations, Scheme Publication #3, Version 1.0, February 2002

[9] Evaluation Technical Report (ETR) for the California Microwave Systems Mail List Agent and Profiling User Agent, Version 1.0, dated 13 August 2003

[10] California Microwave Mail List Agent (MLA) and the Profiling User Agent (PUA) Security Target, Version 1.0, dated 12 August 2003