TIBCO ActiveMatrix BusinessWorks™ Release 5.8 Security Target

Version 2.0
August 19, 2010

Prepared for:

TIBCO Software Inc.

3303 Hillview Avenue
Palo Alto, CA 94304

Prepared By:

Science Applications International Corporation

Common Criteria Testing Laboratory

6841 Franklin Center Drive
Columbia, MD 21046

LIST OF TABLES

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 TIBCO ActiveMatrix BusinessWorks™ provided by TIBCO Software Inc. ActiveMatrix BusinessWorks™ is what is called an "integration server" that provides a runtime environment for distributed multi-tier enterprise applications.

The Security Target contains the following additional sections:

- Section 2 – Target of Evaluation (TOE) Description
  This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Section 3 – TOE Security Environment
  This section details the expectations of the environment, the threats that are countered by the TOE and the environment, as well as the organizational policy that the TOE must fulfill.
- Section 4 – TOE Security Objectives
  This section details the security objectives of the TOE and the environment.
- Section 5 – IT Security Requirements
  The section presents the security functional requirements (SFR) for the TOE and the Environment that supports the TOE, and details the assurance requirements.
- Section 6 – TOE Summary Specification
  The section describes the security functions represented in the TOE that satisfy the security requirements.
- Section 7 – Protection Profile Claims
  This section presents any protection profile claims.
- Section 8 – Rationale
  This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – TIBCO ActiveMatrix BusinessWorks™ Release 5.8 Security Target

ST Version – Version 2.0

ST Date – August 19, 2010

TOE Identification – TIBCO ActiveMatrix BusinessWorks™ Release 5.8

TOE Component Identification –

- TIBCO ActiveMatrix BusinessWorks™ Release 5.8 engine
- TIBCO Administrator™ 5.6.1
- TIBCO Runtime Agent™ 5.6.2 w/ Hotfix #2
- TIBCO Designer™ 5.6.2.5

TOE Guidance Documentation –

- TIBCO ActiveMatrix BusinessWorks Concepts, Software Release 5.8, February 2010
- TIBCO ActiveMatrix BusinessWorks Getting Started, Software Release 5.8, February 2010
- TIBCO ActiveMatrix BusinessWorks Process Design Guide, Software Release 5.8, February 2010
- TIBCO ActiveMatrix BusinessWorks Palette Reference, Software Release 5.8, February 2010
- TIBCO ActiveMatrix BusinessWorks Administration, Software Release 5.8, February 2010

- TIBCO ActiveMatrix BusinessWorks Installation, Software Release 5.8, February 2010
- TIBCO ActiveMatrix BusinessWorks Error Codes, Software Release 5.8, February 2010
- TIBCO ActiveMatrix BusinessWorks Release Notes, Software Release 5.8.0, February 2010
- TIBCO Administrator Release Notes, Software Release 5.6.1, February 2010
- TIBCO Administrator User Guide, Software Release 5.6, July 2008
- TIBCO Administrator Server Configuration Guide, Software Release 5.6, July 2008
- TIBCO Administrator Installation Guide, Software Release 5.6, July 2008
- TIBCO Runtime Agent Release Notes, Software Release 5.6, July 2008
- TIBCO Runtime Agent Scripting Deployment User's Guide, Software Release 5.6, July 2008
- TIBCO Runtime Agent Domain Utility User's Guide, Software Release 5.6, July 2008
- TIBCO Runtime Agent Installing Into a Cluster, Software Release 5.6, July 2008
- TIBCO Runtime Agent Installation, Software Release 5.6, July 2008
- TIBCO Runtime Agent Upgrading to Release 5.6, Software Release 5.6, July 2008
- TIBCO Designer User's Guide, Software Release 5.6, July 2008
- TIBCO Designer Palette Reference, Software Release 5.6, July 2008
- TIBCO Designer Release Notes, Software Release 5.6.2, January 2010
- TIBCO ActiveMatrix BusinessWorks™ (5.8), TIBCO Administrator™ (5.6), and TIBCO Runtime Agent™ (5.6) Security Features User's Guide, Version 1.9, 14 May 2010.

TOE Developer – TIBCO Software Inc.

Evaluation Sponsor – TIBCO Software Inc.

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007

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 3.1, Revision 2, September 2007.
  - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 2, September 2007.
  - Part 3 Conformant
  - Assurance Level: EAL 2 augmented with ALC_FLR.2

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~~ **big** things …").
  - Extended SFRs (i.e., those not found in Part 2 of the CC) are identified with "_EXT" following the associated family descriptor.

- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.4 Terminology

External IT entity --	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
TOE User	A user making use of a communication pathway where the TOE is enforcing authentication characteristics.

2. TOE Description

The Target of Evaluation (TOE) is *TIBCO ActiveMatrix BusinessWorks Release 5.8* (also known as ActiveMatrix BusinessWorks). ActiveMatrix BusinessWorks consists of a set of software applications that allow administrators to create and then host Business Processes that are accessed by other systems, that may access other systems, and which may be accessed by users; it is mainly used as an integration platform.

2.1 TIBCO Applications

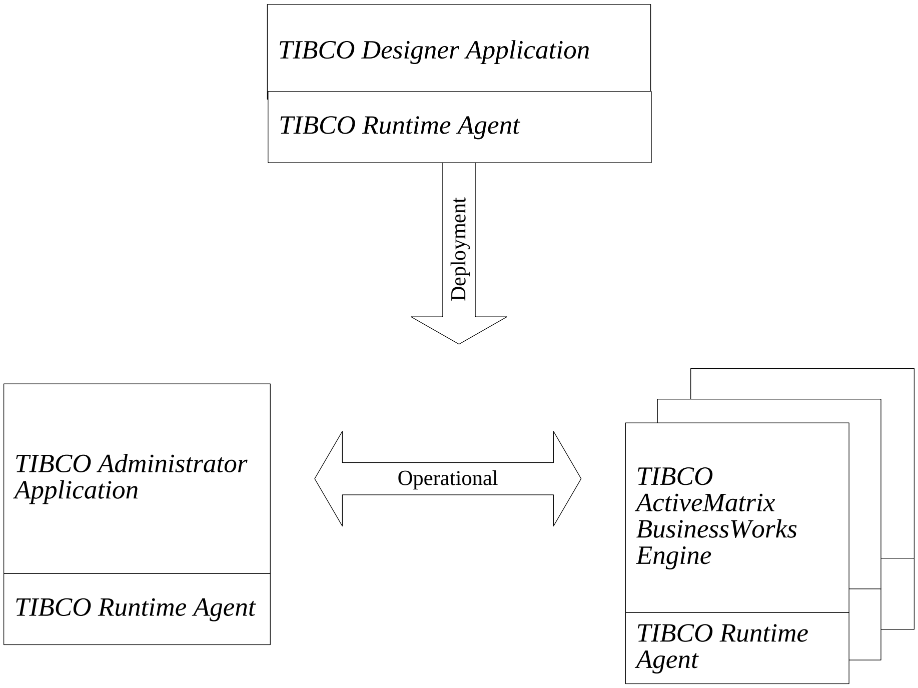
ActiveMatrix BusinessWorks consists of a development application, an administration application, and a runtime integration engine. These applications utilize common libraries. The following are the software applications that make up the TOE.

- *TIBCO Designer* – Provides the ability to develop business processes.
- *TIBCO Administrator* – Provides administrative interfaces that can be used to manage services of the TOE and business processes.
- *TIBCO ActiveMatrix BusinessWorks* – Provides a runtime environment for business processes.
- *TIBCO Runtime Agent* – Provides common functionality in libraries used by ActiveMatrix BusinessWorks applications, including functions used to communicate between TOE components.

Figure 2-1 TIBCO Components depicts a very general view of the components that make up the TIBCO product. The *TIBCO Designer* application creates and deploys a definition of a business process and then plays no part in the operation of the deployed business process. The *TIBCO Administrator* application and *TIBCO ActiveMatrix BusinessWorks* engine each include an instance of *TIBCO Runtime Agent*.

The *TIBCO Designer* application creates an Enterprise Archive (EAR) file to describe a business process and associated resource information; in conjunction with *the TIBCO Designer* application, certain properties may be included in an XML file called ‘bwengine.xml’. Certain aspects of the Design elements and all of the aspects of the bwengine.xml file are exposed to the *TIBCO Administrator* application and may be changed prior to deployment.

Figure 2-1 TIBCO Components


TIBCO Designer Application
TIBCO Runtime Agent
Deployment
TIBCO Administrator Application
TIBCO Runtime Agent
Operational
TIBCO ActiveMatrix BusinessWorks Engine
TIBCO Runtime Agent

TIBCO Runtime Agent is installed on all machines in the network that are participating in the business process.

These EAR files are moved[1] from the *TIBCO Designer* application to the *TIBCO Administrator* application. The *TIBCO Administrator* application is then used to deploy applicable parts of the EAR file to applicable instances of the *ActiveMatrix BusinessWorks* engine. The *TIBCO Administrator* application starts the *ActiveMatrix BusinessWorks* engine to perform activities in the business process.

TIBCO Runtime Agent is an installation package that provides common functionality in libraries used by other ActiveMatrix BusinessWorks applications, including functions used to communicate between TOE components. Two significant pieces of TIBCO Runtime Agent are subsets of other TIBCO products: TIBCO Hawk® Agent and TIBCO Rendezvous® Daemon. The TIBCO Hawk® Agent is configured for a business process (created by the Domain Utility) to use either Rendezvous® or TIBCO Enterprise Message Service™ as a message carrying protocol to pass messages between subsystems. Hawk Agent is used by each subsystem to facilitate communication between subsystems while enforcing constraints defined for the business process. Rendezvous Daemon-based communication provides message passing similar to message passing using the TCP/IP-based socket programming construct. Rendezvous is a connectionless, transport layer protocol carried by UDP/IP packets. The *TIBCO Designer* application, the *TIBCO Administrator* application, and the *ActiveMatrix BusinessWorks* engine all rely upon software installed by *TIBCO Runtime Agent*.

The TOE supports creation of the Business Process, however, the security requirement of this ST define the protections that are available once the business process has been deployed.

2.1.1 Overview

The TIBCO Designer application, the TIBCO Administrator application, the ActiveMatrix BusinessWorks engine, and Runtime Agent™ can be installed on separate computers in a network or combined on the same computer as appropriate for the environment and for the business process. Runtime Agent must be installed as part of each TIBCO software application because it provides common functionality in libraries that are used by other parts of the product.

2.1.1.1 TIBCO Designer

TIBCO Designer is used to create a definition of a business processes. The *TIBCO Runtime Agent* and the *TIBCO ActiveMatrix BusinessWorks* engine installation programs are used to install TIBCO Designer on a computer. The person installing TIBCO Designer first executes the TIBCO Runtime Agent installation package which installs basic TIBCO Designer functionality. The person installing TIBCO Designer then uses the *ActiveMatrix BusinessWorks* installation package to install the ActiveMatrix BusinessWorks design-time component, augmenting the base TIBCO Designer application. The result is a TIBCO Designer application capable of creating definitions of business processes for a TIBCO ActiveMatrix BusinessWorks network.

The TIBCO Designer application is used by trusted individuals to create and test the definition of a business process that will be executed on a network. The network is composed of a computer running the TIBCO Administrator application, one or more computers running the ActiveMatrix BusinessWorks engine, computers that comprise the supporting environment and computers used by business process users.

The TIBCO Designer application is an application used to create the definition of a business process. This definition is represented in a set of files (EAR files) that must be transferred to computers on a network in order for the business process to be made available to end users (i.e., users of the business process). All of the computers in a network that are intended to support a business process are considered to be part of the same 'domain'. A 'domain' is an administrative grouping of computer systems running in support of a business process.

The EAR files must be moved from the TIBCO Designer application to a TIBCO Administrator application in a domain. The TIBCO Administrator application is then used to deploy applicable parts of the EAR files to applicable instances of the ActiveMatrix BusinessWorks engines. The TIBCO Administrator application starts the ActiveMatrix BusinessWorks engines to perform activities in the business process.

[1] The method of moving an EAR file depends upon administrative and physical concerns and is outside the scope of this security target.

The TIBCO Designer application does not implement any security features and plays no role in the enforcement of security checks in a deployed business process. The method of moving an EAR file from a TIBCO Designer application to a TIBCO Administrator application depends upon administrative and physical concerns and is outside the scope of the TIBCO Designer application. Access to the application that is the TIBCO Designer subsystem and to data files used by and created by the TIBCO Designer subsystem is controlled by the operating system that is part of the IT environment of the TOE.

2.1.1.2 TIBCO Administrator

The TIBCO Administrator application provides an interface for administrative users of the TOE to deploy business processes, control business processes, and to perform security management operations. The *TIBCO Runtime Agent* and the *TIBCO Administrator* installation programs are used to install the TIBCO Administrator application on a computer. The person installing TIBCO Administrator first executes the TIBCO Runtime Agent installation package which installs the Runtime Agent functionality. The person installing TIBCO Administrator then uses the *TIBCO Administrator* installation package to install the TIBCO *Administrator Application.* The result is a TIBCO Administrator application offering an administrative interface to the TOE.

The TIBCO Administrator application is used by trusted individuals to perform administration activities for the TOE and for business processes executing on the TOE. Installation of TIBCO Administrator leads to the creation of a domain (See Section 2.1.1.5 below). The TIBCO Administrator application is responsible only for enforcing constraints upon management of a business process and of a domain, auditing those activities and propagating configuration changes to other applications

2.1.1.3 The ActiveMatrix BusinessWorks Engine

The initial configuration of a business process is provided by the TIBCO Designer application in the EAR files that describe the business process. Selected configuration values (those specified by the TIBCO Designer application as externalized) can be modified by the TIBCO Administrator application. The ActiveMatrix BusinessWorks engine uses whatever configuration values are provided to it when the business process is deployed or when the TIBCO Administrator application indicates a configuration change.

One or more ActiveMatrix BusinessWorks engines must exist in a network running TIBCO ActiveMatrix BusinessWorks.

The ActiveMatrix BusinessWorks engine, like every application, depends upon *TIBCO Runtime Agent*. The *TIBCO Runtime Agent* and the *TIBCO ActiveMatrix BusinessWorks* installation programs are used to install the ActiveMatrix BusinessWorks engine on a computer. The person installing an ActiveMatrix BusinessWorks engine first executes the TIBCO Runtime Agent installation package which installs the Runtime Agent functionality. The ActiveMatrix BusinessWorks engine specific functionality is then installed using the *TIBCO ActiveMatrix BusinessWorks* installation program. The person installing an ActiveMatrix BusinessWorks engine uses the *TIBCO ActiveMatrix BusinessWorks* installation package to install ActiveMatrix BusinessWorks runtime. The ActiveMatrix BusinessWorks design part of the installation package is an optional part of the installation which simulates the operation of an ActiveMatrix BusinessWorks engine entirely on a system with a TIBCO Designer application already installed.

2.1.1.4 TIBCO Runtime Agent

Runtime Agent is required for any machine that will participate in a business process whether it is a TIBCO Designer application, a TIBCO Administrator application, or an ActiveMatrix BusinessWorks engine. Machines performing environmental supporting duties (e.g., a DBMS, an LDAP server) do not need to have a Runtime Agent installation.

The TIBCO Runtime Agent installation package includes the following pieces:

- Rendezvous Daemon provides real-time messaging between applications;
- Hawk Agent provides distributed monitoring and management of a business process;
- a Java Runtime Environment in which other applications execute and which provides a reliable timestamp for use by the TOE;
- TIBCO developed libraries (e.g., TIBCrypt library that provides encryption features);
- 3rd Party libraries (e.g., The Entrust library that provides FIPS compliant encryption features[2]);
- a Domain Utility that manages domains and manages machines within a domain; and
- a TIBCO Designer application that provides basic business process design features.

The person installing Runtime Agent executes the TIBCO Runtime Agent installation package and chooses the functionality desired for the type of system (e.g., designer, administrator, or engine) being created. In most cases this will be all parts of the installation (the TIBCO Designer component will usually only be installed on a computer being used to design a business process).

2.1.1.5 Administration Domain

An "administration domain" is a collection of users, machines, and services that is created during initial TOE installation and configuration that will be controlled as a set (e.g., the Accounting Department administration domain, the R&D administration domain). Each domain is managed by a TIBCO Administrator application, which can then be used by administrators to manage TOE functions. Administrators can only log into TOE instances belonging to the same administration domain in which their account is defined.

When the TIBCO Administrator application is installed, a domain name, and username/password pair is provided. That account becomes the domain administrator account for the specified domain. The domain administrator account is used to create other user accounts and assign permissions within the domain. All accounts exist only within the context of a domain.

After installing TIBCO Administrator, additional named domains can be created. The creation of a new domain is always associated with the specification of a username/password pair. The specified username becomes the domain administrator for the named domain. Domains are created using a Domain Utility that is part of Runtime Agent. Anyone with sufficient permission[3] in the environment to execute the Domain Utility can create a new domain and define the domain administrator for that domain.

The TIBCO Designer application does not perform identification and authentication of its users. The TIBCO Designer application can be used to create business process definitions. Similarly, the 'domain utility' application from the Runtime Agent installation package which is used to create new domains does not require identification and authentication. Business process definitions do not affect a running TOE until such time as an authenticated domain administrator deploys the business process.

An "administration domain" defines an administrative scope of control over machines, user accounts, administrative accounts, and configuration values. These configuration values include the following:

- The network transport mechanism (see below) used for communication between machines within a domain can be specified. This is referred to as the "domain transport."
- The storage mechanism for user and group information can be specified to use an LDAP server or storage local to the TIBCO Administrator application.
- The destination for domain information storage can be specified as a DBMS.

The "domain transport" that is chosen for an "administration domain" must provide sufficient protection of the communication between machines within a domain to satisfy the threats posed by the environment. An environment where all communication between applications, an LDAP server and/or a DBMS are in a dedicated and physically protected environment will require a different level of communication protection than one where untrusted users

[2] Entrust is FIPS 140-2 compliant, certificate #802.
[3] Only TIBCO administrators are given sufficient permissions to execute the Domain Utility when the TOE is configured per guidance.

and/or process' can intercept communications. or impersonation partners. The TOE supports a range of options for "domain transport" as described below:

Rendezvous as Domain Transport

Using Rendezvous as the domain transport provides no protection of communication from disclosure or modification when information is transmitted between applications of the TOE. Rendezvous does not provide sufficient protection of communication to be used in anything but a dedicated, physically protected and benign environment.

Tunneling Rendezvous

Rendezvous can be tunneled through either an SSH or IPSec VPN to achieve a desired protection of communication from disclosure and modification when information is transmitted between applications of the TOE. This protection is provided by the environment and can be appropriate communication protections for many environments. The TOE does not provide these protocols and thus the protection is being provided by the environment.

EMS as Domain Transport

The TOE also supports the use of the TIBCO Enterprise Message Service product as the domain transport. Enterprise Message Service™ provides cryptographically secured communication when information is transmitted between applications of the TOE. Enterprise Message Service protects information from both disclosure and modification. The TOE invokes Enterprise Message Service functionality in a manner that provides protected communications between applications.

2.2 Product Usage Overview

A developer uses the *TIBCO Designer* application to create a set of business processes. Developers are users with access to the *TIBCO Designer* application. Developers create and modify a business process. Administrators use the *TIBCO Administrator* application to install and configure the business processes on a ActiveMatrix BusinessWorks engine(s).[4] The ActiveMatrix BusinessWorks engine(s) host the business processes that are created using the *TIBCO Designer* application. After the business processes are installed and configured on the ActiveMatrix BusinessWorks engine(s), business process functionality is available.

The TOE ensures that the business process operates in a manner that is consistent with its configuration defined by the Developer and Administrator. Once a business process is installed, the configuration information associated with that business process defines the operational characteristics of the business process running on the TOE.

Business processes are composed of resources and process definitions. Resources (see Section 6.1.2 for a complete list of resource types) are communication pathways that are controlled by the ActiveMatrix BusinessWorks engine. A resource is used by business process activities. Process definitions are a description of the activities that comprise the business process. An activity is a specific task in a business process definition such as sending e-mail, writing a file, or querying a database.

Business processes and associated resource information are packaged into Enterprise Archive (EAR) files by *TIBCO Designer* application. EAR files contain the redistributable runtime components of business processes. EAR files are run using the ActiveMatrix BusinessWorks engine. An ActiveMatrix BusinessWorks engine creates instances of the processes described by the process definitions. The ActiveMatrix BusinessWorks engine also controls the creation and use of communication paths as defined by the configuration data within the EAR file.

Process definitions are representations of business processes acting upon resources. Process definitions are defined in the *TIBCO Designer* application using what are called "palettes". Palettes are library-type components containing representations of process definition components that are used to design and build business processes. An example of such a component is the "JDBC palette" that provides Java language access to a database in the environment.

Another example is the "Policy palette" that provides the ability to define a security policy over SOAP messages[5]. The "Policy palette" can be used to define authentication characteristics, integrity characteristics, confidentiality

[4] Installation and configuration is referred to as "deployment".

[5] The Policy palette only applies to SOAP messages.

characteristics, and timeout characteristics for SOAP messages only. Other palettes can define transport characteristics for the resources they define.

2.3 TOE Architecture

The intended environment of the TOE can be described in terms of the following components:

- *Operating Systems* – Provides a runtime environment for TOE application components (not for distributed applications developed using the TOE) and a reliable timestamp for use by the TOE.
- *Storage Medium* – Provides storage for TOE configuration information (e.g., files or databases).
- *Cryptomodule* – Performs cryptographic operations on messages at the request of the TOE.
- *Directory Service* – Optionally provides storage for user identification and authentication[6] information that is used by the TOE when user authentication is required for a business process.
- *Web Browser* – Provides a user interface for a *TIBCO Administrator* application.
- *Enterprise Applications* – Optional, applications providing access to data and functionality in the environment.

The TOE can reside on either a single machine or on many machines in a network. The TOE executes as applications that are accessed by users or other systems to implement a business process. Figure 2-2 shows the communication pathways that exist between users or systems, the *TIBCO Administrator* application, the ActiveMatrix BusinessWorks engine, and controlled enterprise applications. Both the *TIBCO Administrator* application and ActiveMatrix BusinessWorks engine implement web servers. The communication pathways labeled as "1st" and "2nd" in Figure 2-2 must be either a HTTP request, HTTPS request, SOAP request, TCP/IP packet, TIBCO Rendezvous messages, JMS message, or RMI call[7]. The following are some examples of these communication pathways:

- A user or system issues an HTTP request to the ActiveMatrix BusinessWorks engine and receives a response.
- A user or system issues a SOAP request to the ActiveMatrix BusinessWorks engine and receives a response.
- A user or system sends TCP/IP messages through the ActiveMatrix BusinessWorks engine and receives a response.

The communication pathway between two ActiveMatrix BusinessWorks engines occurs when one business process activity on the first ActiveMatrix BusinessWorks engine communicates with another business process activity on a second ActiveMatrix BusinessWorks engine. These types of communication pathways include all of the same pathways as can be initiated by a user, but also include a pathway for fault tolerance provided by the environment and is outside the scope of this evaluation. TIBCO Rendezvous messages[8] can be passed between ActiveMatrix BusinessWorks engines to facilitate fault tolerance.

The "3rd" communication pathway is between ActiveMatrix BusinessWorks engines and controlled enterprise applications. These pathways include the same pathways as are available for user process to ActiveMatrix BusinessWorks engine communications and the following pathways.

- The ActiveMatrix BusinessWorks engine issues an FTP request and receives a response.
- The ActiveMatrix BusinessWorks engine issues a JDBC request and receives a response.

[6] A directory service is optional because identification and authentication material can be stored in operating system file, a DBMS or in an LDAP server depending upon the definition of the 'administration domain'.

[7] RMI and raw TCP/IP cannot be secured with SSL because of their relationship to SSL in the protocol stack. Guidance documentation warns administrators about this limitation.

[8] TIBCO Rendezvous is a product that supports fault tolerance, but with respect to this evaluation that functionality is entirely in the environment, is not provided by the TOE and is excluded from this evaluation.

- The ActiveMatrix BusinessWorks engine issues a JMS request and receives a response.
- The ActiveMatrix BusinessWorks engine issues an email and potentially receives a response.
- The ActiveMatrix BusinessWorks engine issues an HTTP request and receives a response.
- The ActiveMatrix BusinessWorks engine issues a SOAP request and receives a response (either over HTTP, HTTPS, or JMS).

The "4th" communication pathway is between *TIBCO Administrator* and an ActiveMatrix BusinessWorks engine. The communication pathways can use the HTTP, HTTPS, JMS, JMS over SSL, or Rendezvous protocols.

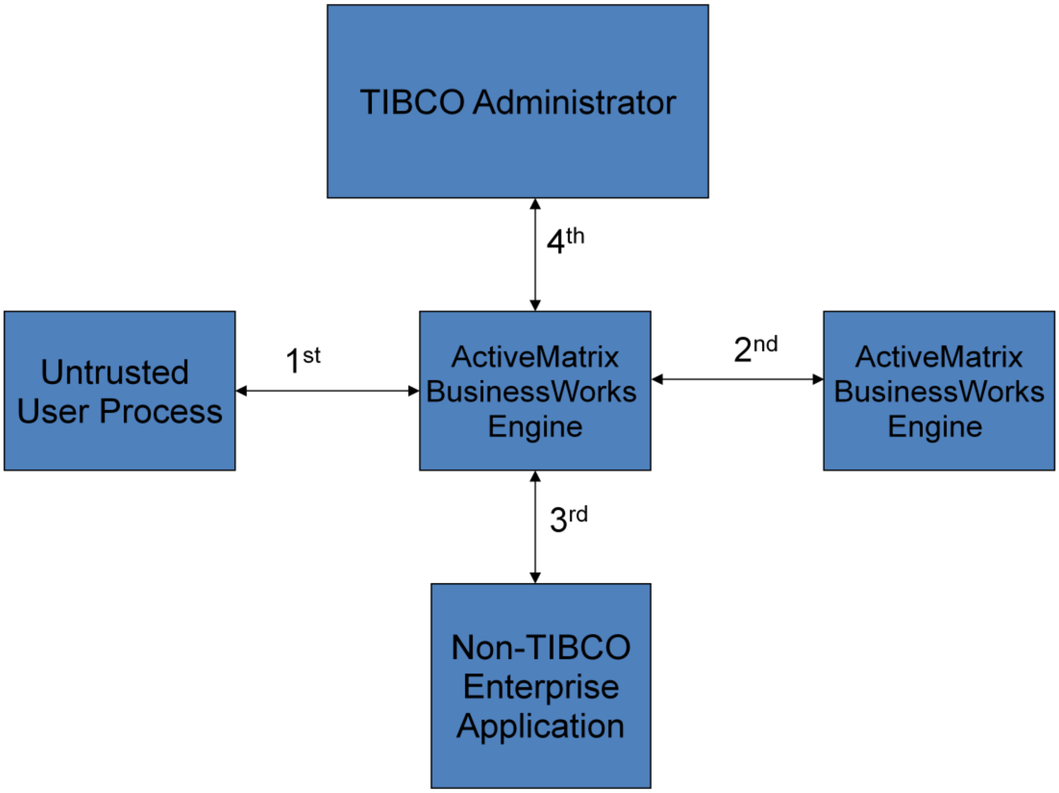

TIBCO Administrator
4th
Untrusted User Process
1st
ActiveMatrix BusinessWorks Engine
2nd
ActiveMatrix BusinessWorks Engine
3rd
Non-TIBCO Enterprise Application

Figure 2-2 TOE Communication Pathways[9]

A user process or a business process activity initiates a request. The ActiveMatrix BusinessWorks engine determines whether the request satisfies the configuration requirements defined for the business process activity being requested. The ActiveMatrix BusinessWorks engine either permits or denies the request.

For example, when the ActiveMatrix BusinessWorks engine is executing a business process configured for HTTP with Basic Authentication, an incoming HTTP request is either permitted or denied. If security characteristics are not defined, say the credentials are missing, or if the security characteristics are invalid, say the credentials are invalid then the HTTP request is denied. Similarly if the business process is configured for HTTPS an HTTP request would be denied.

As another example, a SOAP message is sent by a user to the ActiveMatrix BusinessWorks engine. The ActiveMatrix BusinessWorks engine can ensure that authentication characteristics, confidentiality characteristics, integrity characteristics, transport characteristics, or timeout characteristics are enforced. That is, the ActiveMatrix BusinessWorks engine can ensure that the incoming SOAP request was from a user account permitted to send the request, that the request was encrypted using a sufficiently strong encryption algorithm, or that a sufficient integrity mechanism is included in the request.

[9] The applications represented by the non-TIBCO Enterprise Application box may include TIBCO libraries, but the base functionality of the application is non-TOE.

2.3.1 Physical Boundaries

The components that make up the TOE are:

- TIBCO ActiveMatrix BusinessWorks™ Release 5.8 engine
- TIBCO Administrator™ 5.6.1
- TIBCO Runtime Agent™ 5.6.2 w/ Hotfix #2
- TIBCO Designer™ 5.6.2.5

TOE components require the following environment components to operate:

- Operating systems: Any one of:
  - Microsoft Windows XP, Server 2003 and Server 2008
  - Linux – Red Hat AS 4 and CentOS 5
- Java Runtime Engine:
  - Sun Java Runtime Environment version 1.6.0
- Storage Medium which is either operating system provided files or one of the following databases[10]:
  - Oracle 11g
  - Oracle 11g with RAC
  - Oracle 10g with RAC
  - Oracle 10g
  - Oracle 9i with RAC
  - Oracle 9.x
  - Oracle 8.1.x
  - Microsoft SQL Server 2000
  - Microsoft SQL Server 2005
  - Microsoft SQL Server 2008
  - DB2 8.2

TOE ActiveMatrix BusinessWorks, TIBCO Administrator, and Runtime Agent components rely on the following environment components to provide cryptographic support for both TSF protection and message security purposes:

- Cryptomodules: Any one of: Entrust Authority Security Toolkit for Java 7.2 SP1; Java Cryptography Extension (JCE) compliant security providers (i.e. Java language crypto engine implementations)

TOE ActiveMatrix BusinessWorks components may rely on the following optional environment components:

- Directory Services[11]: To perform authentication for HTTP Basic Authentication or OASIS Web Services Security Authentication using the UsernameToken Profile. Any one of: Sun ONE Directory Server 5.1 with Service Pack 3, Sun ONE Directory Server 5.2, Microsoft Active Directory 2000, Microsoft Active Directory 2003, Microsoft Active Directory Application Mode (ADAM) 2003, Novell eDirectory 8.7.3, CA Directory Server
- Enterprise Applications: Optional, applications providing access to data and functionality in the environment.

[10] The configuration used for the evaluation testing effort utilized the Oracle 10g v2 Database and Microsoft SQLServer 2005.

[11] The configuration used for the evaluation testing effort utilized the Microsoft ActiveDirectory 2003 and Sun ONE Directory Server 6.3,

- Text Editor: Some configuration values must be set by modifing text-based configuration data during set-up to achieve the evaluated configuration (e.g., FIPS mode).

TOE TIBCO Administrator component is accessed by administrators using the following environment components:

- Web Browsers: Any one of:; Microsoft Internet Explorer 5.5; Mozilla Suite 1.7.1; Mozilla Firefox 1.5 and newer versions.

2.3.2 Logical Boundaries

This section summarizes the security functions:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- TSF Protection
- Cryptographic Support provided by the Environment

2.3.2.1 Security Audit

The TOE generates audit records for start-up and shutdown of the audit functions, as well as an unspecified level of audit[12]. The *TIBCO Administrator* application and *ActiveMatrix BusinessWorks engine* both generate audit records when security-relevant events occur. Log files are stored in administrator-configured locations of the environment. The *TIBCO Administrator* application provides the ability to specify a log file name, to specify search conditions (based on date and time of the event, and on type of event), and to view record details. The environment is relied on to provide a reliable time stamp, to protect the audit trail.

See the corresponding section in the TSS for more detailed information.

2.3.2.2 User Data Protection

The *TIBCO ActiveMatrix BusinessWorks* engine enforces security policies that are associated with resources by administrators. When a security policy is attached to a resource, the associated security policy is used for that process' corresponding incoming and outgoing messages[13]. The security policy may define transport characteristics, authentication characteristics, integrity characteristics, confidentiality characteristics, and timeout characteristics. The TOE is permissive by default with respect to message protection which means that in the evaluated configuration, if a security policy is not attached to a resource, no protection is provided. Therefore, in order to enforce the security functions a security policy must always be attached by an administrator to a resource before message transport, authentication, integrity, confidentiality, and timeout characteristics defined in the attached security policy are applied.

See the corresponding section in the TSS for more detailed information.

2.3.2.3 Identification and Authentication

The *TIBCO Administrator* application requires authorized administrators to logon using a username and password before it allows access to its interfaces. Authorized TIBCO administrators are uniquely identified and authenticated and associated with TIBCO administrative roles and TIBCO domains after being successfully authenticated. The ActiveMatrix BusinessWorks engine may, depending on business process activity or resource security policy configuration, require that incoming messages be authenticated to support the protection of messages.

[12] "Unspecified level of audit" refers to the Common Criteria terminology required for proper selection in the FAU_GEN.1 audit requirement (see Section 5.2.1.1). The actual set of audited events can be found in section 6.1.1.

[13] The term message is used in a generic sense to refer to any distinct communication unit appropriate for the protocol type being used. A message can be a single email, a single data request, a single remote function invocation, a single packet or a single session depending upon the protocol being considered.

See the corresponding section in the TSS for more detailed information.

2.3.2.4 Security Management

The *TIBCO Administrator* application component provides command-line utilities and a web based administrator console interfaces. These interfaces are used to manage TOE functions, including configuring security policies, deploying distributed applications, and administering distributed applications. The TOE provides administrative roles that correspond to permissions for items that display in the Security console component of the *TIBCO Administrator* application and that a command-line utility may access.

See the corresponding section in the TSS for more detailed information.

2.3.2.5 TSF Protection

Both the *TIBCO Administrator* application and ActiveMatrix BusinessWorks engine implement web servers. The web server implemented by the *TIBCO Administrator* application is used to provide an administrative console interface. The web server implemented by the ActiveMatrix BusinessWorks engine is used to provide a transport to send and receive messages. TOE web server instances are designed to ensure that TOE interfaces cannot be bypassed and to ensure that a security domain is provided for both administrative and calling application sessions. The TOE uses HTTPS[14] (provided by the Environment) to protect communication with its TIBCO Administrator application GUI. The TOE also uses HTTPS to protect communication between the TIBCO Administrator application and Runtime Agent. TOE application components otherwise rely on the Environment for protection.

The TOE also utilizes mechanisms that are provided by the cryptomodule, operating system, DBMS and LDAP server to protect various pieces of TOE configuration data.

See the corresponding section in the TSS for more detailed information.

2.3.2.6 Cryptographic Support provided by the Environment

The TOE does not contain a cryptomodule but it is packaged with one. In the evaluated configuration, the TOE is delivered to customers with the *Entrust Authority Security Toolkit for Java 7.2*. Authorized administrators can also configure the TOE to use third party cryptographic libraries that are compatible with the Java Cryptography Extension (JCE) standard. JCE defines a standardized Java language framework for implementing cryptographic algorithms and operations. The TOE uses the configured crypto module to perform cryptographic operations according to individual security policy settings. The TOE can perform the following types of cryptographic operations on SOAP messages:

- Certificate-Based Authentication – the ActiveMatrix BusinessWorks engine is used at the request of the TOE. The engine can verify the signature of a certificate and determine validity of a certificate path.
    - There is an administrator-configured root certificate provided by the environment stored in a file on the ActiveMatrix BusinessWorks engine machine and is imported or referenced by business processes.
- Message Signing – the ActiveMatrix BusinessWorks engine is used at the request of the TOE to sign, verify, or sign and verify inbound and/or outbound messages
    - There is an RSA (or DSA) certificate with a variable bit key pair (RSA 512 or 1024 , 2048, or 4096-bit key pair) stored encrypted in a file on the ActiveMatrix BusinessWorks engine machine; it is provided by the environment and used by the environment cryptographic engine
    - There is an administrator-configured signing certificate (called the message signing certificate) provided by the environment (PKCS#10 message provided by the environment using the key pair and PKCS#7 certificate provided by the environment) stored in a file on the ActiveMatrix BusinessWorks engine machine
    - There is support for both SHA-1 and MD5[15] for creating signature

[14] While the product supports several protocols between the *TIBCO Administrator* application and the ActiveMatrix BusinessWorks engine, only HTTPS can be used by the TOE in the evaluated configuration.

[15] Administrators only use FIPS certified mechanisms in the evaluated configuration.

- Message Encrypting – the ActiveMatrix BusinessWorks engine is used at the request of the TOE to encrypt and decrypt inbound and/or outbound SOAP messages
    - There is an Triple DES 168-bit asymmetric key stored encrypted (using an administrator-provided password turned into a DES key) in a file on the ActiveMatrix BusinessWorks engine machine
    - There is an AES 128 or 256-bit asymmetric key stored encrypted (using an administrator-provided password turned into a DES key) in a file on the ActiveMatrix BusinessWorks engine machine

Only TIBCO administrative users with appropriate administrative permissions can modify the configuration of cryptographic operations on SOAP messages.

Within the Entrust toolkit, there are non-FIPS algorithms that are not used in the evaluated configuration, guidance documentation instructs administrators that only FIPS certified algorithms can be used by the TOE in an evaluated configuration. There is a global setting that configures the minimum strength of the ciphers. If the administrator configures it to be 256, then FIPS mode AES-256 is always used.

Because JDBC and LDAP communications utilize JRE services for cryptography, the JRE must be configured to use the Entrust toolkit[16] for communication between the TOE and a DBMS or an LDAP server.

2.4 TOE Documentation

TIBCO offers a series of documents that describe the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features. Refer to Section 6 for information about these and other documentation associated with the TOE.

[16] The Security Features Users Guide provides this instruction.

3. Security Environment

This section summarizes the threats addressed by the TOE and assumptions about the intended environment of the TOE. Note that while the identified threats are mitigated by the security functions implemented in the TOE, the overall assurance level (EAL 2 augmented with ALC_FLR.2) also serves as an indicator of whether the TOE would be suitable for a given environment.

3.1 Threats

T.ACCOUNTABILITY An administrator may not be held accountable for their actions.

T.MASQUERADE An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources.

T.MESSAGE_COMPROMISE An unauthorized external IT entity may inappropriately access or modify inbound or outbound messages by intercepting it while it is in transit across a network.

T.TSF_COMPROMISE An unauthorized external IT entity or malicious user may inappropriately access TSF data by intercepting it while it is in transit across a network.

3.2 Assumptions

A.LOCATE The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NO_EVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.TIME The environment will provide a reliable time stamp for use by the TOE.

A.ENV_ACCESS Access controls provided by the operating system in the environment will be used to ensure that commands to setup the TOE are used only by users associated with establishing the operational TOE.

A.EDIT A tool will be provided by the environment to allow administrators to modify TOE text-based configuration data during set-up to achieve the evaluated configuration (e.g., FIPS mode).

A.LDAP An LDAP server will be provided by the environment to support identification and authentication of administrative and user accounts if the TOE is configured to utilize such a server.

4. Security Objectives

This section summarizes the security objectives for the TOE and its environment.

4.1 Security Objectives for the TOE

O.ADMIN_AUTHENTICATION The TOE will verify the claimed identity of administrators.

O.ADMIN_IDENTIFICATION The TOE will uniquely identify administrators.

O.ADMIN_ROLE The TOE will provide authorized administrator roles to isolate administrative actions.

O.AUDIT_GENERATION The TOE will provide the capability to create audit records of security relevant events associated with administrators.

O.AUDIT_REVIEW The TOE will provide the capability to review audit information.

O.MANAGE The TOE will allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

O.MESSAGE_PROTECTION The TOE will process incoming and outgoing messages according to the security characteristics associated with the corresponding communication pathway.

4.2 Security Objectives for the Environment

OE.TIME The environment will provide reliable time stamps for use by the TOE.

OE.LOCATE The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

OE.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

OE.NO_EVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

OE.AUDIT_PROTECTION The environment will provide the capability to protect audit information.

OE.MESSAGE_PROTECTION The environment will provide cryptographic services at the request of the TOE to support TOE processing of incoming and outgoing messages.

OE.TOE_PROTECTION The environment will protect the TOE and its assets from interference or tampering.

OE.EDIT The environment will provide a text editor to allow configuration values to be set by modifying text-based configuration.

OE.OPTIONAL_LDAP The environment will provide an LDAP server to correctly perform identification and authentication if the TOE is configured to use such a server.

5. IT Security Requirements

This section defines the security functional requirements for the TOE as well as the Security Assurance Requirements against which the TOE has been evaluated. Requirements have been copied from version 3.1 of the applicable Common Criteria documents.

5.1 Extended Component Definition

There are no extended component definitions in the ST.

5.2 TOE Security Functional Requirements

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit data generation
	FAU_GEN.2: User identity association
	FAU_SAR.1: Audit review
	FAU_SAR.3: Selectable audit review
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_SOS.1: Verification of Secrets
	FIA_UAU.1: Timing of authentication
	FIA_UID.1: Timing of identification
FMT: Security management	FMT_MOF.1: Management of security functions behavior
	FMT_MSA.1: Management of security attributes
	FMT_MSA.3: Static attribute initialization
	FMT_MTD.1a: Management of TSF data
	FMT_MTD.1b: Management of TSF data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles

Table 1 TOE Security Functional Components

5.2.1 Security Audit (FAU)

5.2.1.1 Audit Data Generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [***not specified***] level of audit; and c) [**the additional events listed in the table below]**

Requirement	Auditable Event
FAU_GEN.1	Start-up and shutdown of the audit functions (more specifically, of the TOE)
FAU_GEN.2	No corresponding auditable event
FAU_SAR.1	No corresponding auditable event
FAU_SAR.3	No corresponding auditable event
FIA_ATD.1	No corresponding auditable event
FIA_UAU.1	Use of the authentication mechanism (success or failure)
FIA_UID.1	No corresponding auditable event

Requirement	Auditable Event
FMT_MOF.1	Changes to the TOE administration domain settings
FMT_MSA.1	Deployment of a business process
FMT_MTD.1a	Changes to administrator security attributes
FMT_MTD.1b	Changes to TOE user security attributes
FMT_SMF.1	No corresponding auditable event
FMT_SMR.1	Modifications to the group of users that are part of a role

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**none**].

5.2.1.2 User Identity Association (FAU_GEN.2)

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.2.1.3 Audit Review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide **[domain administrator]** with the capability to read **[all audit information]** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.2.1.4 Selectable Audit Review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to apply [**searches**] of audit data based on [**date and time of the event, and type of event**].

5.2.2 User data protection (FDP)

5.2.2.1 Subset Information Flow Control (FDP_IFC.1)

FDP_IFC.1.1 The TSF shall enforce the [**Security Characteristics Policy**] on [

Subjects:	**external IT entities that send and receive information through the TOE and controlled enterprise applications that send and receive information through the TOE,**
Information:	**messages carried over a communication pathway, and**
Operations:	**pass messages on a communication pathway**].

5.2.2.2 Simple Security Attributes (FDP_IFF.1)

FDP_IFF.1.1 The TSF shall enforce the [**Security Characteristics Policy**] based on the following types of subject and information security attributes: [

Subject security attributes:	**transport layer endpoint addresses,**
Information:	**messages carried over a communication pathway, and**
Information security attributes:	**Transport layer protocol** **Transport layer endpoint addresses** **Authentication characteristics of messages** **Integrity characteristics of messages** **Confidentiality characteristics of messages** **Timeout characteristics of messages**

].

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: [

1. **For all messages, if SSL is configured as a required transport layer protocol for the communication pathway, the incoming and outgoing messages on the communication pathway must use SSL as the transport layer protocol, otherwise any transport layer protocol may be used.**
2. **For SOAP messages on a SOAP communication pathway, the characteristics of a message must match the administrator defined characteristics for SOAP messages.**
   - **Authentication characteristics of the message define whether users must be authenticated to send messages.**
   - **Integrity characteristics define whether messages must be validated with a signature to ensure the message has not been altered since its creation.**
   - **Confidentiality characteristics define whether messages must be encrypted.**
   - **Timeout characteristics define whether messages must expire after a certain time.**
3. **For HTTP messages on a HTTP communication pathway, an information flow is allowed if the transport layer endpoint addresses of the flow satisfies the following conditions.**
   - **The transport layer endpoint addresses are identified in the administrator specified list of allowed IP addresses, and**
   - **The transport layer endpoint addresses are NOT identified in the administrator specified list of restricted IP addresses.**].

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

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [**none**].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**for HTTP messages an information flow is denied if the transport layer endpoint addresses of the flow are identified in the administrator specified list of restricted IP addresses none**].

Application Note: A communication pathway is configured by an administrator with characteristics that are required for all messages that utilize the pathway.

5.2.3 Identification and Authentication (FIA)

5.2.3.1 User Attribute Definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

- **user identity**
- **password**
- **role assignment**].

5.2.3.2 Verification of Secrets (FIA_SOS.1)

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [

For TOE defined accounts:

- **a minimum length,**
- **contain a specified number of different character classes (i.e., upper, lower, numeric, special character),**
- **contain a specified set of character classes, or**
- **exclude the current password, user identity or space characters**].

5.2.3.3 Timing of Authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow [**no administrative actions**] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.3.4 Timing of Identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow [**no administrative actions**] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.2.4 Security Management (FMT)

5.2.4.1 Management of Security Functions Behavior (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to [***modify the behavior of***] the functions [**add or remove users, machines, and services to or from an administration domain**] to [**domain administrators**].

5.2.4.2 Management of Security Attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the [**Security Characteristics Policy**] to restrict the ability to [***[deploy]***] the security attributes [**transport layer protocol, authentication characteristics, confidentiality characteristics, integrity characteristics, and timeout characteristics**] to [**domain administrators**].

5.2.4.3 Static Attribute Initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the [**Security Characteristics Policy**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.

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

5.2.4.4 Management of TSF Data (FMT_MTD.1a)

FMT_MTD.1a.1 The TSF shall restrict the ability to [***query, modify, delete, clear***] the [**user security attributes defined in FIA_ATD.1a**] to [**domain administrators**].

5.2.4.5 Management of TSF Data (FMT_MTD.1b)

FMT_MTD.1b.1 The TSF shall restrict the ability to [***modify***] ~~the~~[17] [**their own authentication data**] to [**domain administrators and TOE users**].

5.2.4.6 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

- **read audit information from the audit records**
- **perform searches of audit data**
- **deploy a business process definition**
- **add or remove users, machines, and services to or from an administration domain**
- **query, modify, delete, clear user security attributes]**

5.2.4.7 Security Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [

- **developer,**
- **domain administrator, and**
- **TOE user**].

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

[17] Text from the original CC requirement (i.e., “the”) was deleted for grammatical presentation.

5.3 TOE Security Assurance Requirements

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

EAL 2 augmented with ALC_FLR.2 was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate degree of independently assured security. ALC_FLR.2 was selected to exceed EAL2 assurance objectives in order to ensure that identified flaws are addressed. The TOE is targeted at a relatively benign environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have little attack potential. As such, EAL 2 augmented with ALC_FLR.2 is appropriate to provide the assurance necessary to counter the limited potential for attack.

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.2: Security-enforcing functional specification
	ADV_TDS.1: Basic design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.2: Use of a CM system
	ALC_CMS.2: Parts of the TOE CM coverage
	ALC_DEL.1: Delivery procedures
	ALC_FLR.2: Flaw reporting procedures
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis
ASE: Security Target evaluation[18]	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification

Table 2 EAL 2 augmented with ALC_FLR.2 Assurance Components

5.3.1 Development (ADV)

5.3.1.1 Security Architecture Description (ADV_ARC.1)

ADV_ARC.1.1d The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2d The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3d The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1c The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2c The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3c The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4c The security architecture description shall demonstrate that the TSF protects itself from tampering.

[18] The ASE requirements are not copied into this document as they are intended to define the requirements upon which this document is evaluated. Assurance requirements in this document are those used to evaluate the product.

ADV_ARC.1.5c The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

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

5.3.1.2 Security-Enforcing functional Specification (ADV_FSP.2)

ADV_FSP.2.1d The developer shall provide a functional specification.

ADV_FSP.2.2d The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.2.1c The functional specification shall completely represent the TSF.

ADV_FSP.2.2c The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3c The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4c For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5c For SFR-enforcing TSFIs, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6c The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.3.1.3 Basic Design (ADV_TDS.1)

ADV_TDS.1.1d The developer shall provide the design of the TOE.

ADV_TDS.1.2d The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.1.1c The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2c The design shall identify all subsystems of the TSF.

ADV_TDS.1.3c The design shall describe the behavior of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4c The design shall summarize the SFR-enforcing behavior of the SFR-enforcing subsystems.

ADV_TDS.1.5c The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6c The mapping shall demonstrate that all behavior described in the TOE design is mapped to the TSFIs that invoke it.

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

ADV_TDS.1.2e The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.3.2 Guidance Documents (AGD)

5.3.2.1 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1.1d The developer shall provide operational user guidance.

AGD_OPE.1.1c The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2c The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3c The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4c The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5c The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6c The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7c The operational user guidance shall be clear and reasonable.

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

5.3.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1d The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1c The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

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

AGD_PRE.1.2e The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.3.3 Life-Cycle Support (ALC)

5.3.3.1 Use of a CM System (ALC_CMC.2)

ALC_CMC.2.1d The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.2.2d The developer shall provide the CM documentation.

ALC_CMC.2.1c The TOE shall be labeled with its unique reference.

ALC_CMC.2.2c The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3c The CM system shall uniquely identify all configuration items.

ALC_CMC.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.2 Parts of the TOE CM Coverage (ALC_CMS.2)

ALC_CMS.2.1d The developer shall provide a configuration list for the TOE.

ALC_CMS.2.1c The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2c The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3c For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

ALC_CMS.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.3 Delivery Procedures (ALC_DEL.1)

ALC_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2d The developer shall use the delivery procedures.

ALC_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

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

5.3.3.4 Flaw Reporting Procedures (ALC_FLR.2)

ALC_FLR.2.1d The developer shall document flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2d The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.1c The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2c The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3c The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4c The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5c The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6c The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

ALC_FLR.2.7c The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.2.8c The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

ALC_FLR.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Tests (ATE)

5.3.4.1 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 in the test documentation and the TSFIs 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.

5.3.4.2 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, expected test results and actual test results.

ATE_FUN.1.2c The test plans shall identify the tests to be performed and describe the scenarios for performing each test.

ATE_FUN.1.3c The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4c The actual test results shall be consistent with the expected test results.

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

5.3.4.3 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 execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3e The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.3.5 Vulnerability Assessment (AVA)

5.3.5.1 Vulnerability Analysis (AVA_VAN.2)

AVA_VAN.2.1d The developer shall provide the TOE for testing.

AVA_VAN.2.1c The TOE shall be suitable for testing.

AVA_VAN.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.2.2e The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3e The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4e The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 Security audit

The TOE generates audit records for start-up and shutdown of the TIBCO Administrator application and of the ActiveMatrix BusinessWorks engine. Since the audit functionality cannot be stopped without also stopping the TOE, these audit records indicate the start-up and shutdown of the audit functions. All audit records include date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. The auditable events include:

FAU_GEN.1	Start-up and shutdown of the audit functions (more specifically, of the TOE)
FAU_GEN.2	No corresponding auditable event
FAU_SAR.1	No corresponding auditable event
FAU_SAR.3	No corresponding auditable event
FDP_IFC.1	Enabling or disabling application security policy
FDP_IFF.1	Enabling or disabling application security policy
FIA_ATD.1	No corresponding auditable event
FIA_UAU.1	Use of the authentication mechanism (success or failure)
FIA_UID.1	No corresponding auditable event
FMT_MOF.1	Changes to the TOE administration domain settings
FMT_MSA.1	Changes to the TOE message protection settings
FMT_MSA.3	Changes to the TOE message protection settings
FMT_MTD.1a	Changes to administrator security attributes
FMT_MTD.1b	Changes to TOE user security attributes
FMT_SMF.1	No corresponding auditable event
FMT_SMR.1	Modifications to the group of users that are part of a role

The TIBCO Administrator application and ActiveMatrix BusinessWorks engine both generate audit records when security-relevant events occur. TIBCO Administrator generates audit records related to management activities and writes them to one log file. The TIBCO ActiveMatrix BusinessWorks engine generates audit records related to application security policy changes and writes them to another log file. Log files are stored in administrator-configured[19] locations in the environment as follows:

- TIBCO Administrator log files are stored in the directory:

  <TIBCO_HOME>/Administrator/domain/<domain name>/logs

- TIBCO ActiveMatrix BusinessWorks Engine log files are stored in the directory:

  <TIBCO_HOME>/tra/domain/<domain name>/application/logs/<deployment name>

Audit records that are created by the TIBCO Administrator application always indicate the administrator that caused the event. Records that are generated by the ActiveMatrix BusinessWorks engine can occur on behalf of administrators (in which case an administrator identity is included in the record), on behalf of unauthenticated users (in which case no identity is available) or on behalf of authenticated users (in which case the identity is included in the audit record).

Audit records are initially created by the TIBCO Administrator application and ActiveMatrix BusinessWorks engine using event data generated by the applicable server. TIBCO Administrator and ActiveMatrix BusinessWorks engine then call TIBCO Runtime Agent to write the audit records to the applicable audit trail. The time stamp is added to

[19] *Administrator-configured fields in log file path names are identified using angle brackets ('<' and '>').*

the record by TIBCO Runtime Agent after obtaining it from the operating system before the record is written to the log files. The TIBCO Administrator application includes a GUI that can be used to read from either the TIBCO Administrator application or ActiveMatrix BusinessWorks engine log files. The GUI provides the ability to specify a log file name, to specify search conditions (based on date and time of the event, and on type of event), and to view record details.

There are certain auditable events that cause audit records to be generated by both TIBCO Administrator and ActiveMatrix BusinessWorks engine, such as deploying an EAR file. Deploying an EAR file consists of installing, running, and enabling security policies for a distributed application created using TIBCO Designer. Audit records can be correlated in these instances using a combination of unique log file name, unique distributed application name, and record time stamps. The TIBCO Administrator application and ActiveMatrix BusinessWorks engine records in these instances within each audit record in both logs (in addition to the date and time of the event, type of event, subject identity, and the outcome of the event) the unique distributed application name. Log files for a given administration domain can be retrieved and then records can be examined using event time and distributed application name. An “administration domain” is a collection of users, machines, and services that is initially created during initial TOE installation and configuration. Each domain is managed by a TIBCO Administrator application, which can then be used by administrators to manage TOE functions.

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

- FAU_GEN.1, FAU_GEN.2: The TOE generates audit records for start-up and shutdown of the audit functions, as well as an unspecified level of audit.
- FAU_GEN.2: The TOE indicates the administrator or authenticated user responsible for audited events.
- FAU_SAR.1, FAU_SAR.3: The TOE provides the ability to read from and search through log files generated by both TIBCO Administrator and ActiveMatrix BusinessWorks engines.

6.1.2 User data Protection

The TOE provides the ability to protect incoming and outgoing messages[20] by associating security characteristics with resources (also known as communication pathways[21]). The set of communication pathways supported by the TOE in its evaluated configuration include:

- File resources – the TOE can be used to read, write, delete, or create files
- FTP resources – the TOE can be used to issue FTP commands
- HTTP resources – the TOE can be used to send and receive HTTP requests
- JDBC resources – the TOE can be used to query, update, or call stored procedures in a database
- JMS resources – the TOE can be used to send and receive JMS messages
- Mail resources – the TOE can be used to send and receive email messages
- Rendezvous resources – the TOE can be used to send and receive TIBCO Rendezvous messages
- SOAP resources – the TOE can be used to send and receive SOAP messages
- JAAS resources – the TOE can be used to send and receive messages supporting the Java Authentication and Authorization Service (JAAS) login
- TCP/IP resources – the TOE can be used to send and receive data from servers using TCP/IP commands

The TOE is permissive by default with respect to message protection on a given communication pathway. That is, security characteristics must be attached to a communication pathway before message transport, authentication, integrity, confidentiality, and timeout characteristics for the communication pathway are applied to incoming or outgoing messages.

[20] Note that while some protocols define the data and control information that is passed by the protocol as commands, messages or operations, this security target uses the generic term *message*.

[21] The *TIBCO Designer* application represents communication pathways as resources in a palette.

Administrators attach a security policy to a communication pathway. When messages are sent or received using that communication pathway, the associated security policy is used for the application's corresponding outgoing or incoming messages. Administrators define security policies using an application's Security Policy Association shared configuration. Administrators can define one policy to share among all of a business process' web services, or administrators can define multiple policies to use on a per-communication pathway basis. The Security Policy Association shared configuration allows administrators to associate a security policy with a web service. A security policy can either be associated with individual communication pathways or it can be associated with each operation in a business process activity. Administrators must create a Security Policy Association for each communication pathway or operation that uses a communication pathway that is to be controlled. When administrators associate a policy with an operation, the policy applies to all inbound and outbound messages for the operation. When administrators associate a policy with a specific communication pathway, the appropriate security policies are applied to the messages sent or received using the communication pathway. For example, a SOAP Event Source can only receive messages, therefore a security policy can only be applied to incoming messages; a SOAP Reply, which is paired with a SOAP Event Source, may only have a policy applied to its outgoing messages. A SOAP Request Reply activity can send and receive messages, and it may also receive a fault message. Therefore, an administrator can associate a security policy for the inbound, outbound and fault messages.

Security Policy Association shared configuration are not referenced by communication pathway in process definitions. Therefore, they are not automatically included in EAR files. Administrators must manually add Security Policy Association to the Shared Archive within an EAR for the associations to apply for a deployed application. The security policy for either incoming or outgoing messages may include any combination of authentication characteristics, integrity characteristics, confidentiality characteristics, and timeout characteristics.

The Security Characteristics Policy is composed of the following policies:

- Transport Security Policy
- Authentication Security Policy
- Integrity Security Policy
- Confidentiality security Policy
- Timeout Security Policy

Transport Security Policy characteristics determine whether messages must be carried over the SSL protocol. Transport security policy characteristics specify the characteristics of the transport protocol used by the message. Inbound and outbound messages are rejected if the transport protocol of the message does not match the Transport security policy characteristics. Transport security policy characteristics apply to all types of messages except TCP and file resources (i.e., all communication pathway types shown above).

In addition to the possible required use of the SSL protocol, HTTP messages can be filtered based upon the IP address of the transport layer source endpoints (i.e., source IP addresses). Administrators may specify a set of allowed IP addresses and/or a set of restricted IP addresses. HTTP messages with source IP addresses matching an address in the set of allowed IP addresses are permitted to flow between subjects. HTTP messages with source or destination IP addresses matching an address in the set of restricted IP addresses are not permitted to flow between subjects. If an address appears in both the allowed and restricted list, the address is considered restricted and thus the message is not permitted to flow between subjects.

Authentication Security Policy characteristics determine whether messages must be authenticated. Authentication security policy characteristics specify the characteristics for authenticating to the SOAP message server. Inbound messages can be authenticated against a list of trusted certificates or identities configured as TOE users in TIBCO Administrator and optionally, to a Directory Server if the domain is configured for it. A local user identity (one configured through TIBCO Administrator) has precedence over identities in LDAP. Outbound messages can specify the identity to use to authenticate to an external SOAP server. Authentication security policy characteristics apply to SOAP messages and to HTTP Transport activities.

Authentication Security Policy options for *inbound* messages include:

- Supported Security Tokens option – Specifies the security tokens to allow in inbound messages. One or more of the following supported types can be selected: X.509 Token, UsernamePassword Token

- Trusted Certificates Folder – Specifies the folder containing the trusted certificates for X.509 authentication.

Authentication security policy options for *outbound* messages include:

- Security Token – Specifies the type of security tokens to allow to be placed in outbound messages. One of the following supported types can be selected: X.509 Token, UsernamePassword Token
- X.509 Identity – When X.509 Token is selected in the Security Token field, this field specifies the Identity resource containing the X.509 compliant certificate file.
- Username Password Identity – When UsernamePassword Token is selected in the Security Token field, this specifies the Identity resource that contains the username and password.
- Password Type – Specifies whether to use clear text or to send the password as a digest.

Integrity Security Policy characteristics determine whether messages must be validated with a digital signature to ensure the message has not been altered since its creation. Integrity security policy characteristics specify the characteristics of the signatures attached to messages. Administrators are instructed by guidance documentation to deploy business processes that use only FIPS certified mechanisms in the evaluated configuration. (Note: the algorithms mentioned in the “integrity” and “confidentiality” security policy characteristics discussions that follow identify all supported mechanisms in the product, not just the FIPS certified mechanisms.) Signatures can be used to ensure that messages are not altered after creation. The integrity of inbound messages can be checked against the trusted root certificates and the public certificate. Outbound messages can specify the certificate to use to sign the outgoing message. Integrity security policy characteristics apply only to SOAP messages.

Integrity Security Policy options for *inbound* messages include:

- Supported Signature Methods – Algorithm used to check the signatures of incoming messages. One or more of the following can be selected: SHA1, MD5.
- Supported Security Tokens – Specifies the security token to use for the signature. One or more of the following can be selected: X.509 Token, UsernameToken
- Trusted Certificates Folder – Specifies the folder containing the trusted certificates for signature verification. Note: The certificates in the trusted folder are only necessary in the case when the authenticating user is same as the user that signed the message. In this case, the message contains the public key, so the receiver must verify against the trusted certificate. However, if the authenticating user is not same as the user that signed the message, the user must define a subject key identity that holds the public key.
- Subject Key Identity – No Specifies an Identity resource containing a keystore that holds an X.509 certificate. The inbound message must match the subject key contained in the certificate.

Integrity Security Ppolicy options for *outbound* messages include:

- Signature Method – Algorithm used to create signatures for outgoing messages. One or more of the following can be selected: SHA-1, MD-5
- Security Token – Specifies the type of security token to use for the signature. One or more of the following can be selected: X.509 Token, UsernameToken
- Username Password Identity – When UsernameToken is selected in the Security Token field, this specifies the Identity resource that contains the username and password.
- Password Type – Specifies whether you wish to use clear text or digest passwords.
- X.509 Identity – When X.509 Token is selected in the Security Token field, this field specifies the Identity resource containing the X.509 compliant identity file.
- Certificate Alias –When the Identity resource specified in the X.509 Identity field is a Java Key Store (JKS) formatted keystore, specify the certificate alias in this field to identify the private/public key pair.

Confidentiality Security Policy characteristics determine whether messages should be encrypted or decrypted. Confidentiality Security Policy characteristics specify the encryption characteristics of messages. Inbound messages can be decrypted based on algorithms specified in the message security header and the defined private key. Outbound messages can be encrypted based on algorithms stored in a public key. Confidentiality security policy characteristics apply only to SOAP messages.

Confidentiality Security Policy options for *inbound* messages include:

- Supported Encryption Algorithm – Symmetric key algorithm used to decrypt incoming messages. You can select one or more of the following: 3DES, AES-128, AES-256
- Private key Identifier Type –Specifies whether the private key is one of the following: X.509 Token
- X.509 Identity – When X.509 Token is selected in the Private Key Identifier Type field, this field specifies the Identity resource containing the X.509 compliant private key file to use to decrypt the message.

Confidentiality Security Policy options for *outbound* messages include:

- Encryption Algorithm – Algorithm used to encrypt outgoing messages. One of the following can be selected: 3DES, AES-128, AES-256
- Public Key –Identity resource containing the X.509 compliant public key file to use to encrypt the message.

Timeout Security Policy characteristics determine whether messages should expire after a certain time. Timeout security policy characteristics specify the characteristics of message timeout. Inbound messages can be rejected after the specified number of seconds. Outbound messages can be set to expire after the specified number of seconds. In all cases, expired messages are ignored by the TOE. Timeout security policy characteristics apply only to SOAP messages.

Timeout Security Policy options for *inbound* messages include:

- Reject After (seconds) – The creation time of incoming messages is compared to the time the message was received. If the difference in time is greater than the number of seconds specified in this field, the message is rejected.

Timeout Security Policy options for *outbound* messages include:

- Expire In (seconds) – Outgoing messages and error messages will expire after the specified number of seconds.

The User Data Protection function is designed to satisfy the following security functional requirements:

- FDP_IFC.1: The TOE provides the ability to associate a security policy (that defines transport, authentication, confidentiality, integrity and timeout characteristics) with communication pathway.
- FDP_IFF.1: The TOE provides the ability to associate security policy characteristics with communication pathway types (i.e., types of communication pathways).

6.1.3 Identification and Authentication

The TOE defines users in terms of the following:

- User Identity,
- Password, and
- Role Assignment.

The TOE requires that administrative users log into the *TIBCO Administration* application component using a valid username and password. The TOE implements its own username/password mechanism which uses password composition rules including minimum password length and complexity rules[22]. Optionally, the TOE can be configured to use an LDAP server as the means for the identification and authentication of administrative and user accounts. When queried by the TOE, the LDAP server is expected to take the user credentials (i.e., username and

[22] The evaluated configuration requires the most restrictive password settings.

password) and determine their validity. The TOE then accepts or rejects the authentication material based upon the response from the LDAP server.

The following are the complexity rules that can be specified by an administrator and enforced by the TOE for accounts created within the TOE[23]:

- The number of different character classes (i.e. Numbers, Special Characters, Upper Case, Lower Case) that must be used in the password.
- Whether the password is allowed to contain the current password
- Whether the password is allowed to contain the user identity
- Whether the password is allowed to contain spaces
- Whether the password must contain numbers, special characters, upper case and/or lower case characters.

After an administrator has been successfully authenticated, the administrator has access to TOE interfaces that correspond to the permissions corresponding to the role that the administrator has been assigned. The TOE provides administrative roles that correspond to permissions for items that display in the Security console component of the TIB*CO Administrator* application.

When the *TIBCO Administration* application is installed, a domain name, and username/password pair is provided. That account becomes the domain administrator for the specified domain. The domain administrator account is used to create other accounts and assign permissions within the domain. All accounts exist only within the context of a domain.

After installation of the *TIBCO Administration* application, additional named domains can be created. The creation of a new domain is always associated with the specification of a username/password pair. The specified username becomes the domain administrator for the named domain. Domains are created using a Domain Utility in *TIBCO Runtime Agent*. Anyone with sufficient permission in the environment to execute the Domain Utility can create a new domain and define the domain administrator for that domain.

Without identification or authentication by the TOE, the TIBCO Designer application can be used to create business process definitions and TIBCO Runtime Agent can be used to create new domains. Business process definitions do not affect a running TOE until such time as an authenticated domain administrator deploys the business process.

Administrators can only log into TOE instances belonging to the same administration domain that they belong to. An "administration domain" is a collection of users, machines, and services that is initially created during initial TOE installation and configuration[24]. Each domain is managed by an administration server, which can be used by administrators to manage TOE functions.

Authenticated TOE users can login using the *TIBCO Administrator* application, however, the functionality provided to such users is very limited (i.e., they can change their own password).

The TIBCO Administrator application includes an integrated web server component for HTTPS communications. The TIBCO Administrator application runs as a single process. Use of HTTPS communications ensures that TOE interfaces to operations and communication pathways that the ActiveMatrix BusinessWorks engine controls cannot be bypassed and that separate security domains are created and maintained for individual users after successful logon.

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

- FIA_ATD.1: The TOE defines users in terms of user identity, password, role assignment, and administration domain assignment.
- FIA_UAU.1: While the TOE may authenticate messages depending on security policy settings, the TOE only provides logon services to administrative type users.

[23] While the TOE can be configured to accept LDAP accounts, the LDAP server is responsible for controls on the passwords of LDAP accounts.

[24] The *TIBCO Runtime Agent* domain utility can also create a new domain.

- FIA_UID.1: The TOE offers no TSF-mediated administrative functions until the user is identified.
- FIA_SOS.1: The TOE allows the administrator to specify complexity rules that are enforced by the TOE on all authentication attempts using TOE defined accounts (i.e., administrative logon and message authentication).

6.1.4 Security Management

Developers use the TIBCO Designer application to develop and test distributed applications. Any user with access to the machine on which this application is installed can access the application to create EAR files. However, a domain administrator must logon to the TIBCO Administrator application to deploy an EAR file. That is, TOE administrative permission is required in order to use TIBCO Administrator to deploy an EAR file to an instance of an ActiveMatrix BusinessWorks engine and to subsequently manage it.

One instance of the TOE contains at least one business process. When multiple business processes exist within a single instance of the TOE, each is considered its own domain. Administrative authority for each domain can be assigned to different domain administrators[25]. A domain administrator has “read”, “write” and “administer” permissions to all resources in the administration domain without explicitly having been granted those permissions. This allows the domain administrator to:

- Manage all parts of domain,
- Add a machine to a domain, and
- Create additional users, remove users, reset another user’s password.

The domain administrator user can assign ”administer” access to another user by adding them to the list of domain administrators for the domain managed by the administrator.

TOE user accounts are created by a domain administrator. A TOE user account has a single capability which allows them to change their own password. This capability is granted through read-only permission to a folder that contains no other objects. Thus, a TOE user is allowed to ‘read’ the contents of an empty folder using the TIBCO Administrator application and as a result of having the ability to login to the TIBCO Administrator application the TOE user can change their own password. Such limited accounts are used when authentication characteristics are required for SOAP messages on a communication pathway.

The TIBCO Administrator application provides a mechanism to gather accounts into an easily identified collection referred to as a ‘role’. That ‘role’ can then be used when assigning the permissions associated with an object. This is effectively a grouping mechanism to simplify the management of permissions.

The TIBCO Administrator application provides a web-based administrator console and utilities/commands (e.g., domain utility, Appmanage) that can be used to deploy and manage business processes running in the ActiveMatrix BusinessWorks engine. These administrator tools provide the following interfaces:

- user management interfaces – these interfaces allow creating administrative users and roles (i.e., groups of users) and assign them access rights to communication pathways available in the administration domain.
- resource management interfaces – these interfaces include getting information about installed TOE application components on each domain machine, viewing the operational status of each within the domain.
- application management interfaces – these interfaces allows uploading an application’s Enterprise Archive (EAR) file and optionally change options and global variables that were set for the application when it was configured. These interfaces also can be used to deploy the application and start (or stop) it.

The capabilities available through the commands and utilities that are not web-based implement a subset of each of the above types of TOE management functions. Administrators can use the commands to create for example Windows operating system batch file scripts to automate the starting of a deployed distributed application.

The above-listed types of administrative interfaces can be used to perform the following security-related management functions:

[25] TIBCO documentation uses domain administrator and super user interchangeably.

- Read and search audit data
- Modify the behavior of message protection functions, by:
- Deploying a business process definition[26]
- Allow or disallow the use of an authentication server
- Manage administration domains, including:
- Add or remove users, machines, and services to or from an administration domain
- Manage user security attributes, including:
- Query, modify, delete, clear user identity, password, role assignment, and administration domain assignment

The TIBCO Administrator application is used by domain administrators and TOE users to change their own passwords. A TOE user is granted minimal use of the TIBCO Administrator application such that they can only modify their own password.

The TIBCO Administrator application interacts with an ActiveMatrix BusinessWorks engine using instances of TIBCO Runtime Agent. If the TIBCO Administrator application is not running on the same machine as ActiveMatrix BusinessWorks for example, there is an instance of Runtime Agent on the machine that is running the TIBCO Administrator application and an instance of Runtime Agent on the machine that is running the ActiveMatrix BusinessWorks engine.

By default the security characteristics for communication pathways to a ActiveMatrix BusinessWorks engine are not defined. A developer must assign security characteristics to communication pathways in a business process and the domain administrator must deploy the business process in order for those pathways to be protected.

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

- FMT_MSA.1: Domain administrators can deploy a business process and its corresponding message protection functions. Cryptographic services provided by the environment are configured using TOE message protection security characteristics.
- FMT_MSA.3: Security characteristics on communication pathways must be stated by developers (in an EAR file) and deployed by domain administrators in order for those pathways to be protected.
- FMT_MOF.1: Domain administrators manage administration domains.
- FMT_MTD.1a: Domain administrators manage accounts within the domain.
- FMT_MTD.1b: Administrators and TOE users can change their own passwords.
- FMT_SMF.1: The TOE provides administrative interfaces to review audit data, modify the behavior of message protection functions, manage administration domains, and manage user security attributes.
- FMT_SMR.1: The TOE defines three types of users: developers, domain administrators and TOE users. Developers are responsible for creating business processes. Domain administrators and TOE users have accounts defined to access the TIBCO Administrator application (and possibly the ActiveMatrix BusinessWorks engine) and are distinguished by their permission on items that display in the Security console component of the TIBCO Administrator application.

6.1.5 TSF Protection

The TOE is designed to operate in domains of execution provided by the underlying operating system environment and is in this sense reliant on the environment for a secure domain in which to operate. TIBCO Administrator maintains its domain in a manner that separates threads acting on behalf of administrators, from its own threads. TIBCO ActiveMatrix BusinessWorks also maintains its domain in a manner that separates threads acting on behalf

[26] Security policies are changed by deploying a business process definition having the new security policies.

of calling applications separate from its own threads. Furthermore, both TIBCO Administrator and ActiveMatrix BusinessWorks engine manage threads so that they are kept distinct and separate from one another.

The interfaces offered by the TOE have all been carefully designed, implemented, and tested to ensure that they do not offer opportunities to tamper with or interfere with the operation of the security functions and also to ensure that they do not offer any access to protected resources that is not subject to the various security policies.

The TIBCO Administrator application GUI protects communication with a web browser using cryptographic support provided by the cryptomodule in the Environment as follows:

- There is a RSA (or DSA) certificate with a variable bit key pair (e.g. RSA 512 or 1024 or 2048 or 4096-bit key pair stored encrypted in a file on the ActiveMatrix BusinessWorks engine machine; it is provided by the Environment and used by the Environment cryptographic engine
- There is an administrator-configured SSL certificate (called the administrator application certificate) provided by the Environment (PKCS#10 message provided by the Environment using the key pair and PKCS#7 certificate provided by the Environment) stored in a file on the ActiveMatrix BusinessWorks engine machine
- SSL is provided by the cryptomodule in the Environment at the request of the TOE to support HTTPS communication with a web browser

All of the operating systems upon which the TOE executes are expected to provide an execution environment (in collaboration with the Java Runtime Environment) that protects the TOE from other running processes while allowing access to TOE data to be limited to the TOE. These operating systems must also provide files that must be protected using operating system access controls. These files contain configuration data required for use by TIBCO Administrator and TIBCO ActiveMatrix BusinessWorks. The TOE utilizes the Entrust toolkit to cause passwords that must be stored within these configuration files to be encrypted. (Refer to chapter 4 and 5 of the SFUG for details on the protection of these configuration files and the key used for encryption of passwords).

When (if) the TIBCO Administrator communicates with a DBMS or LDAP server (for the purposes of storing TOE data) it utilizes 3rd party libraries which invoke JRE services for cryptography, the Entrust toolkit is used in communication between the TOE and a DBMS or an LDAP server. The runtime agent communications protects communication between TOE components using cryptographic support provided by the cryptomodule in the Environment as follows:

- There is a RSA 1024-bit key pair stored encrypted in a file on the ActiveMatrix BusinessWorks engine machine; it is provided by the Environment and used by the Environment cryptographic engine
- There is an administrator-configured SSL certificate (called the runtime agent certificate) provided by the Environment (PKCS#10 message provided by the Environment using the key pair and PKCS#7 certificate provided by the Environment) stored in a file on the ActiveMatrix BusinessWorks engine machine
- SSL is provided by the cryptomodule in the Environment at the request of the TOE to support HTTPS communication between TOE components

The TOE utilizes protection mechanisms offered by the DBMS and LDAP servers to protect TOE data stored within the DBMS or LDAP server.

7. Protection Profile Claims

There is no Protection Profile claim in this Security Target Report.

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;
- 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.

	O. ADMIN_AUTHENTICATION	O. ADMIN_IDENTIFICATION	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_REVIEW	O.MANAGE	O.MESSAGE_PROTECTION	OE.AUDIT_PROTECTION	OE.MESSAGE_PROTECTION	OE.TIME	OE.TOE_PROTECTION	OE.LOCATE	OE.MANAGE	OE.NO_EVIL	OE.EDIT	OE.OPTIONAL_LDAP
T.ACCOUNTABILITY				X	X					X						
T.MASQERADE	X	X	X			X										
T.MESSAGE_COMPROMISE							X		X							
T.TSF_COMPROMISE								X			X					
A.LOCATE												X				
A.MANAGE													X			
A.NO_EVIL														X		
A.TIME										X						
A.ENV_ACCESS											X					
A.EDIT															X	
A.LDAP																X

Table 3 Environment to Objective Correspondence

8.1.1.1 T.ACCOUNTABILITY

An administrator may not be held accountable for their actions.

The O.AUDIT_GENERATION objective addresses this threat by generating audit records for security-relevant events to record administrator actions. The OE.TIME objective supports the O.AUDIT_GENERATION objective by providing time stamps for each record. The O.AUDIT_REVIEW objective supports the O.AUDIT_GENERATION objective by providing the ability to review generated records (which are stored in log files in the IT Environment).

8.1.1.2 T.MASQUERADE

An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources.

The O.MANAGE objective addresses this threat by restricting access to functions that can be used to manage the TOE and its security functions to authorized administrators. The O.ADMIN_ROLE objective supports the O.MANAGE objective by requiring the TOE provide authorized administrator roles to isolate administrative actions. The O.ADMIN_IDENTIFICATION and O.ADMIN_AUTHENTICATION objectives provide the ability to authenticate administrative users into authorized administrator roles. The O.MESSAGE_PROTECTION objective addresses this threat by providing the ability to associate security characteristics for authentication with a communication pathway, resulting in processing incoming and outgoing messages only for authorized users.

8.1.1.3 T.MESSAGE_COMPROMISE

An unauthorized external IT entity may inappropriately access or modify inbound or outbound messages by intercepting it while it is in transit across a network.

The O.MESSAGE_PROTECTION objective addresses this threat by providing the ability to associate security characteristics with a communication pathway, resulting in processing incoming and outgoing messages according to the defined security characteristics. The OE.MESSAGE_PROTECTION objective supports the O.MESSAGE_PROTECTION objective by providing a cryptomodule to perform cryptographic operations at the request of the TOE according to security policy configuration.

8.1.1.4 T.TSF_COMPROMISE

An unauthorized external IT entity or malicious user may inappropriately access TSF data by intercepting it while it is in transit across a network.

The OE.MESSAGE_PROTECTION objective supports the O.MESSAGE_PROTECTION objective by providing a cryptomodule to perform cryptographic operations at the request of the TOE according to security policy configuration. The OE.AUDIT_PROTECTION and OE.TOE_PROTECTION objectives further protect TSF data by protecting TOE audit logs from inappropriate access as well as protecting application components from logical interference or tampering.

8.1.1.5 A.LOCATE

The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

The OE.LOCATE addresses this assumption by insisting that the TOE be located within a controlled access facility.

8.1.1.6 A.MANAGE

There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

The OE.MANAGE addresses this assumption by insisting that the TOE be managed by competent individuals.

8.1.1.7 A.NO_EVIL

The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

The OE.NO_EVIL addresses this assumption by insisting that the TOE be managed by administrators that are not hostile, not willfully negligent, and not careless.

8.1.1.8 A.TIME

The environment will provide a reliable time stamp for use by the TOE.

The OE.TIME addresses this assumption by insisting that the environment provide reliable time stamps for use by the TOE.

8.1.1.9 A.ENV_ACCESS

Access controls provided by the operating system in the environment will be used to ensure that commands to setup the TOE are used only by users associated with establishing the operational TOE.

The OE.TOE_PROTECTION addresses this assumption by insisting that the environment not only physical protections but also protection by the operating system for use of TOE setup programs.

8.1.1.10 A.EDIT

A tool will be provided by the environment to allow administrators to modify TOE text-based configuration data during set-up to achieve the evaluated configuration (e.g., FIPS mode).

The OE.EDIT addresses this assumption by assuring that the environment provides a text editor that can be used to modifying text-based configuration.

8.1.1.11 A.LDAP

An LDAP server will be provided by the environment to correctly support identification and authentication of administrative and user accounts if the TOE is configured to utilize such a server.

The OE.OPTIONAL_LDAP objective addresses this assumption by assuring that the environment provides a correctly functioning LDAP server when the TOE is configured to use an LDAP server.

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 4 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. ADMIN_AUTHENTICATION	O. ADMIN_IDENTIFICATION	O.ADMIN_ROLE	O.AUDIT_GNEERATION	O.AUDIT_REVIEW	O.MANAGE	O.MESSAGE_PROTECTION
FAU_GEN.1				X			
FAU_GEN.2				X			
FAU_SAR.1					X		
FAU_SAR.3					X		
FDP_IFC.1							X
FDP_IFF.1							X
FIA_ATD.1		X					
FIA_SOS.1	X						
FIA_UAU.1	X						
FIA_UID.1		X					
FMT_MOF.1						X	
FMT_MSA.1						X	
FMT_MSA.3						X	
FMT_MTD.1a						X	
FMT_MTD.1b						X	
FMT_SMF.1						X	
FMT_SMR.1			X				

Table 4 Objective to Requirement Correspondence

8.2.1.1 O.ADMIN_AUTHENTICATION

The TOE will verify the claimed identity of administrators.

This TOE Security Objective is satisfied by ensuring that:

- FIA_UAU.1: While the TOE may authenticate messages depending on security policy settings, the TOE only provides logon services to administrative type users.
- FIA_SOS.1: The TOE can require users to select a sufficiently complex password.

8.2.1.2 O.ADMIN_IDENTIFICATION

The TOE will uniquely identify administrators.

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1: The TOE defines users in terms of user identity, password, role assignment, and administration domain assignment.
- FIA_UID.1: The TOE offers no TSF-mediated administrative functions until the user is identified.

8.2.1.3 O.ADMIN_ROLE

The TOE will provide authorized administrator roles to isolate administrative actions.

This TOE Security Objective is satisfied by ensuring that:

- FMT_SMR.1: The TOE provides administrative roles that correspond to permissions for items that display in the Security console component of the TIBCO Administrator application. Non-administrative users do not log into the TOE.

8.2.1.4 O.AUDIT_GENERATION

The TOE will provide the capability to create audit records of security relevant events associated with administrators.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: The TOE generates audit records for start-up and shutdown of the audit functions, as well as an unspecified level of audit.
- FAU_GEN.2: The TOE indicates the administrator or authenticated user responsible for audited events.

8.2.1.5 O.AUDIT_REVIEW

The TOE will provide the capability to review audit information.

This TOE Security Objective is satisfied by ensuring that:

- FAU_SAR.1, FAU_SAR.3: The TOE provides the ability to read from and search through log files generated by both the TIBCO Administrator application and ActiveMatrix BusinessWorks engine.

8.2.1.6 O.MANAGE

The TOE will allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

This TOE Security Objective is satisfied by ensuring that:

- FMT_MSA.1: Domain administrators can deploy a business process and its corresponding message protection functions. Cryptographic services provided by the IT Environment are configured using TOE message protection security characteristics.
- FMT_MSA.3: Security characteristics on communication pathways must be stated by developers (in an EAR file) and deployed by administrators in order for those pathways to be protected.
- FMT_MOF.1: Domain administrators manage administration domains.
- FMT_MTD.1a: Domain administrators manage administrator user accounts.
- FMT_MTD.1b: Administrators can change their own passwords.
- FMT_SMF.1: The TOE provides administrative interfaces to review audit data, modify the behavior of message protection functions, manage administration domains, and manage user security attributes.

8.2.1.7 O.MESSAGE_PROTECTION

The TOE will process incoming and outgoing messages according to the security characteristics associated with the corresponding communication pathway.

This TOE Security Objective is satisfied by ensuring that:

- FDP_IFC.1: The TOE provides the ability to enforce the defined security characteristics of communication pathway.
- FDP_IFF.1: The TOE enforces transport characteristics, authentication characteristics, confidentiality characteristics, integrity characteristics, and timeout characteristics on communication pathways.

8.3 Requirement Dependency Rationale

The following table demonstrates the dependencies among the claimed security requirements. It shows that nearly all are satisfied.

The only dependency that is not satisfied is FPT_STM.1 which requires a time mechanism for use by the auditing mechanism. The assumption A.TIME is intended to indicate that the environment (i.e., the operating system) is providing this time information for use by the TOE.

Therefore the requirements work together to accomplish the overall objectives defined for the TOE.

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	[FPT_STM.1]
FAU_GEN.2	FAU_GEN.1 and FIA_UID.1	FAU_GEN.1 and FIA_UID.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 and FMT_MSA.3 and FPT_STM.1[27]	FDP_IFC.1 and FMT_MSA.3 and [FPT_STM.1]
FIA_ATD.1	none	none
FIA_SOS.1	none	none
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UID.1	none	none
FMT_MOF.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
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.1a	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1b	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.1
ADV_ARC.1	ADV_FSP.1 and ADV_TDS.1	ADV_FSP.2 and ADV_TDS.1
ADV_FSP.2	ADV_TDS.1	ADV_TDS.1
ADV_TDS.1	ADV_FSP.2	ADV_FSP.2
AGD_OPE.1	ADV_FSP.1	ADV_FSP.2
AGD_PRE.1	none	none
ALC_CMC.2	ALC_CMS.1	ALC_CMS.2
ALC_CMS.2	none	none
ALC_DEL.1	none	none
ALC_FLR.2	none	none
ATE_COV.1	ADV_FSP.2 and ATE_FUN.1	ADV_FSP.2 and ATE_FUN.1
ATE_FUN.1	ATE_COV.1	ATE_COV.1
ATE_IND.2	ADV_FSP.2 and AGD_OPE.1 and AGD_PRE.1 and ATE_COV.1 and ATE_FUN.1	ADV_FSP.2 and AGD_OPE.1 and AGD_PRE.1 and ATE_COV.1 and ATE_FUN.1
AVA_VAN.2	ADV_ARC.1 and ADV_FSP.1 and ADV_TDS.1 and AGD_OPE.1 and AGD_PRE.1	ADV_ARC.1 and ADV_FSP.2 and ADV_TDS.1 and AGD_OPE.1 and AGD_PRE.1

Table 5 Requirement Dependency Analysis

[27] FPT_STM.1 has been added as a dependency placate concern about a reference to “timeout characteristics.”

8.4 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 6 Security Functions vs. Requirements Mapping demonstrates the relationship between security requirements and security functions.

	Security Audit	User Data Protection	Identification and Authentication	Security Management	TSF Protection
FAU_GEN.1	x				
FAU_GEN.2	x				
FAU_SAR.1	x				
FAU_SAR.3	x				
FDP_IFC.1		x			
FDP_IFF.1		x			
FIA_ATD.1			x		
FIA_UAU.1			x		
FIA_UID.1			x		
FIA_SOS.1			x		
FMT_MOF.1				x	
FMT_MSA.1				x	
FMT_MSA.3				x	
FMT_MTD.1a				x	
FMT_MTD.1b				x	
FMT_SMF.1				x	
FMT_SMR.1				x	

Table 6 Security Functions vs. Requirements Mapping

8.5 PP Claims Rationale

See Section 7, Protection Profile Claims.