National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

High Density Devices SecureD Version 1.6

Report Number: CCEVS-VR-06-0047
Dated: 18 October 2006
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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Franklin Haskell
The MITRE Corporation
Bedford, Massachusetts

Common Criteria Testing Laboratory

SAIC
Columbia, Maryland

Table of Contents

List of Tables

1 Executive Summary

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the SecureD TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 2.2 and International Interpretations effective on 22 March 2005. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.2. Science Applications International Corporation (SAIC) determined that the Evaluation Assurance Level is EAL 4 augmented with AVA_VLA.3.

The product, when configured as specified in the configuration, satisfies all of the security functional requirements stated in the SecureD version 1.6 Security Target. A validator on behalf of the CCEVS Validation Body monitored the evaluation carried out by SAIC. The evaluation was completed in October 2006. Results of the evaluation can be found in the Common Criteria Evaluation and Validation Scheme Validation Report for SecureD, prepared by CCEVS.

The validation team monitored the activities of the evaluation team, examined evaluation testing procedures, witnessed testing, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements 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 validation team notes that the claims made and successfully evaluated for the product represent a set of requirements that, while not the most extensive possible for the product, are nevertheless a reasonable representation of what might be used for a "normal" product deployment. No key management system is evaluated and significant reliance is necessarily placed upon physical protection. On the other hand, no reliance is placed upon host software. The device can operate under any operating system and applications. In fact, the data is protected even while the host is not being operated.

1.1 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	SecureD Version 1.6
Sponsor:	TechSoft, Inc. 31 W. Garden Street, Suite 100 Pensacola, FL 32502
Developer:	High Density Devices, AS Postbocks 1428 N-4505 Mandal, Norway

CCTL:	Science Applications International Corporation 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Kickoff Date:	22 March 2005
Completion Date:	30 December 2005
CC:	Common Criteria for Information Technology Security Evaluation, Version 2.2
Interpretations:	None.
CEM:	Common Evaluation Methodology for Information Technology Security, Part 1: Introduction and General Model, Version 0.6, January 1997; Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 2.2, January 2004.
Evaluation Class:	EAL 4 augmented with AVA_VLA.3
Description	The SecureD® data storage encryption device (SecureD) is a hardware encryption device, which is fully compatible with the Advanced Technology Attachment (ATA) / ATA Packet Interface (ATAPI)-6 (Integrated Drive Electronics (IDE)) interface, that resides in the data path between an IDE controller and one or two IDE devices (including ATAPI CD_ROM devices). Because SecureD resides “on the wire” between the IDE controller and the storage media, it operates both physically and logically at a level below visibility to operating systems and application programs.
Disclaimer	The information contained in this Validation Report is not an endorsement of the SecureD product by any agency of the U.S. Government and no warranty of the netForensics product is either expressed or implied.
PP:	none
Evaluation Personnel	Science Application International Corporation: Shukrat Abbas Kesha Webb Cynthia Reese
Validation Team:	Franklin Haskell The MITRE Corporation 202 Burlington Road

1.2 Interpretations

No interpretations are applicable.

1.3 Threats to Security

The following are the threats that the evaluated product addresses:

Table 2 – Threats

Threat Identifier	Threat Name	Threat Description
T.Cryptanalysis	Cryptanalysis for theft of information	A human threat agent performs cryptanalysis on encrypted data at rest in order to recover information content
T.System_Access	Unauthorized System Access	An unauthorized human threat agent gains access to a system incorporating SecureD due to missing, weak, or incorrectly implemented access control allowing potential violations of integrity, confidentiality, or availability

2 Identification

The product being evaluated is **SecureD Version 1.6**.

3 Security Policy

The following are the security policies for the evaluated product.

Table 1 – Policies

Policy Identifier	Policy Name	Policy Description
P.FIPS_Algorithms	Use of FIPS-approved algorithms	The SecureD TOE shall use only FIPS-approved algorithms for its encryption techniques.
P.Guidance_Docs	Installation and usage guidance	The SecureD TOE shall include guidance for its secure installation, administration, and use.
P.Physical_Control	Physical protection	Those responsible for operational use of the SecureD TOE shall protect it physically from unauthorized use, modification, or destruction.

4 Assumptions

4.1 Physical Assumptions

The following physical assumptions are identified in the Security Target:

Table 3 – Physical Assumptions

Assumption Identifier	Assumption Name	Assumption Description
APh.FIPS_Certification	FIPS certification	The SecureD TOE will be certified according to FIPS PUB 140-2 at Security Level 2 or higher
APh.Crypto_Key_Management	Cryptographic Key Management	The IT Environment contains a Key Management System (policies, procedures, hardware, and software) capable of creating physical cryptographic key materials (e.g., smart cards) compatible with SecureD. This KMS will include the necessary policies and procedures for the proper creation, management, distribution, and destruction of cryptographic Key Tokens compatible with SecureD.
APh.Threat_Agent_Moderate	Moderate Attack Potential	Systems containing SecureD are subject to deliberate attack by threat agents who are proficient-to-expert in the security behavior of the system, possessing specialized equipment, but possessing only public information concerning SecureD.

4.2 Personnel Assumptions

The following personnel assumptions are identified in the Security Target:

Table 4 – Personnel Assumptions

Assumption Identifier	Assumption Name	Assumption Description
APe.Administrator	Designated Administrators	Authorities responsible for operational use of SecureD assign one or more individuals (System Administrators) to administer SecureD and its security. These authorized administrators are properly trained and are not careless, willfully negligent, nor

		hostile.
APe.Administrator_Docs	Documentation for Administrators	System Administrators follow the policies and procedures defined in the SecureD documentation for secure installation, administration, and use of SecureD
APe.Crypto_Token_Management	Cryptographic Token Management	Those responsible for operational use of the SecureD TOE make use of a Key Management System (policies, procedures, hardware, and software) capable of creating physical cryptographic key materials (e.g., smart cards) to enable operation of the SecureD TOE. System administrators follow the policies and procedures necessary for the proper creation, management, distribution, and destruction of cryptographic Key Tokens..
APe.Protect_From_Mods	SecureD Protection From Modification	Those responsible for operational use of the SecureD TOE will physically protect SecureD from unauthorized modification
APe.User	Authorized Users	Information cannot flow between the IDE controller of a protected system and the protected media except through SecureD

4.3 Connectivity Assumptions

The following connectivity assumptions are identified in the Security Target:

Table 2 – Connectivity Assumptions

Assumption Identifier	Assumption Name	Assumption Description
ACo.No_Bypass	Controlled Media Connection	Information cannot flow between the IDE controller of a protected system and the protected media except through SecureD.

5 Architectural Information

The SecureD® data storage encryption device (SecureD) is a hardware encryption device, which is fully compatible with the Advanced Technology Attachment (ATA) / ATA Packet Interface (ATAPI)-6 (Integrated Drive Electronics (IDE)) interface, that resides in the data path between an IDE controller and one or two IDE devices(including ATAPI CD_ROM devices) in a general computing environment. Because SecureD resides "on the wire" between the IDE controller and the storage media, it operates both physically and logically at a level below visibility to operating systems and application programs.

SecureD applies Advanced Encryption Standard (AES) encryption at the sector level to protect data at rest from intentional or inadvertent disclosure. It loads its cryptographic keys from an external Key Token – typically a smart card – through an encrypted external interface, logically and physically separate from the data path. SecureD supports multiple key lengths (128, 192, and 256 bits) and up to 32 different keys per Key Token. Each key can be allocated any non-overlapping sector range on the storage medium. If the operating system or an application requests a storage address that the IDE controller maps to an unallocated sector, SecureD returns an I/O error to provide information hiding about the inaccessible sectors. SecureD incorporates hardware functions for zeroizing the data encryption keys.

6 Documentation

The following documents are delivered to customers and are pertinent to the installation, configuration, and operation of the TOE.

- SecureD Evaluated Configuration Guide, v1.40 2005-11-16

7 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Developer Testing

The vendor provided TOE devices, test scripts, and test results to the lab for analysis, testing and comparison. The evaluation team:

- examined the test objectives and scripts and determined that the test procedures provided provide reasonable coverage of the SFRs;
- installed the TOE in a desktop machine;
- and ran all the developer's tests on that machine obtaining the same results as the developer.

7.2 Evaluation Team Independent Testing

The evaluation team ran the entire set of developer tests on a laptop configuration and obtained the same results as on the desktop configuration.

7.3 Evaluation Team Penetration Testing

For its penetration tests, the Evaluation Team analyzed the SFRs supported by the TOE; the assumptions the TOE is based on; and the developer test procedures. They found a residual vulnerability. That is, a method by which to circumvent the TOE's protections exploiting the

lack of implementation of an assumption. This was indeed found to be a vulnerability, though warnings are in place to prevent it.

The Evaluation Team's ETR, Part 2, provides a detailed description of the tests, the results, and the effects, if any, on the information presented in the ST or other evaluation evidence.

7.4 Moderately Resistant Vulnerability Analysis

Evaluation team testing at NSA was completed in October 2006. Using the results of the evaluation by the CCTL evaluation team, the NSA evaluation team installed the TOE evaluated configuration and conducted AVA_VLA.3 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 was resistant to penetration attacks performed by attackers with moderate attack potential.

The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses 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.

8 Evaluated Configuration

The evaluated configuration of SecureD consists of a Field Programmable Gate Array (FPGA) chip, an FPGA configuration device (a Xilinx Programmable Read-Only Memory (PROM) (Xilinx part no. XCF32) designed to match the FPGA), and a flash memory chip, all of which are mounted to a small, underlying printed circuit board (PCB); the entire PCB and the components mounted to it are encapsulated in a hard, opaque, tamper-evident coating, leaving only the interface pins accessible.

9 Results of the Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.2 and CEM version 2.2. The evaluation determined the HDD TOE to be Part 2 conformant, and to meet the Part 3 EAL 4 augmented with AVA_VLA.3. The rationale supporting each CEM work unit verdict is recorded in the "Evaluation Technical Report for the HDD SecureD Part 2" which is considered proprietary.

10 Validator Comments/Recommendations

The product is hardware. It is a chip with various connectors brought out of it. Its sole purpose is to encrypt the data headed for the IDE devices to which it is connected and decrypt the data coming off those devices. Some flexibility is provided by allowing multiple keys; each of which applies to a non-overlapping range of sector numbers. Key timeouts can also be specified as long periods to allow a single key card to be used on multiple systems.

No key management system is provided as part of the product and therefore none was evaluated. This is an important component of the customer's security arrangements and the appropriate effort must be put into choosing and implementing it.

As demonstrated by the evaluation team's penetration test, correct configuration and physical security are important; yet even should a protected device be exposed to hostile inspection the data would need to be subjected to intensive cryptanalysis to render the data readable. It is therefore important that procedures involving removal or destruction of keying materials be put in place for when the equipment in which the device is installed must be left exposed to hostile action.

11 Annexes

Not applicable.

12 Security Target

The security target for this product's evaluation is **SecureD® Version 1.6 Security Target**, dated December 22, 2005

13 Glossary

The following definitions may be used in this document:

Term	Definition
Advanced Encryption Standard	See AES
AES	"Acronym for Advanced Encryption Standard. A cryptographic algorithm specified by the National Institute of Standards and Technology (NIST) to protect sensitive information. AES is specified in three key sizes: 128, 192, and 256 bits. AES replaces the 56-bit key Data Encryption Standard (DES), which was adopted in 1976." [MS_DICT]
ATA	"Acronym for Advanced Technology Attachment. ANSI group X3T10's official name for the disk drive interface standard for integrating drive controllers directly on disk drives. The original ATA standard is commonly known as Integrated Drive Electronics (IDE)." [MS_DICT]
ATAPI	"…ATAPI […] stands for ATA Packet Interface. ATA/ATAPI is the most popular device interface today. Of the approximately 140 million hard disk drives made in the last year, 90+ percent are ATA. […] [T]he vast majority of CD-ROM drives are

	ATAPI devices. Most PCMCIA and CFA mass storage devices are also ATA or ATAPI devices." [ATA-ATAPI] "The interface used by the IBM PC AT system for accessing CD-ROM devices." [MS_DICT]
FIPS	Federal Information Processing Standard
FPGA	"Acronym for Field Programmable Gate Array. A type of programmable logic chip that can be configured for a wide range of specialized applications after manufacture and delivery. FPGAs can be reprogrammed to incorporate innovations and upgrades. Because of their flexibility and adaptability, FPGAs are used in devices from microwave ovens to supercomputers." [MS_DICT]
IDE	"Acronym for Integrated Device Electronics. A type of disk-drive interface in which the controller electronics reside on the drive itself, eliminating the need for a separate adapter card. The IDE interface is compatible with the controller used by IBM in the PC/AT computer but offers advantages such as look-ahead caching." [MS_DICT]
Key Zeroization	The process of erasing active keys in a cryptographic module
MS_DICT	Microsoft Press Computer Dictionary, 5th ed. Redmond, WA: Microsoft Press, 2002

14 Bibliography

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

Advanced Encryption Standard (AES), FIPS Publication 197. National Institute of Standards and Technology, November 2001, <http://cs-www.ncsl.nist.gov/publications/fips/fips197/fips-197.pdf>.

Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, January 2004, Version 2.2, Revision 256, CCIMB-2004-01-001, <http://niap.nist.gov/cc-scheme/cc_docs/cc_v22_part1.pdf>.

Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, January 2004, Version 2.2, CCIMB-2004-01-002, <http://niap.nist.gov/cc-scheme/cc_docs/cc_v22_part2.pdf>.

Common Criteria for Information Technology Security Evaluation – Part 3: Security Assurance Requirements, January 2004, version 2.2, Revision 256, CCIMB-2004-01-003, <http://niap.nist.gov/cc-scheme/cc_docs/cc_v22_part3.pdf>.

Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, January 2004, Version 2.2, Revision 256, CCIMB-2004-01-004, <http://niap.nist.gov/cc-scheme/cc_docs/cem_v12.pdf>.

[ATA-ATAPI] Landis, Hale. “ATA-ATAPI.COM”.
<http://www.ata-atapi.com>

[MS_DICT] Microsoft Press Computer Dictionary, 5th ed. Redmond, WA: Microsoft Press, 2002

Security Requirements for Cryptographic Modules, FIPS Publication 140-2, National Institute of Standards and Technology, May 2001,
<http://cs-www.ncsl.nist.gov/publications/fips/fips140-2/fips1402.pdf>.