National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

Nexor MMHS Security

Report Number: CCEVS-VR-05-0095
Dated: 14 March 2005

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
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, Maryland 21046

Table of Contents

1 EXECUTIVE SUMMARY

This report documents the NIAP Validators' assessment of the CCEVS evaluation of Nexor MMHS Security, a set of software products that provide security enhancements for electronic messaging. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by Science Applications International Corporation (SAIC) and was completed 23 February, 2005. The information in this report is largely derived from an Evaluation Technical Report (ETR) written by SAIC and submitted to the Validator. The evaluation determined that the product conforms to the CC Version 2.1, Part 2 extended, and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 2, resulting in a "pass" in accordance with CC Part 1 paragraph 175.

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

The Nexor Defender for Outlook component is a user agent designed to extend the functionality of Microsoft Outlook 2000. The component enables users to send and receive military messages. It includes an LDAP Address Book provider to provide integrated directory services into Microsoft Outlook 2000, such as support for multiple servers to allow for redundancy and consolidation of searches across multiple directories to access email addresses and security objects, and directory browsing to allow the user to navigate through the directory information to find the appropriate recipient. Additionally, Nexor Defender for Outlook includes the S/MIME Security Plug-in to provide the ability to attach a label to a message, verify recipient and originator clearances, and encrypt and digitally sign messages before they are sent. .

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

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

2 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

Evaluation Identifiers for Nexor MMHS Security	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Nexor MMHS Security
Protection Profile	N/A
Security Target	Nexor MMHS Security Security Target, Version 1.0, 21 February 2005 [9]
Evaluation Technical Report	Evaluation Technical Report (ETR) for the Nexor MMHS Security Version 2.0, dated 14 March 2005 [11]
Conformance Result	Part 2 extended, 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 15 October 2003
Version of CEM	CEM Version 1.0 [5], [6], and all applicable

Evaluation Identifiers for Nexor MMHS Security	
	International Interpretations effective on 15 October 2003
Sponsor	Nexor Ltd. Nottingham Science and Technology Park University Boulevard Nottingham NG7 2RL United Kingdom
Developer	Nexor Ltd. Nottingham Science and Technology Park University Boulevard Nottingham NG7 2RL United Kingdom
Evaluator(s)	**Science Applications International Corporation** Terrie Diaz Shukrat Abbas
Validator(s)	**NIAP CCEVS** Dr. Jerome Myers

3 Security Policy

The TOE implements the following security policies.

3.1 Communications Policy

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

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

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

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

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

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

3.2 User Data Protection Policy

The TSF ensures that messages can only be sent at a classification level the user is authorized to send messages at. The TSF ensures that messages can only be sent to users authorized to read messages of the classification being sent to them. The TSF ensures that messages can be sent from an originator to a recipient only if the clearance of the recipient is greater than or equal to the message security label and the originator is authorized to send messages to the recipient. The TSF uses external libraries (Secure Message Protocol (SMP) Libraries) to perform label comparisons. In other words, the TSF relies upon libraries in the IT Environment to make access decision recommendations and the TSF then implements its access controls based upon those recommendations.

The available classification labels that can be used by the TSF are derived from the Security Policy Information Files (SPIFs), which can be defined and modified by TOE administrators. SPIFs are ASN.1 encoded objects that are signed for integrity. The SPIF provides details about the security classifications and categories that are appropriate for the security policy. It also defines the relationship between classification and categories and between categories themselves e.g. if EYES ONLY category is chosen, the classification must be RESTRICTED. The SPIF also holds information about how a security label should be displayed.

3.3 Identification and Authentication Policy

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

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

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

3.4 Management Policy

The TSF implements a policy that regulates the management of TSF data. The TSF implements several roles and ensures that the below functionality is restricted to the following roles:

1) The authorized administrator is a user who can perform the administrative task of modifying security attributes upon which the following decision is made: sending of messages. An individual is identified as an authorized administrator by being configured as an Authorized Signer. An Authorized Signer is an individual having the authority to specify a security label for a message and sign messages upon submission.
2) The authorized user is an identified and authenticated user who has been granted authorization to read messages. An individual is identified as an authorized user by being configured as an Authorized Reader. An Authorized Reader is an individual having the authority to read signed and encrypted email messages sent to the role of which they are an authorized reader. An individual can also be identified as an authorized user by being configured as an Alternate or a Role Occupant. An Alternate can be forwarded secure messages when the message is not read within a given time period. A Role Occupant can be sent an alert if a message is delivered into a mailbox that no one is currently logged into.

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

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The evaluation made a set of assumptions concerning the product usage that characterize the physical protection of the system as well as the training and behavior of system administrators and users. The following is a listing of those usage assumptions stated in the ST.

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

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

4.2 Clarification of Scope

Nexor MMHS Security is intended to be used as a set of components in a message handling system. There are other components required to securely handle messages. The evaluated TOE components are add-on packages to Microsoft Outlook 2000, Windows Explorer, and Microsoft Exchange 2000. Those Microsoft products are not within the scope of the TOE. Similarly, the underlying hardware and operating system platforms (Microsoft Windows 2000 Professional and Microsoft Windows 2000 Advanced Server) are not included in the evaluation. Moreover, the TOE relies upon services in the IT environment to perform some of its security functions. Namely, the following products are required to be in the IT Environment:

- Nexor Directory
- A Certificate Authority
- DigitalNet Secure Message Protocol (SMP) Libraries:
    1. S/Mime Freeware Library
    2. Certificate Management Library
    3. Access Control Library

Those products are also not within the scope of the TOE.

The evaluation of this TOE is not directly tied to possible evaluations of any of those other components in a message handling system. In particular, the evaluation of this TOE does not imply that all of the properties required of the Nexor MMHS Security 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 TOE is the set of Nexor Products that includes the Nexor Defender for Outlook component with the S/MIME Security component, the Nexor Directory Administrator with the Strong Authentication component and the Nexor Overseer with the Nexor Security Server component. The set of Nexor products that comprise the TOE are a set of software applications. The Nexor Overseer with the Nexor Security Server component is installed on a server node (the Microsoft Windows 2000 Advanced Server) where mailboxes will be monitored to ensure the timely processing of received messages. The Nexor Defender for Outlook with the S/MIME Security component and the Nexor Directory Administrator with the Strong Authentication components are installed on a workstation node (the Microsoft Windows 2000 Professional) where a user will send and receive messages, and browse and modify the directory.

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

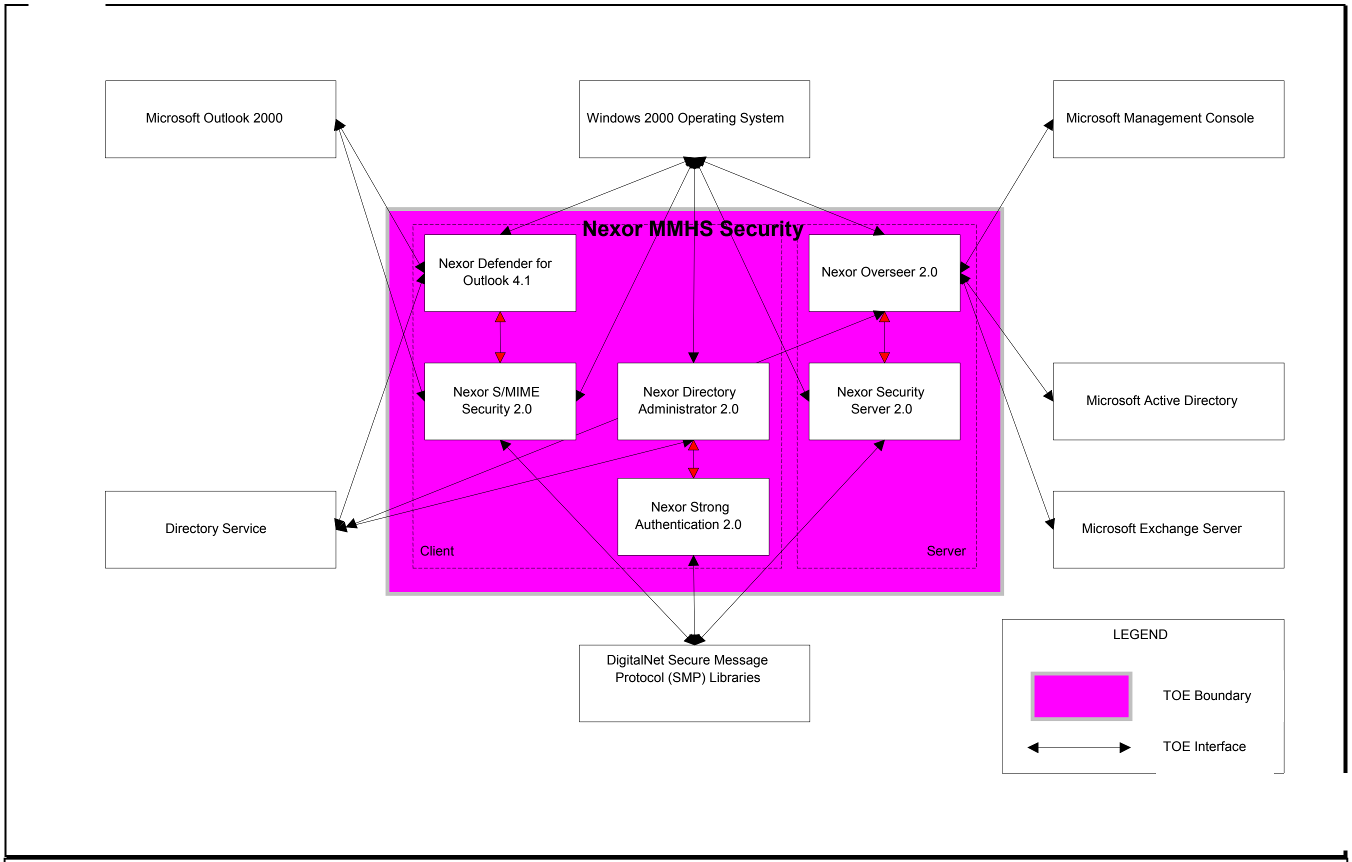
Microsoft Outlook 2000
Windows 2000 Operating System
Microsoft Management Console
Nexor MMHS Security
Nexor Defender for Outlook 4.1
Nexor Overseer 2.0
Nexor S/MIME Security 2.0
Nexor Directory Administrator 2.0
Nexor Security Server 2.0
Microsoft Active Directory
Directory Service
Nexor Strong Authentication 2.0
Client
Server
Microsoft Exchange Server
DigitalNet Secure Message Protocol (SMP) Libraries
LEGEND
TOE Boundary
TOE Interface

Figure 1: TOE Boundary

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

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

- Nexor Directory - used by all of the Nexor components primarily to obtain addressing and security information.
- Certificate Authority (CA) - is used to publish the security objects into the directory for use by the Nexor components to ensure the security of various pieces of data.
- DigitalNet Secure Message Protocol (SMP) Libraries – is used to provide the following services:
    - S/MIME Freeware Library – digital signatures, encryption, decryption, message labeling

- Certificate Management Library – certificate validation, authentication of users
- Access Control Library – provides an Access Control Decision Function that determines if a subject's clearance allows the subject to access data at a given label.

6 Delivery and Documentation

The TOE is purchased as a single item that is delivered on a single CD accompanied by some hardcopy documentation. The printed label on the CD explicitly identifies the versions of each of the software components of the TOE. The distribution media for the evaluated version of Nexor MMHS Security bears the specific version and patch identifiers for each of the components listed in Table 2.

Table 2: TOE Identifiers

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

The delivery CD also contains softcopy of all of the documentation necessary for the correct installation and operation of the TOE. More precisely, the following product documentation is provided in softcopy on the CD:

Title/Description	Order No.	
Nexor Defender for Outlook 4.1 Administrator Guide	NEX0757MAN05	June 2002
Nexor Defender for Outlook 4.1 User Guide	NEX0758MAN04	June 2002
Nexor S/MIME Security Administrator's Guide	NEX0647MAN04	May 2004
Nexor S/MIME Security User's Guide	NEX0648MAN05	May 2004
Nexor Directory Administrator 2.0	NEX0689MAN07	May 2002
Nexor Overseer 2.0 Administrator Guide	NEX0840MAN08	May 2002

Installing and Configuring Nexor MMHS Security February 2005	NEX1653ENG04	
Release Notes	NEX1267MAN10-2	February 2005

The only printed materials that are delivered with the product distribution are a software registration form with associated instructions, a software evaluation agreement, and a printed copy of the "Release Notes". The registration form and software evaluation agreement must be sent back to Nexor before the installer will be provided with the necessary information (which consists of a product key) to complete the product installation. The registration process includes the identification of network specific configuration information that binds the product to the installed configuration.

7 IT Product Testing

7.1 Developer Testing

The developer maintains a suite of tests for confirming that the Nexor MMHS Security product meets its advertised functional requirements. Nexor maintains test documentation that describes how each of the TOE security functions is tested including a test plan, test procedures, expected results and the actual results of applying the tests. The basic test configuration that is used by Nexor is similar to the one described in the following section for the testing that was performed by the evaluation team.

Nexor's approach to security testing is security function based. Essentially, Nexor developed a set of test cases that correspond to a security function. Each test case targets the specific security behavior associated with that security function. The test procedures are designed to be exercised by performing the manual steps that has been designed to test the applicable security function described in the test scenarios. All of the test cases are manual test and the actual results provided indicate a "Pass".

The evaluators were provided with the complete set of test documentation. The evaluators checked that each of the test cases supported the security functions to which it was mapped and that the expected test results matched the actual test results. The Evaluators determined that the "Pass" meant that the expected results where achieved and the TOE behaved as expected.

7.2 Evaluator Testing

CCTL evaluation team testing was conducted at the CCTL facility in Columbia, MD during the first week of February 2005. During testing the evaluators performed the following actions:

1. Execution of all of the developer's functional tests
2. Independent Testing
3. Vulnerability Testing (AVA_VLA.1)

The evaluation team executed the entire set of vendor test procedures per the evaluated configuration as described in the Nexor MMHS Security Test Suites document. The test configuration is illustrated in Figure 2.

The testing environment consisted of a single laptop PC running Windows 2000 Professional SP4 and the VMWare software, Version 4.0.1 that allowed multiple virtual machines to be simultaneously hosted on the same hardware. In addition, a card reader is also used to provide access to security tokens.

Three virtual machines were hosted on the testing hardware:

- Two running the products under test and associated components ("TOE1", "TOE2")
- One providing the infrastructure components required for testing ("Support")

The operating system for the "TOE1" and "Support" components was Windows 2000 Professional SP2 English and the operating system for the "TOE2" platform was Windows 2000 Server SP2 English

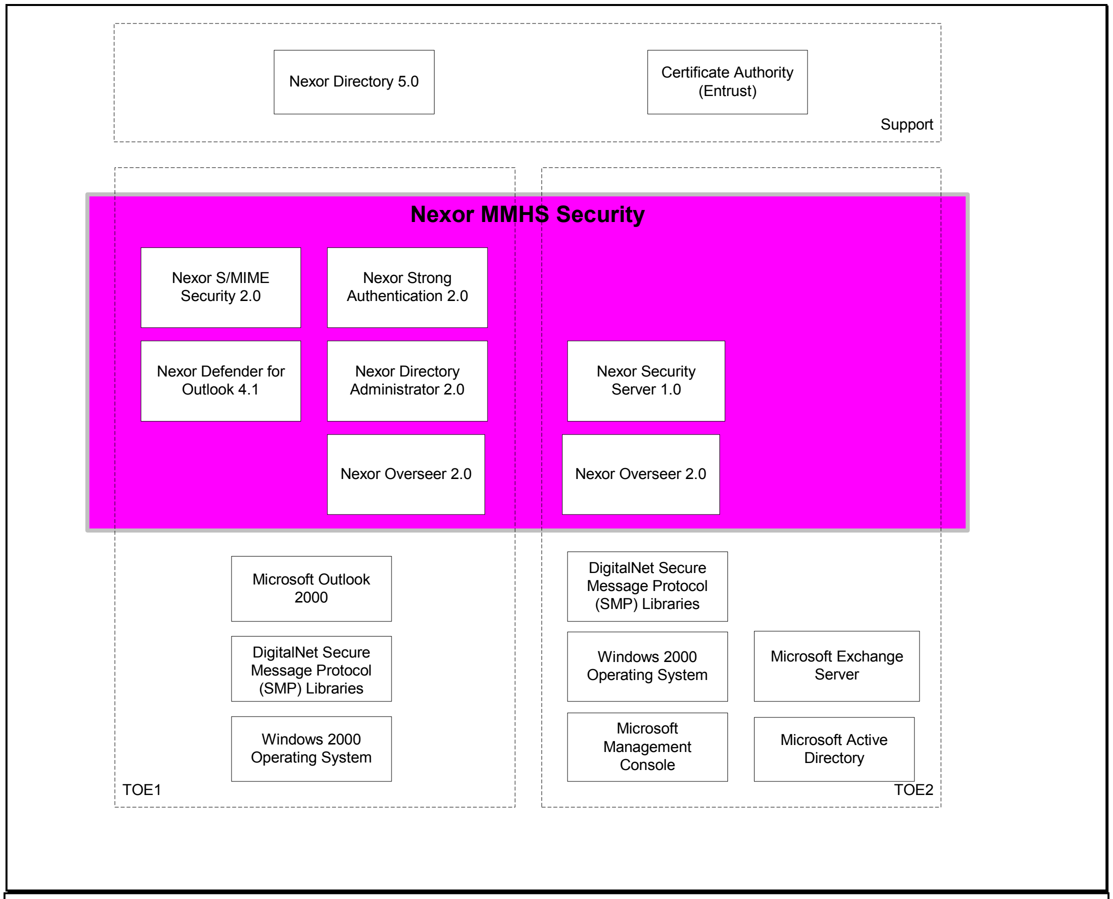
Nexor Directory 5.0
Certificate Authority (Entrust)
Support
Nexor MMHS Security
Nexor S/MIME Security 2.0
Nexor Strong Authentication 2.0
Nexor Defender for Outlook 4.1
Nexor Directory Administrator 2.0
Nexor Security Server 1.0
Nexor Overseer 2.0
Nexor Overseer 2.0
Microsoft Outlook 2000
DigitalNet Secure Message Protocol (SMP) Libraries
Windows 2000 Operating System
DigitalNet Secure Message Protocol (SMP) Libraries
Windows 2000 Operating System
Microsoft Exchange Server
Microsoft Management Console
Microsoft Active Directory
TOE1
TOE2

Figure 2: Logical Machines/Components for Test

The following software items were installed on the respective virtual machines:

Machine	Third Party Product	Nexor Product
TOE1	Outlook 2000 SR1	Nexor Defender for Outlook4.1 Nexor S/MIME Security 2.0 Nexor Directory Administrator 2.0 Nexor Strong Authentication 2.0
TOE2	Exchange Server 2000Active Directory	Nexor Overseer 2.0 Nexor Security Server 2.0
Support	Entrust CA 6.0	Nexor Directory 5.0

In addition, the following patches were installed:

Product	Service Packs(s) or Patch(es) Required
VMWare 4.0.1	None
Window 2000 Advanced Server	Service Pack 2
Windows 2000 Professional	Service Pack 2
Exchange Server 2000	Service Pack 2
Outlook 2000	Service Pack 2
Entrust CA 6.0	None
Nexor Defender for Outlook 4.1	4
Nexor S/MIME Security 2.0	3
Nexor Directory Administrator 2.0	2
Nexor Strong Authentication 2.0	None
Nexor Overseer 2.0	2
Nexor Security Server 1.0	3
Nexor Directory 5.0	Patch 1

The evaluation team performed all of the installation, setup, testing, and test result analysis. Vendor representatives were available to answer questions. The evaluators' testing included all of the tests found in the developer test plan and procedures. During the evaluation of the vendor supplied test documentation, the evaluators identified some supplemental testing that was needed to better test the security functionality. The evaluators devised additional tests to augment and supplement the vendor tests.

Finally, the evaluators performed tests for hypothesized vulnerabilities. The CCTL evaluation team determined that the vendor's own vulnerability analysis was thorough and appropriately tested. As a result, there were only a few additional vulnerabilities hypothesized and tested by the CCTL evaluators.

The end result of the CCTL testing activities on the evaluated product was that all tests gave expected (correct) results. The final evaluator testing did not reveal any residual problems with the TOE. The testing found that the product was implemented as described in the functional specification. The CCTL evaluation team tests and penetration tests substantiated the security functional requirements claimed in the Security Target.

8 Evaluated Configuration

The specific identifiers for the TOE are provided in Table 2: TOE Identifiers~~Table 2: TOE Identifiers~~ on page 5.

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

8.1 Physical Boundaries

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

8.2 Logical Boundaries

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

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

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

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

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

A more detailed description of the dependence upon the IT Environment for the implementation of the functions is included in Section 4 of this report where the security policies associated with each of these security functions is explained.

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 International Interpretations in effect on 15 October 2003.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance. 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 Evaluation Technical Report (ETR) for Nexor MMHS Security, Version 2.0 14 March 2005 [10]* contain the verdicts of "PASS" for all the work units.

The evaluation determined the product to be conformant with Part 2 extended and, as well, meeting the requirements for Part 3, and EAL 2. The details of the evaluation are recorded in the proprietary Evaluation Technical Report (ETR), [10] which are controlled by SAIC.

10 Validator Comments

When discussing the security features provided by a secure messaging system, one would commonly expect to see some support for a non-bypassable reference validation mechanism, requirements for TOE self-protection, and some support for audit. The ST for the TOE does not discuss the absence of those types of SFRs. The add-on characteristics of the TOE components and the strong dependencies upon the TOE environment for any necessary protection of the TOE implies that the bulk of any such omitted security features would be provided by the IT Environment and the TOE would have at most a minor role in supporting the requirements. Hence it is appropriate that those requirements were not discussed in the ST. The absence of these requirements from the TOE should not be interpreted as a statement that they are not supported by the TOE. However, the results of this evaluation will not assist a system integrator in determining whether those security requirements can be met by the overall integrated messaging system.

All other validator comments regarding this evaluated product are already captured in the "Clarification of Scope: section of this report on page 9.

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

11 Security Target

The Security Target, "Nexor MMHS Security Security Target, Version 1.0, dated 23 February 2005" [9] is included here by reference.

12 Glossary

12.1 Definition of Acronyms

ACL	Access Control Library
ASN.1	Abstract Syntax Notation One
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
CM	Configuration Management
DN	Distinguished Name
DSA	Directory System Agent
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
MMHS	Military Message Handling System
NIAP	National Information Assurance Program
NIST	National Institute of Science & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OR	Observation Report
PP	Protection Profile
SAIC	Science Applications International Corporation
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy

SFR	Security Functional Requirements
SMP	Secure Message Protocol
SOF	Strength of Function
SPIF	Security Policy Information File
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

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] Nexor MMHS Security Security Target, Version 1.0, dated 23 February 2005

[10] Evaluation Technical Report (ETR) for Nexor MMHS Security, Version 2.0, dated 14 March 2005