National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

BAE Systems Information Technology, Inc.
XTS-400 Version 6.4.U4

Report Number: **CCEVS-VR-VID10293-2008**
Dated: **July 3, 2008**
Version: **2.3**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, Maryland 20878

National Security Agency
Information Assurance Directorate
9600 Savage Road Suite 6757
Fort George G. Meade, MD 20755-6740

Acknowledgements:

The TOE evaluation was sponsored by:

BAE Systems Information Technology Inc.

Evaluation Personnel:
Arca Common Criteria Testing Laboratory
Ms. Diann Carpenter
Mr. J. David Thompson
Dr. Gary Grainger
Mr. John Boone
Ms. Louise Huang
Mr. Ray Rugen
Mr. Ken Dill

The National Security Agency

.

Validation Personnel:
Dr. Jerome Myers, The Aerospace Corporation
Mr. Daniel Faigin, The Aerospace Corporation

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the BAE XTS-400 Version 6.4.U4 Operating System. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of the BAE XTS-400 Version 6.4.U4 Operating System (TOE) was performed by the Arca Common Criteria Testing Laboratory (CCTL) in the United States and was completed during July 2008. The information in this report is largely derived from an Evaluation Technical Report (ETR) held by the NSA which combines a proprietary ETR written by Arca with a proprietyary NSA report documenting the vulnerability analysis. The combined evaluation determined that the product conforms to CC version 2.3 Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 5 augmented with ALC_FLR.3 (Systemic Flaw Remediation) and ATE_IND.3 (Independent Testing – Complete) resulting in a "pass" in accordance with CC Part 1 paragraph 175. The evaluation determined that the product also conformed to the *Labeled Security Protection Profile (Version 1.b)* and the *Controlled Access Protection Profile (Version 1.d)*.

The XTS-400™ product is a combination of STOP™ revision 6.4.U4, a multilevel secure operating system, and a BAE Systems Information Technology, Inc.-supplied x86 hardware base. STOP is a 32-bit, multiprogramming, multi-tasking, operating system that can support multiple concurrent users. In addition to proprietary interfaces for secure administration, STOP™ provides a Linux®-like user environment and programming interface (API/ABI) that allows many programs written for Linux to be copied to the XTS™ and run without change while benefiting from the designed-in security that STOP™ and the XTS-400™ provide.

An X-windows graphical user interface (GUI) is included within the Target of Evaluations and is available at the console for work by untrusted users. Trusted path initiation causes suspension of the GUI and trusted commands cannot be run from the GUI. All windows on the display are at the same level and multi-level cut-and-paste is not supported.

Network connectivity on up to 17 different networks is allowed in the evaluated configuration. TCP/IP and Ethernet are included in the Target of Evaluation (TOE), but not network servers (e.g., SMTP). Within an evaluated configuration, network attachments must be made according to rules in the Trusted Facility Manual (e.g., the network must be single-level while multiple networks can each be at a different level). Remote users or unusual network traffic cannot compromise the TOE, but the TOE itself does not prevent disclosure of (or loss of integrity by) data on the network.

The system provides mandatory access control that allows for both a security and integrity policy. It provides 16 hierarchical sensitivity levels, 64 non-hierarchical sensitivity categories, eight hierarchical integrity levels, and 16 non-hierarchical integrity categories. The mandatory security policy (MAC) enforced by the XTS-400 is based on the (formal) Bell-LaPadula security model; the mandatory integrity policy (MIC) is based on the (formal) Biba integrity model. The system implements discretionary access control (DAC) and provides for user identification and authentication needed for user ID-based policy enforcement.

Individual accountability is provided with an auditing capability. Data scavenging is prevented through residual data protection mechanisms. A trusted path mechanism is provided by the implementation of a Secure Attention Key (SAK), which provides trusted communications between users and the system.

The separation of administrator and operator roles is enforced using the integrity policy. The system enforces the "principle of least privilege" (i.e., users should have no more authorization

than that required to perform their functions) for administrator and operator roles. All actions performed by privileged (and normal) users can be audited. The audit log is protected from modification using integrity and subtype mechanisms. STOP™ also provides an alarm mechanism to detect the accumulation of events that indicate an imminent violation of the security policy.

STOP™ was designed from the ground up with strong internal architectural characteristics to resist penetration and minimize the chance of bugs. STOP uses hardware privilege level and memory protection mechanisms to protect itself from tampering and to isolate processes from one another.

STOP™ consists of the TOE Security Functions (TSF) software and a body of untrusted application code and commands. The TSF consists of the hardware and four major software components:

- The Security Kernel operates in the most privileged domain and provides all mandatory, subtype, and a portion of the discretionary access control.
- TSF System Services operates in the next-most-privileged domain, and implements a hierarchical file system, supports user I/O, and implements the remaining discretionary access control.
- Operating System Services (OSS) operates in a less privileged domain and provides the Linux-like interfaces.
- Trusted Software operates in the lowest privileged domain and provides the remaining security services and user commands.

The XTS-400™ is available on Intel Xeon (P4) based server class systems, available in tower, and rack-mount chassis. All components are commercial-off-the-shelf (COTS). The XTS-400™ uses specific Intel-brand motherboards and industry standard ISA or PCI peripheral cards or chips built into the motherboard.

In addition to more basic components, the evaluated configuration allows:

- CD-ROM drive
- 4mm DAT tape drive
- PC card readers
- Add-in Ethernet cards
- Add-in SCSI host adapters
- Parallel PCL-5 printer
- Serial terminal
- Touchpads
- Flat panel displays

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the Common Evaluation Methodology (CEM) work unit verdicts), and reviewed successive versions of the ETR and test report.

The validation team determined that the evaluation team showed that the product satisfies all of the functional and assurance requirements defined in the Security Target for an EAL 5 augmented with ALC_FLR.3 and ATE_IND.3 evaluation. Therefore the validation team concludes that the Arca CCTL findings are accurate, and the conclusions justified.

2 Identification

The CCEVS is a National Security Agency (NSA) 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) or candidate CCTLs using the CEM for EAL 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs and candidate 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 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
- The organizations and individuals participating in the evaluation

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	BAE-IT XTS 400 Version 6.4.U4
Protection Profile	Labeled Security Protection Profile (Version 1.b) and the Controlled Access Protection Profile (Version 1.d)
Security Target	Security Target, Version 1.22 for XTS-400, Version 6.4.U4 dated June 2008
Evaluation Technical Reports	• ASE Evaluation Technical Report for Security Target, Version 1.22 for XTS-400 Version 6.4.U4, Version 2.0 dated July 3, 2008. • BAE XTS 400 V6.4.U4 EAL 5 Augmented Evaluation Technical Report Version 2.0 dated July 3, 2008. • XTS-400 V6.4.U4 Vulnerability Assessment ETR, dated June 2008.
Conformance Result	CC Part 2 and CC Part 3 conformant, EAL 5 augmented with ALC_FLR.3 and ATE_IND.3
Version of CC	CC Version 2.3
Applicable interpretations and precedents	Compliant with all international interpretations with effective dates on or before July 11, 2007.
Sponsor/Developer	BAE Systems Information Technology, Inc. 2525 Network Place Herndon, VA 22171

Item	Identifier
Evaluators	SAVVIS Communications Arca Common Criteria Testing Laboratory NVLAP Lab Code 200429 45901 Nokes Boulevard Sterling, VA 20166 The National Security Agency
CCEVS Validator(s)	Dr. Jerome Myers Mr. Daniel Faigin

3 Security Policy

The TOE is the XTS-400 product, which is a combination of STOP revision 6.4.U4, a multilevel secure operating system, and a BAE-IT-supplied x86 hardware base. STOP is a 32-bit, multiprogramming, multi-tasking, operating system that provides these features:

- Associate sensitivity labels with all objects and all its users will have an associated clearance level identifying the maximum security label of data that they may access
- Allow simultaneous use of the system by multiple users, all with different clearances and needs-to-know
- Allow simultaneous network connectivity to networks of differing sensitivities/ classifications;
- Mandatory integrity protection of files
- An untrusted operating environment that includes common Linux commands and tools
- An Application Programming Interface/Application Binary Interface that is suitable for running most Linux applications in their binary format (no recompilation required)

The TOE implements the following security policies.

3.1 Identification and Authentication Policy

The TSF ensures that each user is uniquely identified and authenticated prior to being able to perform any TSF-mediated functions. The identification and authentication policy ensures that sufficient information is available for the TOE to bind user attributes (e.g. sensitivity clearance, role, integrity level) to user sessions for the purpose of implementing the other security policies described below. The identification and authentication policy also enforces a lockout policy that locks out users based upon an administratively specified number of failed login attempts.

3.2 Mandatory Access Control Policy

The TSF implements a Bell-LaPadula style Mandatory Access Control (MAC) based on user clearance (level and category(ies)) of the subject and classification (level and category(ies)) of the object. The MAC policy is enforced over all identified system resources (i.e., subjects, storage objects, and I/O devices) that are accessible, either directly or indirectly, to subjects external to the TSF. The TSF provides *16* hierarchical sensitivity levels and 64 non-hierarchical sensitivity categories. The combination of mandatory sensitivity hierarchical and non-hierarchical levels is called the *Mandatory Access Control (MAC) label.*

The TOE provides a dominates function that is used to compare sensitivity labels; this comparison is done whenever a subject external to the TSF accesses an object. Every user has an identification and authentication database record that specifies the MAC label of the user's clearance. The TSF enforces the restriction that any subject created on behalf of a user has a current MAC label dominated by the user's clearance.

The types of access that are relevant are read and write — execute is considered the same as read. The MAC label of processes and some objects can not be modified. Only administrators can change the MAC label of an object, except that a user (who has been granted an appropriate capability) can change the label of objects that s/he owns. A MAC label change to an object will take effect immediately, even if that means denying access to the object by a process which already has the object "open."

Mandatory security control is used internally by the TSF to prevent viewing of sensitive TSF data, including the audit trail and authentication data.

.

3.3 Mandatory Integrity Control Policy

The TOE implements a Biba style Mandatory Integrity Control (MIC) Policy that enforces an integrity policy on all authorized users and TOE resources to prevent malicious entities from corrupting data. The TOE provides 8 hierarchical integrity levels and non-hierarchical integrity categories. The combination of mandatory integrity hierarchical and non-hierarchical levels is called the Mandatory Integrity Control (MIC) label. Some of the hierarchical integrity levels are used by the system to provide role separation, and the others are available to users.

The MIC is based on user clearance, user integrity label of the subject, and integrity label of the object. The TSF enforces a MIC policy over all identified system resources (i.e., subjects, storage objects, and I/O devices) that are accessible, either directly or indirectly, to subjects external to the TSF. The TOE provides a dominates function that is used to compare integrity labels; this comparison is done whenever a subject external to the TSF accesses an object. Every user has an identification and authentication database record that specifies the MIC label of the user's clearance. The TSF enforces the restriction that any subject created on behalf of a user has a current MIC label that dominates the user's MIC clearance.

The types of access that are relevant are read and write — execute is considered the same as read. The MIC label of processes and some objects can not be modified. Only administrators can change the MIC label of an object, except that a user (who has been granted an appropriate capability) can change the label of objects that s/he owns. A MIC label change to an object will take effect immediately, even if that means denying access to the object by a process which already has the object "open."

Mandatory integrity control is used internally by the TSF to prevent modification or deletion of TSF data, including the audit trail and configuration parameters for "alarm" mechanisms (such as low disk space, low audit trail space, excessive failed login attempts).

3.4 Discretionary Access Control Policy

The TOE implements a Discretionary Access Control Policy (DAC) that restricts access to objects based on the identity of subjects and/or groups to which they belong, and allows authorized user to specify protection for objects that they control.

The TOE allows owning users to define and control access to named objects through the use of an Access Control List (ACL). Every subject has associated with it an effective user and group; every named object has an ACL. Each ACL contains permissions that specify the allowable access for the owning user, the owning group, up to seven other user or groups, and any user or group not explicitly listed. These permissions can either grant or deny a particular form of access to a named object. When a subject introduces an object into its address space, the ACL is checked to ensure that the subject can access the object.

The types of access that are controlled are read, write, and execute. Write does not imply the ability to delete and some objects cannot be executed.

Only administrators can introduce new users and groups to the system, establish the group membership of users, or set the default group for users. Normal users can change the discretionary attributes of only the objects they own, but administrators can change the attributes of any object.

3.5 Audit Policy

The TOE implements an audit policy that allows authorized administrators to detect and analyze potential security violations. The audit policy mandates that the TOE:

- Provide a means to generate audit records of security-relevant events
- Allow only authorized administrator to define the criteria used for the selection of events to be audited, include or exclude auditable events from the set of audited events based on specified attributes
- Recognize and creates an audit record resulting from a change of management functions
- Provide mechanisms to prevent audit data loss such as loss of audit records due to audit storage failure

Audit events are generated by the Trusted Software, Operating System Software, TSF System Services, and the Kernel and include the following types of events:

- Startup and shutdown of the operating system
- Use of special permissions that circumvent the access control policies
- Login attempts
- Logout commands issued
- Opens and closes of file system objects
- Creates and deletes of file system objects
- Operator commands issued
- Administrator commands issued
- Print request issued with no markings

The Audit policy also mandates that all audit records include the following attributes:

- Date and time of the event
- Type of event
- Process ID of the process causing the audit event
- MAC and MIC label of the process
- Effective privileges of the process
- Real user ID
- Real group ID

3.6 Separation of Roles Policy

The XTS-400 product provides pre-defined “operator”, and “administrator” roles. The separation of administrator and operator roles is enforced using the integrity policy. The system enforces the “principle of least privilege” (i.e., users should have no more authorization than that required to perform their functions) for administrator and operator roles.

3.7 Management Policy

The TSF implements a policy that regulates the management of TSF data. A combination of MAC, DAC, MIC, and roles are used to specify which users are authorized to initialize, view, modify, or delete the security attributes maintained by the TSF.

3.8 Residual Information Protection Policy

The TOE implements a policy that prevents the scavenging of residual data. The TSF ensures that all previous information content of a resource is made unavailable before the resource is reallocated to an object.

3.9 Trusted Path Policy

The TOE implements a trusted path policy that permits a user to be sure s/he is interacting directly with the TSF during sensitive operations. Note that “remote” users (i.e., across a network) are not supported. Users on serial terminals are considered local users. The <Break> key invokes the Trusted Path key for serial terminal users. On the console the sequence is <Ctrl-Alt-SysRq>. These are known as the SAK (Secure Attention Key). Any invocation of the SAK leads to a Trusted Path.

SAK must be used to initiate a login. Any time SAK is used, the user will obtain a prompt from a part of the TSF known as the Secure Server. If the terminal is not already handling a login session, a login is initiated; otherwise the user can request running of any trusted command. Use of SAK when processes are already running, returns the display to a known state and severs access by those processes to the display. Access to the display by those processes can be restored with the trusted “reattach” command.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

- **Physical protection of communications**

  Physical protection of the communications to the system is adequate to guard against unauthorized access or malicious modification of communications by users.

- **Documentation for administrators**

  System Administrators follow the policies and procedures defined in the TOE documentation for secure administration of the TOE.

- **Potential for administrator errors**

  System administrators are fallible and may make errors that compromise security.

- **Authorization procedures**

  Procedures exist for granting users authorization for access to specific security labels. This includes procedures for establishing one or more operators and administrators.

- **Competent system administrators**

  System administrators are competent to manage the TOE and the security of the information it contains.

- **Cooperative users**

  Users cooperate with those responsible for managing the TOE to maintain TOE security, follow TOE user guidance, protect TOE secrets, and follow site procedures.

- **Disposal of user data**

  System Administrators properly dispose of user data after access has been removed (e.g., due to job termination, change in responsibility).

- **Data handling procedures**

  Procedures exist for how sensitive, classified, and high-integrity data and secrets are to be handled when they are in possession of an authorized user. Procedures also exist for pick-up and distribution of hardcopy output at multi-user or multilevel printers.

- **Trained in Social Engineering methods**

Administrators and Users of the system are properly trained to recognize and resist social engineering attacks.

- **No abusive system administrators**

  System Administrators are trusted not to abuse their authority.

- **Expert threat agents**

  The TOE is subject to deliberate attack by experts with advanced knowledge of security principles and concepts employed by the TOE. These experts are assumed to have substantial resources and high motivation.

- **Password management promoting user compliance**

  System Administrators follow password management policies and procedures to ensure users comply with password policies.

- **Connectivity to other systems**

  Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints.

- **Physical access**

  The TOE is located within controlled access facilities that prevent unauthorized physical access by outsiders.

- **TOE protection from outsiders**

  The TOE will be physically protected from unauthorized modification by potentially hostile outsiders.

- **Administrators review audit logs**

  System Administrators review audit logs regularly.

- **Terminal procedures**

  Procedures exist for how to restrict individuals from viewing terminal output on an authorized user's terminal. This includes considerations such as "looking over the shoulder", an authorized user leaving his or her terminal unattended, and terminal-specific instructions to erase terminal-local data following a logout.

- **Procedures for setting labels and marking**

Procedures exist for establishing the security attributes of all information imported into the system, for establishing the security attributes for all peripheral devices (e.g., printers, tape drives, disk drives) attached to the TOE, and marking a sensitivity label on all hardcopy output generated.

- **Trusted users**

  Authorized users are trusted not to compromise security.

- **Mistakes by users**

  Users are fallible and may make errors that compromise security.

- **Secure Physical Location**

  It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the operating system and the value of the stored, processed, and transmitted information.

- **Network Security Levels**

  Networks are single-level and unlabeled at layers 3 and below.

4.2 Clarification of Scope

The product that a customer would purchase directly from BAE-IT matches with the evaluated TOE. The TOE does not provide a particular trusted application out-of-the- box, but is a general-purpose system that can support many kinds of highly trusted applications. BAE-IT and its customers have developed a number of trusted applications which rely on the security features provided by the XTS-400. In particular, the XTS is often used as an application host platform for programs that provide automated filtering of an information flow. Information which meets the security policy criteria will pass through the filter and can safely flow between networks of differing sensitivity/classification. These filters are often called “guards” because they guard against inadvertent release of sensitive information. These applications are not part of the TOE addressed by this ST. In particular, the following BAE-IT provided products **are not covered** by this evaluation:

- A Software Development Environment (SDE) package that allows programming of trusted and untrusted applications for use on the XTS. Frequently, initial programming and debug is done on a “real” Linux system and the binary copied to the XTS for execution. This package includes library functions to allow use of the security-enforcing XTS API (separate from the Linux API used for UNIX® functions).

- A middleware package called Secure Automated Guard Environment (SAGE1M), which provides transaction processing support for many of the tasks common to file-oriented filtering applications. SAGE provides pre-written and pre-tested functions permitting the application developer to focus on the “security filter” logic. There are turn-key applications programmed by BAE-IT that provide specific filtering or Guard capability.

This report **makes no claims** with regards to the trust or correctness of implementation associated with those applications. Installation of these applications could invalidate the security

rating of the TOE due to the presence of privileged software. Customers should use sources other than this report to determine the trust or correctness of implementation associated with those applications.

The TOE also provides an additional policy mechanism, “subtypes,” which can be used in a customer-specific way in conjunction with MAC, MIC and DAC controls. Although the implementation of the subtype mechanism is within the TOE, there are no specific security policies associated with that mechanism that are included in this evaluation. However, the subtype mechanism has been reviewed by the evaluators as it is used in the TOE to supplement protection for audit records.

The vendor has designed the product for a generic hardware platform that meets a well documented set of specific criteria. The basis for the platform is the x86 architecture. The vendor has a process in place for determining whether specific hardware configurations meet their specifications and to incorporate additional hardware into evaluated configurations. However, the specific hardware platforms listed for this evaluation (the Model 2800 and the Model 3200) with the associated list of optional hardware additions are the only platforms for which this specific evaluation applies.

The TOE does not include multi-processor hardware platforms, but the evaluated configurations do support concurrent use by multiple users.

The evaluated configuration includes the device driver (software) for the MSCU. The MSCU is a proprietary PCI Board that supports “Type 1” cryptography and has been separately scrutinized by the U.S. National Security Agency. The MSCU interfaces to the TOE in a manner that would require design, implementation, and testing details about the MSCU that were not available to BAE-IT for inclusion in the evaluation. Therefore the MSCU hardware is not part of this TOE, and may need to be the subject of a separate certification and accreditation effort. Customers that need to use the MSCU in conjunction with XTS-400 Version 6.4.U4 will need to rely upon other means to determine the impact of incorporating MSCU hardware into their application environment.

The evaluated configuration supports up to sixteen network interfaces. Each network interface is treated as a single-level interface. The TOE is not a distributed system, though it can be attached to multiple Ethernet 10baseT and 100baseT networks concurrently.

The user identification and authentication mechanism utilizes one-way hashes to store passwords and to compare provided passwords against the stored passwords. The strength of the actual algorithm used is not within the scope of this evaluation.

5 Architectural Information

The TOE consists of the following architectural components:

- The Kernel, TSS, OSS, and the Trusted Application Domain Software components
- Some BAE-IT written untrusted software to ease use of the untrusted environment that executes in Ring 3, the application domain
- Some third-party untrusted software that is shipped with XTS systems to customers by BAE-IT to ease installation by the customer and to provide the look and feel of a Linux system
- BIOS software to perform certain kinds of hardware configuration or diagnostics
- The hardware platforms Model 2800 and Model 3200

The BAE-IT XTS-400 operating system was designed using strong architectural principals including layering, modularity, and data hiding. As an EAL5+ product, the evaluation team looked at internal architecture of the XTS-400, in particular modularity, and the team developed strong evidence that the product met its EAL5+ architectural requirements.

The high level design of the XTS-400 decomposes the TOE into four layered subsystems that utilize the ring architecture of the x86 processor family to support the separation of the layers. The allocation of TOE functionality to the four basic software components is described below. The software within the layers exhibits further characteristics of layering and modularity.

The four subsystems of the software components are:

- **Kernel:** The Security Kernel software occupies the innermost and most privileged ring (**Ring 0**) and performs all Mandatory Access Control (MAC), and Mandatory Integrity Control (MIC). The kernel provides a virtual process environment that isolates one process from another. The kernel implements a variation of the reference monitor concept. When a process requests access to an object, the kernel performs the access checks, and, given that the checks pass, maps the object into the process' address space. Subsequent accesses are mediated by the hardware. The Security Kernel also provides I/O services and an Inter-Process Communication (IPC) message mechanism. The Security Kernel is part of every process' address space and is protected by the ring structure supported by the hardware.

- **TSS:** The TSS software executes in **Ring 1.** TSS provides trusted system services required by both trusted and untrusted processes. The Kernel, TSS and OSS have the responsibility for creation and loading of both trusted and untrusted programs, respectively, in XTS-400, Version **6.4.U4**. TSS software enforces the Discretionary Access Control (DAC) policy to file system objects.

- **OSS:** The OSS executes in **Ring 2**. OSS provides a UNIX-like Linux interface for user-written and trusted and untrusted software applications. The purpose of OSS is to make the multilevel security execution environment hidden to software running in the Application Domain (Ring 3).

- **Application Domain: Ring 3** is the Application Domain, in which all applications, both trusted and untrusted, execute. Software is considered trusted in XTS-400, Version 6.4.U4 if it performs functions upon which the system depends to enforce the security policy (e.g., the establishment of user authorization). This determination is based on integrity level and privileges. Untrusted software runs at a low integrity label. Some processes require privileges to perform their functions. An example of a process that

requires privileges is the Secure Server, which needs access to the User Access Authentication database, kept at system high access label, while establishing a session for a user at another security label.

6 Documentation

The hardware and software for the TOE are purchased as a single item. The evaluated product is available on two basic hardware platforms — the Model 2800 and the Model 3200. There is some optional hardware that may be included in the base hardware for the evaluated platform. The hardware options are described in further detail in the Security Target.

The software is installed by BAE-IT prior to delivery. However distribution media are also provided with the product. The following items are included in the media distribution:

STOP 6.4.U4 Base CD-ROM	Order No. XTSOF0231-00
STOP 6.4.U4 Application CD-ROM	Order No. XTSOF0230-00
STOP 6.4.U4 Documentation CD-ROM	Order No. XTDOC0144-00

The following product documentation is provided in softcopy on the Docmentation CD ROM:

Title/Description	**Order No.**
XTS-400 STOP 6.4.U4 Trusted Facility Manual	XTDOC0004-16
XTS-400 STOP 6.4.U4 User's Manual	XTDOC0005-16
XTS-400 STOP 6.4.U4 Software Release Bulletin	XTDOC0001-18
XTS-400 Installation and Setup Manual (XEON Model 2800 Systems), (BIOS Revision 1.00)	XTDOC0108-03
XTS-400 Installation and Setup Manual (XEON Model 3200 Systems), (BIOS Revision 3.00)	XTDOC0129-00
XTS-400 Installation and Setup Manual (XEON Model 2800 SBC), (BIOS Revision 1.00)	XTDOC0101-02

In addition, the product distribution includes a "checksum" delivery that is contained in the Software Release Bulletin. The Software Release Bulletin explains the procedure for using the checksums to verify the integrity of the distribution.

All of the documentation listed above is included within the scope of the evaluation.

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team.

7.1 Developer Testing

The developer maintains a suite of tests for confirming that the XTS-400 product meets its advertised functional requirements. Testing was performed at a developer facility in Herndon, VA. Since the vendor considers the evaluated configuration to be the base platform for many of their hosted applications, the vendor's normal functional testing was directly applicable to the TOE. Although some test documentation and tests may have initially been developed to support the product evaluation, all of that documentation and testing has been incorporated into the regular product test suite. The developer tested the TOE operating system on a combination of configurations that included both of the platform models and each of the optional hardware components.

The developer has categorized its testing into "programmatic" and "scripted" tests. The test package includes a programmatic test driver and a scripted test driver with procedures designed to verify each identified security relevant rule. There are essentially three types of functional tests: "automated", "interactive", and "manual". The vast majority of the testing is automated with no human interaction required once the automated test suite is started. The "automated" tests are included in the programmatic test suite. Thorough logs of the automated tests are maintained so the results may be retained and manually reviewed. Interactive tests require a human to perform an action at some point, but do not require further human activity or interpretation of the results to determine whether the tests were successful. Examples of interactive tests are those that pause and prompt the tester to insert a tape as part of the test. Manual tests require a tester to observe the behavior of the system, such as the clearing of a screen or the presentation of other visual information to interpret the test results. The interactive and manual tests are contained in the scripted test suite. Logs are also maintained for the interactive and manual tests.

The developer provided the evaluators with a CD-ROM containing documentation evidence in electronic form. Hyperlinks were provided between all related evidence. The developer's Test Plan, Test Procedures, Test implementation code, expected results, and test coverage documentation were included on the CD-ROM. The CD-ROM also included the functional specifications, design documentation, and a hypertext representation of the implementation code. The evaluators reviewed the developer's tests and test results to ensure that the developer's testing and test results were appropriate for the evaluated configuration. The developer's test documentation showed that the external interfaces were thoroughly tested. At least one test case was mapped to every external interface. Many of the interfaces were exercised by multiple tests. An evaluation team review of all of the security functions and the mapping between security functions and tests confirmed that security functions were appropriately tested by the developer tests.

7.2 Evaluation Team Independent Testing

CCTL evaluation team testing was conducted at the BAE-IT development facility in Herndon, VA. NSA evaluator testing was conducted at the NSA Facilities in Linthicum, MD.

The CCTL evaluation team performed the following activities during testing:

- Execution of all of the developer's functional tests
- Independent Testing
- Vulnerability Testing

The NSA evaluation team performed the following activities during testing:

- Installation of the TOE in its evaluated configuration
- Testing of changes from STOP 6.1.E to STOP 6.4.U4
- Vulnerability Testing for AVA_VLA.3

Most of the tests were installed, executed, logged, and analyzed directly on the individual hardware platforms. A second host was also attached to the network to support port scanning.

The Model 3200 platform test configuration included:

- Intel Xeon (P4) CPU
- SE7520 motherboard (SE7520BD23.86B.P.03.0.0019)
- Seagate Cheetah SCSI hard disk (models ST336753LW, and ST373287LW in the SCSI list)
- Seagate Barracuda ATA hard disk (model ST380011A)
- Ethernet controller on motherboard (model Intel 82541GI/PI Gigabit Ethernet Controller)
- PCIExpress four-port Ethernet card (device ID 10A4 for model 82571EB)
- PCIX Intel 82546 Pro/100 GB Quad port Ethernet card
- Floppy drive
- HP C5683A tape drive (BIOS) HP StorageWorks DAT 40 (label on device)
- Adaptec 29160 SCSI host adapter (two)
- ATI RageXL video controller on motherboard
- Lite-On DVD C LH52C1P CD-ROM/DVD drive
- Monitor
- Keyboard
- Mouse
- Three ADTRON (SDDS N18012 DUAL) card readers
- HP 4250 printer
- Honeywell Bull Vip 7800 serial terminal

The Model 2800 SBC platform test configuration included:

- Intel Xeon (P4) 2.8 GHz CPU
- Portwell ROBO-8820VG2 motherboard (Phoenix v6.00PG BAE BIOS (8820-016))
- Seagate Cheetah SCSI hard disk (model ST318453LW)
- Znyx Ethernet card (model ZX3704-NWSS-A4)
- Floppy drive

- HP C1537A tape drive
- Adpatec SCSI host adapter (SCSI BIOS v3.10.0)
- On-board video controller
- Toshiba DVD-ROM CD-ROM/DVD drive (model SD-M1711)
- ViewSonic PF790 monitor
- Keyboard
- Mouse

The test environment included the following peripherals:

- HP LaserJet 4200 printer
- WANG terminal (WYSE WY-60)

The BAE test suite does not require external hosts on network connections. However, the suite does require a functional TCP/IP daemon. Hence, the test environment does not include any network hosts.

The evaluation team performed the installation, setup, testing, and test result analysis, except for the Model 2800 SBC installation which was performed by BAE and observed by the evaluation team. Vendor representatives were available to answer questions and assist as needed during the testing process. The evaluators' testing included all of the tests found in the developer test plan and procedures. All security functions were tested, as well as all external interfaces. Testing of internal subsystem interfaces was done implicitly. The evaluators devised additional tests to augment and supplement the vendor tests. The CCTL evaluation team determined that the vendor's vulnerability analysis was very thorough and appropriately tested.

The NSA evaluation team expanded upon the vendor the CCTL vulnerability analysis to perform additional penetration testing.

Tools employed by the NSA evaluation tam for independent testing included the same category of tools employed by the Arca evaluation team, as well as in-house developed tools which assisted in determining that the TOE was resistant to penetration attacks performed by attackers possessing a moderate attack potential.

The initial National Security Agency vulnerability testing on STOP 6.4.U3 revealed several code flaws that needed correction and the final evaluated product was retested by the NSA team to assure that those problems were successfully corrected. STOP 6.4.U4 contains the "fixed" product and should be used to replace any prior 6.4 products.

The end result of the CCTL and NSA testing activities on the evaluated product was that all tests gave expected (correct) results. The final evaluator testing did not reveal any residual problems with the TOE. The testing found that the product was implemented as described in the functional specification. The CCTL and NSA evaluation team tests and penetration tests substantiated the security functional requirements claimed in the Security Target.

8 Evaluated Configuration

The TOE includes the entire XTS-400 Version 6.4.U4 Software and the underlying hardware platform. The TOE hardware consists of standard-PC, commercial off-the-shelf (COTS) components. The configurations included in the evaluated product are termed the “Model 2800” and the “Model 3200”. The model 2800 has a single board computer (SBC) variant. All three configurations are built around an Intel Xeon (P4) CPU. The Model 2800 uses either an Intel SW7501 motherboard or Robo-8820VG2 motherboard (SBC). The Model 3200 uses an Intel SE7520 motherboard. There are different form factor solutions (tower, 6U, 5U, 3U, 2U, etc.) and optional add-on hardware. The Robo-8820VG2 is a single-board computer, but is always connected by passive backplane to a SCSI controller (and potentially other controllers) in an XTS-400.

In addition to the basic platform components the evaluated configuration has the following additional components:

- Floppy Drive
- CD-ROM drive
- 4mm DAT tape drive
- Add-in SCSI host adapters
- Keyboard
- Touchpad or mouse
- Video Controller
- Monitor
- PCI Parallel Port

The evaluated configuration allows the following optional components:

- PC Card Reader
- Gigabit Ethernet Controller
- 2/4 port 10/100 Ethernet Card
- Printer
- Serial Terminal

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 2.3; CEM, Version 2.3, and all applicable NIAP CCEVS and International Interpretations in effect on July 11, 2007.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 5 assurance component and for the augmented assurance components: ALC_FLR.3, and ATE_IND.3.

For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. 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.

The evaluation determined the product to be Part 2 conformant and, as well, meeting the requirements for Part 3, and EAL 5 augmented by ALC_FLR.3 and ATE_IND.3. The details of the evaluation are recorded in the Evaluation Technical Reports (ETRs) which combines a proprietary ETR written and controlled by Arca CCTL together with a proprietary supplemental AVA_VLA.3 Evaluation Report that is written and controlled by the National Security Agency.

10 Validator Comments

- The TOE included two very explicitly defined hardware platforms. However, the vendor has designed STOP for a fairly generic x86 based platform. The vendor maintains a list of hardware characteristics that are required for a porting of STOP 6.1 .E to meet the CC requirements in the Security Target. As part of this evaluation, the explicit hardware platforms included in this evaluation were determined to meet the vendors' criteria. The generic requirements were not included as part of this evaluation because of evaluation constraints imposed by the LSPP and CAPP protection profiles. The vendor has procedures in place for incorporating changes to the evaluated platforms into future updates to this evaluation.
- The analysis for this product was definitely facilitated by the architectural design as well as the automated HTML-presentation documentation and testing evidence that was prepared by the vendor for the evaluation.
- During the evaluation there were three topics that the validation team thought needed some further communication to the intended users of this TOE. These have been captured in Appendices A1 through A3, and are respectively, XTS-400 STOP 6.4.U4 Privileges; Random Number Generation; SHA-256 Cryptographic Hash.

11 Security Target

Security Target, Version 1.22 for XTS-400, Version 6.4.U4, dated June 2008.

12 List of Acronyms

ACL	Access Control List
CAPP	Controlled Access Protection Profile (Version 1.d)
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme (US CC Validation Scheme)
CCIMB	Common Criteria Implementation Board
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
CI	Configuration Items
CLI	Command Line Interface
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
I&A	Identification and Authentication
I/O	Input/Output
IP	Internet Protocol
IPC	Interprocess Communication
IT	Information Technology
LSPP	Labeled Security Protection Profile (Version 1.b)
MAC	Mandatory Access Control
MIC	Mandatory Integrity Control
MSCU	Mission Support Cryptographic Unit
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OR	Observation Report
OS	Operating System
OSS	Operating System Services
PP	Protection Profile
SAK	Secure Attention Key
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
STOP	Secure Trusted Operating System
TCP	Transmission Control Protocol
TOE	Target Of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
URL	Uniform Resource Locator
VR	Validation Report

13 Bibliography

The following documents referenced during preparation of the validation report.

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 2005, Version 2.3.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, Version 2.3.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 2005, Version 2.3.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, Version 2.3.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated August 2005, Version 2.3.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 2005, Version 2.3.

[7] Common Criteria Evaluation and Validation Scheme for IT Security, *Guidance to Validators of IT Security Evaluations*. Scheme Publication # 3, Version 1.0, January 2002.

[8] ASE Evaluation Technical Report for Security Target, Version 1.22 for XTS-400 Version 6.4.U4 Version 2.0 dated July 3, 2008.

[9] BAE XTS 400 V6.4.U4 EAL 5 Augmented Evaluation Technical Report Version 2.0 dated July 3, 2008.

[10] XTS-400 V6.4.U4 Vulnerability Assessment ETR, dated June 2008.

[11] BAE Systems Information Technology Security Target Version 1.22 for XTS-400 Version 6.4.U4, dated June 2008.

[12] Impact Analysis Report for STOP 6.4 Release, includes all ISNs

[13] XTS-400 Installation and Setup Manual (XEON Model 2800 Systems), (BIOS Revision 1.00)

[14] XTS-400 Installation and Setup Manual (XEON Model 2800 SBC Systems), (BIOS Revision 1.00)

[15] XTS-400 Installation and Setup Manual (XEON Model 3200 Systems), (BIOS Revision 3.00)

[16] XTS-400 Series Trusted Facility Manual Release STOP 6.4.U4

[17] XTS-400 Series User's Manual Release STOP 6.4.U4

[18] XTS-400 STOP 6.4.U4 Software Release Bulletin

[19] XTS C Coding Standards and Guidelines, Version 3.14 dated June 2007

[20] XTS-400 Documentation Guidelines, Version 1.5 dated June 2007

[21] XTS-400 Configuration Management Plan dated June 2007

[22] XTS-400 STOP 6.4.U4 Evidence CD dated June 2008 with the following:

- Covert Channel Analysis
- Functional Specification
- High Level Design (5 parts; Generic, Kernel, TSS, OSS, and Trusted Software)
- Low Level Design Document (5 parts: Generic, Kernel, TSS, OSS, and Trusted Software)
- Security Model
- TSF Test Procedures
- TSF Test Guide
- Vulnerability Analysis
- Source Code

14 Interpretations

14.1 International Interpretations

Official start date of the evaluation was August 30, 2007. The evaluation team performed an analysis of the international interpretations and determined that there are no international Common Criteria Interpretations Management Board (CCIMB) finalized interpretations that are published as of the date given above.

Interpretations relevant to this evaluation are listed below. Interpretations that were superseded, too new, not relevant to the CC itself, or not relevant to the requirements claimed in this ST have been excluded. Interpretations that affect the wording of this ST are marked with "*".

The following NIAP interpretations were applied to this ST (or TOE itself).

- *I-0347: Including Sensitive Information In Audit Records
- I-0420: Attribute Inheritance/Modification Rules Need To Be Included In Policy
- I-0459: CM Systems May Have Varying Degrees Of Rigor And Function
- I-0350: Clarification Of Resources/Objects For Residual Information Protection
- *I-0407: Empty Selections Or Assignments
- *I-0410: Auditing Of Subject Identity For Unsuccessful Logins
- I-0414: Site-Configurable Prevention Of Audit Loss
- I-0429: Selecting One Or More
- I-0421: Application Notes In Protection Profiles Are Informative Only
- I-0427: Identification Of Standards
- *I-0375: Elements Requiring Authentication Mechanism
- I-0405: American English Is An Acceptable Refinement
- I-0418: Evaluation Of The TOE Summary Specification: Part 1 Vs Part 3
- *I-0422: Clarification Of "Audit Records"
- I-0426: Content Of PP Claims Rationale
- I-0432: List Of Subjects And Objects Refers To Types Thereof

14.2 Interpretations Validation

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations that it identified.

15 Appendix A.1: XTS-400 STOP 6.4 U4 Privileges

15.1 Feature Description

The Privilege mechanism provides a way to grant exceptions to the mandatory security and integrity policies in the TOE. It is an internal TOE mechanism used to implement least privilege. The ST describes the privilege mechanism and the TFM describes its use. Privileges are applied to executable programs in the file system via the trusted tp_edit command.

The use of privileges by end users (i.e., adding trusted programs) is not allowed in the evaluated configuration. Such use takes the TOE out of the evaluated configuration. Both the ST and TFM contain warnings to this effect.

The XTS-400 STOP privileges are:

kill_exempt	The ability to send a signal to process that has a different owner.
set_level	The ability to modify the mandatory security attributes of an object (security and integrity level).
upgrade_level	The ability to upgrade the mandatory security attributes of an object (security and integrity level).
set_discretionary_access	The ability to modify the discretionary security attributes of an object (access control information).
set_owner_group	The ability to change the owner and group associated with an object (for processes, the ability to change the real owner/group identifiers).
set_process_attributes	The ability to change restricted status information on a process (i.e., clearance level and process family identifier).
set_subtype_access	The ability to modify the object subtypes to which a process has access.
subtype_exempt	The ability to bypass subtype checks.
device_control_exempt	The ability to obtain control access to a device (i.e., the ability to issue privileged control functions).
simple_security_exempt	The ability to bypass the simple security property check (i.e., allows read up).
security_star_property_exempt	The ability to by-pass the *-property security check (i.e., allows write down).
simple_integrity_exempt	The ability to bypass the simple integrity property check (i.e., allows read down).
integrity_star_property_exempt	The ability to by-pass the *-property integrity check (i.e., allows write up).
discretionary_access_exempt	The ability to bypass the discretionary access checks.
trusted_parent_exempt	The ability to be loaded by an untrusted process. Unlike the other privileges, this is not a privilege of a running process; rather it is a property of a program file.

15.2 Developer Testing

The vendor provides both positive and negative tests to verify the proper functioning of the privilege mechanism. The positive tests show that granting a privilege allows the action associated with the privilege. The negative tests show that an action is not allowed without the privilege associated with the action. The negative tests also show that an action is not allowed even when all privileges except the one associated with the privilege are granted.

16 Appendix A.2: Random Number Generation

16.1 Feature Description

The vendor is moving towards compliance with the protection profile for multilevel operating systems in medium robustness environments. As part of this effort, the vendor has included in STOP 6.4 U4 devices to provide user applications with random and pseudo-random numbers (/dev/random and /dev/urandom, respectively).

The vendor makes no security claims about /dev/random and /dev/urandom in the XTS-400 ST. The vendor documents and tests the behavior of these devices. The evaluators examined the

new TOE interfaces presented by the devices as part of the evaluation. See analysis document Logical Devices (RNG). The evaluators did not validate the cryptographic properties of the random and pseudo-random number generator devices.

The vendor documents the devices in a manual page and the Trusted Facility Manual. The manual page describes the devices, their intended use, and their interfaces. The interface description includes function calls and responses, including error behavior. The manual page identifies start up tests for /dev/random and /dev/urandom and references the medium robustness multilevel operating system protection profile for a description of the tests. The tests are: Poker, Monobit, Runs, and Long Runs.

The TFM describes configuring the start up tests in Chapter 8: Administrator and Operator commands Section param_edit (1T). Specifically, the subsection System Security Parameters addresses parameter *test random number generation devices.* The subsection points out the trade off between assurance in the random number devices and start up speed. Chapter 7: Other Security Functions and Warnings lists the TSF messages related to random number devices in Section 7.9 Console Messages.

16.2 Developer Testing

The vendor test suite includes tests of /dev/random and /dev/urandom. Test fips140-1_test.c performs the start up tests:

- Poker test
- Monobit test
- Runs test
- Long run test

Test nist_sp800_22_test.c and driver.py perform tests described in NIST Special Publication 800-22: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. The correspondence between NIST SP 800-22 section and vendor test is:

- 2.01 frequency.c: FREQUENCY TEST
- 2.02 blockFrequency.c: BLOCK FREQUENCY TEST
- 2.03 runs.c: RUNS TEST
- 2.04 longestRunOfOnes.c: LONGEST RUNS TEST
- 2.05 rank.c: RANK TEST
  matrix.c: RANK ALGORITHM ROUTINES
- 2.06 discreteFourierTransform.c: DISCRETE FOURIER TRANSFORM TEST
  special-functions.c: SPECIAL FUNCTIONS
- 2.07 nonOverlappingTemplateMatchings.c: NONOVERLAPPING TEMPLATE TEST
- 2.08 overlappingTemplateMatchings.c: OVERLAPPING TEMPLATE TEST
- 2.09 universal.c: UNIVERSAL TEST
- 2.10 lempelZivComplexity.c: LEMPEL ZIV COMPRESSION TEST
- 2.11 linearComplexity.c: LINEAR COMPLEXITY
- 2.12 serial.c: SERIAL TEST
- 2.13 approximateEntropy.c: APPROXIMATE ENTROPY TEST
- 2.14 cusum.c: CUMULATIVE SUMS TEST
- 2.15 randomExcursions.c: RANDOM EXCURSIONS TEST
- 2.16 randomExcursionsVariant.c: RANDOM EXCURSIONS VARIANT TEST

The tests are automated with much of the source code originating from NIST.

17 Appendix A.3: SHA-256 Cryptographic Hash

17.1 Feature Description

In STOP 6.4 U4, the vendor upgraded to SHA-256 for cryptographic hashes. In particular, the trusted distribution (tdc command) and system integrity (sit command) checksums are now SHA-256 hashes computed by the TSF. In the previously evaluated STOP 6 release (STOP 6.1.E), tdc had used CRC checksums and sit had used SHA-1 hashes.

An end user cannot access the SHA-256 functions directly. There is limited access to the SHA-256 hash values. The vendor provides the trusted distribution hash values to a customer out of band and the customer compares these values to the output of the tdc command. (CRC checksums are provided in addition for backward compatibility.) The sit command uses SHA-256 hash values internally, but the hash values are not visible to the user.

The vendor implemented the SHA-256 cryptographic hash. The vendor created an internal, trusted library for SHA-1. This code was moved from the sit command. The sit code was based on RFC 3174. The vendor added a second library for SHA-256. This code was based on the code in the SHA-1 library and a public-domain implementation of SHA-256.

17.2 Developer Testing

The vendor confirmed that hash values from the new SHA-1 library were consistent with SHA-1 hash values from the previous sit command implementation.

The vendor performed unit testing of the SHA-256 function. They computed hashes for the strings listed in the FIPS specification. The resulting hash values were correct. The vendor developed and ran a test program to compare SHA-256 hash values of random files as computed by the TSF to hash values of the same files as computed by FreeBSD 5.3 sha2 lib SHA256 implementation.

The vendor script tests demonstrate the behavior of the tdc and sit commands, which use SHA-256 in STOP 6.4 U.4.

The evaluation team repeated the vendor's tdc and sit script tests. The evaluation team did not repeat the SHA-256 function unit tests independently. The vendor has not had the SHA-1 and SHA-256 implementations validated under the NIST Cryptographic Algorithm Validation Program.