National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Sybase, Inc., One Sybase Drive, Dublin, CA 94568

Sybase® Adaptive Server® Enterprise 15.0.1

Report Number:	**CCEVS-VR-VID10234-2007**
Dated:	**21 September 2007**
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

<u>Validation Team</u>

Santosh Chokhani
Scott Shorter
Orion Security Solutions
McLean, VA

<u>Common Criteria Testing Laboratory</u>

Tammy Compton
Quang Trinh
Roland Zeender
Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Sybase Adaptive Server Enterprise (henceforth referred to as ASE). It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in September 2007. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Extended and Part 3 Conformant**, and meets the assurance requirements of EAL 4 augmented with ALC_FLR.2.

ASE is a relational database management system (RDBMS) server that operates in the context of a commercial operating system, providing services to local and remote clients via the Tabular Data Stream (TDS) protocol.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 4 augmented with ALC_FLR.2) have been met.

The technical information included in this report was obtained from the Sybase Adaptive Server Enterprise Security Target and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- 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
TOE:	Sybase Adaptive Server Enterprise, Version 15.0.1
Protection Profile	None
ST:	Sybase Adaptive Server Enterprise 15.0.1 Security Target, Version 1.0, 9/18/2007
Evaluation Technical Report	*Evaluation Technical Report for the Sybase Adaptive Server Enterprise 15.0.1 Part 1 (Non-Proprietary)*, Version 1.0, September 18, 2007. *Science Applications International Corporation. Evaluation Technical Report for the Sybase Adaptive Server Enterprise 15.0.1 Part 2 (Proprietary), Version 2.0, August 31, 2007.* *Science Applications International Corporation. Evaluation Team Test Report for the Sybase Adaptive Server Enterprise 15.0.1, ETR Part 2 Supplement (SAIC and Sybase Proprietary), Version 5.0, August 31, 2007.*
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3 Part 2: Evaluation Methodology, Supplement: ALC_FLR- Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R
Conformance Result	CC Part 2 extended, CC Part 3 conformant

Item	Identifier
Sponsor	Sybase, Inc.
Developer	Sybase, Inc.
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validators	Santosh Chokhani, Orion Security Solutions, McLean VA Scott Shorter, Orion Security Solutions, McLean VA

3 Architectural Information

Adaptive Server Enterprise (ASE) is a Database Management System (DBMS) designed to execute as a set of applications in the context of commercially available operating systems, specifically Microsoft Windows 2000 (SP4) for x86, Microsoft Windows Server 2003 for x86, Sun Solaris Version 8 for sparc (32- and 64-bit), Sun Solaris Version 9 for sparc (32- and 64-bit), Sun Solaris Version 10 for sparc (32- and 64-bit), IBM AIX 5L Version 5.2 (64-bit), Hewlett-Packard HP-UX 11i v1 for PA-risc (64-bit), Hewlett-Packard HP-UX 11i v2 for PA-risc (64-bit), Red Hat Enterprise Linux 3.0 for x86and Red Hat Enterprise Linux 4.0 for x86.

Note that ASE version 15.0.1 is a revised version of the previously evaluated ASE Version 12.5.2. Among a number of non-security relevant feature additions and modifications (such as partitioned databases on a given server and a new query processing engine), ASE version 15.0.1 includes resource governor enhancements and the ability to encrypt database columns.

The ASE Server runs as an application on top of an operating system and depends on the services exported by the operating system to function. ASE uses operating system services for process creation and manipulation; device and file processing; shared memory creation and manipulation; and security requests such as inter-process communication. The hardware upon which the operating system runs is completely transparent to ASE - ASE sees only the operating system’s user interfaces.

The ASE Server is one or more operating system processes that service client requests. Multiple processes can be configured to enhance performance on multiprocessor systems. An ASE process has two distinct components, a DBMS component and a kernel component. The DBMS component manages the processing of SQL statements (data manipulation language - DML, data definition language - DDL, stored procedures and administrative commands), accesses data in a database, and manages different types of Server resources. The kernel component performs low-level functions for the DBMS component, such as task and engine management; network and disk I/O; and low-level memory management. Note that the TDS engine, that part of ASE that processes a TDS request, also uses the kernel component for low-level services.

All of the ASE processes attach to one or more shared memory segments. The shared memory contains data structures that relate to task management and operating system services, caches of database buffers, object descriptors, and other resources (e.g., other caches, queues, and stream I/O buffers) required to manage and process database commands.

Each ASE process manages multiple ASE tasks. A task is a thread of execution within the Server. Each client is associated with its own ASE task. In addition, there are several system tasks that perform specific services (e.g., tasks to write buffers to disk, tasks to write audit data to disk, and tasks to communicate with the network.).

4 Security Policy

ASE provides database management system (DBMS) services while it supports eight security functions upon objects in its scope of control.

4.1 Security Audit

ASE has an audit mechanism that is invoked for access checks, authentication attempts, administrator functions, and at other times during its operation. When invoked, the date, time, responsible individual and other details describing the event are recorded to the audit trail.

The Audit log is stored as tables within ASE itself so that audit records can be protected from unauthorized access or modification. Furthermore, the SQL select command provided by ASE can be used by System Security Officers to effectively review the audit trail, including searching and sorting by user identities and other audit record attributes

4.2 Cryptographic Support

ASE supports the ability to encrypt data at the column level. Encryption of only the sensitive data minimizes processing overhead as compared to encrypting an entire database.

SQL statements are available to create applicable encryption keys and specify columns for encryption. ASE handles key generation and storage and also provides System Security Officers the ability destroy keys that are no longer needed. Encryption and decryption of data occurs automatically and transparently as data is written to and read from encrypted columns. No client application changes are required.

4.3 User Data Protection

ASE implements a Discretionary Access Control Policy over applicable database objects - databases, tables, views, and stored procedures. Note that there are other database objects that are either always private, always public, or are part of one of the afore-mentioned objects. In each case, the objects each have an owner which is initially the creator of the object. Object owners have special permissions, while other users can subsequently be granted specific access permissions based on user identity, group memberships and active roles allowing applicable operations on objects.

ASE also implements a Policy-based Access Control Policy over the content of database tables. This policy controls access based on Application Contexts of the current subject in conjunction with Access Rules associated with columns in database tables. This policy effectively allows access to be controlled on very specific and widely varying information about users.

4.4 Identification and Authentication

ASE provides its own identification and authentication mechanism in addition to the underlying operating system. Users must provide a valid username and password before they can access any security-related functions. Once identified and authenticated, all subsequent actions are associated with that user and policy decisions are based on the users identity, group memberships and active roles.

4.5 Security Management

ASE provides functions necessary to manage users and associated privileges, access permissions, and other security functions such as audit. The functions are restricted based on Discretionary Access Control Policy rules including role restrictions. While all of the administrative functions are available through and restricted at the TDS ASE Server interface, an application (isql) is provided to support ASE administrators.

ASE defines a number of system-defined roles - System Administrator (SA), System Security Officer (SSO), Operator, etc.. Otherwise, there are users of the TOE of which the Database Owner (DBO) has special rights with regard to their own database. However, of these roles, only the SA and SSO have any special rights with respect to the security functions claimed in this Security Target. While it seems the DBO has special rights, their rights are all based on access permissions associated with the database they own.

4.6 Protection of the TOE Security Functions

ASE protects itself and ensures that its policies are enforced in a number of ways. While there is dependence on the underlying operating system to separate its process constructs, enforce file and memory access restrictions, and to provide communication services, ASE protects itself by keeping its context separate from that of its users and also by making effective use of the operating system mechanisms to ensure that memory and files used by ASE have the appropriate access settings. Furthermore, ASE interacts with users through well-defined interfaces designed to ensure that the ASE security policies are always enforced.

4.7 Resource utilization

ASE provides resource limits to help System Administrators prevent queries and transactions from monopolizing server resources. Specifically, System Administrators can configure ASE to prevent queries and transactions that: exceed estimated or actual I/O costs, return too many rows, exceed the temporary database space allocated, and/or exceed a specified elapsed time.

When a System Administrator configures a resource limit, all current users are immediately subject to the new limits unless resource limits are not enabled. If resource limits are not enabled, the System Administrator is notified that the configured limits would become effective when resource limits are enabled for the server.

4.8 TOE access

ASE allows System Security Officers to construct login triggers that can be used to restrict logins to a specific number of sessions and specified times. ASE also allows System Security Officers to restrict access based on user identities

5 Assumptions

The following assumptions were made during the evaluation of ASE:

- System administrators and system security officers are non-hostile, appropriately trained and follow all administrator guidance.

- There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration and support of the DBMS.

- Appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.

- The IT environment provides support commensurate with the expectations of the TOE.

- The environment protects network communication media appropriately.

6 Documentation

The following documentation was used as evidence for the evaluation of the ASE:

6.1 Configuration Management

1. Sybase Adaptive Server Enterprise Configuration Management Plan, Rev 0.1, 2/23/2007
2. Sample DCR Record

6.2 Delivery and Operation

1. Sybase Adaptive Server Enterprise Delivery and Operations Procedures, Rev 0.1, 2/21/2007
2. Installation Guide Adaptive Server Enterprise for HP-UX
3. Installation Guide Adaptive Server Enterprise for IBM RISC System/6000 AIX
4. Installation Guide Adaptive Server Enterprise for Linux/Intel
5. Installation Guide Adaptive Server Enterprise for Sun Solaris
6. Installation Guide Adaptive Server Enterprise for Windows NT
7. Supplement for Installing Adaptive Server for Common Criteria Configuration, Document ID DC00080-01-1501-01.

6.3 Design Documentation

1. Sybase Adaptive Server Enterprise 15.0.1 Security Target, Sybase, Issue 0. 5, 3/6/2007
2. Object Reuse Design Specifications 1.2 Rev, April 29, 2004
3. Object Reuse Prevention Functional Specification, 10/27/04
4. Discretionary Access Control Functional Specification, May 22, 2007
5. Policy Based / Row Level Access Control Functional Specification, May 24, 2007
6. Adaptive Server Enterprise - Groups and System Defined Roles Functional Spec, May 21, 2007
7. Resource Governor Functional Specification, June 27, 2007
8. ASE Self Protection Functional Specification, June 5, 2007
9. ASE Self Protection Design Specification, June 6, 2007
10. Adaptive Server Enterprise Architecture Summary, Sybase, June 6, 2007
11. Adaptive Server Enterprise Auditing Functional Specification, Sybase, May 18, 2007
12. Adaptive Server Enterprise Auditing Design Specification, Sybase, May 18, 2007
13. TDS Correspondence, 7/9/2007
14. T-SQL Correspondence, 6/12/2007
15. Adaptive Server Enterprise - Identification & Authentication Functional Spec, September 20, 2004
16. TDS 5.0 Functional Specification, Version 3.7
17. Identification and Authentication Design Specification, October 8, 2004
18. User Defined Roles Functional Specification, March 19, 2004
19. User Defined Roles Design Spec., April 20, 2004
20. Groups and System Defined Roles Design Spec, June 6, 2007
21. Configuration Interface functional specification, April 1, 2004
22. ISQL Functional Specification, June 12, 2007
23. Security Management Functions functional spec, May 18, 2007
24. Encrypted Columns Functional Specification, June 5, 2007
25. Encrypted Columns Design Specification, July 9, 2007
26. Implementation subset

6.4 Guidance Documentation

1. Supplement for Installing Adaptive Server for Common Criteria Configuration, Document ID DC00080-01-1501-01
2. Sybase ASE 15.0 System Administration Guide, Sybase, October 2005
3. Using Encrypted Columns in Adaptive Server, April 2006
4. Sybase ASE 15.0 Reference Manual: Commands, Sybase, October 2005
5. Sybase ASE 15.0 Reference Manual: Procedures, Sybase, September 2005

6.5 Life Cycle

1. Sybase Adaptive Server Enterprise Life Cycle Document Draft Revision 0.3, 07 May 2004

6.6 Testing

1. Common Criteria Test Plan, Version 5.0, July 10, 2007
2. Test Suite Documents and associated tests
    a. DAC Test Specification, Version 2.0, July 3, 2007
    b. Auditing Test Specification, Version 2.0, June 29, 2007
    c. I&A Test Specification, Version 2.0, June 25, 2007
    d. Self-Protection Test Specification, Version 5.0, July 1, 2007
    e. User-Defined Roles Test Specification, Version 2.0, June 29, 2007

    f. System-Defined Roles Test Specification, Version 2.0, July 3, 2007
    g. Security Management Test Specification, Version 2.0, July 1, 2007
    h. Configuration Interface Test Specification, Version 2.0, July 1, 2007
    i. Encrypted Column Test Specification, Version 3.0, July 2, 2007
    j. Auditing Test Specification, Version 2.0, June 29, 2007
    k. Resource Governor Test Specification, Version 3.0, July 9, 2007
    l. Row Level Access Control (RLAC) Test Specification, Version 2.0, June 29, 2007
    m. TDS Test Specification, Version 3.0, August 2, 2007
    n. Dynamic Reconfiguration Test Specification, Version 2.0, June 22, 2007
    o. isql Test Specification, Version 2.0, July 6, 2007
    p. Sybase ASE TSQL Test Coverage Analysis, 7/13/2007 (TSQL-Corr_test.xls)
3. Actual Test Results

6.7 Vulnerability Assessment

1. Sybase ASE Vulnerability Analysis, Version 1.3, August 13, 2007

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the Sybase Adaptive Server Enterprise, Version 5.0, July 20, 2007.

7.1 Developer Testing

At EAL4, testing must demonstrate correspondence between the tests and the functional specification and high level design. The vendor testing was extensive and covered all of the security functions identified in the ST and interfaces in the design. These security functions include:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- User Data Protection
- Security Management
- Protection of the TSF
- Resource Utilization
- TOE Access

7.2 Evaluation Team Independent Testing

The evaluation team installed the product according the Evaluated Configuration Guide, reran all developer tests and verified the results, then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Sybase Adaptive Server Enterprise 15.0.1 running on Microsoft Windows 2000 (SP4) for x86, Microsoft Windows Server 2003 for x86, Sun Solaris Version 8 for sparc (32- and 64-bit), Sun Solaris Version

9 for sparc (32- and 64-bit), Sun Solaris Version 10 for sparc (32- and 64-bit), IBM AIX 5L Version 5.2 (64-bit), Hewlett-Packard HP-UX 11i v1 for PA-risc (64-bit), Hewlett-Packard HP-UX 11i v2 for PA-risc (64-bit), Red Hat Enterprise Linux 3.0 for x86and Red Hat Enterprise Linux 4.0 for x86. To use the product in the evaluated configuration, the product must be configured as specified in *Supplement for Installing Adaptive Server for Common Criteria Configuration*, Document ID: DC00080-01-1501-01.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL4 augmented with ALC_FLR.2 work units received a passing verdict.

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 and CEM version 1.0 [5], [6]. The evaluation determined the Sybase ASE TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 4) augmented with ALC_FLR.2 requirements.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Sybase ASE product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 4 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. The evaluation team ensured the procedure included automated support to control and track changes to the implementation representation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation. To support the ACM evaluation, the evaluation team received Configuration Management (CM) records from Sybase.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 4 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer. The evaluation team followed the Configuration Guide to test the installation procedures to ensure the procedures result in the evaluated configuration.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 4 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification, a high-level design document, a low-level design document, and a security policy model. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

Additionally, the evaluation team ensured that the security policy model document clearly describes the security policy rules that were found to be consistent with the design documentation.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 4 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 4 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The evaluation team ensured the procedures described the life-cycle model and tools used to develop and maintain the TOE.

In addition to the EAL 4 ALC CEM work units, the evaluation team applied the ALC_FLR.2 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that flaw reporting procedures exist for managing flaws discovered in the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 4 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.8 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 4 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the developer misuse analysis, and the evaluation team’s misuse analysis and vulnerability analysis, and the evaluation team’s performance of penetration tests.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.9 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of the entire vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

- Validators were pleased to see that the encryption is performed using a FIPS 140-2 validated software cryptographic module, operating in accordance with its Security Policy.
- While the vendor does not provide a tool for doing this, it is recommended that the system encryption password be randomly generated – a simple script could be written to accomplish this, or various freeware and commercial tools are available for this. The generated value should then be securely stored separate from the TOE.
- For greatest protection of sensitive data, it is recommended that administrators configure columns to be encrypted prior to inserting data in them.
- In the validators' interpretation of the A.NETWORK assumption, no one except administrators and database users should be able to access the network on which the TOE resides. This can be achieved by physical protection of the network or by network protection mechanisms (e.g. IPSec).

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *Sybase Adaptive Server Enterprise 15.0.1 Security Target,* Version 1.0, 9/18/2007.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.

- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

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

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 2.3, August 2005.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 2.3, August 2005.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 2.3, August 2005.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, Version 0.6, 11 January 1997.

[5] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 1.0, August 1999.

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

[7] Science Applications International Corporation. *Evaluation Technical Report for the Sybase Adaptive Server Enterprise 15.0.1 Part 1 (Non-Proprietary)*, Version 1.0, September 18, 2007.

[8] Science Applications International Corporation. *Evaluation Technical Report for the Sybase Adaptive Server Enterprise 15.0.1 Part 2 (Proprietary)*, Version 2.0, August 31, 2007.

[9] Science Applications International Corporation. *Evaluation Team Test Report for the Sybase Adaptive Server Enterprise 15.0.1, ETR Part 2 Supplement (SAIC and Sybase Proprietary)*, Version 5.0, August 31, 2007.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.

[10] *Sybase Adaptive Server Enterprise 15.0.1 Security Target, Version 1.0, Date 9/18/2007*