National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Secure Systems Limited

Silicon Data Vault ® Laptop Version SDV18A03-A2-0003 and Desktop Version SDV201B03-0003

Report Number: CCEVS-VR-05-0110

Dated: 15 October 2005

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

Mike Allen

Jerome Myers

Aerospace Corporation

Columbia, Maryland

Royal Purvis

Mitretek Systems

Falls Church, Virginia

Scott Shorter

Orion Security Solutions

McLean, Virginia

Common Criteria Testing Laboratory

COACT, Incorporated

Columbia, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

This report documents the NIAP validation team's assessment of the evaluation of Secure Systems Limited's Silicon Data Vault ® Laptop Version SDV18A03-A2-0003 and Desktop Version SDV201B03-0003. 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 was performed by COACT Incorporated, and was completed during September 2005. The information in this report is largely derived from the Security Target provided by the vendor, and the Evaluation Technical Report (ETR) and associated test reports, all written by COACT. The evaluation determined that the product is both **Common Criteria Part 2 and Part 3 conformant,** and meets the assurance requirements of **EAL 2.** The product is not conformant with any published Protection Profiles, but rather is targeted to satisfy the needs for protection of sensitive information as defined by DoD Standard 8500.2. All security functional requirements are derived from Part 2 of the Common Criteria.

The product family enables multiple users to share a workstation or laptop computer without exposing their data stored on the hard drive to unauthorized users who may have access to the same workstation or laptop computer. The device works independent of any Operating System (OS), with any standard ATA-5 Hard Disk Drive (HDD), and resides in the IDE channel, blocking and controlling all access to the HDD. It provides FIPS 140-2 approved AES encryption of each user's data partitions stored on the HDD. **It is important to note that the TOE is limited to providing access controls to hard disk partitions on devices that are attached to the SDV. The TOE is not aware of any other security features that may or may not be implemented by the platform, the selected operating system or software applications loaded onto the platform. In particular, if an operating system is loaded that enables a network interface, then, from the perspective of the TOE, all access attempts from a remote user or attacker will be granted precisely the same capabilities as the authorized user that booted the operating system and successfully accessed his protected partitions of the HDD through the SDV. Administrators should be careful to configure partition access authorizations appropriate for the potential data exposure from remote users over the network (see Clarification of Scope below).**

The validation team monitored the activities of the COACT evaluation team, participated in team meetings, 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 validation team 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 validation team concludes that the COACT 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	Secure Systems Limited Silicon Data Vault ® Laptop Version SDV18A03-A2-0003 and Secure Systems Limited Silicon Data Vault ® Desktop Version SDV201B03-0003.
Protection Profile	None
Security Target	*Secure Systems Limited Silicon Data Vault ® Security Target*, September 7, 2005.
Evaluation Technical Report	*Evaluation Technical Report for the Secure Systems Limited Silicon Data Vault* ®, September 7, 2005
Conformance Result	Part 2 and Part 3 conformant, EAL 2
Sponsor	Secure Systems Limited
Developer	Secure Systems Limited
Evaluators	COACT Incorporated
Validation Team	The Aerospace Corporation, Mitretek Systems and Orion Security Solutions

3. SECURITY POLICY

The Silicon Data Vault system enforces the following security policies:

3.1. Identification and Authentication Policy

The SDV requires the authorized Administrator and authorized users to be identified and authenticated prior to allowing any security function actions to be taken. The TOE has two roles, the authorized Administrator and authorized users. Identification and Authentication is accomplished by the use of a Username/Passphrase combination. A SHA-1 hash of the Passphrase is compared with the stored known value. When booting the system from the TOE management software CD, the management software performs Identification and Authentication independent and prior to the loading of any Operating System (OS). During the boot sequence of the PC, when the CD housing the TOE management software is not present, the PC's Bios attempts to boot from the HDD, the SDV mocks a HDD Master Boot Record (MBR) and executes the embedded Authentication Application (AA) firmware for user identification and authentication. Once the user selects to load the Operating System, control is passed to the runtime firmware and the SDV appears transparent to the user and OS.

3.2. Access Control Policy

The SDV implements an Access Control mechanism based on users, their access permissions, and the partitions of the protected HDD. The user and access permissions are defined during user account creation. The System Administrator chooses to which partitions of the HDD the user has access and the type of access the user has to the data on that partition. The System Administrator may choose to grant the user read-only access to the partition or read/write access to the partition. If the System Administrator chooses not to assign any level of access for a particular partition to a given user, that user will have no access to the partition and not even know of its existence (i.e., neither the user nor the OS acting on behalf of the user have any knowledge that the partition even exists on the HDD).

3.3. Data Protection Policy

The SDV provides a data protection feature by encrypting all data on the HDD. Each partition on the HDD is encrypted with its own key. All keys within the SDV are randomly generated using the Pseudo-Random Number Generator (PRNG) in Appendix 3.1 of FIPS PUB 186-2. Each user is allocated access to the keys for partitions for which they have access. All keys are encrypted and stored along with user authentication data on the SDV "Stealth" partition, with the exception of the key used to encrypt the Stealth partition itself. The Stealth partition key is stored within the SDV's FLASH memory. The partitions are encrypted using the AES algorithm with 128-bit keys. The SDV is validated for conformance with the FIPS PUB 140-2.

3.4. Security Management

The software held on the SDV management CD provides a Graphical User Interface (GUI) for the System Administrator to manage the SDV and the SDV's user security attributes. The CD is a bootable device whose code executes on the host machine's main processor and allows the administrator to log into the SDV prior to the loading any Operating System installed on the HDD. The SDV provides the ability for the System Administrator to create and delete user accounts. Each account is associated with a Username, a Passphrase, and a set of permissions detailing the partitions to which the user has access and the type of access permitted. The management software allows the System Administrator to complete the SDV initialization, including encrypting the entire HDD, with each partition having its own key on the HDD.

3.5. Self Protection Policy

The SDV operates as three separate processes, each firmware/software component corresponding to its own process. The runtime firmware is executed on the SDV hardware. The SDV hardware provides the runtime firmware its own domain for execution that cannot be bypassed due to the design of the hardware. The SDV management software and embedded AA firmware execute independently and before the loading of any underlying Operating System. The Management software is located on a bootable CD-ROM and the embedded AA firmware is located on the SDV's FLASH memory. Both execute on the host machine without any user intervention or host operating system, and prohibit an operator from bypassing the functionality once it has started execution. These features of the SDV management software and embedded AA firmware make the remaining processes non-bypassable while executing in a separate domain.

4. ASSUMPTIONS

The Secure Systems Limited Silicon Data Vault ® Laptop Version and Secure Systems Limited Silicon Data Vault ® Desktop Version devices are designed to be used in a laptop or workstation that may be configured using various operating systems and applications which may support a variety of security features and policies. The SDV is limited to controlling the access to the data stored on the ATA-5 type disk drive used as part of the workstation or laptop. The SDV provides no control over the security of the workstation on which it is used. Users of the SDV must take care to ensure that their data, when present on the workstation, are protected from other unauthorized users that may be present on a network attached to the laptop or workstation during normal operation. This involves appropriate security measures implemented by the operating system and network interface, both of which are beyond the scope of this evaluation.

4.1. Usage Assumptions

Administrators and authorized users are assumed to be trusted (i.e., non-malicious) and competent to carry out their responsibilities.

Users will power off the workstation or laptop after each use.

4.2. Environmental Assumptions

The SDV has been delivered, installed, and configured in accordance with documented procedures.

The SDV is installed on an IBM compatible PC with a CD-ROM reader.

The PC must have an ATA-5 compatible Hard Disk Drive (HDD).

The file system used on the HDD must be one of the following:

1) FAT 16/FAT 32

2) NTFS

3) EXT 2/EXT 3

4) Reiser

4.3. Clarification of Scope

The SDV TOE implements access controls that restrict platform access to the partitions of the hard disk drives that are attached to the SDV. The TOE operates transparently to any operating system or maintenance applications that are loaded onto the supporting platform. Once an authenticated user boots the system, all access to the drives that are attached to the SDV is restricted by the SDV to the access capabilities of that authenticated user. The TOE is not aware of any other security features of the hardware platform. Therefore, if software is loaded onto the platform that provides for remote users through a network interface or multi-user terminals, then, from the perspective of the SDV, all of those remote users appear to be the same as the locally authenticated user. In other words, connecting the SDV platform to a network interface will allow remote authorized users to assume the same privileges as the locally authenticated user. In addition, a remote unauthorized user (attacker) may be able to exploit a vulnerability of the platform's operating system or applications to be granted the same access privileges. This evaluation did not assess the security of the likely operating systems or applications that may be used in conjunction with the SDV. Any further restrictions on the access permissions to the data stored on the TOE protected disk partitions are the responsibility of the software that is loaded after the SDV authenticates an authorized user.

Because of this limitation, the vendor recommends in its documentation that customers who choose to install the TOE on a platform that will support remote users carefully separate into distinct partitions data and applications that they are willing to expose to network users from data and applications that should only be accessible by local users. Those customers should consider two modes of operations for the SDV platform, namely network connected and stand-alone. They should then create separate authorized user accounts for configurations that will permit network connectivity and separate those for which access is limited to stand-alone operations disconnected from any network.

5. ARCHITECTURAL INFORMATION

The Target of Evaluation (TOE) is manufactured in two models, identified as the Secure Systems Limited Silicon Data Vault ® Laptop Version SDV18A03-A2-0003 and Secure Systems Limited Silicon Data Vault ® Desktop Version SDV201B03-0003. The functionality of the two models is identical with the only difference being the physical layout of the underlying hardware. This distinction allows the Secure Systems Limited Silicon Data Vault ® (SDV) to work on standard Desktop and Notebook (Laptop) computers. Both models execute the same underlying firmware and individual hardware components and are administered by the same management software. The SDV works independent of any Operating System (OS), with any standard ATA-5 HDD, and resides in the IDE channel, blocking and controlling all access to the HDD. The SDV works transparently to the Operating System and users.

The TOE encrypts the system HDD on a per partition basis using the FIPS PUB 140-2 Approved Rijndael algorithm with 128-bit keys in the Advanced Encryption Standard, FIPS PUB 197. For each HDD partition, a separate key is used for encryption. The SDV can encrypt a HDD with up to thirty-one partitions. One partition is reserved as a stealth partition that is used to hold management and configuration information. The stealth partition is unavailable to all users.

The TOE encompasses the SDV hardware board and all its components. The components include the firmware residing on the board and the supporting hardware. Additionally, the SDV management software, stored and run from a bootable CD-ROM, is included as part of the TOE. This management software is a stand-alone executable known as the System Administrator Utility (SAU). When the SAU is executing, the administrator is required to login to the SAU. Should this CD not be present, the user is required to login to the AA firmware prior to loading the Operating System. The HDD protected by the SDV is not included in the TOE boundary.

6. DOCUMENTATION

The following documentation is provided to purchasers of the Secure Systems Limited's Silicon Data Vault ®.

1. Silicon Data Vault® Administrator Guide Desktop, Version 1.4, dated December 6, 2004;
2. Silicon Data Vault® Administrator Guide Laptop, Version 1.4, dated December 6, 2004;
3. Silicon Data Vault® Quick Reference Guide for Desktops
4. Silicon Data Vault® Quick Reference Guide for Laptops

7. IT PRODUCT TESTING

7.1. Developer Testing

Evaluator analysis of the developer's test plan, test scripts, and test results indicate that the developer's testing is adequate to satisfy the requirements of EAL2.

The developer's tests covered all aspects of the normal operation of the SDV including some elements not included in the evaluated configuration. The encryption mechanisms and the management of the encryption keys were tested during FIPS certification.

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

7.2. Evaluator Testing

Although the developer's testing was considered adequate, the evaluators also repeated partial tests of some of the security functions as defined in the Security Target. In addition, several independent tests were developed to further test scenarios not explored by the developer and security functions deemed not adequately tested. The repeated tests are listed below:

- System Administrator and Authorized User Authentication (FIA_AFL.1, FIA_UAU.7, FIA_SOS.1)
- Access Control to the HDD (FDP_ACF.1)
- Management of the TOE (FMT_SMR.1, FMT_MSA.3)
- Self-protection of the TOE (FPT_SEP.1)
- Data Protection (Cryptography) tested under FIPS

Areas tested by the team in the independent tests are as follows:

- FDP_ACC.2
- FDP_ACF.1
- FPT_SEP.1

In addition, a separate test was performed to confirm that a remote user on a shared network could access the data on the SDV when being viewed by an authorized user of the SDV. The testing verified that the access permissions of the remote user were limited by the permissions of the authorized user of the SDV. The test case turned file sharing on to allow other to view that data.

During penetration testing, the evaluators also executed a number of tests to determine if the HDD could be read when removed from the host system. They attempted to find key information on a number of partitions and thus perhaps compromise the key. They attempted to find authentication data on the encrypted partitions using known information and pass phrase cracking tools. In addition, they attempted to use poorly formed password entries to determine if access could be achieved. Finally, they attempted to use a slightly different Operating System configuration in order to change the operation of the TOE.

7.2.1. System Administrator and Authorized User Authentication

Evaluator tests were performed to show that after 3 unsuccessful attempts the user couldn't be authenticated without restarting the computer. Also a test was run to show that the pass phrases are always displayed as asterisks. Finally a test was run demonstrating the limitations on pass phrase creation. Pass phrases that were too short and too long were tried as well as pass phrases with not enough complexity.

7.2.2. Access Control to the HDD

Evaluator tests were performed to verify that when the Administrator logs into SDV all partitions of the HDD are accessible with the exception of the stealth partition.

7.2.3. Management of the TOE

The evaluators performed tests to confirm that only the Administrator has access to the configuration screen, and when a user logs onto the SDV, he only has access to the partitions the administrator granted him permission to see.

7.2.4. Self-protection of the TOE

The evaluators performed tests to verify that the SDV blocks all access to the controlled partition containing the operation system so Bios looks for an alternate boot drive to join.

7.2.5. Data Protection (Cryptography) tested under FIPS

The evaluators confirmed the testing accomplished in order to meet the FIPS certification of the Cryptographic modules on the SDV. The following certificates have been granted:

- FIPS 140-2 Certificate #477
- FIPS PUB 197 Certificate #136
- FIPS PUB 180-2 Certificate #219

7.2.6. FDP_ACC.2

The evaluators further tested SDV access by creating users with various permissions and then confirming the limits on their access to these and other partitions. The testing verified that the access permissions of remote users were limited by the permissions of the authorized user of the SDV.

7.2.7. FDP_ACF.1

The evaluators further tested SDV access by confirming that the Administrator had access to the boot partition and all the other partitions created by the earlier test. They further confirmed the limits on users to read and write data to the partitions based on their permissions as set by the administrator

7.2.8. FPT_SEP.1

The evaluators attempted to locate and read the data on the stealth partition using a set of disk utilities available to the general user.

7.2.9. Vulnerability Testing

All of the evaluator attempts to compromise the HDD data failed. In some cases they were able to see that partitions were present, however, they were unable to decrypt any data including pass phrases and user IDs. The following conclusions were made based on the results of the vulnerability tests performed:

- The stealth partition could not be located or read by conventional disk reading tools.
- The TOE enforces its password policy of minimum 6 characters from a set of 93 characters.
- The OS configuration alteration did not interfere with the correct operation of the TOE.
- The TOE in its intended environment mitigates the identified vulnerabilities.
- All identified TOE vulnerabilities had an attack potential greater than Low so the TOE SOF – Basic claim is valid.

8. EVALUATED CONFIGURATION

The evaluated configuration consists of the Secure Systems Limited's SDV installed in an IBM-compatible PC workstation or laptop. The evaluated configuration requires:

- A power cycle of the workstation or laptop between each use.
- Use of an ATA-5 Hard Disk Drive (HDD).

NOTE: If the SDV is used on a system that is connected to a network, the user should be aware that other users on the network might be able to access the user's data depending on the security policies in place in the user's defined Operating System and the security policies in effect on the network. The System Administrator and the user are responsible for maintaining operating system and network security policies to prevent unauthorized access following SDV authentication.

9. RESULTS OF THE EVALUATION[1]

The evaluation was conducted based upon the Common Criteria (CC), Version 2.2 Revision 256, dated January 2004 [1,2,3]; the Common Evaluation Methodology (CEM), Version 2.2, dated January 2004 [4]; and all applicable National and International Interpretations in effect on 5 August 2004. The evaluation confirmed that the Secure Systems Limited's Silicon Data Vault Laptop Version SDV18A03-A2-0003 and Desktop Version SDV201B03-0003 products are compliant with the Common Criteria Version 2.2, functional requirements (Part 2) and assurance requirements (Part 3) for EAL2. The details of the evaluation are recorded in the CCTL's evaluation technical report, Evaluation Technical Report for the Secure Systems Limited Silicon Data Vault ®, dated July 18, 2005 [6]. The product was evaluated and tested against the claims presented in the Secure Systems Limited Silicon Data Vault ® Security Target, dated September 7, 2005 [5].

The validation team followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The validation team 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 validation team therefore concludes that the evaluation team's results are correct and complete.

9.1. Evaluation of the Security Target (ASE)

The evaluation team applied each EAL 2 ASE CEM work unit. Evaluation team action during the course of the ST evaluation ensured that the ST contained a description of the environment in terms of threats, assumptions and policies; a statement of security requirements claimed to be met by the SDV TOE 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 ensures that the integrity of the TOE is adequately preserved; in particular, that configuration management provides confidence to the consumer that the TOE and documentation used for evaluation are the ones prepared for distribution. It also ensures that the TOE is accurately and uniquely identified such that the consumer is able to identify the evaluated TOE and discern one version from another. Configuration Management (CM) systems are put in place to ensure the integrity of the portions of the TOE that they control, by providing a method of tracking changes and by ensuring that all changes are authorized. The Evaluation Team identified and analyzed the Secure Systems Limited CM process to ensure that its documented procedures were followed and the procedures were employed during the course of this evaluation. The evaluation team ensured that the following items

[1] The terminology in this section is defined in CC Interpretation 008, specifying new language for CC Part 1, section/Clause 5.4.

were considered configuration items: TOE implementation, design documentation, test documentation, and Administrator and user guidance.

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 securely deliver, install, configure, and operationally use the TOE; and ensured that the security protection offered by the TOE was not compromised during that process.

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 implements/employs 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.

9.5. Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 2 AGD CEM work unit. The evaluation team verified the adequacy of the administrator guidance in describing how to securely administer the SDV TOE. In addition, the team verified that the user guidance adequately describes how the use the TOE in a secure manner.

9.6. 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 functional specification and as stated in the TOE security functional requirements. The evaluation team performed a sample of the Secure Systems Limited test suite, and devised an independent set of team tests and penetration tests. The Secure Systems Limited tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

9.7. 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 obvious vulnerabilities that can be exploited in the evaluated configuration, based upon the Secure Systems Limited's strength of function analysis and the Secure Systems Limited vulnerability analysis as well as the evaluation team's performance of penetration tests.

9.8. 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 the vendor test suite, several independent tests, and the penetration test further demonstrated the claims in the ST.

10. VALIDATOR COMMENTS

The validation team's observations support the evaluation team's conclusion that the Secure Systems Limited's Silicon Data Vault ® Laptop Version SDV18A03-A2-0003 and Desktop Version SDV201B03-0003 meet the claims stated in the Security Target. The validation team also wishes to emphasize that the TOE must be installed and operated in the evaluated configuration in order to ensure that the TOE provides the security functionality described in the security target. In addition, it is important for System Administrators and users to understand that when the desktop or laptop is connected to a network, other users on the network may have access to the decrypted user data from the SDV (see Section 4.3). The System Administrator and the user are responsible for maintaining operating system and network security policies to prevent unauthorized network access following SDV authentication, and for defining and using user IDs and permissions appropriate for the level of risk of data exposure to remote network users. That is, users and Administrators should separate data partitions into those that they are willing to allow remote network access from those that they are unwilling to risk remote connectivity. The SDV is capable of segregating these different partitions and preventing unauthorized access from one partition to another.

11. SECURITY TARGET

F2-0705-007(1) Secure Systems Limited Silicon Data Vault® Security Target, dated September 7, 2005.

12. GLOSSARY

AA	Authentication Application
AES	Advanced Encryption Standard
API	Application Program Interface
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CM	Configuration Management
DoD	Department of Defense
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standards
HDD	Hard Disk Drive
IT	Information Technology
MBR	Master Boot Record
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PKI	Public Key Infrastructure

PP	Protection Profile
PRNG	Pseudo-Random Number Generator
SAU	System Administrator Utility
SDV	Silicon Data Vault
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

13. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated January 2004, Version 2.2 Revision 256.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated January 2004, Version 2.2 Revision 256.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated January 2004, Version 2.2 Revision 256.

[4] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated January 2004, Version 2.2 Revision 256.

[5] Secure Systems Limited Silicon Data Vault ® Security Target, dated September 7, 2005.

[6] Evaluation Technical Report for the Secure Systems Limited Silicon Data Vault ®, dated September 5, 2005.