National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

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

Sybase Replication Server, Version 15.2

Report Number: CCEVS-VR-VID10227-2009
Dated: 30 July 2009
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 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Scott Shorter
Orion Security Solutions
Takoma Park, MD

Roberta Medlock
The MITRE Corporation
McLean, VA

Common Criteria Testing Laboratory

Dawn Campbell
Tammy Compton
Terrie Diaz
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 the Sybase Replication Server (henceforth referred to as SRS). 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 June 2009. 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 Conformant and Part 3 Conformant**, and meets the assurance requirements of EAL 2.

The Target of Evaluation (TOE) is Sybase Replication Server (SRS) provided by Sybase, Inc. The SRS is designed to replicate data in multiple databases in order to provide database clients local access even to data that would otherwise be remote.

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 2.3) 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 2) have been met.

The technical information included in this report was obtained from the Sybase Replication Server 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 Replication Server, version 15.2
Protection Profile	None
ST:	Sybase Replication Server Security Target, Version 1.0, July 23 2009
Evaluation Technical Report	Evaluation Technical Report For the Sybase Replication Server (Proprietary), Version 1.0, May 22, 2009
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3
Conformance Result	CC Part 2 conformant, CC Part 3 conformant
Sponsor	Sybase, Inc
Developer	Sybase, Inc
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validators	Scott Shorter, Orion Security Solutions, Takoma Park, MD
	Roberta Medlock, Mitre Corporation, Bedford, MA

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

3.1 TOE Overview

SRS is an Open Server application. SRS uses the Sybase Open Client/Server (OC/S) for network communication and other platform dependent functions, such as connection management, login protocol, data transmission, T-SQL interface, inter-process communication, etc. SRS uses operating system services for process creation and manipulation, device and file processing, memory management and security requests such as inter-process communication, albeit indirectly through the OC/S. The hardware upon which the operating system runs is transparent to SRS which sees only the operating system's user interfaces.

SRS maintains replicated data in multiple databases. Data in the replicate database is 'loosely consistent' with the data in the primary database, lagging behind primary data by the amount of time it takes to distribute updates from the primary to the replicate databases. Note that the notion of primary data server is data dependent. At any given time, all data servers known to SRS could be the primary for some data that they host.

As indicated above, the SRS uses a basic publish and subscribe model for replicating data across networks. Users 'publish' data in a primary database, and other users 'subscribe' to the data for delivery into a replicate database. Changes to both data and stored procedures can be replicated. Instructions to publish and subscribe to data are given at replication servers that control or have a connection to each database. Users create replication definitions at the primary Replication Server, which controls the primary database with the data to be published. The user creates a subscription at the replicate Replication Server, which controls the replicate database that will receive the information.

Connections and routes define the structure of the replication system. A connection conveys messages from a SRS to a database. A route transfers requests from a source SRS to a destination SRS.

SRS distributes database operations from a primary database to a destination SRS, using the Log Transfer Language (LTL[1]), as functions that consist of a name and a set of data parameters. The destination SRS then uses function strings to map functions to the commands recognized by the destination SRS. These commands may be transaction-control directives such as begin transaction or commit transaction, or data manipulation instructions such as insert, update or delete. Function strings are categorized into function string classes based on the type of replicate data server.

[1] LTL is the language Replication Server uses to process and distribute replicated transactions and procedure invocations throughout a replication system.

SRS depends on data servers to provide the transaction-processing services needed to protect stored data. Data servers must comply with the following conventions:

- A transaction is one unit of work – either all operations in the transaction are performed, or none are performed.
- Transactions results are permanent. A transaction cannot be undone after it is committed.

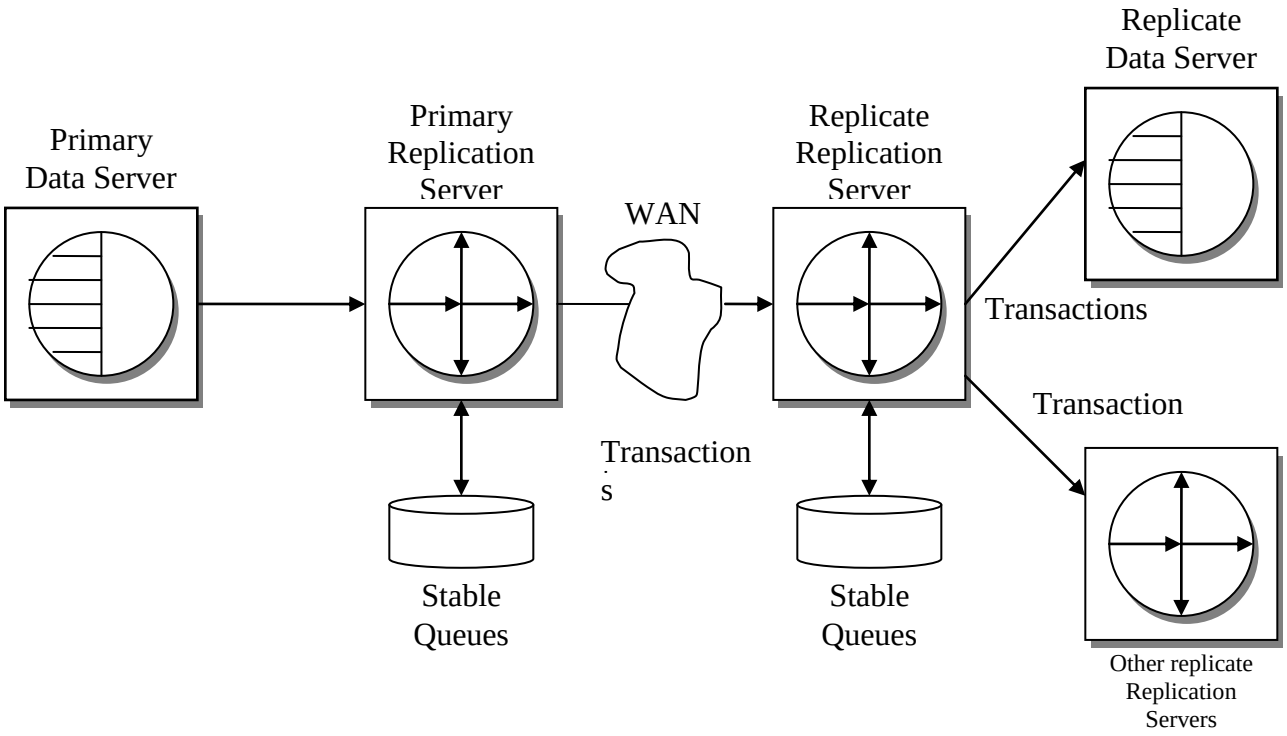

Figure 1: Replication System Overview

SRS configuration data is stored in an instance of Sybase Adaptive Server Enterprise (ASE) database called the Replication Server System Database (RSSD) or an instance of SQL Anywhere database called the Embedded Replication Server System Database (ERSSD). Note that Sybase ASE is not included in the TOE, but rather is required to be configured in the environment to support the TOE. Note that ERSSD is not part of this evaluation. Note also that it is expected that the RSSD/ERSSD would be configured such that only SRS can access and modify its own configuration data. The data in these tables are modified only internally within the SRS, and only the SRS Administrator can alter the system tables.

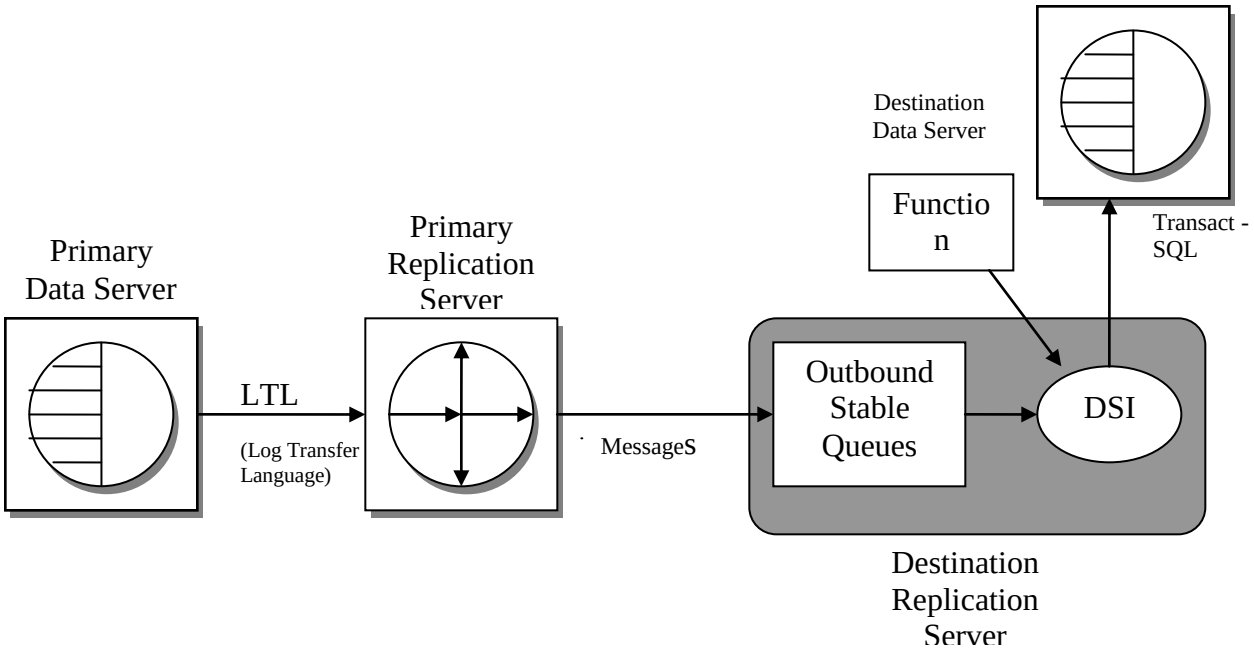

Figure 2: Replication Server Internals

SRS uses a disk partition to establish stable queues. During replication operations, updated data is temporarily stored in these queues. There are 3 types of queues:

- Inbound Queue – holds messages only from a Replication Agent for primary data. A Replication Agent scans the database transaction log and sends transaction information to the Replication Server for distribution to subscribing databases.
- Outbound Queue – holds messages for a replicate database or a replicate SRS. For each replicate database managed by a SRS, there is a Data Server Interface (DSI) outbound queue. For every SRS to which a SRS has a route, there is a Replication Server Interface (RSI) outbound queue.
- Subscription materialization queue – holds messages related to newly dropped or created subscriptions.

SRS has several threads that manage different specific tasks. Below are some of the SRS threads and functions:

- Reads and writes to each queue are managed by a Stable Queue Manager (SQM) thread.
- Connection with the data server is managed by a DSI thread. The DSI thread executes the transactions in the replicate database in the correct commit order.
- Connection with each destination SRS is managed by an RSI thread. RSI threads send messages from one SRS to another when a route exists between them.

Client applications are programs that access the data server. In a simple replication system, clients update primary databases and the SRS updates the replicate databases. However,

SRS allows replication rules to be created allowing data updated at a replicate data server to be reflected back on the primary and other replicate servers.

Support for Sybase Adaptive Server Enterprise data servers is provided via an associated Replication Agent shipped with the SRS. Interfacing with other data servers can be done by providing applications (i.e., additional Replication Agents) that interface with the SRS and the foreign data server[2]. Existing databases and applications need not be converted to build the replication system.

SRS manages login names, passwords and permissions (associated with roles) that are essential for system security. SRS login names and specific permissions are required for:

- Each component of the replication system, such as the RSSDs, Replication Agents, Replication Servers, data servers, etc.
- Each user who is setting up replicated data or is monitoring and managing the SRS.

Users require specific permissions to perform specific Replication Command Language (RCL) commands. Encrypted passwords are supported throughout the system. Replication Server uses Sybase Common Security Infrastructure (CSI) to provide server or client authentication, cryptography for encryption and decryption of passwords that are stored in the RSSD tables, and key-pair generation to support extended password encryption. CSI is an Open Client / Server feature, which is utilized by linking Replication Server with OCS provided CSI (Common Security Infrastructure) libraries. SRS also supports third party security services such as Kerberos and DCE that ensure secure message transmission over the network, and enable user authentication for login to SRSs in the replication system. Note that such third party capabilities are not addressed in this evaluation. Isql interface to Replication Server also supports network based user authentication. with –V option. With this option, the user must log in to the network's security system before running the utility. Replication Server version 12 and later supports MIT Kerberos version 5 or later, CyberSafe Kerberos version 5 Security Server, and Transarc DCE version 1.1 Security Server. Note that these third-party softwares are not part of TOE. However, they can be used in Replication Server's IT environment to provide network-based security. Replication Server secure sockets layer (SSL) Advanced Security option provides session-based security. SSL is the standard for securing the transmission of sensitive information, such as credit card numbers and stock trades, over the Internet. Note that SSL is a third-party software and is not part of TOE. However, it can be used in Replication Server's IT environment to provide session-based security.

3.2 TOE Physical Boundaries

The TOE itself consists of the Sybase Replication Server (SRS), version 15.2, product. The TOE configuration includes one or more SRS products configured as a replication system and attached to various data servers (e.g., Sybase Adaptive Server Enterprise).

[2] Note that while additional Replication Agents can be developed for other data servers and can interface with the TOE using LTL, for the purpose of testing only the Sybase ASE Replication Agent is being considered.

SRS operates on any of the following operating systems: Sun Sparc 32 (version 8, 9, 10, 32 bit & 64 bit), Sun X64 (version 10, 32 bit & 64 bit), HP Itanium (version 11.23, 11.31, 64 bit), Microsoft Windows (2003 SP2, XP, Vista, Longhorn, 32 bit & 64 bit), IBM AIX (version 5.3, 32 bit & 64 bit), IBM P-Series (RHEL 4.4, SuSE SLES 10, 64 bit), and Linux X86 (RHEL 4.4, RHEL 5.0, SuSE SLES 10, 32 bit & 64 bit).

SRS also utilizes services of the Sybase Open Client/Server (OCS), Version 15.2 product as indicated previously as well as an instance of Sybase ASE.

Note that the TOE relies on the underlying OS for protection and on OC/S to secure network communications.

3.3 TOE Logical Boundary

This section identifies the security functions that the TSF provides.

- User data protection
- Identification and authentication
- Security management

3.3.1 User Data Protection

SRS controls the flow of information among associated data sources. An authorized administrator can define primary data sources, replicate data sources, and the replication routes that will be used to replicate data throughout the replication system represented by one or more SRS products working in concert.

3.3.2 Identification and Authentication

SRS maintains login information for its own access to other components so it can perform its functions, but also requires users and other components to be identified and authenticated prior to offering any of its services. Users are required to login before they can manage aspects of the replication system and other components must be identified and authenticated before SRS will interact (e.g., accept or provide data) with that other component.

3.3.3 Security Management

SRS restricts its own management functions by requiring users to be logged in before they can access security management functions. Users are associated with a set of roles defined within SRS and once logged in the functions available to the user are restricted based on their associated role. While SRS supports multiple roles for its own management for the purposes of this ST, they are treated abstractly as an authorized administrator due to the substantial overlap in authority. In general, SRS provides functions to monitor and manage the replication of data throughout the replication system.

4 Assumptions

The following assumptions were made during the evaluation of Replication Server:

- Authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.
- The environment protects network communication media appropriately.
- There are no general-purpose computing capabilities (e.g., compilers or user applications) available on replication servers, other than those services necessary for the operation, administration and support of the replication server.
- 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.

5 Documentation

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

5.1 Configuration Management

1. Sybase Replication Server Configuration Management Plan, Revision 0.1, January 23, 2009

5.2 Delivery and Operation

1. Sybase Replication Server Delivery and Operations Procedures, Rev 0.1, Feb 06, 2009
2. Installation Guide Replication Server 15.2 for UNIX
3. Installation Guide Replication Server 15.2 for Windows
4. Configuration Guide Replication Server 15.2 for UNIX
5. Configuration Guide Replication Server 15.2 for Windows.

5.3 Design Documentation

1. Replication Server Security Functional Specification, version .5, 14 April 2009
2. Replication Server Security Design Specification, version .4, 3 April 2009
3. Replication Server Correspondence Worksheet, 6 April 2009
4. TDS 5.0 Functional Specification, Version 3.6
5. ISQL Functional Specification, March 19, 2004

5.4 Guidance Documentation

1. Administration Guide: Volume 1 Replication Server 15.2
2. Administration Guide: Volume 2 Replication Server 15.2
3. SySAM 2.0
4. Getting Started Replication Server 15.2
5. Heterogenous Replication Guide Replication Server 15.2
6. System Tables Diagram Replication Server 15.2
7. Troubleshooting Guide Replication Server 15.2
8. New Features Guide Replication Server 15.2
9. Design Guide Replication Server 15.2
10. Reference Manual Replication Server 15.2
11. Release Bulletin Sybase Replication Server 15.2 for HP-UX
12. Release Bulletin Sybase Replication Server 15.2 for IBM AIX
13. Release Bulletin Sybase Replication Server 15.2 for Linux
14. Release Bulletin Sybase Replication Server 15.2 for Sun Solaris
15. Release Bulletin Sybase Replication Server 15.2 for Windows

5.5 Testing

1. Replication Server 15.2 Common Criteria Test Plan, Version: 2.0, May 8, 2009
2. Test Coverage Mapping spreadsheet
3. Test Code
4. Actual Test Results

5.6 Vulnerability Assessment

1. Sybase Replication Server Vulnerability Analysis, Version .2, April 14, 2009

6 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 Replication Server, Version 1.0, May 22, 2009.

6.1 Developer Testing

At EAL2, the developer testing must demonstrate correspondence between the tests and the functional specification. The vendor testing was extensive and covered all of the security functions identified in the ST and interfaces in the design, thus including all of the TSFI. These security functions in the ST include user data protection, identification and authentication, and security management. The vendor testing specifically addressed:

- Publication Associations
- Login
- Managing Associations
- Manage Replication Tables

- Manage Publications
- Managing Users

All security functions were tested and the TOE behaved as expected. The evaluation team determined that the developer's actual test results matched the expected results.

6.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the Installation Guide Replication Server 15.2 for UNIX/Windows. The evaluation team re-ran the entire automated test suite and verified the results. In addition to re-running the developer's test, the evaluation team then developed and performed functional and vulnerability testing. The set of independent team tests augmented the vendor testing by exercising different aspects of the security functionality including:

- Password Creation
- Failed Login Attempts
- Admin Guide Tests
- Port Scans
- Open Source Searches
- Administrator Password Access
- Windows Memory Protection Flaws

All tests were run as manual test.

6.3 Vulnerability Testing

The evaluation team developed vulnerability tests to address the Protection of the TSF security function, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE.

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Sybase Replication Server version 15.2 running on one of the following platforms: Sun Sparc 32 (version 8, 9, 10, 32 bit & 64 bit), Sun X64 (version 10, 32 bit & 64 bit), HP Itanium (version 11.23, 11.31, 64 bit), Microsoft Windows (2003 SP2, XP, Vista, Longhorn, 32 bit & 64 bit), IBM AIX (version 5.3, 32 bit & 64 bit), IBM P-Series (RHEL 4.4, SuSE SLES 10, 64 bit), and Linux X86 (RHEL 4.4, RHEL 5.0, SuSE SLES 10, 32 bit & 64 bit).

To use the product in the evaluated configuration, the product must be configured as specified in the Installation Guide Replication Server 15.2 for UNIX or the Installation Guide Replication Server 15.2 for Windows documents.

8 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 EAL2 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 2.3 [5], [6]. The evaluation determined the Sybase SRS TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 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.

8.1 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 SRS 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.

8.2 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 2 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated 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

8.3 Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to 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. 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.

8.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

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.

8.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 2 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.

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

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the 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. The evaluation team re-ran the entire 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.

8.7 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 2 augmented with AVA_MSU.1 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, 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.

8.8 Summary of Evaluation Results

The evaluation team applied each EAL 2 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, and the evaluation team's performance of penetration tests.

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.

9 Validator Comments/Recommendations

- Encrypted passwords were not evaluated because that functionality is not required to satisfy the security objectives of the system. The evaluation makes no claim to the security of the password encryption capability.
- Much of the cryptography is not FIPS validated, refer to the ST for details on the use of the FIPS validated cryptographic module.

10 Annexes

Not applicable.

11 Security Target

The Security Target is identified as Sybase Replication Server Security Target, Version 1.0, July 23 2009.

12 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.

13 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*, Version 2.3, August 2005.

[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 Replication Server Part 2 (Proprietary)*, Version 1.0, May 22, 2009.

[8] Science Applications International Corporation. *Evaluation Team Test Report for the Sybase Replication Server Part 2 Supplement (SAIC and Sybase Proprietary)*, Version 1.0, May 22, 2009.

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

[10] Sybase Replication Server Security Target, Version 1.0, July 23 2009.