Sybase Replication Server, Version 15.2
Security Target

Version 1.0
23 July 2009

Prepared for:
Sybase, Inc.

One Sybase Drive
Dublin, CA 94568

Prepared By:
Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

1. SECURITY TARGET INTRODUCTION 4

1.1 SECURITY TARGET, TOE AND CC IDENTIFICATION 4
1.2 CONFORMANCE CLAIMS 4
1.3 CONVENTIONS 4

2. TOE DESCRIPTION 5

2.1 TOE OVERVIEW 5
2.2 TOE ARCHITECTURE 5
2.2.1 Physical Boundaries 8
2.2.2 Logical Boundaries 9
2.3 TOE DOCUMENTATION 9

3. SECURITY ENVIRONMENT 10

3.1 THREATS 10
3.2 ASSUMPTIONS 10

4. SECURITY OBJECTIVES 11

4.1 SECURITY OBJECTIVES FOR THE TOE 11
4.2 SECURITY OBJECTIVES FOR THE IT ENVIRONMENT 11
4.3 SECURITY OBJECTIVES FOR THE ENVIRONMENT 11

5. IT SECURITY REQUIREMENTS 12

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 12
5.1.1 User data protection (FDP) 12
5.1.2 Identification and authentication (FIA) 13
5.1.3 Security management (FMT) 13
5.2 IT ENVIRONMENT SECURITY FUNCTIONAL REQUIREMENTS 14
5.2.1 User data protection (FDP) 14
5.2.2 Protection of the TSF (FPT) 14
5.3 TOE SECURITY ASSURANCE REQUIREMENTS 14
5.3.1 Configuration management (ACM) 15
5.3.2 Delivery and operation (ADO) 15
5.3.3 Development (ADV) 15
5.3.4 Guidance documents (AGD) 16
5.3.5 Tests (ATE) 17
5.3.6 Vulnerability assessment (AVA) 18

6. TOE SUMMARY SPECIFICATION 19

6.1 TOE SECURITY FUNCTIONS 19
6.1.1 User data protection 19
6.1.2 Identification and authentication 19
6.1.3 Security management 20
6.2 TOE SECURITY ASSURANCE MEASURES 20
6.2.1 Configuration management 20
6.2.2 Delivery and operation 20
6.2.3 Development 21
6.2.4 Guidance documents 21
6.2.5 Tests 21
6.2.6 Vulnerability assessment 22

7. PROTECTION PROFILE CLAIMS 23

8. RATIONALE 24

8.1 SECURITY OBJECTIVES RATIONALE 24

8.1.1 Security Objectives Rationale for the TOE and Environment *24*
8.2 SECURITY REQUIREMENTS RATIONALE 26
8.2.1 Security Functional Requirements Rationale *26*
8.3 SECURITY ASSURANCE REQUIREMENTS RATIONALE 27
8.4 STRENGTH OF FUNCTIONS RATIONALE 27
8.5 REQUIREMENT DEPENDENCY RATIONALE 27
8.6 EXPLICITLY STATED REQUIREMENTS RATIONALE 28
8.7 TOE SUMMARY SPECIFICATION RATIONALE 28
8.8 PP CLAIMS RATIONALE 29

LIST OF TABLES

Table 1 TOE Security Functional Components 12
Table 2 TOE Security Management Roles 13
Table 3 IT Environment Security Functional Components 14
Table 4 EAL 2 Assurance Components 15
Table 5 Environment to Objective Correspondence 24
Table 6 Objective to Requirement Correspondence 26
Table 7 Security Functions vs. Requirements Mapping 29

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The 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 Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Environment (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8).

1.1 Security Target, TOE and CC Identification

ST Title – Sybase Replication Server Security Target

ST Version – Version 1.0

ST Date – 23 July 2009

TOE Identification – Sybase Replication Server, version 15.2

TOE Developer – Sybase, Inc.

Evaluation Sponsor – Sybase, Inc.

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005.
  - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.
  - Part 3 Conformant
  - Assurance Level: EAL 2
  - Strength of Function Claim: SOF-basic

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ things …"). Note that deletions are indicated only when not replaced with an addition.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

2. TOE Description

The Target of Evaluation (TOE) is Sybase Replication Server (SRS), version 15.2.

2.1 TOE Overview

SRS maintains replicated data in multiple databases and provides clients using databases in the replication system with local data access, thereby reducing load on the network and centralized computer systems. The SRS has the following features:

- A Replication Command Language (RCL) enables replication functions to be managed and monitoring and maintenance of the replication system.
- SRS supports heterogeneous data servers.
- SRS uses a basic publish-and-subscribe model for replicating data across networks.
- SRSs communicate with each other via user-defined *routes*.

2.2 TOE Architecture

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.

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.

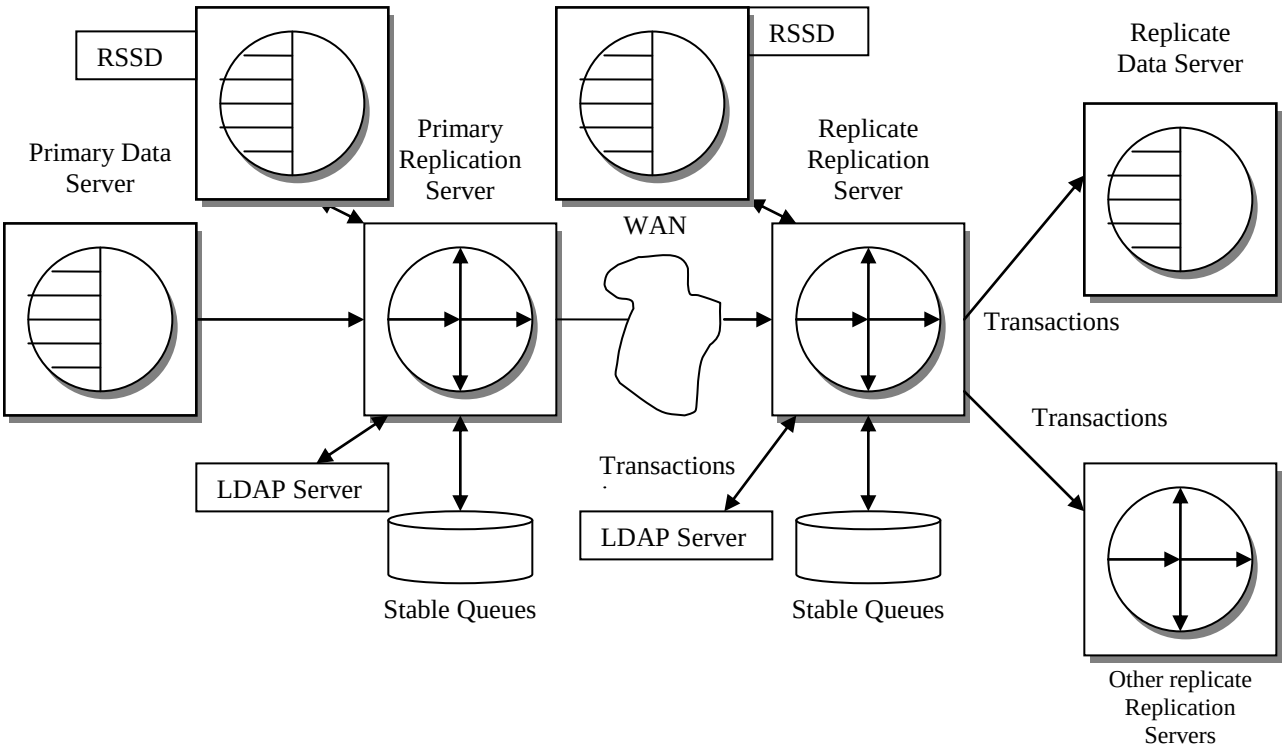

Figure 1: Replication System Overview

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

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.

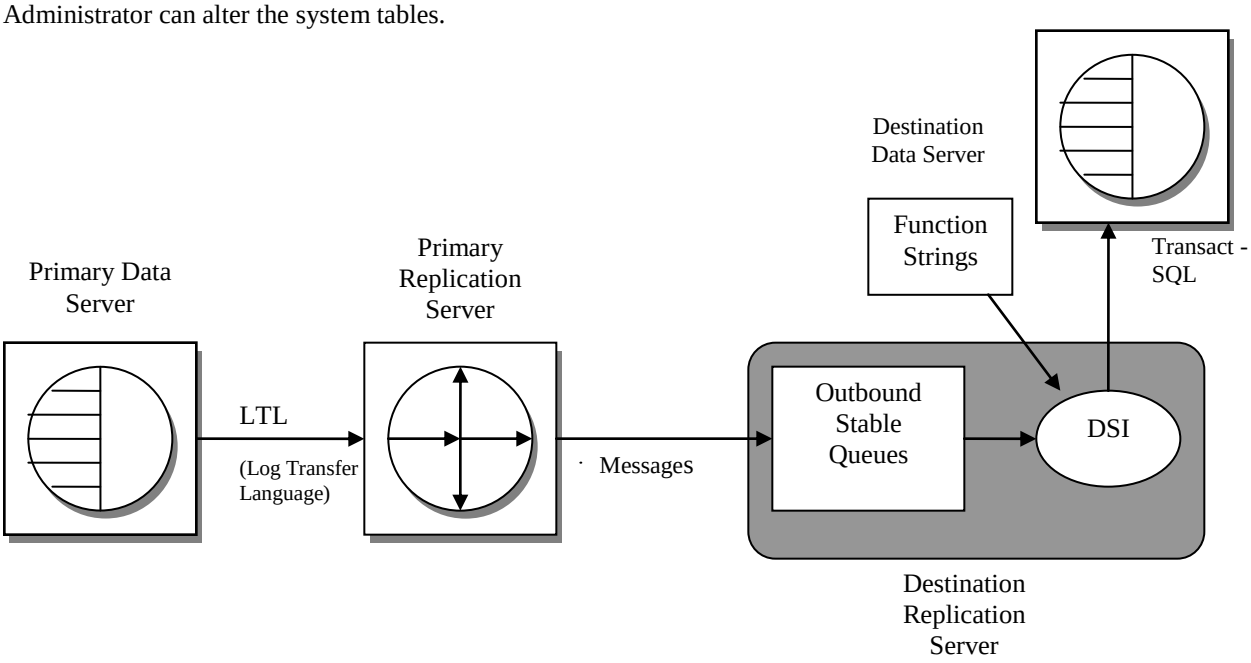

Figure 2: Replication Server Internals

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, but are not evaluated because they are not required to satisfy the security objectives of the TOE. 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. FIPS 140-2 (certificate #542 Security Builder FIPS module from Certicom Security Builder GSE Version 2.0) applies to cryptographic function to support the following function: AES algorithm with 128-bit encryption key is used to encrypt passwords that are stored in the RSSD. In addition, Security Builder GSE Version 2.2 from Certicom is used to support extended password encryption (RSA public and private cryptography algorithm). In addition, Certicom SSL Plus 5.2.2 and Certicom Security Builder GSE 2.0 are used to support SSL 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.

SRS uses LDAP server which provides global directory services for sharing component information such as server names and connection properties. LDAP is a third party software and Replication Server only uses Open Client/ Open Server libraries interface to use this service. LDAP is not part of the TOE. LDAP should be considered a component of the IT environment which can be used to provide global directory services.

2.2.1 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).

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.

[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.

2.2.2 Logical Boundaries

This section summarizes the security functions provided by SRS:

- User data protection
- Identification and authentication
- Security management

2.2.2.1 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.

2.2.2.2 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.

2.2.2.3 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.

2.3 TOE Documentation

Sybase offers a series of documents that describe the installation of SRS as well as guidance for subsequent use and administration of the applicable security features (see section 6.2 for details).

3. Security Environment

The TOE security environment describes the security aspects of the intended environment in which the TOE is to be used and the manner in which it is expected to be employed. The statement of the TOE security environment defines the following:

- Threats that the TOE and the environment of the TOE counters and
- Assumptions made about the operational environment and the intended method of use for the TOE.

Furthermore, the TOE is intended to be used in environments where the relative assurance that its security functions are enforced is commensurate with EAL 2 as defined in the CC.

3.1 Threats

T.MISROUTE Data being replicated from between primary and secondary data sources may be misdirected by an unauthorized user.

T.SECURREP Data being replicated from a primary to a secondary data source may be subject to unauthorized disclosure or modification.

3.2 Assumptions

A.NETWORK It is assumed that the environment protects network communication media appropriately.

A.NO_EVIL Authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.

A.NO_GENERAL_PURPOSE
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.

A.PHYSICAL It is assumed that 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.

A.ROBUST_ENVIRONMENT
It is assumed that the IT environment provides support commensurate with the expectations of the TOE.

4. Security Objectives

This section defines the security objectives for the TOE and its supporting environment. The security objectives are intended to counter identified threats and address applicable assumptions.

4.1 Security Objectives for the TOE

O.AUTHUSER The TOE must ensure that only authorized users can control the flow of replicated data within the TOE.

O.INFOFLOW The TOE must ensure that replicated data flows within the TOE in accordance with defined information flow rules.

4.2 Security Objectives for the IT Environment

OE.PROTECT The IT environment must ensure that the TOE and its means of communication are protected from tampering and disclosure.

4.3 Security Objectives for the Environment

OE.CONFIG The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation and applicable security policies and procedures by appropriately trained and trusted administrator personnel.

OE.NETWORK The environment must protect network traffic to and from the TOE from unauthorized disclosure.

OE.NO_GENERAL_PURPOSE
There will be 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.

OE.PHYSICAL Physical security will be 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.

OE.TRUST_IT Each IT entity the TOE relies on for security functions will be installed, configured, managed, maintained and provide the applicable security functions in a manner appropriate to the IT entity, and consistent with the security policy of the TOE and the relationship between them.

5. IT Security Requirements

The security requirements for the TOE have all been drawn from Parts 2 and 3 of the Common Criteria. The security functional requirements have been selected to correspond to the actual security functions implemented by the TOE while the assurance requirements have been selected to offer a low to moderate degree of assurance that those security functions are properly realized by users of the TOE.

5.1 TOE Security Functional Requirements

The following table describes the SFRs that are candidates to be satisfied by Replication Server.

Requirement Class	Requirement Component
FDP: User data protection	FDP_IFC.1: Subset information flow control
	FDP_IFF.1: Simple security attributes
FIA: Identification and authentication	FIA_ATD.1: User attribute definition
	FIA_UAU.2: User authentication before any action
	FIA_UID.2: User identification before any action
FMT: Security management	FMT_MSA.1: Management of security attributes
	FMT_MSA.3: Static attribute initialization
	FMT_MTD.1: Management of TSF data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles

Table 1 TOE Security Functional Components

5.1.1 User data protection (FDP)

5.1.1.1 Subset information flow control (FDP_IFC.1)

FDP_IFC.1.1 The TSF shall enforce the [**Replication SFP**] on [
subjects: data servers,
information: data, and
operations: replication].

5.1.1.2 Simple security attributes (FDP_IFF.1)

FDP_IFF.1.1 The TSF shall enforce the [**Replication SFP**] based on the following types of subject and information security attributes: [
subjects: data server - identity
information: data – data server type (primary and replicate), replication rules].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**data will be replicated from a data server to another data server only as specifically configured, based on data server identities and types, in accordance with the applicable replication rules**].

FDP_IFF.1.3 The TSF shall enforce the [**no additional information flow control SFP rules**].

FDP_IFF.1.4 The TSF shall provide the following [**no additional SFP capabilities**].

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: [**no rules that explicitly authorise information flows**].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [**data will not be replicated if there is no defined rule or its data server is not defined**].

5.1.2 Identification and authentication (FIA)

5.1.2.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**identity, authentication data, and role**].

5.1.2.2 User authentication before any action (FIA_UAU.2)

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.2.3 User identification before any action (FIA_UID.2)

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.3 Security management (FMT)

Security Management Functions	Security Relevant Attributes and/or Data
Create and delete associations between data servers	Data server attributes (see FDP_IFF.1)
Create, modify (except authentication data), and delete replications rules	Replication SFP rules, including the disposition (i.e., type) of data servers in relation to specific data (see FDP_IFF.1)
Create, modify, and delete user accounts	User attributes (see FIA_ATD.1)
Modify another user's password	Authentication data (see FIA_ATD.1)

Table 2 TOE Security Management Roles

5.1.3.1 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the [**Replication SFP**] to restrict the ability to [***[see Table 2]***] the security attributes [**see Table 2**] to [**authorized administrator**].

5.1.3.2 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the [**Replication SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**authorized administrator**] to specify alternative initial values to override the default values when an object or information is created.

5.1.3.3 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to [***[see Table 2]***] the [**see Table 2**] to [**the authorized administrator**].

5.1.3.4 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [**see Table 2 (Security Management Functions)**].

5.1.3.5 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [**authorized administrator**].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.2 IT Environment Security Functional Requirements

The following table describes the SFRs that are candidates to be satisfied by the IT environment of Replication Server.

Requirement Class	Requirement Component
FDP: User data protection	FDP_ITT.1: Basic internal transfer protection
FPT: Protection of the TSF	FPT_ITT.1: Basic internal TSF data transfer protection
	FPT_RVM.1: Non-bypassability of the TSP
	FPT_SEP.1: TSF domain separation

Table 3 IT Environment Security Functional Components

5.2.1 User data protection (FDP)

5.2.1.1 Basic internal transfer protection (FDP_ITT.1)

FDP_ITT.1.1 The TSF shall enforce the [**Replication SFP**] to prevent the [***disclosure* and *modification***] of user data when it is transmitted between physically-separated parts of the TOE.

5.2.2 Protection of the TSF (FPT)

5.2.2.1 Basic internal TSF data transfer protection (FPT_ITT.1)

FPT_ITT.1.1 The TSF shall protect TSF data from [***disclosure* and *modification***] when it is transmitted between separate parts of the TOE.

5.2.2.2 Non-bypassability of the TSP (FPT_RVM.1)

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.2.2.3 TSF domain separation (FPT_SEP.1)

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.2: Configuration items
ADO: Delivery and operation	ADO_DEL.1: Delivery procedures
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.1: Descriptive high-level design
	ADV_RCR.1: Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing

	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

Table 4 EAL 2 Assurance Components

5.3.1 Configuration management (ACM)

5.3.1.1 Configuration items (ACM_CAP.2)

ACM_CAP.2.1d The developer shall provide a reference for the TOE.
ACM_CAP.2.2d The developer shall use a CM system.
ACM_CAP.2.3d The developer shall provide CM documentation.
ACM_CAP.2.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.2.2c The TOE shall be labeled with its reference.
ACM_CAP.2.3c The CM documentation shall include a configuration list.
ACM_CAP.2.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.2.6c The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.
ACM_CAP.2.7c The CM system shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and operation (ADO)

5.3.2.1 Delivery procedures (ADO_DEL.1)

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2d The developer shall use the delivery procedures.
ADO_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
ADO_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.
ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.
ADO_IGS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.
ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.1.2c The functional specification shall be internally consistent.
ADV_FSP.1.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4c The functional specification shall completely represent the TSF.
ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Descriptive high-level design (ADV_HLD.1)

ADV_HLD.1.1d The developer shall provide the high-level design of the TSF.
ADV_HLD.1.1c The presentation of the high-level design shall be informal.
ADV_HLD.1.2c The high-level design shall be internally consistent.
ADV_HLD.1.3c The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.1.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.1.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.1.6c The high-level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.1.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
ADV_HLD.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_HLD.1.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.
ADV_RCR.1.1c For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.
ADV_RCR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.
AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.
AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.
AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.
AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.
AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.
AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_ADM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.
AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.
AGD_USR.1.3c The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4c The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.
AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.
AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.
AGD_USR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Tests (ATE)

5.3.5.1 Evidence of coverage (ATE_COV.1)

ATE_COV.1.1d The developer shall provide evidence of the test coverage.
ATE_COV.1.1c The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.2 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.
ATE_FUN.1.2d The developer shall provide test documentation.
ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.
ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.3 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.
ATE_IND.2.1c The TOE shall be suitable for testing.
ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.6 Vulnerability assessment (AVA)

5.3.6.1 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.3.6.2 Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.

AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.

AVA_VLA.1.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 User data protection

The TOE implements an information flow policy whereby data from a data server is replicated to other data servers. The authorized administrator can define the primary data sources as well as replicate data servers for given data. Further, they can then define specifically how data is to be replicated among the data servers.

In general, primary data servers provide data to the TOE and it uses its current configuration (i.e., replication rules associated with the applicable data) to determine how to replicate the data. As a result, the applicable data is provided to the appropriate replicate data servers. Note that the data servers only provide or accept information. The TOE doesn't support specific requests (i.e., form a data server) about what should happen to that data (e.g., where to send it or get it from).

While normally data travels from primary data servers to one or more replicate servers that is not actually required. The replication rules can be defined to allow data be updated at a replicate and be replicated back toi the primary. It is at the discretion of the rule designed to define how replication should actually occur.

The process of replication is that a Replication Agent, representing a specific data server by virtue of an account established for that data server, logs into the TOE and submits LTL requests representing data to be replicated. If the data server is not defined (i.e., it doesn't have an account) it cannot log in and submit data. Once data is submitted, it is placed in an inbound queue for replication. If there is no replication rule for the data, the data will be discarded. Otherwise, the data will be distributed in accordance with the replication rules, taking into account the type of the applicable data servers (e.g., primary or replicate). It is, for example, possible to define rules allowing data to flow only from primary to replicate data servers. When the data is distributed, it is placed in outbound queues. The TOE then distributes data in the outbound queues to the corresponding replicate data server.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_IFC.1: The TOE controls the replication of data among associated data servers.
- FDP_IFF.1: The TOE replicates data in accordance with specific rules configured by an authorized administrator. Replication occurs from a data server to other replicate servers depending specifically on rules associated with the data to be replicated and only data with replication rules can be replicated and only from/to defined data servers.

6.1.2 Identification and authentication

The TOE implements login mechanisms for its users via a direct application interface. In order to obtain any services of the TOE, each user (i.e., authorized administrator as well as Replication Agents acting on behalf of data servers) must provide the appropriate username and corresponding password, which is verified by the TOE. Once a user is logged in they are associated with a user role associated with their user account (i.e., user definition) that is used to limit the available functions.

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1: Each user is defined with a username, password, and role (see below).
- FIA_UAU.2: In order to access any function of the TOE, the applicable user must first by authenticated.
- FIA_UID.2: In order to access any function of the TOE, the applicable user must first by identified.

6.1.3 Security management

The TOE defines two administrative roles: Database Administrator (DBA) and Replication System Administrator (RSA). These are collectively referred to as authorized administrator in the context of this ST since their functions have substantial overlap. Logically, the DBA has responsibilities outside the TOE (e.g., managing actual data servers), but in the context of the TOE they share the responsibilities associated with defining data servers and establishing replication rules.

The other type of role is the Replication Agent role (or Replication Agent User). Replication Agent Users are allowed to provide information to the TOE to be replicated (i.e., put data in the inbound queue).

When a user logs in, the resulting session is associated with the role that is assigned to their username. The assigned role will serve to dictate the permissible set of operations the user can perform. Replication system administrators manage Replication Server permissions with the grant and revoke commands. Permissions determine which RCL commands users are permitted to execute.

Authorized administrators are allowed to manage the replication system (i.e., one or more SRSs working in concert). The can create, modify, and delete replication rules as well as create and delete associations between data servers and SRSs within replication system. Note that no replication can occur until the TOE is specifically configured to implement that replication. This also includes managing (create, modify, and delete) user accounts within the replication system. Users can be assigned more than user account, but each account is associated with a single role in which they will be functioning while logged in.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MSA.1: The security management functions are limited as indicated above.
- FMT_MSA.3: The security management functions are limited as indicated above. Also, the information flow policy is restrictive in that there is no replication until it is specifically defined.
- FMT_MTD.1: The security management functions are limited as indicated above.
- FMT_SMF.1: The security management functions are identified above.
- FMT_SMR.1: The security management roles are identified above.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by Sybase ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. Sybase performs configuration management on the TOE implementation representation, design, tests, user and administrator guidance, and the CM documentation.

These activities are documented in:

- Sybase Replication Server Configuration Management Plan Version 0.1 (RS_eal2_ACM.doc)

The Configuration management assurance measure satisfies the following EAL 2 assurance requirements:

- ACM_CAP.2

6.2.2 Delivery and operation

Sybase provides delivery documentation and procedures to identify the TOE, secure the TOE during delivery, and provide necessary installation and generation instructions. Sybase's delivery procedures describe all applicable procedures to be used to prevent in appropriate access to the TOE. Sybase also provides documentation that describes the steps necessary to install Replication Server in accordance with the evaluated configuration.

These activities are documented in:

- Sybase Replication Server Delivery and Operation Procedures Version 0.1 (RS_eal2_ADO.doc)

The Delivery and operation assurance measure satisfies the following EAL 2 assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

Sybase has documents describing all facets of the design of the TOE. These documents serve to describe the security functions of the TOE, its interfaces both external and between subsystems, the architecture of the TOE (in terms of subsystems), and correspondence between the available design abstractions (including the ST).

These activities are documented in:

- Replication Server Security Functional Specification Version 0.4 (RS_eal2_FuncSpec.doc)
- Replication Server Security Design Specification Version 0.3 (RS_eal2_DesignSpec.doc)

The Development assurance measure satisfies the following EAL 2 assurance requirements:

- ADV_FSP.1
- ADV_HLD.1
- ADV_RCR.1

6.2.4 Guidance documents

Sybase provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

These activities are documented in:

- Replication Server Administration Guide Volume 1: version 15.2
- Replication Server Administration Guide Volume 2: version 15.2
- Replication Server Reference Manual: version 15.2
- Sybase Replication Server Design Guide version 15.2
- Replication Server Heterogeneous Replication Guide 15.2
- Installation Guide for Unix V15.2
- Installation Guide for Windows V15.2
- Replication Server Configuration Guide UNIX V15.2
- Replication Server Configuration Guide Windows V15.2

The Guidance documents assurance measure satisfies the following EAL 2 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Tests

The test documents describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. In addition, these documents describe how the functional specification has been appropriately tested.

These activities are documented in:

- Replication Server 15.2 Common Criteria Test Plan Version 2.0 (RS152CC_testplan.doc)
- RS152CC_testsuit.xls (This excel spreadsheet contains the test results)

The Tests assurance measure satisfies the following EAL 2 assurance requirements:

- ATE_COV.1
- ATE_FUN.1
- ATE_IND.2

6.2.6 Vulnerability assessment

Sybase has conducted a strength of function analysis wherein all permutational or probabilistic security mechanisms have been identified and analyzed resulting in a demonstration that all of the relevant mechanisms fulfill the minimum strength of function claim, SOF-basic.

Sybase performs regular vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE.

These activities are documented in:

- Sybase Replication Server Vulnerability Analysis Version 0.2 (RS_eal2_AVA.doc)

The Vulnerability assessment assurance measure satisfies the following EAL 2 assurance requirements:

- AVA_SOF.1
- AVA_VLA.1

7. Protection Profile Claims

There are no Protection Profile claims in this Security Target.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the security objectives.

	T.MISROUTE	T.SECURREP	A.NETWORK	A.NO_EVIL	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.ROBUST_ENVIRONMENT
O.AUTHUSER	X						
O.INFOFLOW		X					
OE.PROTECT	X	X					
OE.CONFIG				X			
OE.NETWORK			X				
OE.NO_GENERAL_PURPOSE					X		
OE.PHYSICAL						X	
OE.TRUST_IT							X

Table 5 Environment to Objective Correspondence

8.1.1.1 T.MISROUTE

Data being replicated from between primary and secondary data sources may be misdirected by an unauthorized user.

This Threat is satisfied by ensuring that:

- O.AUTHUSER: By implementing a well defined set of information flow rules, the potential for misdirected data flows is reduced.
- OE.PROTECT: By protecting the TOE and its means of communication, the IT environment serves to help ensure that unauthorized users could not redirect or otherwise misdirect the flow of replicated data within the TOE.

8.1.1.2 T.SECURREP

Data being replicated from a primary to a secondary data source may be subject to unauthorized disclosure or modification.

This Threat is satisfied by ensuring that:

- O.INFOFLOW: By ensuring that replicated data flows in accordance with defined information flow rules, the potential for unauthorized disclosure is reduced.
- OE.PROTECT: By protecting the TOE and its means of communication, the IT environment serves to help ensure that unauthorized modifications and disclosures cannot occur.

8.1.1.3 A.NETWORK

It is assumed that the environment protects network communication media appropriately.

This Assumption is satisfied by ensuring that:

- OE.NETWORK: The environment is responsible to protect network traffic to and from the TOE from unauthorized disclosure. Note that this is an environment objective since the possible mechanisms could range from physical protection of the network media to cryptographic tunneling.

8.1.1.4 A.NO_EVIL

Authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.

This Assumption is satisfied by ensuring that:

- OE.CONFIG: Authorized administrators are trained and trusted to properly configure the IT environment so it enforces its security policies.

8.1.1.5 A.NO_GENERAL_PURPOSE

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.

This Assumption is satisfied by ensuring that:

- OE.NO_GENERAL_PURPOSE: The DBMS server must not include any general-purpose commuting or storage capabilities. This will protect the TSF data from malicious processes.

8.1.1.6 A.PHYSICAL

It is assumed that 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.

This Assumption is satisfied by ensuring that:

- OE.PHYSICAL: The TOE, the TSF data, and protected user data is assumed to be protected from physical attack (e.g., theft, modification, destruction, or eavesdropping). Physical attack could include unauthorized

intruders into the TOE environment, but it does not include physical destructive actions that might be taken by an individual that is authorized to access the TOE environment.

8.1.1.7 A.ROBUST_ENVIRONMENT

It is assumed that the IT environment provides support commensurate with the expectations of the TOE.

This Assumption is satisfied by ensuring that:

- OE.TRUST_IT: The IT entities in the environment are correctly installed, configured, managed, maintained and provides the applicable security functions.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that **Table 6** indicates the requirements that effectively satisfy the individual objectives. .

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.AUTHUSER	O.INFOFLOW	OE.PROTECT
FDP_IFC.1		X	
FDP_IFF.1		X	
FIA_ATD.1	X		
FIA_UAU.2	X		
FIA_UID.2	X		
FMT_MSA.1	X		
FMT_MSA.3		X	
FMT_MTD.1	X		
FMT_SMF.1	X		
FMT_SMR.1	X		
FDP_ITT.1			X
FPT_ITT.1			X
FPT_RVM.1			X
FPT_SEP.1			X

Table 6 Objective to Requirement Correspondence

8.2.1.1 O.AUTHUSER

The TOE must ensure that only authorized users can control the flow of replicated data within the TOE.

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1: The TOE must have well defined users in order to distinguish authorized users.
- FIA_UAU.2: The TOE must ensure that users are authenticated in order to ensure that authorized users are who they claim to be.
- FIA_UID.2: The TOE must identify users in order to determine what they are authorized to do.

- FMT_MSA.1: The TOE must limit the ability to manipulate security attributes in order to protect the data replication function.
- FMT_MTD.1: The TOE must limit the ability to manipulate security data in order to protect the data replication function.
- FMT_SMF.1: The TOE must provide functions suitable to configure the flow of data.
- FMT_SMR.1: The TOE must distinguish security management roles in order to assign appropriate authorities to users.

8.2.1.2 O.INFOFLOW

The TOE must ensure that replicated data flows within the TOE in accordance with defined information flow rules.

This TOE Security Objective is satisfied by ensuring that:

- FDP_IFC.1 and FDP_IFF.1: The TOE must implement well-defined rules for the replication of data among data servers so that data flows only in accordance with its configured policies.
- FMT_MSA.3: The TOE must ensure that replication does not occur unless it is specifically authorized (configured).

8.2.1.3 OE.PROTECT

The IT environment must ensure that the TOE and its means of communication are protected from tampering and disclosure.

This IT Environment Security Objective is satisfied by ensuring that:

- FDP_ITT.1: The IT environment must protect replicated data as it is communicated via potentially insecure media.
- FPT_ITT.1: The IT environment must protect security-related data as it is communicated via potentially insecure media.
- FPT_RVM.1: The IT environment must ensure that the TOE cannot be bypassed so that its security policies can always be enforced.
- FPT_SEP.1: The IT environment must protect not only itself, but also the TOE from tampering and interference.

8.3 Security Assurance Requirements Rationale

The TOE is intended for an environment requiring a low to moderate level of assurance in the security functionality of conventional commodity TOEs, as presented in the statement of security environment (Section 3). The target assurance level of EAL 2 is appropriate for such an environment.

8.4 Strength of Functions Rationale

In accordance with EAL 2, a Strength of Functions claim of SOF-basic has been made. EAL 2 represents a low to moderate level of security assurance and hence SOF-basic should represent an appropriate strength of function.

The only permutational or probabilistic mechanism in the TOE is the password-based user authentication mechanism used to satisfy FIA_UAU.2.

8.5 Requirement Dependency Rationale

The following table identifies the dependencies of the requirements in this ST, including the requirements explicitly defined in this ST. As indicated in the table, all of the dependencies are satisfied.

ST Requirement	CC Dependencies	ST Dependencies
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1

ST Requirement	CC Dependencies	ST Dependencies
FDP_IFF.1	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.1 and FMT_MSA.3
FIA_ATD.1	none	none
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	none	none
FMT_MSA.1	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_IFC.1
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1 and FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FDP_ITT.1	none	none
FPT_ITT.1	none	none
FPT_RVM.1	none	none
FPT_SEP.1	none	none
ACM_CAP.2	none	none
ADO_DEL.1	none	none
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1	ADV_RCR.1
ADV_HLD.1	ADV_FSP.1 and ADV_RCR.1	ADV_FSP.1 and ADV_RCR.1
ADV_RCR.1	none	none
AGD_ADM.1	ADV_FSP.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1	ADV_FSP.1
ATE_COV.1	ADV_FSP.1 and ATE_FUN.1	ADV_FSP.1 and ATE_FUN.1
ATE_FUN.1	none	none
ATE_IND.2	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1
AVA_SOF.1	ADV_FSP.1 and ADV_HLD.1	ADV_FSP.1 and ADV_HLD.1
AVA_VLA.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1

8.6 Explicitly Stated Requirements Rationale

There are no explicitly stated requirements in this Security Target.

8.7 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 7 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	User data protection	Identification and authentication	Security management
FDP_IFC.1	X		
FDP_IFF.1	X		
FIA_ATD.1		X	
FIA_UAU.2		X	
FIA_UID.2		X	
FMT_MSA.1			X
FMT_MSA.3			X
FMT_MTD.1			X
FMT_SMF.1			X
FMT_SMR.1			X

Table 7 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.