122-B

CERTIFICATION REPORT No. CRP242

XTS-400 STOP
Version 6.4(UKE)
running on XTS-400 Model 3200UKE

Issue 1.0

March 2008

UK Certification Body
CESG, Hubble Road
Cheltenham, GL51 0EX
United Kingdom

**ARRANGEMENT ON THE
RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY**

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements contained in the certificate and in this report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the specified Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.	
Sponsor	BAE Systems Integrated System Technologies Limited
Developer	BAE Systems Information Technology, LLC
Product and Version	XTS-400 STOP Version 6.4(UKE)
Platform	XTS-400 Model 3200UKE
Description	XTS-400 STOP is a multi-tasking operating system implementing mandatory access, mandatory integrity and discretionary access control policies.
CC Part 2	Conformant
CC Part 3	Conformant
EAL	EAL5 augmented by ATE_IND.3, ALC_FLR.3
SoF	SoF-High
PP Conformance	CAPP, LSPP
CLEF	LogicaCMG
Date Certified	6 March 2008

The *IT Security Certified* logo which appears above:

- confirms that this certificate has been issued under the authority of a party to an international Recognition Agreement ('RA') designed to ensure that security evaluations are performed to high and consistent standards
- indicates that it is the claim of the evaluating party that its evaluation and certification processes meet all the conditions of the RA.

The judgements[1] contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. Use of the logo of this Agreement does not imply acceptance by other Members of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 [UKSP01] and 02 [UKSP02P1, UKSP02P2]. The Scheme has established a Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [ST], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issue of a Certification Report is a confirmation that the evaluation process has been carried out properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

Trademarks:

All product or company names are used for identification purposes only and may be trademarks of their respective owners.

[1] All judgements contained in this Certification Report, excluding the ATE_IND.3 component and any components above EAL4, are covered by the Recognition Arrangement.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of XTS-400 STOP Version 6.4(UKE) to the Sponsor, BAE Systems Integrated System Technologies Limited, as summarised in the Certification Statement, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [ST], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The following product completed evaluation, to CC **EAL5** augmented by ATE_IND.3 and ALC_FLR.3, on 25 January 2008:

   - **XTS-400 STOP Version 6.4(UKE)**

4. The Developer was BAE Systems Information Technology, LLC.

5. The product is a combination of a multilevel secure operating system, Secure Trusted Operating Program (STOP) revision 6, with BAE Systems supplied hardware. STOP is a 32-bit multiprogramming, multi-tasking operating system that can support multiple concurrent users. It provides proprietary interfaces in support of security management, together with a Linux-like user environment and Application Programming Interface (API). Whilst not a distributed product, network connectivity on up to 8 different networks is permitted within the evaluated configuration. TCP/IP and Ethernet are included in the TOE, but not network servers such as SMTP.

6. The TOE enforces a mandatory access control (MAC) and mandatory integrity control (MIC) policy, based on the Bell-LaPadula [BELL] and Biba [BIBA] security policy models. It also provides for identification and authentication of users, enforces a discretionary access control (DAC) policy, provides a trusted path mechanism by means of the implementation of a Secure Attention Key (SAK), and ensures individual user accountability through the provision of a security auditing capability.

7. The evaluated configuration of this product is described in this report as the Target of Evaluation (TOE). Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III ‘Evaluated Configuration’.

8. An overview of the TOE and its security architecture can be found in Chapter IV ‘TOE Security Architecture’. Configuration requirements are specified in Section 2 of [ST].

Protection Profile Conformance

9. The Security Target (ST) is certified as achieving conformance to the following protection profiles:

   - Controlled Access Protection Profile [CAPP].
   - Labeled Security Protection Profile [LSPP].

10. The ST also includes objectives and SFRs additional to those of the protection profiles, whilst the EAL5 augmented level of assurance exceeds that mandated by the PPs.

Security Claims

11. The ST fully specifies the TOE's Security Objectives, the Threats which these Objectives counter, the OSPs which these Objectives meet and the Security Functional Requirements (SFRs) and Security Functions that achieve the Objectives. All of the SFRs are taken from CC Part 2 [CC2]; use of this standard facilitates comparison with other evaluated products.

12. The TOE security policies are detailed in ST [ST]. The OSPs that must be met are specified in [ST] Section 3.3.

13. The environmental assumptions related to the operating environment are detailed in Chapter III under 'Environmental Requirements'.

Strength of Function Claims

14. The minimum Strength of Function (SoF) was claimed to be SoF-High. This is claimed for the Identification and Authentication Security Function (IDNAUT). The Evaluators have determined that these claims were met.

Evaluation Conduct

15. The TOE SFRs and the security environment, together with much of the supporting evaluation deliverables, remained mostly unchanged from that of XTS-400 STOP Version 6.1E, which had previously been certified [VR] by the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) to the CC EAL5 assurance level, augmented by ATE_IND.3 and ALC_FLR.3. For the evaluation of XTS-400 STOP Version 6.4(UKE), the Evaluators made some reuse of the previous evaluation results where appropriate and within the scope of mutual recognition.

16. The Certification Body monitored the evaluation which was carried out by the LogicaCMG Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the ST. The results of this work, completed in January 2008, were reported in the Evaluation Technical Report [ETR].

Conclusions and Recommendations

17. The conclusions of the Certification Body are summarised in the Certification Statement on page 2.

18. Prospective consumers of XTS-400 STOP Version 6.4(UKE) should understand the specific scope of the certification by reading this report in conjunction with the ST. The TOE should be used in accordance with the environmental assumptions specified in the ST. Prospective consumers are advised to check that the SFRs and the evaluated configuration match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

19. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration. Chapter II 'TOE Security Guidance' below includes a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

20. In addition, the Evaluators' comments and recommendations are as follows:

- Greater use of diagrammatic representations of how the SFRs are provided by the TSF subsystems working together could be made in the High-Level Design, in order to aid evaluator understanding in any future evaluation of XTS-400 STOP. This would be consistent with the spirit of the requirement for a semiformal design.

- Some apparent vulnerabilities were found in the source code, that the evaluators confirm as being non-exploitable in the target evaluation, but which the evaluators nonetheless recommend are addressed by updates to the low-level design or source code, as appropriate.

- Attention is drawn to the need (highlighted as assumption A.Phys_Acs_To_Out in the ST) for appropriate controls to prevent physical access to the TOE. In addition to this the BIOS password should be set appropriately to help prevent unauthorised access.

- The claimed Strength of Function of SOF-High was considered valid for the minimal (default) configuration of the Identification & Authentication security function. However, appropriate use should be made of the controls over the choice of passwords, so as to minimise the risk of users choosing passwords that would be easy for an attacker to guess. In particular, the TOE password policy should be configured either in conformance with CESG Infosec Memorandum Number [IM26], or in conformance with the security policy of the TOE owner by the appropriate selection and setting of the following password policy parameters:

    a. **Minimum Password Length:** This should be increased from 6 to at least 8 characters.

    b. **Maximum Password Lifetime:** This is the length of time during which a password can be used. A password older than this may not be used.

c. **Password Expiration Time:** This is the length of time after which a password must be changed when logging into the TOE. This time cannot be greater than the maximum password lifetime. A user who logs in with a password that is older than the password expiration time (but not older than the maximum password lifetime) will be required to change the password before completing the login.

d. **Password Warning Period:** This is the number of days, before the password expires, that messages will appear on the terminal during login warning the user that his/her password is about to expire.

e. **Password History Count:** This is the number of old passwords that will be checked for duplication when a new password is selected.

f. **Mixed Case Flag:** If set, this requires that any new password on the TOE consists of both upper and lower case letters.

g. **Non-Alphabetic Flag:** If set, this requires that any new password on the TOE consists of both alphabetic (a-z, A-Z) letters and non-alphabetic characters (everything else).

h. **Lexical Analysis Flag:** If set, this requires that any new password (and its reverse) should not be found in the TOE password dictionary, a list of approximately 400,000 common passwords. It will also require that a new password (and its reverse) should not be a word in the dictionary with 1, 2, or 3 characters either prepended or appended. Lexical analysis will also require that the password does not contain the same character repeated more than 3 times in succession, and that the password has at least 5 different characters in it.

i. **Consecutive Login Error Field:** If non-zero, this is the number of consecutive login failures before a user account is locked. It is separate from the terminal login tries, which will lock a single terminal. This count is tracked over all terminals for each user account, and when the number of failures reaches the configured count, the account is locked. This should be subject to appropriate safeguards to prevent denial of service (eg to administrators).

- The TOE contains a number of known covert channels (that were present in previously evaluated versions of the TOE), which are not normally exploitable in practice because of channel noise that would be present in an operational environment:

a. The bandwidth of the Resource Exhaustion Covert Channels can be reduced significantly by setting the *resource exhaustion delay* parameter to the trusted command `param_edit`.

b. The bandwidth of the Timing Covert Channels can be reduced by additional non-technical measures, such as strict control over the importing of programs that might contain code that would attempt to exploit any covert channels.

Disclaimers

21. This Certification Report is only valid for the evaluated TOE. This is specified in Chapter III 'Evaluated Configuration'.

22. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with higher Evaluation Assurance Levels) that exploitable vulnerabilities may be discovered after an evaluation has been completed. This Certification Report reflects the Certification Body's view at the time of certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since the ETR was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE. However, note that unevaluated patching will invalidate the certification of the TOE, unless the TOE has undergone a formal re-certification or is covered by a Scheme-approved Assurance Continuity process.

II. TOE SECURITY GUIDANCE

Introduction

23. The following sections provide guidance that is of particular relevance to purchasers of the TOE.

Delivery

24. On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery. In particular the procedures described in [SRB] *Assuring Secure Delivery* should be followed.

Installation and Guidance Documentation

25. The TOE Installation and Configuration documentation is as follows:

- *Installation and Setup Manual for Model 3200UKE Systems* [ISM], which details hardware-specific aspects of the installation and configuration.
- *XTS-400 Software Release Bulletin* [SRB], which describes the software delivery package and the software installation and configuration procedures.
- *XTS-400 Series Trusted Facility Manual* [TFM], which provides guidance on the use of the administrator and operator commands that are used in the installation and configuration of the TOE.

26. The TOE User Guide and Administration Guide documentation is as follows:

- *XTS-400 Series Trusted Facility Manual* [TFM], which provides guidance to administrators and operators.
- *XTS-400 Series User Manual* [UM], which provides guidance that is applicable to all users.

III. EVALUATED CONFIGURATION

TOE Identification

27. The TOE is XTS-400 STOP Version 6.4(UKE), which consists of the following components:

- Model 3200UKE hardware, which is built around an Intel Xeon processor and Intel SE7520BD2SCSI motherboard.
- STOP 6.4(UKE) Software (on the Model 3200UKE Base Operating System CD).
- STOP 6.4(UKE) Applications CD-ROM.
- STOP 6.4(UKE) Model 3200UKE Recovery Diskette.

TOE Documentation

28. The relevant guidance documentation for the evaluated configuration is identified above under 'Installation and Guidance Documentation'. The identified product documentation is distributed in softcopy on the CD-ROM.

TOE Scope

29. The TOE Scope is defined in [ST] Section 2. Functionality that is outside the scope of the TOE is defined in [ST] Section 1.2. In particular, BAE Systems also supplies the following products to augment XTS-400 STOP, but which are not part of the TOE (and hence are not covered by this certification report):

- 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. The SDE includes library functions to allow access to the security enforcing XTS API (separate from the Linux API used for UNIX functions).
- A middleware package called Secure Automated Guard Environment (SAGE) which provides transaction processing support for many of the tasks common to file-oriented filtering applications. SAGE reduces the risk and expense of developing custom applications by providing pre-written and pre-tested functions so the application developer can focus on the "security filter" logic.
- Turn-key applications programmed by BAE Systems to provide specific filtering capability.

TOE Configuration

30. The evaluated configuration of the TOE is defined in [ST] Section 2, comprising the software and hardware listed above under 'TOE Identification'. The product that a customer would purchase directly from BAE Systems is identical to the evaluated TOE. The minimum hardware configuration is defined in [ST] section 2.1.3.

Environmental Requirements

31. The environmental assumptions for the TOE are stated in [ST] Section 3.1.

Test Configuration

32. The following configuration was used by the Developers and Evaluators for testing:

- Model 3200UKE (Xeon based) hardware (3.2GHz processor, 2048MB RAM).
- SCSI-320 hard drives (2).
- DVD Drive (used as a CD Drive).
- HP DDS-3 tape drive.

IV. PRODUCT ARCHITECTURE

Introduction

33. This Chapter gives an overview of the main TOE architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration'.

Product Description and Architecture

34. A description of the product is provided in section 2 of the ST [ST].

35. The TOE enforces the following security policies:

- **Identification and Authentication,** which mandates authorised users to be uniquely identified and authenticated before accessing information stored on the TOE. It also enforces a lockout policy on individual user accounts or terminals, based on the number of consecutive login failures against that account or at that terminal, and enforces a highly configurable password complexity policy.

- **Discretionary Access Control (DAC),** which restricts access to objects based on the identity of subjects and/or groups to which they belong, and allows authorised users to specify protection for objects that they control. Each subject has an associated effective user and group. Each named object has an ACL containing permissions that specify the access allowed for the owning user, the owning group, up to seven other user or groups, and any user or group not explicitly listed.

- **Mandatory Access Control (MAC),** which enforces the data sensitivity classification model on all authorised users and all TOE resources, in accordance with the Bell-LaPadula [BELL] security policy model. The TSF provides 16 hierarchical sensitivity levels and 64 non-hierarchical sensitivity categories.

- **Mandatory Integrity Control (MIC),** which enforces an integrity policy on all authorised users and TOE resources to prevent malicious entities from corrupting data, in accordance with the Biba security policy model [Biba]. The TSF provides 8 hierarchical integrity levels (some of which are used to enforce role separation) and 16 non-hierarchical integrity categories.

- **Audit,** which allow authorised administrators to detect and analyse potential security violations.

- **Trusted path,** which allows users to be sure they are interacting directly with the TSF when executing trusted commands (e.g. to provide authentication data or security attributes to the TSF).

- **Isolation** of the TSF code and data files from the activity of untrusted users and processes.

- **Separation** of processes from one another (so that one process/user can not tamper with the internal data and code of another process).

36. The architecture of the TOE is based around the use of hardware privilege level and memory protection mechanisms to protect the TSF from tampering and to enforce process separation. The TOE is itself separated into four distinct domains, from Ring 0 (the most privileged) to Ring 3 (the least privileged).

TOE Design Subsystems

37. The TOE subsystems, and their security features/functionality, are as follows:

- Kernel executes in Ring 0 and is responsible for enforcing the MAC and MIC policies for all objects, and also DAC for objects other than filesystem objects (i.e. process, device, memory object, shared memory, and semaphore objects). It is also responsible for auditing, privilege checks, residual information protection, as well as making appropriate use of hardware protection mechanisms in support of TSF isolation.

- TSF System Services (TSS) runs in Ring 1 and provides trusted system services required by both trusted and untrusted processes. It enforces the DAC policy on accesses to filesystem objects.

- Operating System Services (OSS) executes in Ring 2 and provides a 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).

- Trusted Software executes in Ring 3. It includes trusted commands, for example to edit trusted databases such as the User Access Authentication database. It also incorporates the Secure Server, which is responsible for enforcing identification and authentication.

- Internal OS Library comprises a set of utility routines that are of use to more than one other subsystem, and includes DAC and MAC/MIC policy checking routines.

- Internal OS Headers comprises a set of header files that are of use in two or more other subsystems, and includes some macros in support of TSF isolation.

- External OS Headers is a set of header files that are of use in two or more other subsystems, and includes some macros that are used in support of MAC/MIC policy enforcement (specifically, associated with dominance checking between labels).

- Hardware: the hardware required by STOP is part of the TSF. This is because some of the hardware components play a critical role in providing domain separation, reference validation, residual information protection, and time stamps.

- System Loader is a tool to read portions of the TSF off disk into memory and to transfer control to the Kernel. Because the loaders know nothing about security, do not enforce policy, and do not execute during execution of the TSF, they are not part of the TSF.

- Untrusted Application Code comprises libraries, commands, daemons, tools, and applications which are untrusted, i.e. run only at low integrity, with no privileges. It is not trusted to perform secure operations and is not relied upon for proper functioning of the TSF.

TOE Dependencies

38. The TOE has no dependencies on its environment: hardware and firmware are included within the scope of the TOE.

TOE Interfaces

39. The external TOE Security Functions Interface (TSFI) is described as follows:

- Trusted Commands.

- Linux system calls.

- XTS-400 specific system calls.

- Hardware interfaces (these cover: terminal input, CPU, Ethernet Interfaces, PCI bus interface, serial controller interface).

V. TOE TESTING

TOE Testing

40. The Developer's tests covered all SFRs, all TOE high-level subsystems (as identified under 'TOE Design Subsystems' in Chapter IV), all TSF modules (as identified in the Low-Level Design) and the TSFI (as identified under 'TOE Interfaces' in Chapter IV). The tests included those TOE interfaces which are internal to the product and thus had to be exercised indirectly.

41. The developer's Security Test Suite comprises two types of test:

- Programmatic Tests (i.e. compiled C programs).
- Scripted Tests.

42. The Programmatic Tests cover the testing of the Linux and XTS-specific syscalls, including buffer overflow tests. They also address hardware tests, TSF isolation and object reuse tests. The Scripted Tests cover the TSFI presented by the Trusted Software subsystem, such as trusted and untrusted commands, and login tests. Most tests are fully automated; however there are a small number of tests that require manual intervention by a user (e.g. to press a key, perform a shutdown/reboot, or check a display). The results of all tests are logged.

43. The Evaluators repeated all tests performed by the Developer, in accordance with the requirements of ATE_IND.3. They also devised and performed 16 independent tests of the Security Functions to complement the Developer testing. The evaluators also devised and performed 65 penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

Vulnerability Analysis

44. The Evaluators' vulnerability analysis, which preceded penetration testing, was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables. It included (as required for EAL5) a search for covert channels, validating and building on the Developer's Covert Channel Analysis.

Platform Issues

45. Testing was performed on the Intel Xeon Model 3200UKE hardware, which (as explained under 'TOE Design Subsystems' in Chapter IV) is part of the TOE. There are no platform issues arising from this evaluation.

VI. REFERENCES

[A&R] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
Issue 1.3, March 2006.

[BELL] Secure Computer System: Unified Exposition and Multics Interpretation,
D.E. Bell and L.J. LaPadula, The Mitre Corporation,
Electronic Systems Division (AFSC), ESD-TR-75-306, March 1976.

[BIBA] Integrity Considerations for Secure Computer Systems,
K.J. Biba, The Mitre Corporation,
MTR-3153, April 1977.

[CAPP] Controlled Access Protection Profile (CAPP),
National Security Agency,
Version 1.d, October 1999.

[CC1] Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Maintenance Board,
CCMB-2005-08-001, Version 2.3, August 2005.

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Requirements,
Common Criteria Maintenance Board,
CCMB-2005-08-002, Version 2.3, August 2005.

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Requirements,
Common Criteria Maintenance Board,
CCMB-2005-08-003, Version 2.3, August 2005.

[CEM] Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Maintenance Board,
CCMB-2005-08-004, Version 2.3, August 2005.

[ETR] Evaluation Technical Report,
LogicaCMG UK Limited,
310.EC230306.30.1, Issue 1.2, 22 February 2008.

[IM26] CESG Infosec Memorandum Number 26,
Passwords for Identification and Authentication,
CESG, Issue 4.0, February 2008.

[ISM] Installation and Setup Manual for Model 3200UKE Systems,
BAE Systems Information Technology, LLC,
XTDOCC0129-00, April 2007.

[LSPP] Labeled Security Protection Profile (LSPP),
National Security Agency,
Version 1.b, October 1999.

[SRB] XTS-400 Series Software Release Bulletin, STOP 6.4.U1,
BAE Systems Information Technology, LLC,
XTDOC0001-14, June 2007.

[ST] XTS-400 UK EAL5 Security Target – XTS-400 Version 6.4(UKE),
BAE Systems Information Technology, LLC,
A2N 45009531, Version 02, November 2007.

[TFM] XTS-400 Series Trusted Facility Manual,
BAE Systems Information Technology, LLC,
Release STOP 6.4.U1, June 2007.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.1, March 2006.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4, April 2003.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.1, March 2006.

[UM] XTS-400 Series User Manual,
BAE Systems Information Technology, LLC,
Release STOP 6.4.U1, June 2007.

[VR] XTS-400 / STOP 6.1E Validation Report,
US Common Criteria Evaluation and Validation Scheme,
Report Number: CCEVS-VR-05-0094, 1 March 2005.

VII. ABBREVIATIONS

This list does not include well known IT terms (such as GUI, HTML, LAN, PC) or standard Common Criteria abbreviations (such as TOE, TSF; see Common Criteria Part 1 [CC1]) or Scheme abbreviations (such as CESG, CLEF; see [A&R]).

OSS	Operating System Services
STOP	Secure Trusted Operating Program
TSS	TSF System Services