National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Secutor Systems, Inc.
DataVault X4 V1.0
EAL4

Report Number: CCEVS-VR-05-0118
Dated: September 23, 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

Timothy J. Bergendahl
The MITRE Corporation
Bedford, MA 01730

Common Criteria Testing Laboratory

Science Applications International Corporation
7125 Gateway Drive
Columbia, MD 21046

Evaluation Team

Cynthia Reese
Shukrat Abbass
Dawn Campbell
Kesha Webb

Table of Contents

I. Executive Summary

The purpose of this Validation Report (VR) is to document the results of the EAL4 evaluation of the `Secutor Systems, Inc. DataVault X4 v1.0` (hereafter `DataVault X4`), a product of Secutor Systems, Inc., Chesapeake, VA.

The purpose of the `DataVault X4` is to provide two completely isolated hardware-based security domains simultaneously where no information, memory, storage devices, BIOS, or CPU is shared between domains. Each domain, however, shares a mouse, keyboard, case with power supply, and a keyboard and mouse (K&M) switch with the other domain. One domain is called UNSECURE and the other is called SECURE. Separate components within each domain (e.g., network interface card (NIC); CD-ROM; hard drive; floppy drive; Microsoft Windows 2000 operating system) allow the `DataVault X4` to provide network and multi-tasking functionality on a per-domain basis simultaneously while maintaining isolation between the domains. Additional security features of the `DataVault X4` include hardware-based access control via locks and keys, and the use of a smart card to access the SECURE domain.

Evaluation of the `DataVault X4` at EAL4, was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL), Columbia, MD. Evaluation results identified in this validation report (VR) were drawn from the Evaluation Technical Report (ETR) prepared by the SAIC CCTL.

This Validation Report is not an endorsement of the `DataVault X4` product by any agency of the United States Government, and no warranty of the product is either expressed or implied.

The TOE includes security functions implemented at the TOE interfaces, as follows:

- User data protection
- Mandatory Access Control and Identification and Authentication
- Security Management
- Protection of the TSF

No Strength of Function claim is made for the *`DataVault X4`*.

The `DataVault X4 v1.0` TOE was evaluated using the *Common Criteria for Information Technology Security Evaluation*, Version 2.2, Revision 256, January 2004 [CCV2.2], and the *Common Methodology for Information Technology Security Evaluation*, Evaluation Methodology, Version 2.2, Revision 256, January 2004 [CEMV2.2]. The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme

(CCEVS) best practices as described within CCEVS Publication #3 [CCEVS3] and Publication #4 [CCEVS4].

The Security Target (ST) for the `DataVault X4` is contained within the document *Secutor Systems, Inc. Data Vault X4 v1.0 EAL4 Security Target*, Version 1.0, 23 September 2005 [ST_SEC4].

The project, which also involved evaluation of the associated Security Target, was completed on September 23, 2005.

II. Identification

The National Information Assurance Partnership (NIAP) is a U.S. Government initiative involving the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). The Common Criteria Evaluation and Validation Scheme (CCEVS) is an activity of the NIAP.

The focus of the CCEVS is to establish a national program for the evaluation of information technology products for conformance to the *International Common Criteria for Information Technology Security Evaluation* (*Common Criteria*).

The CCEVS Validation Body approves the participation of Common Criteria Testing Laboratories (CCTLs) for the purpose of performing evaluations of IT products or Protection Profiles. During the course of an evaluation, the Validation Body provides technical guidance to the CCTL and validates the results of the evaluation for conformance to the *Common Criteria*.

When appropriate, the Validation Body issues a Common Criteria Certificate. The Certificate, together with its associated Validation Report (VR), confirms that an IT product or Protection Profile has been evaluated at an accredited CCTL using the *Common Evaluation Methodology* for conformance to the *Common Criteria*.

The following table identifies the evaluated product.

Item	**Identifier**
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Secutor Systems Inc. `DataVault X4 v1.0`
Security Target	*Secutor Systems, Inc. Data Vault X4 v1.0 EAL4 Security Target*, Version 1.0, 23 September 2005. [ST_SEC4]

Item	Identifier
CC Identification	*Common Criteria for Information Technology Security Evaluation*, Version 2.2, Revision 256, January 2004. [CCV2.2]
CEM Identification	*Common Methodology for Information Technology Security Evaluation*, Evaluation Methodology, Version 2.2, Revision 256, January 2004. [CEMV2.2] Part 2: Evaluation Methodology, Supplement, ALC_FLR – Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R. [CEM-2001/0015R]
Interpretations	There are no applicable interpretations.
Evaluation Technical Report	Provided by the SAIC Evaluation Team, August 2005.
Conformance Result	Security Target, [ST_SEC4]: [CCV2.2] conformant; TOE (`DataVault X4 v1.0`) [CCV2.2] Part 2 and Part 3 conformant.
Sponsor	Secutor Systems, Inc., Chesapeake, VA
Developer	Secutor Systems, Inc., Chesapeake, VA
Evaluators	Science Applications International Corporation (SAIC), Columbia, MD
Validator	The MITRE Corporation, Bedford, MA

2.2 TOE Overview

The TOE is the `Secutor Systems, Inc. DataVault X4 v1.0`. An image of the TOE is shown in the Figure 1, and TOE components are enumerated in Annex A.

Figure 1. Data Vault X4 TOE.

The purpose of the DataVault X4 is to provide two completely isolated hardware-based security domains where no information, memory, storage devices, BIOS, or CPU is shared between domains. Each domain, however, shares a mouse, keyboard, case with power supply, and a keyboard and mouse (K&M) switch with the other domain. One domain is called UNSECURE and the other is called SECURE. Separate components within each domain (e.g., network interface card (NIC); CD-ROM; hard drive; floppy drive; Microsoft Windows 2000 operating system) allow the DataVault X4 to provide network and multi-tasking functionality on a per-domain basis simultaneously while maintaining isolation between the domains. Additional security features of the DataVault X4 include hardware-based access control via locks and keys, and the use of a smartcard to access the SECURE domain.

Two locked panels (front and back) protect the TOE from unauthorized access. The same physical key labeled #1 is used to unlock these panels. Inside of the front panel is an on/off key/lock switch that is used to activate the system. A key labeled #2 is required for the on/off key/lock switch. Key #2 can also be used for a lock inside of the back panel used to activate or deactivate a case-open alarm that, when activated, will sound when the top of the DataVault X4 case is removed. A third key, labeled #3, can be used for a lock inside of the front panel that is used to remove the removable hard drive in the SECURE domain.

A Key Administrator is a person who controls key #1 key #2, and key #3. In addition, the Key Administrator controls a smart card (not a TOE component) that plays a role when a person attempts to access the SECURE domain. The Key Administrator retains key #1 at all times, but might provide another person with key #2, key #3, or the smart card. If only key #2 is provided to another person, that person is known as a User. If key #2 and the smart card are provided to another person, that person is known as a Trusted User. Key #3 would only be provided to a Trusted User.

The Key Administrator could, of course, retain all of the keys and have access to all of the functionality of the DataVault X4. In addition, the Key Administrator does not need a smart card to access the SECURE domain.

Before anyone can use the DataVault X4, the Key Administrator must open the front locked panel using Key #1. Key #2 can then be used by a User or Trusted User to turn on the system (both domains boot at the same time), with access to the UNSECURE domain resulting. Since a User would not possess a smartcard, a User can only access the UNSECURE domain.

To access the SECURE domain, a Trusted User (while in the UNSECURE domain) inserts the smart card into the smart card reader located on the front of the TOE and switches to the SECURE domain (e.g., by using the domain selector switch mounted the front of the TOE). The SECURE domain monitor is inactive except for a GUI that requests the PIN associated with the smart card. After PIN entry, if the smart card identification and authentication is correct, access to the SECURE domain is granted. The

Trusted User can then switch between domains (e.g., using the domain selector switch), both of which remain active but separate from each other.

The SECURE domain has a removable hard drive, with Key #3 being required to open the lock that allows for its removal.

Use of key #3 (needed to remove the hard drive in the SECURE domain) is restricted to a Key Administrator and the Trusted User.

The inside of the back panel of the `DataVault X4` contains ports and other components that must be protected from unauthorized access. Only the Key Administrator can open the back panel via key #1.

After the back panel is open, the holder of key #2 can activate or deactivate a case-open alarm that, when activated, will sound when the top of the `DataVault X4` case is removed.

Other features provided by the TOE include:

- UNSECURE domain
  - internal hard drive (Read/Write enabled)
  - floppy drive (Read/Write enabled)
  - DVD/CDRW (Read/Write enabled)
- SECURE domain
  - removable hard drive (Read/Write enabled) - key #3 required for removal
  - floppy drive (Read enabled, Write disabled mechanically)
  - DVD/CDRW (Read enabled, Write disabled mechanically)

The features identified above allow a Trusted User to move data from the UNSECURE to the SECURE domain using a floppy disk or a CD, but not vice-versa.

It is also possible to export data from the SECURE domain via a USB port located inside of the rear panel (after the panel is opened with key #1 by the Key Administrator).

III. Security Policy

The security policy for the `DataVault X4` TOE is as follows.

- User data protection
- Mandatory Access Control and Identification and Authentication
- Security Management
- Protection of the TSF

User Data Protection is enforced via complete information flow control between security domains, where each domain (SECURE and UNSECURE) provides separate isolated hardware and software. The TOE allows data to be copied from the UNSECURE domain (floppy or CD-ROM), then transferred to the SECURE domain, but not vice versa, since the "Write" function feature of the floppy disk and CD-ROM is disabled on the SECURE domain.

Mandatory Access Control and Identification and Authentication is enforced by requiring users to be successfully identified prior to gaining access to the TOE and its functions (e.g., possession of key #2 to power on the DataVault X4 in order to access the UNSECURE domain). To further access the SECURE domain, the Trusted User or Key Administrator needs a smart card for authentication and identification.

Security management is enforced by requiring roles (Key Administrator; Trusted User; User) before access to the TOE is granted.

Protection of the TSF is enforced since access to the domains is via the keys and smart card the user possess. The TSF also controls the information that can flow between domains.

IV. Threats and Assumptions

4.1 Threats that the TOE is designed to counter

Threat	Description
T.LOCK	The TOE's panels (front, back, and top) may be compromised by an unauthorized user, therefore exposing the TOE hardware.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE to access and exploit security functions provided by the TOE.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.

4.2 Assumptions made on the operational environment

Assumption	Description
A.KEYS	Access to specific keys and Smart Card is restricted to users, trusted users, and Key Administrators.
A.LOCATE	The TOE will be located within controlled access facilities that will

Assumption	Description
	prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The Key Administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.

4.3 Usage assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL4 assurance requirements.

ADO_DEL.2 Detection of modification
ADO_IGS.1 Installation, generation, and start-up procedures
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

V. Security Functional Requirements

The security functional requirements against which the `DataVault X4` was evaluated are displayed in the table below. The requirements were taken from Part 2 of the *Common Criteria* [CCV2.2].

Requirement Class	Functional Component Name
FDP: User data protection	FDP_IFC.2 Complete information flow control
	FDP_IFF.1 Simple security attributes
FIA: Identification and authentication	FIA_ATD.1 User attribute definition
	FIA_UID.2a User identification before any action
FMT: Security management	FMT_SMR.1 Security roles
FPT: Protection of the TSF	FPT_PHP.1 Passive detection of physical attack
	FPT_RVM.1 Non-bypassability of the TSP
	FPT_SEP.1 TSF domain separation

VI. Assurance Requirements

The EAL4 security assurance requirements against which the `DataVault X4` was evaluated are displayed in the table below. The requirements were taken from Part 3 of the *Common Criteria* [CCV2.2].

Requirement Class	Assurance Component Name
ACM: Configuration management	ACM_AUT.1 Partial CM automation
	ACM_CAP.4 Generation support and acceptance procedures
	ACM_SCP.2 Problem tracking CM coverage
ADO: Delivery and operation	ADO_DEL.2 Detection of modification
	ADO_IGS.1 Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.2 Fully defined external interfaces
	ADV_HLD.2 Security enforcing high-level design
	ADV_IMP.1 Subset of the implementation of the TSF
	ADV_LLD.1 Descriptive low-level design
	ADV_RCR.1 Informal correspondence demonstration
	ADV_SPM.1 Informal TOE security policy model
AGD: Guidance documents	AGD_ADM.1 Adminitrator guidance
	AGD_USR.1 User guidance
ALC: Life cycle support	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cysle model
	ALC_TAT.1 Well-defined development tools
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.1 Validation of analysis
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.2 Independent vulnerability analysis

VII. Evaluated Configuration

The evaluated configuration is the `Secutor Systems, Inc. DataVault X4 v1.0` TOE.

VIII. TOE Testing

Testing of the `DataVault X4` took place during 19-20 July 2005, at Secutor Systems, Inc., Chesapeake, VA.

For testing purposes, the TOE was connected to two separate live networks simultaneously, one on the UNSECURE domain side and the other on the SECURE domain side. An authentication server was interfaced with the network on the SECURE domain side in order to support the smart card functionality of the TOE.

The SAIC evaluation team executed all of the developer tests, as well as tests they devised. Testing covered each security functional component claimed for the TOE, and demonstrated the validity of each component.

The SAIC evaluation team also performed penetration testing as required at EAL4.

IX. Validation Process and Conclusions

The SAIC Evaluation Team followed the procedures outlined in *Guidance to CCEVS Approved Common Criteria Testing Laboratories*, Scheme Publication #4, Version 1.0, March 20, 2001 [CCEVS4].

The Evaluation Team concluded that (a) the ST [ST_SEC4] is *Common Criteria* V2.2 conformant, and (b) the TOE is *Common Criteria* V2.2 Part 2 and Part 3 conformant, and recommended that an EAL4 certificate rating be issued for the `DataVault X4 v1.0`.

The Validator agreed with the conclusion of the SAIC Evaluation Team (for EAL4), and recommended to CCEVS Management that a certificate be issued for the `Secutor Systems, Inc. DataVault X4 v1.0`.

X. Validator Comments

- Although not part of the TOE, the IT environment authentication server and its interaction with the SECURE domain operating system of the `DataVault X4`

plays an important role in the smart card authentication described in [ST_SEC4]. As such, it is essential that a consumer fully understands how to properly configure the authentication server.

- The Security Target [ST_SEC4] indicates that the purpose of the `DataVault X4` is for processing classified and unclassified data. However, such a purpose is not stated in this VR, since the Validator believes a purpose such as "processing data of different sensitivities" is more appropriate.

- The `DataVault X4` is an interesting product that can only be fully appreciate via hands-on interaction.

XI. Documentation

Documentation applicable to the `DataVault X4` Delivery Procedures, Installation and Generation, Administrator Guidance, and User Guidance is identified in the table below.

Delivery Procedures
• *SSI Configuration Management*, Version 1.2 • *SSI Administrator Guidance*, Version 1.4 • *SSI User Guidance*, Version 1.1
Installation and Generation
• *SSI Administrator Guidance*, Version 1.4
Administrator and User Guidance
• *SSI Administrator Guidance*, Version 1.4 • *SSI User Guidance*, Version 1.1

Additional documentation, most of which is proprietary, was available to the Evaluation Team during the evaluation of the `DataVault X4`.

ANNEXES

Annex A: TOE Components

The DataVault X4 TOE includes the hardware and software identified below (or their functional equivalents) as well as the user documentation provided.

- SSI case
- Domain selector switch (K&M) 2 port
- SSI power pack
- Processor: CPU - Intel Pentium IV x 2
- Motherboard: AAEON P860 x 2
- Chipset: Intel 440BX
- BIOS:
  - 2 MB AMI Flash BIOS
  - APM 1.2, DMI 2.1, Plug and Play
- Memory: 512 MB DDR 333 x 2
- Video: (64MB) Intel (build-in)
- Hard Drives:
  - 80.0GB ATA (internal)
  - 80.0GB ATA (removable. Secure domain)
- 5.5-inch removable SECURE hard drive case (1)
- CD-ROM: CD-ROM drive x 1 (slim secure domain)
- DVD/CDRW drive x 1 (slim unsecured domain)
- Floppy drive: 3.5-inch 1.44MB x 1 (slim secure domain)
- Floppy drive: 3.5-inch 1.44MB x 1 (unsecured domain)
- Network Interface Card (NIC): Intel x 2
- Keyboard: STC E05300
- Mouse or Trackball
- Monitor: dual Double Sight 15-inch LCD x 2
- Sound Card: Creative SB16
- Speakers: Mli-699
- Tamper-proof case
- Fortezza FIPS 140-1/2 certified crypto/Smart Card identification and authentication combo drive
- Operating System: Windows 2000
- Keys # 1, 2, 3 (one set)
- Cables

Annex B: Glossary

Acronym	Expansion
CC	*Common Criteria for Information Technology Security Evaluation*. [Note: Within this Validation Report, CC always means Version 2.2, January 2004.]
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
K&M	Keyboard and mouse
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
PCMCIA (card)	Personal Computer Memory Card International Association (card)
PP	Protection Profile
SAIC	Science Applications International Corporation
SSI	Secutor Systems Inc.
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
USB	Universal Serial Bus
VR	Validation Report

Annex C: Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS) (www.niap.nist.gov/cc-scheme).

- Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) (www.saic.com/infosec/cctl/)

- Secutor Systems, Inc. (www.secutorsystems.com)

CCEVS Documents

[CEMV2.2] *Common Criteria for Information Technology Security Evaluation*, Evaluation Methodology, Version 2.2, Revision 256, January 2004, CCIMB-2004-01-004.

[CEM-2001/0015R] *Common Methodology for Information Technology Security Evaluation*, Part 2: Evaluation Methodology, Supplement: ALC_FLR – Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R [CEM-2001/0015R].

[CCV2.2] *Common Criteria for Information Technology Security Evaluation*, Version 2.2, Revision 256, January 2004, Part 1 (CCIMB-2004-01-001); Part 2 (CCIMB-2004-01-002); and Part 3 (CCIMB-2004-01-003).

[CEMV2.2] *Common Criteria for Information Technology Security Evaluation*, Evaluation Methodology, Version 2.2, Revision 256, January 2004, CCIMB-2004-01-004.

[CEM-2001/0015R] *Common Methodology for Information Technology Security Evaluation*, Part 2: Evaluation Methodology, Supplement: ALC_FLR – Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R [CEM-2001/0015R].

[CCEVS3] *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, February 2002.

[CCEVS4] *Guidance to CCEVS Approved Common Criteria Testing Laboratories*, Scheme Publication #4, Version 1.0, March 20, 2001.

Security Target

[ST_SEC4] *Secutor Systems, Inc. Data Vault X4 v1.0 EAL4 Security Target*, Version 1.0, 23 September 2005.