National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Green Hills Software
INTEGRITY-178B Separation Kernel

Report Number: CCEVS-VR-10119-2008
Dated: 01 September 2008
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

Shaun Gilmore
Santosh Chokhani
Ken Elliott
Jerry Myers
Paul Bicknell

Common Criteria Testing Laboratory

SAIC, Inc.
Columbia, Maryland

Table of Contents

List of Tables

1 Executive Summary

The evaluation of **Green Hills Software (GHS) INTEGRITY-178B Separation Kernel** was performed by SAIC, in the United States and was completed in April 2008. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the GHS INTEGRITY-178B Separation Kernel TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 2.3 and the US Government Protection Profile for Separation Kernels in Environments Requiring High Robustness, Version 1.03, 29 June 2007 (SKPP). The evaluation methodology used by the evaluation team to conduct the evaluation was a combination of that available in the Common Methodology for Information Technology Security Evaluation versions 2.3, 3.0, and 3.1 along with additional methodology developed in the context of this evaluation. Note that the methodology selected and/or developed by the evaluation team was necessary due to the number of high assurance and explicit requirements in the SKPP.

Science Applications International Corporation (SAIC) determined that the while the product doesn't technically satisfy any evaluation assurance level (EAL) as defined within the Common Criteria (CC), it does satisfy the requirements for "High Robustness" as defined within the SKPP. The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the Green Hills Software (GHS) INTEGRITY-178B Separation Kernel Security Target.

This Validation Report applies only to the specific version of the TOE as evaluated. In this case the TOE is a combination of software and hardware components as follows:

- **GHS INTEGRITY-178B Real Time Operating System (RTOS), version IN-ICR750-0101-GH01_Rel**, running on a
- **Compact PCI card, version CPN 944-2021-021**, including a
- **PowerPC, version 750CXe**, CPU.

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. This Validation Report is not an endorsement of the GHS INTEGRITY-178B Separation Kernel by any agency of the US Government and no warranty of the product is either expressed or implied.

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 successive versions of the ETR. Also, at three points during the evaluation, validators formed a Technical Oversight Panel in order to review the Security Target, Design, and Test evaluation findings and plans 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 Evaluation Technical Report for the Green Hills Software INTEGRITY-178B Separation Kernel Parts 1 and 2 and the associated test report produced by SAIC.

1.1 Evaluation Details

Evaluated Product:	GHS INTEGRITY-178B Separation Kernel
Sponsor & Developer:	Green Hills Software, Inc. 30 West Sola Street Santa Barbara, CA 93101 USA
CCTL:	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Completion Date:	April 2008
CC:	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
Interpretations:	There were no applicable interpretations used for this evaluation.
CEM:	Common Methodology for Information Technology Security Evaluation: • version 2.3, August 2005 • version 3.0 (rev2), July 2005 • version 3.1 (rev1), September 2006 Note that substantial evaluation methodology was developed by the evaluators and approved by the validators in order to address requirements in the SKPP for which no pre-defined work units and/or guidance was otherwise available.
PP:	US Government Protection Profile for Separation Kernels in Environments Requiring High Robustness, Version 1.03, 29 June 2007 (SKPP)
Evaluation Class:	High Robustness (per the SKPP): • The following CC Part 3 requirements: ACM_AUT.2, ACM_CAP.5, ACM_SCP.3, ADO_IGS.1, ADV_RCR.3, ADV_SPM.3, AGD_USR.1, ALC_DVS.2, ALC_FLR.3, ALC_LCD.2, ALC_TAT.3, ATE_COV.3, ATE_DPT.3, ATE_FUN.2, ATE_IND.3, AVA_MSU.3, AVA_SOF.1 • and the following explicitly defined requirements: ADO_DEL_EXP.2, ADO_IGS.1, ADV_ARC_EXP.1, ADV_CTD_EXP.1, ADV_FSP_EXP.4, ADV_HLD_EXP.4, ADV_IMP_EXP.3, ADV_INI_EXP.1, ADV_INT_EXP.3, ADV_LLD_EXP.2, ADV_LTD_EXP.1, AGD_ADM_EXP.1, AMA_AMP_EXP.1, APT_PDF_EXP.1, APT_PSP_EXP.1, APT_PCT_EXP.1, APT_PST_EXP.1, APT_PVA_EXP.1,

AVA_CCA_EXP.2, and AVA_VLA_EXP.4.

Note that given the explicit assurance requirements in the SKPP, the resulting combination of assurance requirements do not technically satisfy any EAL defined within the CC.

Description

The GHS INTEGRITY-178B Separation Kernel is a separation kernel designed to instantiate and separate partitions that serve to host custom applications. The GHS INTEGRITY-178B Separation Kernel manages access to memory, devices, communications, and processor resources to ensure that partitions can be entirely separated and can interact only in well defined ways configured by System Architects.

The GHS INTEGRITY-178B Separation Kernel is an embedded real time operating system, in that it does not include operating system constructs such as a file system, shell prompt, or user logins. It does schedule partitions to execute on the actual hardware and provides granular scheduling capability to entities (i.e., tasks) operating within a given partition.

Disclaimer

The information contained in this Validation Report is not an endorsement of the GHS INTEGRITY-178B Separation Kernel product by any agency of the U.S. Government and no warranty of the GHS INTEGRITY-178B Separation Kernel product is either expressed or implied.

Evaluation Personnel:

James Arnold

Gary Grainger

Quang Trinh

Validation Team:

Shaun Gilmore

Santosh Chokhani

Ken Elliott

Jerry Myers

Paul Bicknell

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:	Green Hills Software INTEGRITY-178B Separation Kernel Security Target, version 1.0, 30 May 2008
TOE Identification:	INTEGRITY-178B Separation Kernel, comprising: • INTEGRITY-178B Real Time Operating System (RTOS), version IN-ICR750-0101-GH01_Rel • PowerPC, version 750CXe • Compact PCI card, version CPN 944-2021-021
Operating Platform:	Compact PCI card, version CPN 944-2021-021 with a PowerPC, version 750CXe

3 Threats to Security

The following are the threats that the evaluated product addresses.

Table 2 Threats to Security

T.ADMIN_ERROR	An administrator may incorrectly install or configure the TOE (including the misapplication of the protections afforded by the PIFP), or install a corrupted TOE resulting in ineffective security mechanisms.
T.ALTERED_DELIVERY	The TOE may be corrupted or otherwise modified during delivery such that the on-site version does not match the master distribution version.
T.CONFIGURATION_CHANGE	The lack of TSF-enforced constraints on the ability of an authorized subject to invoke or dictate how the TOE is reconfigured may result in the TOE transitioning to an insecure (unknown, inconsistent, etc) state.
T.CONFIGURATION_INTEGRITY	The TOE may be placed in a configuration that is not consistent with that of the configuration vector due to the improper loading of the configuration vector or incorrect use of the configuration vector during TOE initialization.
T.COVERT_CHANNEL_EXPLOIT	An unauthorized information flow may occur between partitions as a result of covert channel exploitation.
T.DENIAL_OF_SERVICE	A malicious subject may block others from system resources (e.g., system memory, persistent storage, and processing time) via a resource exhaustion attack.
T.INCORRECT_CONFIG	The configuration vectors are not an accurate and complete description of the operational configuration of the TOE as used by an organization.
T.INCORRECT_LOAD	The software portion of the TSF implementation and/or configuration vectors are not correctly converted into a TOE-useable form.
T.INSECURE_STATE	The TOE may be placed in an insecure state as a result of an erroneous initialization, halt, reconfiguration or restart, transition to maintenance mode, or as a result of an unsuccessful recovery from a system failure or discontinuity.
T.LEAST_PRIVILEGE	The design and implementation of the TSF internals may not suffice to limit the damage resulting from accident, error or unauthorized use.

T.POOR_DESIGN	Unintentional or intentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a malicious subject.
T.POOR_IMPLEMENTATION	Unintentional or intentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a malicious subject.
T.POOR_TEST	Lack of or insufficient evaluation and runtime tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being undiscovered.
T.TSF_COMPROMISE	A malicious subject may cause TSF data or executable code to be inappropriately accessed (viewed, modified, executed, or deleted).
T.UNAUTHORIZED_ACCESS	A subject may gain access to resources or TOE security management functions for which it is not authorized according to the TOE security policy.

4 Security Policy

The following are the organizational policies fulfilled by the product.

Table 3 Organizational Security Policies

P.ACCOUNTABILITY	The TOE shall provide the capability to make available information regarding the occurrence of security relevant events.
P.CONFIGURATION_CHANGE	The TOE shall support the capability to perform a static configuration change. The TOE may also provide the capability for an authorized subject to select or redefine the configuration vector to be used upon TOE startup, TOE restart or TOE reconfiguration.
P.CRYPTOGRAPHY	The TOE shall use NSA approved cryptographic mechanisms.
P.INDEPENDENT_TESTING	The TOE shall undergo independent testing.
P.RATINGS_MAINTENANCE	A plan for procedures and processes to maintain the TOE's rating shall be in place to maintain the TOE's rating once it is evaluated.
P.SYSTEM_INTEGRITY	The TOE shall provide the ability to periodically validate its correct operation.
P.USER_GUIDANCE	The TOE shall provide documentation regarding the correct use of the TOE security features.
P.VULNERABILITY_ANALYSIS_AND_TEST	The TOE shall undergo independent vulnerability analysis and penetration testing by NSA to demonstrate that the TOE is resistant to an attacker possessing a high attack potential.

5 Assumptions

5.1 Physical Assumptions

The following physical assumptions are identified in the Security Target.

Table 4 Physical Assumptions

A.PHYSICAL	It is assumed that the non-IT environment provides the TOE with appropriate physical security commensurate with the value of the IT assets protected by the TOE.

5.2 Personnel Assumptions

The following personnel assumptions are identified in the Security Target.

Table 5 Personnel Assumptions

A.TRUSTED_INDIVIDUAL	It is assumed that any individual allowed to perform procedures upon which the security of the TOE may depend is trusted with assurance commensurate with the value of the IT assets.

5.3 Connectivity Assumptions

The following operational assumptions are identified in the Security Target.

Table 6 Operational Assumptions

A.SUBJECT_ALLOCATION	It is assumed that a properly trained trusted individual will create configuration vectors such that, for those partitions to which subjects are allocated, each partition is allocated one or more subjects (i.e., subjects with homogeneous access requirements, or subjects with heterogeneous access requirements) that are appropriate for the policy abstraction supported by the TOE.
A.COVERT_CHANNELS	If the TOE has covert storage and/or timing channels, then for all subjects executing on that TOE, it is assumed that relative to the IT assets to which they have access, those subjects will have assurance sufficient to outweigh the risk that they will violate the security policy of the TOE by using those covert channels.
A.TRUSTED_FLOWS	For any subject configured to have unrestricted access in multiple policy equivalence classes, it is assumed that the subject is trusted at least with assurance commensurate with the value of the IT assets in all equivalence classes to which it has access.

6 Architectural Information

The GHS INTEGRITY-178B Separation Kernel is a separation kernel designed to instantiate and separate partitions that serve to host custom applications. It manages access to memory, devices, communication resources, and processor resources to ensure that partitions are entirely separated and can interact only in well defined manners configured by a System Architect.

A System Architect creates a static configuration file that defines the partitions of the system, the subjects (i.e., sets of tasks) and resources (such as memory objects, links, connections and clocks) allocated to each partition, and the rules for sharing of information between partitions, at the granularity of subjects and resources. The configuration file also defines the mechanism by which the TSF schedules partitions and their corresponding tasks to execute.

Each partition provides an environment for a multi-tasking application. Applications communicate with the kernel and with applications in other partitions via a well-defined kernel API. The GHS INTEGRITY-178B Separation Kernel is an object-based operating system. In order to communicate with the kernel or (via the kernel) an application in another partition, an application invokes an API specific to the target object type. The application uses the API to pass an object reference to the kernel. The kernel operates on the referenced object.

The GHS INTEGRITY-178B Separation Kernel comprises the GHS INTEGRITY-178B real time operating system (RTOS) running on an embedded PowerPC processor on a Compact PCI card. The card plugs into its IT environment via the PCI bus, but other than drawing power from that bus it has no security dependency on the bus or other devices connected to it. Devices on the bus, or devices that can be installed on the embedded card directly, can be made available to partitions, although the TOE itself does not include any device drivers. Access to such devices can be provided to partitions by mapping their control and data registers to memory regions in a given partition and device drivers can be implemented outside the TOE in the partitions as necessary. Alternately, development of restricted device drivers that partially run in privileged mode is included in the scope of ratings maintenance changes. Procedures for ensuring changes are compliant within the scope of ratings maintenance are described in the rating maintenance plans. For the evaluated configuration, device drivers that run in privileged mode were not included.

The INTEGRITY-178B RTOS comprises the following architectural components:

- Common Kernel
- Hardware Dependent Components, comprising:
    - Architecture Support Package (ASP), which provides a processor-independent interface between the Common Kernel and the underlying processor
    - Board Support Package (BSP), which provides a board-independent interface between the Common Kernel any peripheral hardware (which may include devices in the processor).The BSP can be provided by either the user or by Green Hills Software. A Green Hills Software-supplied BSP is supported in the evaluated configuration.
- Kernel API, which provides the interface between applications running in a partition and the Common Kernel. The Kernel API is linked in with the application.

7 Documentation

Following is a summary of user documents supplied by the developer for the TOE:

- High Assurance Security Products User and Administrator Guidance (AGD), DO-NNNNNN-0102-HASP_AGD
- High Assurance Security Products Installation, Generation, and Start-up Document (IGS), DO-NNNNNN-0102-HASP_IGS
- Safety Critical Products DO-178B Level A Product Specification, DO-NNNNNN-0375-P_SPEC
- INTEGRITY Reference Manual
- Integrate User's Guide
- INTEGRITY Development Guide
- INTEGRITY BSP User's Guide
- AdaMULTI: Building Applications for Embedded PowerPC
- Green Hills Software INTEGRITY-178B Separation Kernel Assurance Maintenance Requirements,
  IN-INNNNN-0101-ISKAMR

The security target used is:

- Green Hills Software INTEGRITY-178B Separation Kernel Security Target, version 1.0, 30 May 2008

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 a High Robustness evaluation.

8.1 Developer Testing

Given the high safety and security assurance goals of the product, the developer tests are entirely automated and designed to comprehensively test the product. The tests are derived from the developer requirement documents in a manner facilitating tracing between the tests and the requirements.

The tests themselves are instrumented so that when they are run, specific code segments and decision points (i.e., conditions) in the code are reported as they are encountered by the tests. Using this information, the developer effectively ensures that every code instruction and every decision branch is subject to tests.

8.2 Independent Testing

The test configuration included of a single instance of the TOE plugged into a chassis suitable to meet the necessary power requirements. A laptop was used to host the product, tests, development tools, and configuration tools necessary to build, deploy, and test the TOE. Finally, a 'probe' device was provided by the developer to facilitate communication between a port on the PCI card included in the TOE and the laptop (via network and serial interfaces).

The evaluators installed the TOE according to the installation guidance and subsequently used the user and administrator guidance documents while performing tests.

Once the test configuration was established the evaluators built the tests, the product, and exercised the entire suite of automated tests provided by the developer. The evaluation team found the automated tests relatively easy to use and the results coherent and informative. Note that there were not any manual test procedures.

Given the comprehensive nature of the developer tests, additional independent testing performed by the evaluators was limited. The evaluators did examine test source code in order to gain assurance in the actual test coverage in addition to examining all the test results. Most of the additional testing was related to the configuration and deployment tools to ensure that those tools worked as advertised and were not prone to lead a Security Architect to make undesirable mistakes.

8.3 Highly Resistant Vulnerability Analysis

Evaluation team testing at NSA was completed in August 2008. Using the results of the evaluation by the CCTL evaluation team, the NSA evaluation team installed the TOE evaluated configuration and conducted AVA_VLA_EXP.4 vulnerability testing. The NSA team utilized the same category of tools used by the CCTL for penetration testing, as well as in-house developed tools, which enabled the team to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a high attack potential.

9 Evaluated Configuration

The evaluated configuration is a single instance of the Green Hills Software INTEGRITY-178B Separation Kernel, comprising:

- INTEGRITY-178B Real Time Operating System (RTOS), version IN-ICR750-0101-GH01_Rel
- Compact PCI card, version CPN 944-2021-021 including a PowerPC, version 750CXe.

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 High Robustness 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 1, states:

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR.

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 2.3 ([1], [2], and [3]) and CEM versions 2.3, 3.0, and 3.1 ([4], [5], [6]) and additional methods developed as necessary. The evaluation determined the Green Hills Software INTEGRITY-178B Separation Kernel TOE to be Part 2 conformant, and to meet the High Robustness requirements. The rationale supporting each CEM work unit verdict is recorded in the "Evaluation Technical Report For the Green Hills Software INTEGRITY-178B Separation Kernel 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 Green Hills Software INTEGRITY-178B Separation Kernel Security Target, version 1.0, 30 May 2008, is a CC compliant ST.
>
> Section 6.2, TOE Evaluation: The verdicts for each CEM work unit in the ETR sections included in Section 15 are each "PASS". Therefore, when configured and operated according to the following guidance documentation identified as 'IGS' and 'AGD' in Section 7. The Green Hills Software INTEGRITY-178B Separation Kernel TOE satisfies the claims made in the Green Hills Software INTEGRITY-178B Separation Kernel Security Target, version 1.0, 30 May 2008.

Additionally, the evaluation team's performance of the entire vendor test suite, the independent tests, and the penetration test also demonstrates the accuracy of the claims in the ST.

11 Validator Comments/Recommendations

The Administrative Guidance document for the TOE contains useful information on Covert Channels. However, customers that need to employ the measures described in the guidance to mitigate potential illicit information flows are likely to require additional information from the developers. The TOE contains mechanisms for eliminating most covert channels and reducing the capacities of the residual channels to below any desired bandwidth. However, as should be expected, there are performance impacts associated with the reductions in covert channel capacities. The Administrator Guidance provides a high level overview of the relationships. The mathematical relationship between the numerical values that can be set to control covert channels and the numerical impact on potential residual capacities is beyond the scope of the Administrator Guidance. Customers that need to craft their system configuration to optimize system performance while also ensuring specific numerical limitations on covert channels capacities will need to perform further covert channel analysis. As part of the evaluation evidence, the product developer prepared a report on its covert channel analysis that contains most of the information that a customer would need to craft a configuration that meets specific quantitative objectives. The covert channel analysis report is not normally available as customer documentation. Green Hills Software has confirmed that support for more detailed capacity analysis will be made available to customers on a contractual basis.

The Validation Team observed that the evaluation and all of its activities were performed in accordance with the CC, the CEM, and CCEVS practices. The Validation Team agrees that the CCTL presented appropriate rationales to support the Results presented in Section 5 of the ETR and the Conclusions presented in Section 6 of the ETR.

12 Annexes

Not applicable.

13 Security Target

Green Hills Software INTEGRITY-178B Separation Kernel Security Target, version 1.0, 30 May 2008

14 Acronym List

API	– Application Programming Interface
CC	– Common Criteria
CEM	– Common Evaluation Methodology
CCEVS	– Common Criteria Evaluation and Validation Scheme
CCTL	– Common Criteria Testing Laboratory
EAL	– Evaluation Assurance Level
ETR	– Evaluation Technical Report
GHS	– Green Hills Software
IT	– Information Technology
NIAP	– National Information Assurance Partnership
RTOS	– Real Time Operating System
SAIC	– Science Applications International Corporation
SFR	– Security Functional Requirement
SKPP	– US Government Protection Profile for Separation Kernels in Environments Requiring High Robustness, Version 1.03, 29 June 2007
ST	– Security Target
TOE	– Target of Evaluation

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 2.3, August 2005, ISO/IEC 15408-2.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005, ISO/IEC 15408-2.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005, ISO/IEC 15408-2.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005, ISO/IEC 15408-2.

[5] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.0, July 2005, Revision 2.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, September 2006, Revision 1.

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