National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

for

Sigaba SigabaNet 2.2

Report Number: CCEVS-VR-06-0002

Dated: 7 February 2006

Version: 2.2

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

Validator

Nicole M. Carlson
The Aerospace Corporation
El Segundo, California

Dr. Deb Downs, Senior Validator

Common Criteria Testing Laboratory

Science Applications International Corporation (SAIC)
Columbia, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

This report documents assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the two SigabaNet 2.2 components that comprise the target of evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in January 2006. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both Common Criteria Part 2 and Part 3 Conformant, and meets the assurance requirements of EAL 2 augmented with ADV_SPM.1. The product is not conformant with any published Protection Profiles. All security functional requirements are derived from Part 2 of the Common Criteria or expressed in the form of Common Criteria Part 2 requirements.

The TOE is comprised of two components within the larger SigabaNet 2.2 product: the Authentication Server and the Key Management Server. The Authentication Server provides the credentials (called "name assertions") that a SigabaNet user must present in order to use other SigabaNet components (including the Key Management Server). The Key Management Server generates, stores, and manages secret keys for SigabaNet users for use by client applications outside of the TOE boundary (including other SigabaNet components).

During this evaluation, the validators monitored the activities of the SAIC evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test reports. The validator determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the validator concludes that the SAIC findings are accurate, the conclusions justified, and the conformance claims correct.

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, 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 conduct security evaluations.

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.

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;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Sigaba SigabaNet 2.2 Authentication Server and Key Management Server
Protection Profile	None
Security Target	Sigaba SigabaNet 2.2 Security Target, Version 4.0, 7 January 2006
Evaluation Technical Report	Evaluation Technical Report for Sigaba SigabaNet 2.2 • Part 1 (Non-Proprietary), Version 3.0, January 20 2006 • Part 2 (Propriety), Version 1.0, January 20, 2006
Conformance Result	Part 2 and Part 3 Conformant, EAL 2 augmented with ADV_SPM.1
Sponsor	Secure Data In Motion, Inc. dba Sigaba
Developer	Secure Data In Motion, Inc. dba Sigaba
Evaluators	Science Applications International Corporation (SAIC)
Validator	The Aerospace Corporation

3. SECURITY POLICY

P.AUTHORIZED_USERS Only those users who have been authorized to access the information within the system may access the TOE.

P.NEED_TO_KNOW The TOE must limit the access to, modification of, and destruction of the information in protected resources to those authorized users which have a "need to know" for that information.

P.ACCOUNTABILITY The users of the TOE shall be held accountable for their actions within the system.

4. ASSUMPTIONS [1]

4.1. Usage Assumptions

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NO_EVIL_ADM The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.

A.COOP Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.

4.2. Environmental Assumptions

It is assumed that the IT environment provides support commensurate with the expectations of the TOE. This is achieved by using evaluated products (or products in evaluation at the time of the writing of this VR) in the environment. The expectations of the TOE with respect to the security provided by the IT environment are captured in the ST in the environmental objectives, but *were not* verified by the evaluation.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities which will prevent unauthorized physical access.

A.PROTECT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

A.PEER Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints. Conformant TOEs are applicable to networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain. There are no security requirements which address the need to trust external systems or the communications links to such systems.

A.CONNECT All connections to peripheral devices reside within the controlled access facilities. Conformant TOEs only address security concerns related to the manipulation of the TOE through its authorized access

[1] Information drawn from Sigaba SigabaNet 2.2 Security Target v4.0, dated 7 January 2006

points. Internal communication paths to access points such as terminals are assumed to be adequately protected.

5. ARCHITECTURAL INFORMATION[2]

The TOE consists of two components that operate within the framework of a larger product, SigabaNet 2.2. Both components are implemented as Java servlets; their respective bytecodes are stored in operating system files. The TOE also stores information in operating system files. The TOE is administered via web-based administrative forms.

The underlying product, SigabaNet 2.2, also used the following software:

- Windows 2000 Server SP4
- Application Server - Tomcat 4.1.24
- Database - Postgres 7.1.3
- Courier Service (A SigabaNet 2.2 component)
- SigabaNet 2.2 Administration Server
- SigabaNet 2.2 Client APIs

[2] Drawn from Sigaba SigabaNet 2.2 Security Target; version 4.0, 7 January 2006

6. DOCUMENTATION

The following documentation was used as evidence for the evaluation of Sigaba SigabaNet 2.2 Authentication Server and Key Server components:[3]

6.1. Design documentation

Document	Version	Date
SigabaNet 2.2 High-Level Design	5	December 2005
SigabaNet 2.2 Security Policy Model	1.1	January 20, 2006

6.2. Guidance documentation

Document	Version	Date
SigabaNet Servers Installation & Configuration Guide	2.2 rev G	January 2006

6.3. Configuration Management and Lifecycle documentation

Document	Version	Date
SigabaNet 2.2 Configuration Items	2.2 rev B	January 2006

6.4. Delivery and Operation documentation

Document	Version	Date
SigabaNet Servers Delivery Procedures	2.2	October 2004
SigabaNet Servers Installation & Configuration Guide	2.2 rev G	January 2006

6.5. Test documentation

Document	Version	Date
Sigaba Test Plan and Procedures	1.3.2	January 2006

[3] This documentation list is extracted from the Final Evaluation Technical Report, Part 1, developed by SAIC.

6.6. Vulnerability Assessment documentation

Document	Version	Date
SigabaNet 2.2 Vulnerability Assessment and Strength of Function Analysis	1.1	December 20, 2005

6.7. Security Target

Document	Version	Date
Sigaba SigabaNet 2.2 Security Target	4.0	7 January 2006

7. IT PRODUCT TESTING

A complete description of the tests run may be found in the ETR Part 2 Supplement (v 4.0, 2 February, 2006). This is intended to be a non-proprietary summary.

7.1. Developer Testing

Evaluator analysis of the developer's test plans, test scripts, and test results indicate that the developer's testing is adequate to satisfy the requirements of EAL 2.

The developer's tests were non-automated, and consisted of a suite of manual tests that covered the security functions claimed in the ST. The test verified the basic functionality of the TOE, and exercised the parameters and verified the exception conditions documented in the user and administrative guidance.

For each of the developer tests, the evaluators analyzed the test procedures to determine whether the procedures were relevant to, and sufficient for the function being tested. The evaluators also verified that the test documentation showed results that were consistent with the expected results for each test case.

7.2. Evaluator Testing

7.2.1. Functional Testing

In addition to developer testing, the CCTL conducted its own suite of tests, which were developed independently of the sponsor. These also completed successfully.

7.2.2. Vulnerability Testing

The evaluators developed vulnerability test to address both management and TOE access security functions, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE.

8. EVALUATED CONFIGURATION

The test machine consisted of:

Hardware:

One server consisting of:

- 3 GHz Pentium 4 processor (or equivalent)
- 2GB memory
- 30 GB available disk space

Software:

- Windows 2000 Server SP4
- Application Server - Tomcat 4.1.24
- Database - Postgres 7.1.3
- Courier Service (A SigabaNet 2.2 component)
- SigabaNet 2.2 Administration Server
- SigabaNet 2.2 Client APIs
- TOE - SigabaNet 2.2 (SigabaNet Authentication Server and the SigabaNet Key Server)

9. RESULTS OF THE EVALUATION

The evaluation was conducted based upon the Common Criteria (CC), Version 2.1, dated August 1999 [1,2,3,4]; the Common Evaluation Methodology (CEM), Version 1.0, dated August 1999 [6]; and all applicable International Interpretations in effect on 1 April 2004. The evaluation confirmed that the Sigaba SigabaNet 2.2 product is compliant with the Common Criteria Version 2.1, functional requirements (Part 2), and assurance requirements (Part 3) for EAL2 augmented with ADV_SPM.1. The details of the evaluation are recorded in the CCTL's evaluation technical report, Evaluation Technical Report for the Sigaba SigabaNet 2.2, Part 1 (Non-Proprietary) and Part 2 (SAIC and Sigaba Proprietary). The product was evaluated and tested against the claims presented in the Sigaba SigabaNet 2.2 Security Target v4.0, dated 7 January 2006.

The validator followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The validator has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validator therefore concludes that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL.

9.1. Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Sigaba SigabaNet 2.2 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

9.2. Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 2 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation.

9.3. Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification while in transit. The evaluation team followed the Configuration Guide to test the installation procedures to ensure the procedures result in the evaluated configuration.

9.4. Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

In addition to the EAL 2 ADV CEM work units, the evaluation team applied the ADV_SPM.1 work units from the CEM supplement. The security policy model was evaluated to determine that it clearly and consistently described the rules and characteristics of the security policies and whether this description corresponds with the functional specification.

9.5. Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 2 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

9.6. Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 2 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance.

9.7. Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

9.8. Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 2 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the developer misuse analysis, and the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

9.9. Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

10. VALIDATOR COMMENTS

The TOE makes use of cryptographical functions evaluated under FIPS 140-2. This is a separate standard from CCEVS, and these functions were not evaluated further during this evaluation.

11. SECURITY TARGET

Sigaba SigabaNet 2.2 Security Target, v 4.0, 7 January 2006

12. GLOSSARY

Application Server	A server in a network that is used to remotely run applications.
Bytecode	A form of compiled code that is still higher-level (more abstract) than machine code; used to reduce dependence on hardware.
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
CM	Configuration Management
CMP	Configuration Management Plan
DoD	Department of Defense
DBMS	Database Management Server
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PP	Protection Profile
SAIC	Science Applications International Corporation
Servlet	A Java program that creates content (usually HTML) on the fly, much like CGI or PHP.
ST	Security Target

TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface
VR	Validation Report

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] Sigaba SigabaNet 2.2 Security Target, v 4.0, 7 January 2006

[8] Evaluation Technical Report for Sigaba SigabaNet 2.2, January 20, 2006; Part 1 (Non-Proprietary) v 4.0; 7 February 2006.

[9] Evaluation Technical Report for Sigaba SigabaNet 2.2, Part 2 (SAIC and Sigaba Proprietary), Version 1.0, 20 January 2006.

[10] Evaluation Team Test Plan for Sigaba SigabaNet 2.2, ETR Part 2 Supplement (SAIC and Sigaba Proprietary), Version 4.0, 2 February 2006.