National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

TIBCO ActiveMatrix BusinessWorks™

Release 5.8

Report Number: CCEVS-VR-VID10230-2010
Dated: 30 July 2010
Version: 3.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Dr Patrick Mallett (Lead Validator)
Olin Sibert (Senior Validator)

Common Criteria Testing Laboratory

Terrie Diaz, Lead Evaluator
Science Applications International Corporation (SAIC)
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the TIBCO ActiveMatrix BusinessWorks™ Release 5.8.

The Validation Report presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of TIBCO ActiveMatrix BusinessWorks Release 5.8 was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory in the United States and was completed on 25 May 2010.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by SAIC. The ETR and Team Test Report used in developing this validation report were written by SAIC. The evaluation team determined the product to be Part 2 and Part 3 conformant, and meets the assurance requirements of EAL 2 augmented with ALC_FLR.2. All security functional requirements are derived from Part 2 of the Common Criteria.

The TOE is TIBCO ActiveMatrix BusinessWorks Release 5.8 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 evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced.

During this validation, the Validators determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the Validator concludes that the SAIC findings are accurate, the conclusions justified, and the conformance claims correct.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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

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

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant; and
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	TIBCO ActiveMatrix BusinessWorks™ Release 5.8
Protection Profile	None
ST:	TIBCO ActiveMatrix BusinessWorks™ Release 5.8 Security Target, Version 2.0, August 18, 2010
Evaluation Technical Report	Evaluation Technical Report for TIBCO ActiveMatrix BusinessWorks™ Release 5.8, Part 1 (Non-Proprietary), Version 3.0, 30 July 2010, Part 2 (Proprietary), Version 3.0, 7 July 2010, and Supplemental Team Test Report, Version 2.0, 7 July 2010.

Item	Identifier
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007
Conformance Result	CC Part 2 and Part 3 conformant, EAL 2 augmented with ALC_FLR.2
Sponsor	TIBCO Software Inc
Developer	TIBCO Software Inc
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation (SAIC), Columbia, MD
CCEVS Validator	Dr Patrick Mallett (Lead Validator), mallett@mitre.org Olin Sibert (Senior Validator), osibert@orionsec.com

3 Organizational Security Policy

The Target of Evaluation (TOE) is TIBCO ActiveMatrix BusinessWorks Release 5.8 (also known as ActiveMatrix BusinessWorks). Active Matrix 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.

Below in Figure 2.1 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.

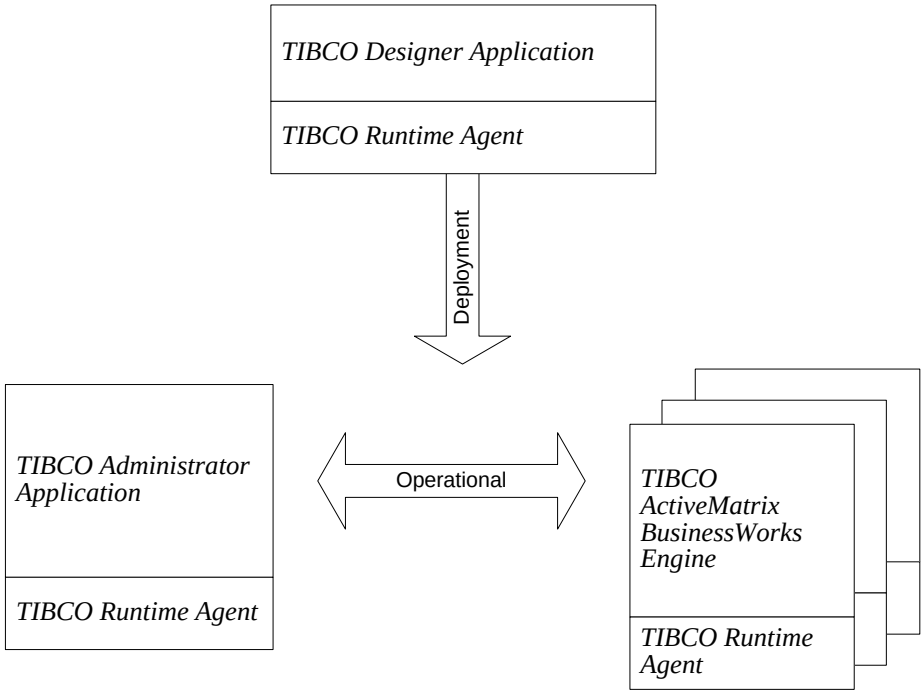

Figure 2 1 TIBCO Components

TIBCO 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 TIBCO ActiveMatrix BusinessWorks engine. The TIBCO Administrator application starts the ActiveMatrix BusinessWorks engine 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.

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. 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 connection-less, 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 described in the ST define the protections that are available once the business process has been deployed.

4 Assumptions and Clarification of Scope

The statement of TOE security environment describes the security aspects of the environment in which it is intended that the TOE will be used and the manner in which it is expected to be employed. The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the intended method for the product and defines the threats that the product is designed to counter.

Following are the assumptions identified in the Security Target:

- It is assumed the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- It is assumed there will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- It is assumed authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
- It is assumed the environment will provide a reliable time stamp for use by the TOE.
- It is assumed the access controls provided by the operating system in the environment will be used to ensure that commands to set up the TOE are used only by users associated with establishing the operational TOE.
- It is assumed 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).

Following are the threats levied against the TOE and its environment as identified in the Security Target. The threats that are identified are mitigated by the TOE and its environment. All of the threats identified in the ST are addressed.

- An administrator may not be held accountable for their actions.
- An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources.
- 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.
- 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 TOE is TIBCO ActiveMatrix BusinessWorks Release 5.8 (also known as ActiveMatrix BusinessWorks). Active Matrix 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.

5 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target.

As described above, 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.

The TIBCO Designer application, the TIBCO Administrator application, the TIBCO ActiveMatrix BusinessWorks engine, and TIBCO 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. TIBCO 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.

TIBCO Designer

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 engine. The TIBCO Administrator application starts the ActiveMatrix BusinessWorks engines to perform activities in the business process.

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.

TIBCO Administrator

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. 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.

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.

TIBCO Runtime Agent

TIBCO 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 TIBCO 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);
- A Domain Utility that manages domains and manages machines within a domain; and
- A TIBCO Designer application that provides basic business process design features.

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.

6 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor).

6.1 Design documentation

Document	Version[2]	Date
TIBCO High-Level Design	Revision 0.8	May 25, 2010

6.2 Guidance documentation (this documentation is delivered with the TOE)

Document	Version	Date
TIBCO ActiveMatrix BusinessWorks (5.8), TIBCO Administrator (5.6), TIBCO Runtime Agent (5.6) Security Features User's Guide	Version 1.9	14 May 2010
TIBCO ActiveMatrix BusinessWorks		

[2] Several versions of certain documents were examined in the course of the evaluation, and updates were made as the evaluation proceeded. The referenced version satisfies all evaluation requirements. Where no version number is specified, no updates were needed to satisfy evaluation requirements.

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	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

6.3 Lifecycle documentation

Document	Version	Date
TIBCO ActiveMatrix BusinessWorks Configuration Management Plan	Version 0.5	March 16, 2010
TIBCO Software, Inc. Delivery Procedures	Revision 0.9	February, 2010
Post-Release Management Lifecycle	Version 0.5	9/17/2007

6.4 Test documentation

Document	Version	Date
Assurance Test Evidence TIBCO ActiveMatrix BusinessWorks Suite	Version 0.7	12 May 2010

LINUX TESTS TIBCO ActiveMatrix BusinessWorks Suite	Version 0.7	12 May 2010

6.5 Security Target

Document	Version	Date
TIBCO ActiveMatrix BusinessWorks Release 5.8 Security Target	Version 1.9	July 7, 2010

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function, more specifically to the security functional requirements tested. The scope of the developer tests included all the TSFI. The testing covered the security functional requirements in the ST including: Security Audit, User Data Protection, Identification and Authentication, Security Management, and Protection of the TSF. All security functions were tested and the TOE behaved as expected. The evaluation team determined that the developer's actual test results matched the vendor's expected results.

7.2 Evaluation Team Independent Testing

The evaluation team exercised the entire automated test suite and a subset of the vendor's manual test suite. The tests were run within three distinct domains.

- Domain A had Oracle 10g as the Domain Storage, Active Directory 2003 as the LDAP source, and it used Enterprise Message Service as the Domain Transport. ActiveMatrix BusinessWorks clients were tested on Windows and Linux, TIBCO Administrator will be run on Windows Server 2008. The Port for TIBCO Administrator was 18443. Active Directory, proFTP, and Oracle 10g were configured to accept TLS/SSL communications with a single, well-known Certificate Authority providing a chain-of-trust for the whole environment (cclabCA.pem). The TIBCO Administrator instance that defines this domain was also configured so that it would only accept TLS/SSL communications and required mutual X.509 authentication in addition to the ID/Passphrase during login.
- Domain B had SQL Server 2005 as the Domain Storage, Sun Directory Server 6.3 as the LDAP source, and it used Rendezvous as the Domain Transport, configured with SSH. ActiveMatrix BusinessWorks clients were tested on Windows and Linux. TIBCO Administrator was run on the Linux system. The Port for TIBCO Administrator was 18080. SQL Server 2005 and Sun Directory Server were configured to accept TLS/SSL.
- Domain C consisted of TIBCO Administrator on the Linux system with an Windows XP client. Test cases were limited to testing access of domain data from

the file system – login information for TIBCO Administrator access as well as TOE user access from an ActiveMatrix BusinessWorks process (Basic Authentication).

All machines had the Unlimited Strength Jurisdiction Policy files applied to the JRE responsible for the TOE's Java runtime and had the X.509 PKI Chain-of-Trust enabled in the JRE's "cacerts" file for purposes of performing TLS/SSL for LDAP services.

In addition to developer testing, the evaluation team conducted its own suite of tests, which were developed independently of the sponsor. These also completed successfully.

7.3 Vulnerability Testing

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

8 Evaluated Configuration

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[3] information that is used by the TOE when user authentication is required for a business process.
- *Web Bbrowser* – Provides a user interface for the *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 8-1 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 8-1 must be a HTTP request, HTTPS request,

[3] 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'.

SOAP request, TCP/IP packet, Rendezvous messages, JMS message, or RMI call[4]. 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 engine 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[5] 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.
- 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 TIBCO Rendezvous protocols.

[4] 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.

[5] 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.

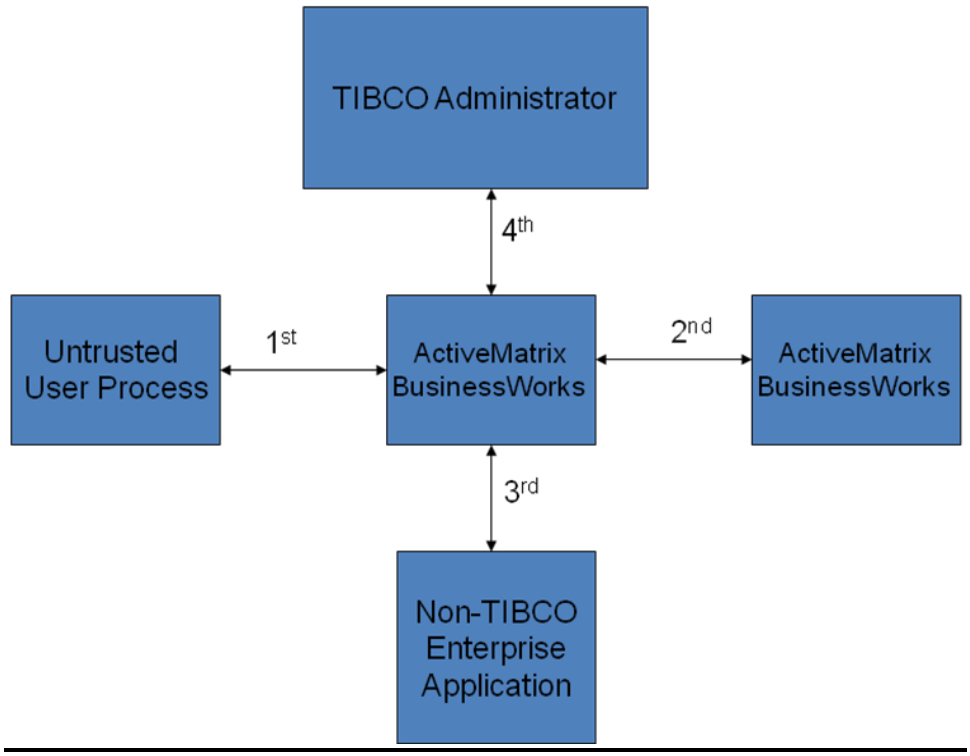

Figure 8-1 TOE Communication Pathways[6]

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.

The physical boundaries and the components that make up the TOE are:

- TIBCO ActiveMatrix BusinessWorks™ Release 5.8 engine

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

- 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[7]:
  - Microsoft ActiveDirectory 2003
  - Sun ONE Directory Server 6.3
  - Oracle 10g v2 Database
  - Oracle 11g v1 Database
  - Microsoft SQLServer 2005

ActiveMatrix BusinessWorks, TIBCO Administrator, and TIBCO 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[8]: To perform authentication for HTTP Basic Authentication or OASIS Web Services Security Authentication using the UsernameToken Profile. Any one of: Sun ONE Directory Server 6.3, Microsoft Active Directory 2003, , CA Directory Server
- Enterprise Applications: Optional, applications providing access to data and functionality in the environment.

[7] The configuration used for the evaluation testing effort utilized the Oracle 10g v2 Database and Microsoft SQLServer 2005.
[8] 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).

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.

9 Results of the Evaluation

The evaluation was conducted based upon the Common Criteria (CC), Version 3.1, Revision 2, September 2007; the Common Evaluation Methodology (CEM), Version 3.1, Revision 2, September 2007; and all applicable International Interpretations in effect on February 2008. The evaluation confirmed that TIBCO ActiveMatrix BusinessWorks Release 5.8 product is compliant with the Common Criteria Version 3.1 Revision 2, functional requirements (Part 2), Part 2 conformant, assurance requirements (Part 3) conformant for EAL2 augmented with ACL_FLR.2. The details of the evaluation are recorded in the CCTL's evaluation technical report; Final Evaluation Technical Report for the TIBCO ActiveMatrix BusinessWorks™ Release 5.8, Part 1 (Non-Proprietary) and Part 2 (Proprietary). The product was evaluated and tested against the claims presented in the TIBCO ActiveMatrix BusinessWorks Release 5.8 Security Target, Version 1.9, July 7, 2010.

The Validator followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The Validator has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The Validator therefore concludes that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL.

9.1 Evaluation of the TIBCO ActiveMatrix BusinessWorks Release 5.8 Security Target (ST) (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of threats, policies, and assumptions, a statement of security requirements claimed to be met by the TIBCO ActiveMatrix BusinessWorks Release 5.8 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each EAL2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a Security Architecture, a Functional Specification, and a Technical Design Document. The

evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

9.3 Evaluation of the guidance documents (AGD)

The evaluation team applied each EAL2 AGD CEM work unit. The evaluation team ensured the adequacy of the TIBCO ActiveMatrix BusinessWorks Installation, TIBCO ActiveMatrix BusinessWorks Getting Started, TIBCO ActiveMatrix BusinessWorks Administration, and TIBCO ActiveMatrix BusinessWorks (5.8), TIBCO Administrator (5.6), and TIBCO Runtime Agent (5.6) Security Features User's Guide in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The administrator guide was assessed during the design and testing phases of the evaluation to ensure it was complete. The complete set of documentation is provided in the TIBCO ActiveMatrix BusinessWorks Release 5.8 Security Target.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL2 ALC CEM work unit. The evaluation team ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control, and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. The evaluation team ensured the procedure included automated support to control and track changes to the implementation representation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation.

The evaluation team also ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer. The evaluation team followed the TIBCO ActiveMatrix BusinessWorks Installation, TIBCO ActiveMatrix BusinessWorks Getting Started, TIBCO ActiveMatrix BusinessWorks Administration, and TIBCO ActiveMatrix BusinessWorks (5.8), TIBCO Administrator (5.6), and TIBCO Runtime Agent (5.6) Security Features User's Guide to test the installation procedures to ensure the procedures result in the evaluated configuration.

Furthermore, the evaluation team ensured the adequacy of the developer procedures to protect the TOE implementation representation and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance.

Finally, the evaluation team also examined the flaw tracking and remediation procedures and guidance that addressed the TOE developer procedures that are used to accept, track, and act upon reported security flaws and requests for corrections to those flaws, as well as the distribution of reports and corrections to registered users.

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

The evaluation team applied each EAL2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and Technical Design Document. The evaluation team exercised a sample of the manual test suite. The evaluation team also devised an independent set of team test and vulnerability tests. The vendor tests, team tests, and vulnerability tests substantiated the security functional requirements in the ST.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL2 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the evaluation team's vulnerability analysis, and the evaluation team's performance of vulnerability tests.

9.7 Summary of Evaluation Results

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

10 Validator Comments/Recommendations

All Validator concerns with respect to the evaluation have been addressed. No issues are outstanding.

11 Security Target

The Security Target is identified TIBCO ActiveMatrix BusinessWorks Release 5.8 Security Target, Version 2.0, August 19, 2010. The document identifies the Security Functional Requirements (SFRs) that are levied on the TOE, which are necessary to implement the TOE security policies. Additionally, the Security Target specifies the Security Assurance Requirements necessary for EAL 2 augmented with ALC_FLR.2.

12 Glossary

The following definitions are used throughout this document:

CC	Common Criteria
CEM	Common Evaluation Methodology
CCEVS	Common Criteria Evaluation and Validation Scheme
EAL	Evaluation Assurance Level

GUI	Graphical User Interface
NIAP	National Information Assurance Partnership
OS	Operating System
PP	Protection Profile
SAIC	Science Applications International Corporation
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
US	United States

13 Glossary of Terms

The terminology below is described in order to clarify and distinguish the terms used in the Protection Profile, the ST and those used in the TOE product documentation.

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.

14 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 1, September 2006

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 2, September 2007

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 2, September 2007

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 2, September 2007.

[5] TIBCO ActiveMatrix BusinessWorks™ Release 5.8, Final Non-Proprietary ETR – Part 1, Version 3.0 dated 30 July 2010

[6] TIBCO ActiveMatrix BusinessWorks™ Release 5.8, Final Proprietary ETR – Part 2, Version 3.0 dated 7 July 2010 and Supplemental Team Test Report, Version 2.0, 7 July 2010.

[7] TIBCO ActiveMatrix BusinessWorks Release 5.8 Security Target, Version 2.0, August 19, 2010.

[8] NIAP Common Criteria Evaluation and Validation Scheme Publication #4, Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, September 8, 2008.