National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Mobile Armor FileArmor v3.0 & PolicyServer v3.1

Report Number:	**CCEVS-VR-VID10298-2010**
Dated:	**2010-11-29**
Version:	**1.0**

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 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Dr. Jerome Myers, The Aerospace Corporation
Ralph Broom, Noblis, Inc.

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 FileArmor 3.0 SP7. 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 FileArmor v3.0 & PolicyServer v3.1** was performed by SAIC, in the United States and was completed in August 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 FileArmor v3.0 & 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 FileArmor v3.0 & PolicyServer v3.1 Security Target, Version 0.14, 7 September 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 FileArmor 3.0 SP7

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 adduced.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and versions of the ETR. Also, at some 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 found that the evaluation showed that the product satisfies all of the security functional and assurance requirements stated in the Security Target (ST). Therefore 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 FileArmor v3.0 & PolicyServer v3.1 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 FileArmor 3.0 SP7

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: November 8, 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 FileArmor 3.0 and Mobile Armor PolicyServer 3.1 products represents a client/server-based file and folder encryption solution for personal computers.

Disclaimer The information contained in this Validation Report is not an endorsement of the Mobile Armor PolicyServer 3.1 and FileArmor 3.0 product by any agency of the U.S. Government and no warranty of Mobile Armor PolicyServer 3.1 or FileArmor 3.0 is either expressed or implied.

Evaluation Personnel:
James Arnold
Katie Sykes
Quang Trinh

Validation Team:
Jerome Myers
Ralph Broom

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 FileArmor v3.0 & PolicyServer v3.1 Security Target, Version 1.0, 7 September 2010
TOE Identification:	Mobile Armor PolicyServer v3.1 (3.1.0.445) and Mobile Armor FileArmor v3.0 SP7
Operating Platform:	PolicyServer Operating systems For the PolicyServer Service Microsoft Windows Server 2003 SP1+, Standard or Enterprise Editions For the PolicyServer Management console Microsoft Windows Server 2003 SP1+, Standard or Enterprise Editions Database Microsoft SQL Server 2005 with Service Pack 2+ External Mail Server FileArmor platforms Microsoft Windows XP SP3 Microsoft Windows Vista SP2 **Optionally** - Authentication servers (for external authentication integration): Microsoft Active Directory

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.

4.4 Clarifications of Scope

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

5 Architectural Information

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

Mobile Armor FileArmor application – Provides encryption and invocation and enforcement of authentication decisions implemented within the TOE or in the TOE environment, depending on how the TOE is configured. Includes pre-access authentication components (to invoke configured authentication services) and data encryption components.

Mobile Armor PolicyServer – Provides administrative interfaces that can be used to manage FileArmor 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". Only the Policy Server elements that are used for file Armor have been included in the evaluation.

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 FileArmor 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. The green boxes indicate optional services which can be connected to the system, but which are not required.

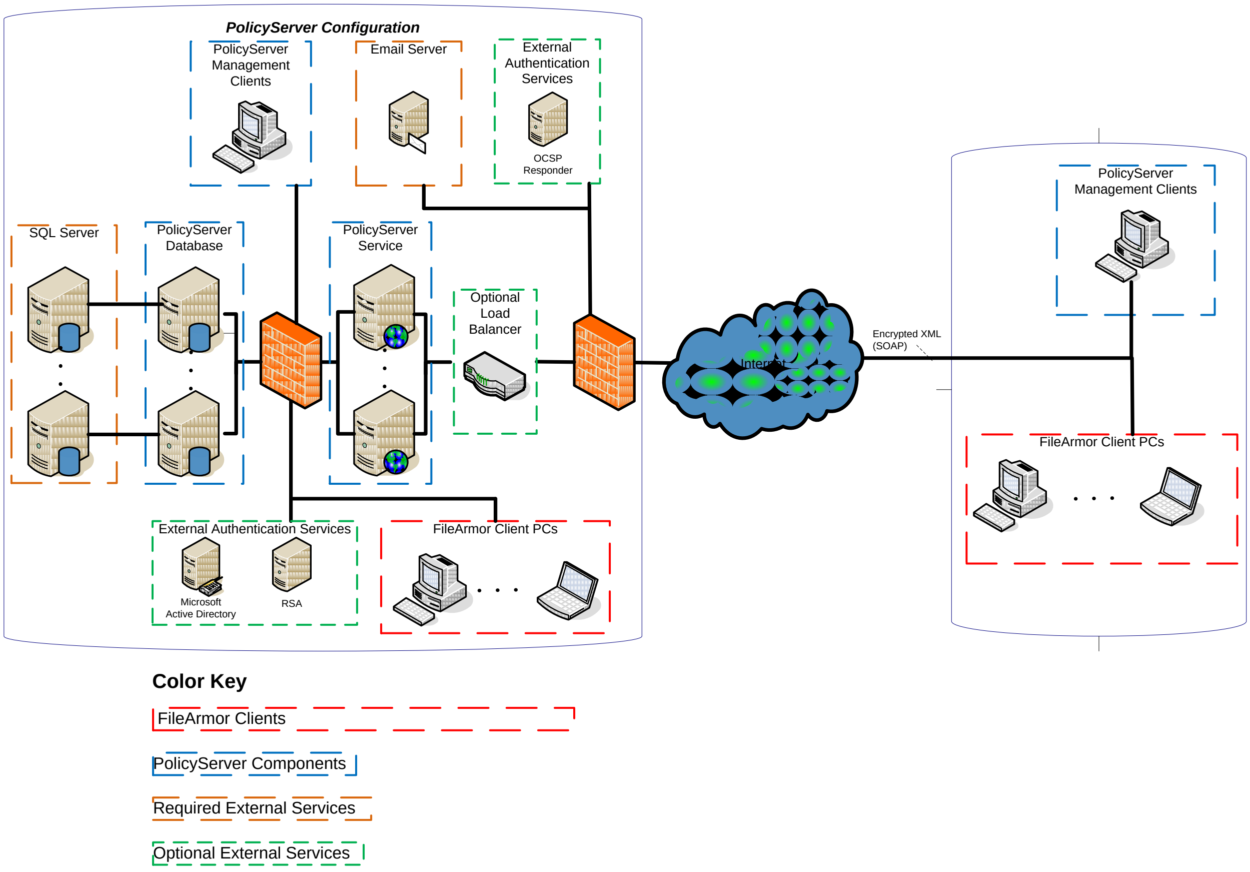
PolicyServer Configuration
PolicyServer Management Clients
Email Server
External Authentication Services
OCSP Responder
SQL Server
PolicyServer Database
PolicyServer Service
Optional Load Balancer
Internet
Encrypted XML (SOAP)
PolicyServer Management Clients
FileArmor Client PCs
External Authentication Services
Microsoft Active Directory
RSA
FileArmor Client PCs
Color Key
FileArmor Clients
PolicyServer Components
Required External Services
Optional External Services

Figure 1 - Mobile Armor Solution Architecture

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

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

Operating systems – Provides the runtime environment for FileArmor application components.

Authentication servers – Provides optional external authentication services for FileArmor.

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

Operating systems – Provides the runtime environment for the PolicyServer application components. Provides operating system GUI interfaces for PolicyServer. Provides web server for interface between PolicyServer and clients.

SQL Database – Provides the storage for FileArmor and PolicyServer user and device information, policies and centralized audit storage. PolicyServer maintains two separate databases, one specifically for log events and one for all other data.

Mail Server – Provides the SMTP server for use in email alert configuration.

Authentication servers – Provides optional external authentication services for FileArmor users. The PolicyServer acts as a proxy for authentication.

- Load Balancer – Provides optional scalability by allowing multiple PolicyServers to be configured together as one.

5.1 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

FileArmor client

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 Server 2003 SP1+, Standard or Enterprise Editions

Database

Microsoft SQL Server 2005 with Service Pack 2+

External Mail Server

FileArmor platforms

Microsoft Windows XP SP3

Microsoft Windows Vista SP2

- Optionally - Authentication servers (for external authentication integration):
  - Microsoft Active Directory

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

6 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 v1.2, Document ID Number: CG-31-09
- PolicyServer v3.1 Administrator Guide, Document ID Number: PSAG-31-01
- PolicyServer v3.1 Appendices, Document ID Number: PSA-31-09
- PolicyServer v3.1 Installation Guide, Document ID Number: PSIG-31-01
- Mobile Armor FileArmor v3.0 SP7 Administrator Guide, v0.4, Document ID Number: MAFAAG-30SP6-09
- Mobile Armor FileArmor Installation Guide version 0.4, Document ID Number: FAIG-30SP6-20
- Mobile Armor FileArmor v3.0 User Guide, Document ID Number: FAIG-30SP6-09
- Mobile Armor v3.1 Certification Guide FIPS 140 and Common Criteria v1.4, Document ID Number: CG-31-09

7 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.

7.1 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, screen shots, and summaries for each of the applicable test platforms.

7.2 Independent Testing

Independent testing took place in essentially two phases.

The evaluators received the TOE in the same manner as normal customers, installed and configured the TOE in accordance with the provided guidance, and exercised a subset of the developers test plan on equipment configured in the testing laboratory. This effort involved installing and configuring both the FileArmor and PolicyServer products on a representative subset of the supported operating systems. Subsequently, the evaluators exercised a subset of the available developer's test procedures for both the FileArmor and PolicyServer products. The subset of tests was selected in order to ensure that each of the claimed security functions was meaningfully sampled.

Also, 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 functions worked as described in the design documentation (and as summarized in the ST). The evaluators also examined product source code made available by the developer primarily to ensure that aspects of the cryptographic mechanisms (e.g., invocation of FIPS functions and audit generation) were implemented in accordance with the design documentation and security claims.

In addition to the use of developer provided and independently devised security functional tests, the evaluators also explored 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 examination of encrypted files 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.

8 Evaluated Configuration

The TOE is one or more Mobile Armor FileArmor 3.0 SP7 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 5.1 above.

9 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™ FileArmor™ v3.0

Mobile Armor™ PolicyServer™ v3.1

PolicyServer™ v3.1 Administration Guide

PolicyServer™ v3.1 Installation Guide

PolicyServer™ v3.1 Administration Appendices

FileArmor™ v3.0 PC Installation Guide

FileArmor™ v3.0 PC User Guide

FileArmor™ v3.0 PC Administration Guide

Mobile Armor™ Certification Guide”

Additionally, the evaluation team’s performance of developer tests, independent tests, and penetration tests further demonstrates the accuracy of the claims in the ST.

10 Validator Comments/Recommendations

1. While the TOE could potentially be used in environments subject to DoD Std 8500 requirements, it should be noted that the product must be carefully configured since it includes features out-of-the-box that by default are not in compliance. 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.
2. 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).
3. There are a number of security claims that are dependent upon the interaction and support of a Policy Server used in conjunction with a FileArmor 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 avoided.
4. The TOE stores audit logs and cryptographic key material (thought not keys) in an associated MS SQL database. To ensure the integrity of this data the databases should either be hosted on the same servers as the main Policy Servers, or be on dedicated servers with an exclusive, direct network connection to the Policy Servers, and managed by the same administrators.

11 Annexes

Not applicable.

12 Security Target

Mobile Armor FileArmor v3.0 & PolicyServer v3.1 Security Target, Version 1.0, 9/7/2010, included by reference.

13 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
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

14 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 FileArmor v3.0 & PolicyServer v3.1 Security Target, version 1.0, 7 September 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 3.1r3, 30 November 2009.