National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Mobile Armor DataArmor & PolicyServer V3.1

Report Number: CCEVS-VR-VID10259-2011
Dated: 31 January 2011
Version: 0.4

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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Ken Eggers
John Nilles

Common Criteria Testing Laboratory

SAIC, Inc.
Columbia, Maryland

Table of Contents

List of Tables

1 Executive Summary

This document is intended to assist the end-user of this product with determining the suitability of the product in their environment. End-users should review both the Security Target (ST) which is where specific security claims are made, and this Validation Report (VR) which describes how those security claims were evaluated.

This report documents the NIAP validators' assessment of the evaluation of Mobile Armor PolicyServer 3.1 (version 3.1.0.445) and Mobile Armor DataArmor 3.1. It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The evaluation of **Mobile Armor DataArmor & PolicyServer V3.1** was performed by SAIC, in the United States and was completed in April 2010. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the Mobile Armor DataArmor & PolicyServer V3.1 TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 2. The evaluation methodology used by the evaluation team to conduct the evaluation was available in the Common Methodology for Information Technology Security Evaluation versions 3.1, revision 2.

Science Applications International Corporation (SAIC) determined that the product satisfies evaluation assurance level (EAL) 4 augmented with ALC_FLR.3 as defined within the Common Criteria (CC). The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the Mobile Armor DataArmor & PolicyServer V3.1 Security Target, Version 1.72, 2 April 2010.

This Validation Report applies only to the specific version of the TOE as evaluated. In this case the TOE is a collection of software applications as follows:

- Mobile Armor DataArmor 3.1 (Version 3.1.0 for Windows, Version 3.1.0.594 for Linux, Version 3.1.0.8 for Mobile Device, and Version 3.1.0.788 for the Mac)
- Mobile Armor PolicyServer 3.1 (Version 3.1.0.445)

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence.

The validation team examined evaluation evidence and reviewed individual work units and versions of the ETR. At discrete points during the evaluation, validators formed a Validation Oversight Review panel in order to review the Security Target and other evaluation evidence materials along with the corresponding evaluation findings in detail. The validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Final Evaluation Technical Report for the Mobile Armor DataArmor & PolicyServer 3.1 Parts I and II and the associated test report produced by SAIC.

1.1 Evaluation Details

Evaluated Product:	Mobile Armor PolicyServer 3.1 (Version 3.1.0.445) and Mobile Armor DataArmor 3.1 (Version 3.1.0 for Windows, Version 3.1.0.594 for Linux, Version 3.1.0.8 for Mobile Device, and Version 3.1.0.788 for the Mac)
Sponsor & Developer:	Mobile Armor, Inc 400 South Woods Mill Road Suite 300 St. Louis, MO, 63017 USA
CCTL:	Science Applications International Corporation Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date:	May 2010
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007
Interpretations:	There were no applicable interpretations used for this evaluation.
CEM:	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 2, September 2007
PP:	None
Evaluation Class:	Evaluation Assurance Level (EAL) 4 augmented with ALC_FLR.3
Description	The evaluated combination of Mobile Armor DataArmor 3.1 and Mobile Armor PolicyServer 3.1 products represents a client/server-based full volume disk encryption solution for both personal computers and mobile devices.
Disclaimer	The information contained in this Validation Report is not an endorsement of the Mobile Armor PolicyServer 3.1 and DataArmor 3.1 product by any agency of the U.S. Government and no warranty of Mobile Armor PolicyServer 3.1 or DataArmor 3.1 is either expressed or implied.

Evaluation Personnel: James Arnold
Katie Sykes
Quang Trinh

Validation Team: Ken Eggers
John Nilles

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. Note that assurance requirements outside the scope of EAL 1 through EAL 4 are addressed at the discretion of the CCEVS.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring 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's Validated Products List.

The following table serves to identify the evaluated Security Target and TOE.

Table 1 ST and TOE identification

ST Title:	Mobile Armor DataArmor & PolicyServer v3.1 Security Target, Version 1.72, 2 April 2010
TOE Identification:	Mobile Armor PolicyServer 3.1 (Version 3.1.0.445) and Mobile Armor DataArmor 3.1 (Version 3.1.0 for Windows, Version 3.1.0.594 for Linux, Version 3.1.0.8 for Mobile Device, and Version 3.1.0.788 for the Mac)
Operating Platform:	• PolicyServer o Operating systems ▪ For the PolicyServer Service • Microsoft Windows Server 2003 SP1+, Standard or Enterprise Editions ▪ For the PolicyServer Management console • Microsoft Windows 2000 Professional SP4 • Microsoft Windows XP or XP Tablet Edition SP3 • Microsoft Windows Vista SP1 • Microsoft Report Viewer 2005 o Database ▪ Microsoft SQL Server 2005 with Service Pack 2+ o External Mail Server

	• DataArmor PC platforms
	  ○ Microsoft Windows 2000 Professional SP4
	  ○ Microsoft Windows XP or XP Tablet Edition SP3
	  ○ Microsoft Windows Vista SP1
	  ○ Red Hat Enterprise Linux 5 (kernel 2.6.18-92)
	  ○ SUSE Linux Enterprise Desktop 10 (kernel 2.6.16.60-0.21)
	  ○ Intel-based Mac OS X 10.5
	• DataArmor mobile device platforms
	  ○ Microsoft Windows Mobile 6.0
	• Optional Authentication servers (for external authentication integration):
	  ○ Microsoft Active Directory
	  ○ OCSP Responder Server (such as Tumbleweed Valicert Validation Authority or Windows Server 2008)

3 Threats to Security

The following are the threats that the evaluated product addresses:

3.1 TOE Threats

T.ACCOUNTABILITY	A user may not be held accountable for their actions.
T.ADMIN_ERROR	An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.MASQUERADE	An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources.
T.SUBVERT	A malicious user may cause non-configuration data at rest to be inappropriately accessed (viewed, modified or deleted).
T.TSF_COMPROMISE	A malicious user may cause configuration data to be inappropriately accessed (viewed, modified or deleted).
T.UNAUTH_ACCESS	A user may gain unauthorized access (view, modify, delete) to configuration data.

4 Assumptions & Clarifications of Scope

The following assumptions are identified in the Security Target:

4.1 Physical Assumptions

The following physical assumptions are identified in the Security Target.

A.LOCATE	The server portion of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

4.2 Personnel Assumptions

The following personnel assumptions are identified in the Security Target.

A.NO_EVIL_USER	Users of the TOE are properly trained in the use of the TOE and will cooperate with those responsible for administration in maintaining TOE security.

4.3 Intended Use Assumptions

The following intended use assumptions are identified in the Security Target.

A.NO_EVIL	The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation.
A.DEVICE_USE	Users of the TOE will follow policies to prevent unauthorized physical access to a TOE-protected device.
A.REPORTS	Administrators who need to generate print or export the audit trail, or view generated reports, will have the proper environment.

4.4 Clarifications of Scope

While the product supports off-line mode for DataArmor product, the evaluation covered only on-line cases.

5 Security Functions

This section summarizes the security functions provided by the TOE, as documented by the Security Target.

5.1 Security Audit

The TOE generates audit records for actions taken in DataArmor and the PolicyServer. The management console provides a way to restrict access to the audit records to authorized administrators. The OS is relied on to provide reliable time stamps for use in audit records. On PC clients it is expected that the OS will properly set the BIOS hardware clock and utilize that time as accurate since the OS is not available before authentication.

The audit records that are taken can be divided into three broad categories: authentication actions, management actions and status messages. Authentication logs cover all attempts to login to the client or server, and record success and failure, as well as conditions such as locking the device or user. Management actions cover all actions taken on the PolicyServer (managing users, policies, etc) as well as those actions taken through the DataArmor recovery console. Status messages cover events such as the startup and shutdown of functions which can provide audit records, failure messages related to TOE functions (such as a client not being able to contact the server), and encryption status.

Audit records recorded on the client are stored there until a connection is made with the PolicyServer at which time they are sent to the PolicyServer for central storage (they will be stored in the PolicyServer log database). While stored on the client, the audit records are stored in a secure DADB and protected against tampering. The clients are capable of storing at least 4000 log messages before wrapping will occur and the oldest messages will be lost (a first in-first out system). Audit records generated on the PolicyServer are stored directly into the PolicyServer log database.

The PolicyServer provides tamper detection for audit records once they have been stored in the PolicyServer log database, but relies on the TOE environment to prevent the actual tampering.

The PolicyServer provides an alert notification system via email to notify administrators of potential security violations. The DataArmor login will notify authenticated users of potential security violations on systems where they login.

5.2 Cryptographic Support

The TOE provides its own FIPS-validated cryptographic module which performs symmetric encryption and decryption operations on cryptographic keys, storage media, and data or commands sent over a network. AES algorithm is used for this encryption. Additional algorithms are also supported for random number generation and various hashing functions. All algorithms are FIPS-validated.

5.3 User Data Protection

The TOE provides the ability to restrict access to any data and the services that may be provided by that data (such as an OS) on a supported device. All users are subject to the Data Access Control Policy where data access is controlled by the TOE.

5.4 Identification and Authentication

The TOE requires users to be identified and authenticated before access is allowed to protected data. Administrators can choose from several different authentication mechanisms based on the needs of the organization, including the ability to link to external authentication services.

5.5 Security Management

The TOE provides the ability to manage users and groups, encryption settings, and authentication server settings. The TOE provides five levels of authority: Enterprise Administrator, Enterprise Authenticator, Group Administrator, Group Authenticator and User. Administrators and Authenticators have access to the management console and the DAOS recovery console, with their access being determined by where their authority is granted in the hierarchy. Users only have the ability to login to DataArmor clients.

5.6 Protection of the TSF

For the DataArmor component, the TOE provides pre-access authentication components (DAOS) and filter driver components. Configuring bootstrap information ensures that TOE interfaces cannot be bypassed. When the TOE starts, it performs several tests to ensure it is properly functioning and that security has not been compromised. Once the OS has started, DataArmor relies on the secure execution environment of the OS to provide protection for the filter driver.

For the PolicyServer component, the TOE relies on the operating system to restrict access to its software as well as the database where the TOE information is stored.

The TOE encrypts its communication between DataArmor and the PolicyServer by encrypting and decrypting SOAP messages sent and received using HTTP. Commands sent by the PolicyServer to mobile devices using SMS or email are encrypted uniquely for the device receiving the command.

5.7 Resource Utilization

The TOE client, DataArmor is able to maintain and ensure the proper application of its existing policies even when communications are unavailable.

5.8 TOE Access

The TOE can provide a login banner to all users accessing DataArmor as well as all authorized administrators accessing the management console.

5.9 Trusted Path/Channels

The TOE provides a method of establishing a trusted session with the user for authentication through a restart of the DataArmor-protected device.

6 Architectural Information

The TOE can be described in terms of the following components:

- Mobile Armor DataArmor client – Provides encryption and enforcement of authentication decisions implemented within the TOE. Includes pre-operating system DAOS and data encryption components.
- Mobile Armor PolicyServer – Provides administrative interfaces that can be used to manage DataArmor encryption and authentication policy functions. The administrative PolicyServer interface implemented as a Microsoft Management Console (MMC) "snap-in", which displays PolicyServer GUI components within a MMC GUI window pane called a "console".

Figure 1 below illustrates the TOE as it can be deployed in a customer environment. The pieces in the configuration are color coded to illustrate the different components and how they relate to the TOE. The red box indicates DataArmor clients. The blue box indicates PolicyServer components, including both the server pieces and the management client. The orange box indicates external services which are required for the evaluated configuration, in this case an Email server and the DBMS. The green boxes indicate optional services which can be connected to the system, but which are not required.

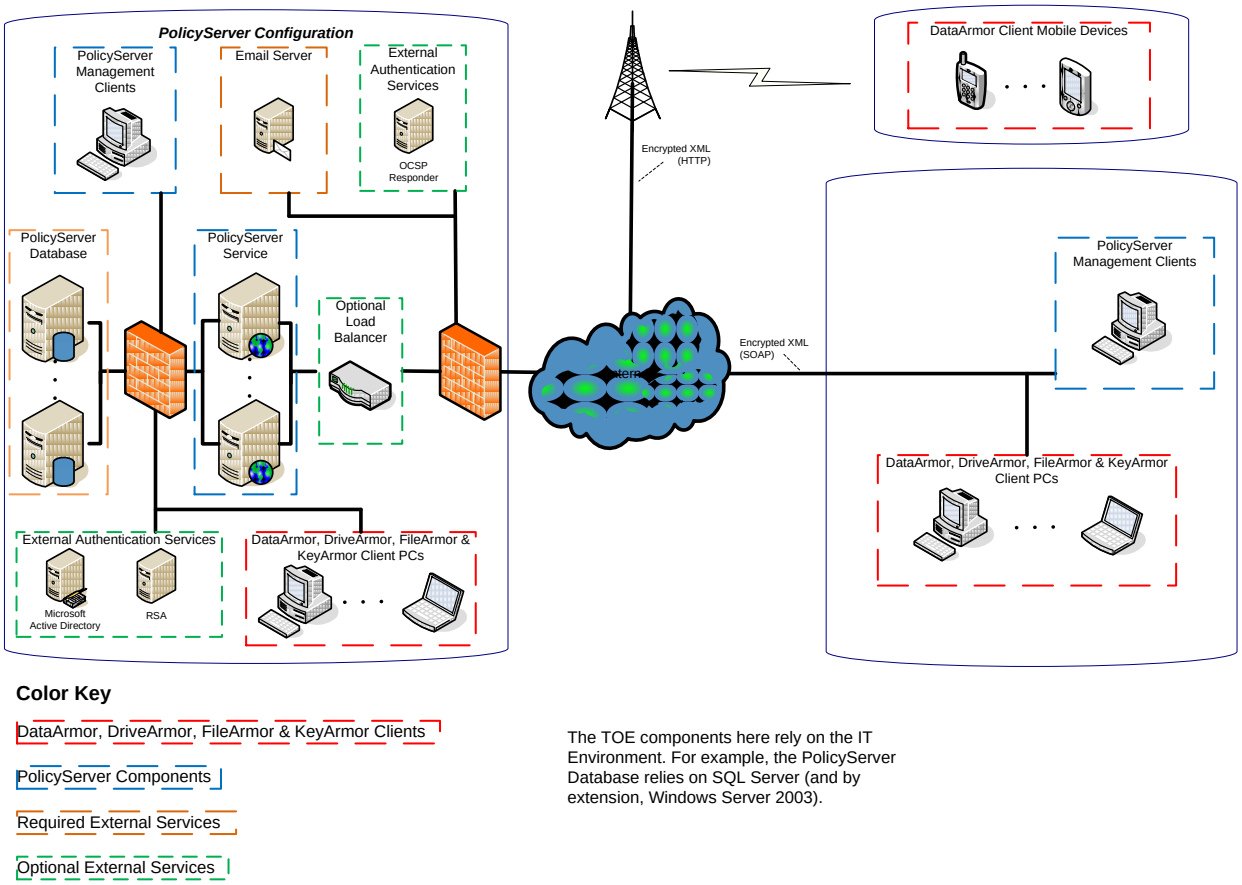

Figure 1 - Mobile Armor Solution Architecture

The intended environment of the TOE is dependent on the piece of the TOE being described.

The DataArmor portion of the intended environment can be described in terms of the following components:

- Operating systems – Provides runtime environment for DataArmor application components.
- OCSP Responder Server – Provides optional external authentication services for DataArmor for direct verification of smart card certificate status.

The PolicyServer portion of the intended environment can be described in terms of the following components:

- Operating systems – Provides runtime environment PolicyServer application components. Provides operating system GUI interfaces for PolicyServer. Provides web server for interface between PolicyServer and clients.
- Database – Provides storage for PolicyServer policy and log databases.
- Mail Server – Provides SMTP server for use in email alert configuration.
- Authentication servers – Provides optional external authentication services for DataArmor users by proxy through the PolicyServer.
- Load Balancer – Provides optional scalability by allowing multiple PolicyServers to be configured together as one.

6.1 Physical Boundaries

The TOE is a software product, and as such the physical boundary of the TOE is defined as the files and information stored on the device where it is installed. The TOE functions are implemented uniformly across all supported OS platforms.

The following software packages are considered to be the TOE:

- PolicyServer Service
- PolicyServer Database (the database created in SQL Server)
- PolicyServer Management Console
- Active Directory Plug-in
- DataArmor for PC on the platforms listed below
- DataArmor for Windows Mobile on the platforms listed below

Any other products which may be attached to this configuration are not considered part of the evaluated configuration.

The operational environment of TOE depends on the following:

- PolicyServer
    - Operating systems
        - For the PolicyServer Service
            - Microsoft Windows Server 2003 SP1+, Standard or Enterprise Editions

        - For the PolicyServer Management console
            - Microsoft Windows 2000 Professional SP4
            - Microsoft Windows XP or XP Tablet Edition SP3
            - Microsoft Windows Vista SP1
            - Microsoft Report Viewer 2005
    - Database
        - Microsoft SQL Server 2005 with Service Pack 2+
    - External Mail Server
- DataArmor PC platforms
    - Microsoft Windows 2000 Professional SP4
    - Microsoft Windows XP or XP Tablet Edition SP3
    - Microsoft Windows Vista SP1
    - Red Hat Enterprise Linux 5 (kernel 2.6.18-92)
    - SUSE Linux Enterprise Desktop 10 (kernel 2.6.16.60-0.21)
    - Intel-based Mac OS X 10.5
- DataArmor mobile device platforms
    - Microsoft Windows Mobile 6.0
- Optionally - Authentication servers (for external authentication integration):
    - Microsoft Active Directory
    - OCSP Responder Server (such as Tumbleweed Valicert Validation Authority or Windows Server 2008)

Please refer to the Security Target for more technical details about the product and its associated security claims.

7 Documentation

Following is a summary of documents received by the TOE user. These documents were reviewed during the evaluation.

- Mobile Armor v3.1 Certification Guide FIPS 140 and Common Criteria, Document ID Number: CG-31-09 2009
- PolicyServer v3.1 Administration Guide, Document ID Number: PSAG-31-01, 2010
- PolicyServer v3.1 Appendices, Document ID Number: PSA-31-09, 2009
- PolicyServer v3.1 Installation Guide, Document ID Number: PSIG-31-01, 2010
- DataArmor v3.1 for PCs Administration Guide, Document ID Number: DAPCAG-31-09, 2009
- DataArmor v3.1 for PCs Installation Guide, Document ID Number: DAPCIG-31-09, 2009
- DataArmor v3.1 for PCs User Guide, Document ID Number: DAPCUG-31-09, 2009
- DataArmor v3.1 for Windows Mobile Installation Guide, Document ID Number: DAWMIG-31-09, 2009
- DataArmor v3.1 for Windows Mobile User Guide, Document ID Number: DAWMUG-31-09, 2009
- Mobile Armor PolicyServer & DataArmor product verification (Mobile Armor v3.1 Product MD5 check.pdf)

8 IT Product Testing

The purpose of this activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST for an EAL4+ evaluation.

8.1 Developer Testing

The developer created test procedures specifically to fulfill the test requirements for an EAL4+ evaluation. The tests were developed to provide good coverage of the security functions related to each of the security requirements in the Security Target. The developer has documented their tests in a test plan where the results of the tests are presented as prose conclusions, notes, and summaries for each of the applicable test platforms.

8.2 Independent Testing

Independent testing took place in two phases.

During the initial phase, the evaluators went to the developer's facility and exercised a subset of the developers test plan on equipment available within the developer's testing laboratory. This effort involved installing and configuring both the DataArmor and PolicyServer products on a representative subset of the supported operating systems (note that only the PC version of DataArmor was tested during the initial phase). Subsequently, the evaluators exercised a subset of the available developer's test procedures for both the DataArmor (for PCs) and PolicyServer products. The subset of tests was selected in order to ensure that each of the claimed security functions was meaningfully sampled.

Also during the initial phase, the evaluators devised independent tests to ensure that all claimed audit events were generated appropriately and also to ensure that all of the claimed security

management functions worked as described in the design documentation (and as summarized in the ST). The evaluators also examined product source code while on-site primarily to ensure that aspects of the cryptographic mechanisms were implemented in accordance with the design documentation and security claims.

The second phase of testing occurred at the evaluator's test facility. The developer provided access to an Internet-accessible PolicyServer and also provided a PolicyServer installed within a virtual machine environment. These were used in conjunction with a mobile device and Mac provided by the developer for further testing. The mobile device and Mac were subjected to evaluator testing using a representative subset of developer tests and additional independently devices tests.

In addition to the use of developer provided and independently devised security functional tests, the developers also explore the possibility to penetrate or bypass the security mechanisms. Much of this work was based on analysis of the design, source code, and actual configuration information derived from the installed and configured products. However, the evaluators also devised some tests including scans of the installed products, examination of actual network traffic between the client and server products, and also full volume scans of the encrypted media in order to ensure that there were no obvious vulnerabilities.

Given the complete set of test results from test procedures exercised by the developer and the sample of tests directly exercised by the evaluators, the testing requirements for EAL4+ are fulfilled.

9 Evaluated Configuration

The TOE is one or more Mobile Armor DataArmor 3.1 (Version 3.1.0 for Windows, Version 3.1.0.594 for Linux, Version 3.1.0.8 for Mobile Device, and Version 3.1.0.788 for the Mac) products installed in conjunction with a Mobile Armor PolicyServer 3.1 (Version 3.1.0.445) product. Each of these products can be installed on or with the products identified in section 6.1 above.

10 Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the CC, the CEM, and the CCEVS.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL4+ assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing notes, comments, or vendor actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. 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. Verdicts were not assigned to assurance classes.

Section 5, Results of Evaluation, in the Evaluation Team's ETR, Part I, states:

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary part of the ETR (see Chapter 15).

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 3.1 and CEM version 3.1. The evaluation determined the TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level (EAL 4) requirements, augmented with ALC_FLR.3. The rationale supporting each CEM work unit verdict is recorded in the "Evaluation Technical Report for the Mobile Armor DataArmor & PolicyServer V3.1 Part 2" which is considered proprietary.

Section 6, Conclusions, in the Evaluation Team's ETR, Part 1, states:

Section 6.1, ST Evaluation: "Each verdict for each CEM work unit in the ASE ETR is a 'PASS'. Therefore, the ST is a CC compliant ST."

Section 6.2, TOE Evaluation: "The verdicts for each CEM work unit in the ETR sections included in the proprietary part of the ETR (see Chapter 15) are each 'PASS'. Therefore, the TOE (see below product identification) satisfies the Security Target, when configured according to the following guidance documentation:

- Mobile Armor™ DataArmor™ v3.1
- Mobile Armor™ PolicyServer™ v3.1
- PolicyServer™ v3.1 Administration Guide
- PolicyServer™ v3.1 Installation Guide
- PolicyServer™ v3.1 Administration Appendices
- DataArmor™ v3.1 PC Installation Guide
- DataArmor™ v3.1 PC User Guide
- DataArmor™ v3.1 PC Administration Guide
- DataArmor™ v3.1 Windows Mobile Installation Guide
- DataArmor™ v3.1 Windows Mobile User Guide
- Mobile Armor™ Certification Guide"

11 Validator Comments/Recommendations

1. The default TOE configuration does not satisfy DoD Standard 8500.2 requirements. For example, while the password requirement can be changed by a product administrator, the product requires fixed passwords with a minimum length of only 6 characters by default. TOE users required to comply with DOD STD 8500.2 must ensure that the TOE and all external servers/services are configured in accordance with DOD requirements.

2. The TOE stores critical data (audit logs and cryptographic key material) in an external Microsoft SQL Server 2005 database. This DBMS is required for correct TOE operation but has been excluded from TOE analysis and testing. The DBMS presents local and network interfaces which allow access to critical data and bypass some TOE protections. To ensure the integrity of this data, all database security patches and service packs must be installed and the database server must be physically and/or electronically segregated such that it is accessible to only database administrators who are trusted at the same level as those that administer the TOE.
3. The mechanism used to notify administrators that the Policy Server product may have exhausted its available storage space for audit records is a Windows event log. As such, there is no prominent or obvious warning to an administrator other than the likely malfunctioning of this and other applications due to a lack of disk space. As such, it is recommended that user consider finding alternate solutions to become aware of imminent disk space exhaustion (e.g., Windows notifications).
4. There are a number of security claims that are dependent upon the interaction and support of a Policy Server used in conjunction with a DataArmor products. As the evaluation covers only the specific version of the product identified in the Security Target and the mechanism for delivery of updates from a Policy Server were not evaluated, updates to the product, especially those potentially made available via the Policy Server, should be analyzed in a benign environment prior to use and only installed when required to patch or mitigate security vulnerabilities or correct flaws in functionality that is operationally required by the user organization.

12 Annexes

Not applicable.

13 Security Target

Mobile Armor DataArmor & PolicyServer v3.1 Security Target, Version 1.72, 2 April 2010

14 Acronym List

CC	Common Criteria
CCTL	CC Testing Laboratory
CI	Configuration Item
CM	Configuration Management
CMP	Configuration Management Plan
CVE	Common Vulnerabilities and Exposures
CVS	Concurrent Versioning System
DADB	DataArmor Database
DAOS	DataArmor Operating System
DEK	Disk Encryption Key
DoD	Department of Defense
DoS	Denial of Service
EAL	Evaluation Assurance Level
FSP	Functional Specification
GUI	Graphical User Interface
HLD	High-level Design
HTTP	Hyper-text Transfer Protocol
ID	Identity/Identification
IP	Internet Protocol
IT	Information Technology
MBR	Master Boot Record
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OCSP	Online Certificate Status Protocol
OS	Operating System
PP	Protection Profile
SAIC	Science Applications International Corporation
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSO	Single Sign-on
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification

15 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model, Version 3.1, September 2006.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 2, September 2007.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 3.1, Revision 2, September 2007.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 2, September 2007.

[5] Mobile Armor DataArmor & PolicyServer V3.1 Security Target, Version 1.72, 2 April 2010.

[6] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[7] SAIC CCTL Evaluation Procedures Annex, Version .20, January 31 2004.