National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

TIBCO Enterprise Message Service^{TM} Version 4.3.0

Report Number: CCEVS-VR-06-0053
Dated: 29 December 2006
Version: 2.3

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Victoria A. Ashby
The MITRE Corporation
McLean, VA

Common Criteria Testing Laboratory

Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

The evaluation of TIBCO Enterprise Message Service^{TM} Version 4.3.0 was performed by Science Applications International Corporation (SAIC) in the United States and was completed on 18 December 2006. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.3, August 2005 and the Common Methodology for IT Security Evaluation (CEM), Version 2.3, August 2005.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 2.3) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3). The TOE is TIBCO Enterprise Message Service^{TM} (EMS) provided by TIBCO Software Inc. EMS is a Java Messaging Service (JMS) version 1.1 provider (server), which is a messaging system server application. The TOE acts as an intermediary for message senders and message receivers in the IT environment that access TOE messaging services using TOE programmatic interfaces. The TOE can be described in terms of the following components:

EMS Server application – Provides JMS messaging system server application interfaces. Supports messaging APIs including those compatible with the JMS standard as well as non-JMS APIs, specifically the EMS APIs.

EMS Message APIs – Provides messaging system programming interfaces that can be used to access EMS Server application messaging services. There are both C and Java language interfaces.

EMS Administrator API – Provides Java language programmatic administrative console interfaces that can be used to manage EMS Server application services.

- EMS Administration Tool application – Provides command-line administrative console interfaces that can be used to manage EMS Server application services.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by SAIC.

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. This Validation Report is not an endorsement of the TIBCO EMS product by any agency of the US Government and no warranty of the product is either expressed or implied.

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

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

2.2 Interpretations

This evaluation used the Common Criteria for Information Technology Security Evaluation Parts 2 and 3, Version 2.3, August 2005. The evaluation started in September 2005; therefore no additional interpretations existed to be applied.

1.1 Threats to Security

The Security Target identified the following threats that the Target of Evaluation (TOE) addresses:

A user may not be held accountable for their actions within the TOE.

An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms

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

A user may gain unauthorized access (view, modify, delete) to user data

2 Identification

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

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

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

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

Table 1: Evaluation Identifiers

Item	**Identifier**
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	TIBCO Enterprise Message Service™ Version 4.3.0
Protection Profile	Not applicable.
ST:	TIBCO Enterprise Message Service™ Version 4.3.0 Security Target, Version 1.0, 8 December 2006
Evaluation Technical Report	*Evaluation Technical Report for* TIBCO Enterprise Message Service™ Version 4.3.0, Version 4.0, 30 January 2007
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

Item	Identifier
Conformance Result	CC Part 2 Extended and Part 3 conformant
Sponsor	TIBCO Software Inc
Developer	TIBCO Software Inc
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validator	Vicky Ashby, The MITRE Corporation

3 TOE Security Services

The security services provided by the TOE are summarized below:

2.3 Security audit

The TOE generates audit records for start-up and shutdown of the audit functions, as well as unsuccessful use of the authentication mechanism, all requests to send a message using a topic or a queue, and use of the management functions. The IT environment is relied on to provide a reliable timestamp, to protect the audit trail as well as provide the ability to review its contents.

2.4 Cryptographic Support

The TOE provides its own FIPS-evaluated cryptographic engine (an instance of OpenSSL 0.9.7i) which performs symmetric encryption and decryption of messages and digital signature verification of certificates. The TOE may also be configured to use a FIPS-evaluated cryptomodule in the IT environment (Entrust SSL v6.1).

2.5 User data protection

All messaging users (subjects) are subject to the Messaging Access Control Policy for all available operations on topics and queues (objects) that are used to send and receive publish/subscribe and point-to-point messages, respectively. The TOE restricts access to topics and queues using ACLs. ACLs are used to grant access to either individual users or groups. ACLs also specify the necessary permissions that a user or group must possess in order to perform a requested operation.

The TOE also provides the ability to implement security domains of subjects by grouping users into administrative domains so that administrators can only perform actions within their domain. Grouping users into domains is implemented using “protection permissions”. Protection permissions allow grouping users into administrative domains so that administrators can only perform actions within their domain. An administrator can only perform administrative operations on a user that has the same protection permission as the user.

2.6 Identification and authentication

2.2.2.4 The TOE defines users in terms of user identity, authentication data, group memberships, and permissions. The TOE can authenticate users using its password mechanism or an LDAP authentication mechanism provided by the IT Environment. The TOE can be configured to allow users to attempt to authenticate using either mechanism.

2.7 Security management

The ability to manage topic and queue ACLs as well as message user security attributes is limited to administrators or users that have been granted the necessary administrative permission by restricting access to interfaces. By default, access to topics and queues must be explicitly granted by administrators or users that have been granted the necessary administrative permission using restricted interfaces. The TOE provides administrative interfaces to manage topics and queues, and users.

2.8 Self protection

The TOE prevents users from bypassing implicit and explicit policies that it enforces by requiring authenticated messaging users as well as authenticated administrators.

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 in which the TOE operates.

Following are the assumptions are identified in the Security Target:

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

- The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation.

The scope of this evaluation includes the TIBCO Enterprise Message Service™ product. The Enterprise Message Service™ (EMS) TOE is a software application that sits on a server and that enables information, packaged as JMS messages to flow between different infrastructure applications. A typical install has minimal prompts and installs standard components in default locations; hence does not give the user the opportunity to install component individually. A custom install prompts you to choose which components of the product suite to install and installs only those components. EMS provides an Administration Tool for administrative management functions.

The EMS TOE depends on services provided by the IT environment which are not within the TOE boundary. These services include tools for audit review, protection of the audit trail data, a reliable time stamp, encryption services, LDAP services, and identification and authentication of user identity prior to any action taken by the TOE.

More details about the TOE are given in the section that follows.

5 Architectural Information

The TOE creates and delivers messages. Messages are structured data that one application sends to another. The creator of the message is located in the IT environment and is known as the producer. The receiver of the message is also located in the IT environment and is known as the consumer. The TOE acts as an intermediary for the message and sends it to the correct destination.

The TOE provides two types of JMS messaging services: point-to-point and publish/subscribe. A point-to-point (PTP) product or application is built around the concept of message queues, senders, and receivers. A publish/subscribe product or application is built around the concept of clients (subscribers) addressing messages to a topic provided by a server (publishers).

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

EMS Server application – Provides JMS messaging system server application interfaces. Supports messaging APIs including those compatible with the JMS standard as well as non-JMS APIs, specifically the EMS APIs.

EMS Message APIs – Provides messaging system programming interfaces that can be used to access EMS Server application messaging services. There are both C and Java language interfaces.

EMS Administrator API – Provides Java language programmatic administrative console interfaces that can be used to manage EMS Server application services.

EMS Administration Tool application – Provides command-line administrative console interfaces that can be used to manage EMS Server application services.

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

Operating system – Provides a runtime environment for the EMS Server application component, as well as for IT environment components.

Java Virtual Machine – Provides Java Virtual Machine (JVM) runtime environment for the EMS Server application and for applications in the IT environment calling Java language EMS message interfaces.

Certification Authority (CA) – Provides digital certificates for SSL used to protect communication between the EMS Server application and EMS Message and Administrator APIs, as well as between the EMS Server application and the EMS Administration Tool application.

LDAP server – Provides authentication server services for the EMS Server application to authenticate users calling EMS Message and Administrator API.

6 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. Following is the list of documentation that was evaluated and is provided to the end user.

Guidance Documentation

Document	**Version**	**Date**
TIBCO Enterprise Message Service™ User's Guide, Software Release 4.3		February 2006
TIBCO Enterprise Message Service™ Installation, Software Release 4.3		February 2006
TIBCO Enterprise Message Service™ Release Notes, Software Release 4.3		February 2006

Delivery and Operation Documentation

Document	**Version**	**Date**
TIBCO Process Definition Description, Operations – Supplier Management	1.0	10/16/03
TIBCO Process Definition Description, Operations – Security Access Control Policy	1.0	04/06/04
TIBCO Order Management (OM) Process, Contract to Order Processing		January 2005
TIBCO Enterprise Message Service™ Installation, Software Release 4.3		February 2006
Security Features User's Guide For TIBCO Enterprise Message Service™ 4.3	0.52	

Security Target

Document	**Version**	**Date**
TIBCO Enterprise Message Service™ Version 4.3.0 *Security Target*	1.0	8 December 2006

7 IT Product Testing

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

7.1 Developer Testing

TIBCO's approach to security testing for TIBCO Enterprise Message Service^{TM} Version 4.3.0 is interface based. Essentially, TIBCO developed a set of test suites that correspond to a security function enforced by a particular subsystem interface. Each test suite targets the specific security behavior associated with that interface and security function. The developer tested interfaces for the audit mechanism, the access control policy and attributes, the SSL invocation and the administrative permissions and restrictions. The test procedures are designed to be exercised by running a script that has been designed to test the applicable security function described in the test scenario.

Depth analysis is based on an understanding of the high-level design and is intended to show that the TOE as presented in the high-level design has been adequately tested. The team analyzed each test suite, determined which SFRs were addressed by that test suite, and compared the analysis results to the ST description of that security function. Each SFR maps to one or more test suites, and the rationale for each test suite demonstrates why that test suite covers that particular SFR. All of the vendor's tests are automated scripts run by a test harness.

Prior to independent testing, the evaluation team analyzed the vendor test procedures to ensure adequate coverage and to determine if the interfaces between subsystems were behaving as expected. The Evaluation Team added tests to the team test plan in cases where additional tests were indicated to ensure complete test coverage.

Before testing, the vendor provided a complete set of expected and actual test results for analysis. The evaluation team examined the vendor's actual test results for the TOE configuration. During this examination, the Evaluation Team discovered several instances of test failures. The vendor provided the rationale for the failure of such test cases and successfully ran such test cases with the correct input values. During analysis of the vendor test suite prior to actual testing, the vendor test suite, expanded by the team tests, was shown to adequately address all security functions claimed in the ST for the TOE.

7.2 Evaluation Team Independent Testing

The vendor provided the TOE configuration at a vendor site for installation and testing. The tests were executed on a machine connected to an isolated lab network. Also on this network were an LDAP server for use in the access control tests, and sniffers used in tests described below.

The evaluation team followed the download instructions as documented in the Delivery document to download and verify the TOE for testing. The TOE was installed as indicated in *TIBCO Enterprise Message Service^{TM} Installation Software* and the *Security Features User's Guide for TIBCO Enterprise Message Service*^{TM}.

While installing each TOE configuration, the Evaluation Team also tested the installation, generation, and start-up procedures to determine, in accordance with ADO_IGS.1.2E, that those procedures result in a secure configuration. Some issues were noted during the set up and testing. Updates to the vendor documentation have corrected the cause of these issues.

The evaluation team ran a sample of the vendor's test suite on Linux, Solaris, and Windows 2003 platforms during testing. The sampling included the entire set test set evenly split between the three platforms. For instance every third test was run on one of the platforms. The Evaluation Team sampled the log files to compare actual to expected results as outlined in Appendix A. The actual results were as expected:

all API calls were executed when the user had the proper authorities, and access was denied when the user did not have the proper authorities;

- a user was added and removed from the identified groups accordingly,
- and all communication is secured using FIPS-evaluated cryptographic engine (an instance of OpenSSL 0.9.7i) and/or FIPS-evaluated cryptomodule in the IT environment (Entrust SSL v6.1).

In addition to rerunning the vendor's tests, the Evaluation Team developed a set of independent team tests to address areas of the ST that did not seem completely addressed by the vendor's test suite, or areas where the ST did not seem completely clear. All were run as manual tests. These independent team tests included confirmation of the following:

- Only a user that has been granted administrator permissions can perform security management functions and they can only be performed in the domain in which the administrator had been assigned.
- An authorized administrator can issue the commands to grant and revoke administrative permissions.
- Wildcards and inheritance work as expected for queues and topics.
- The Messaging Access Control Policy rules include explicit authorize access based on the group the user is assigned and the proper permissions.
- For each auditable event an audit record is generated and the records contain the required information.

The evaluation team has determined the TOE behaves as expected and all test suites have been successfully executed on all identified platforms.

The following hardware and software is necessary to create the test configurations used during independent testing:

1) LDAP Server machine:

HW: IBM ThinkPad T30

CPU: Pentium 4, 2GHz

Memory: 512 MB

Hard Disk: 30GB

OS: Windows 2000 SP4

LDAP Server: Sun ONE Server 5.2

2) Linux machine (OS Platform-1):

HW: HP Pavilion

CPU: Dual Intel(R) Xeon(TM), 2.00GHz

Memory: 3 GB

Hard Disk-1: 10 GB (OS is installed on this disk)

Hard Disk-2: 25 GB (/local:- used for the execution of the test harness)

OS: Linux version 2.6.9-11.ELsmp (bhcompile@decompose.build.redhat.com) (gcc version 3.4.3 20050227 (Red Hat 3.4.3-22)) #1 SMP Fri May 20 18:26:27 EDT 2005

3) Solaris 10 (Sparc) machine (OS Platform-2):

HW: Sun-Fire V240

CPU: Dual UltraSPARC IIIi (64-bit), 1.5 GHz

Memory: 2 GB

Hard Disk-1: 100 GB (OS is installed on this disk)

Hard Disk-2: 70 GB (/local:- used for the execution of the test harness)

OS: Solaris 10 (SunOS cccsol1 5.10 Generic_118822-25 sun4u sparc SUNW,Sun-Fire-V240)

4) Machine running Exceed as front-end to Solaris 10 (Sparc) machine:

HW: IBM ThinkPad T41

Memory: 1 GB

Hard Disk: 60GB

OS: Windows XP Pro SP4

5) Windows XP machine (OS Platform-3):

HW: Dell Precision 360

CPU: Pentium 4, 2.8GHz

Memory: 2 GB

Hard Disk: 80 GB

OS: Windows XP Pro SP2

Test Harness

TOE (TIBCO Enterprise Message Service^{TM} Version 4.3.0)

7.3 Evaluation Team Penetration Testing

For its penetration tests, the Evaluation Team used a combination of vulnerability test tools, open-source vulnerability documentation, and a set of test procedures proposed by the Evaluation Team to identify penetration test cases based on the developer's vulnerability assessment documentation. The Evaluation Team used the developer's test configuration to successfully perform its penetration tests. The open-source vulnerability search produced no vulnerabilities not already included in the vendor's vulnerability analysis. The penetration test ensured that communication between the TOE components was in fact encrypted and therefore protected from modification and disclosure.

The Evaluation Team's Final ETR, Part 2 Supplement, provides a detailed description of the tests and the results. No effects were found on the information presented in the ST or other evaluation evidence.

8 Evaluated Configuration

Each of the TOE components described above is a software application designed to execute within an operating system context provided by the environment.
The TOE depends on the following:

Operating system – Any one of: Microsoft Windows 2000 (Professional, Server, and Advanced Server) with Service Pack 2; Microsoft Windows XP, Microsoft Windows 2003; Sun Solaris 2.7, 2.8, 2.9, 2.10; HP-UX 11.0, 11i; HP-UX Itanium 11.22; IBM AIX 5.1; Linux (kernel 2.4); Linux Itanium (kernel 2.4); HP Tru 64 UNIX 5.1A; Mac OS X 10.3

Java Virtual Machine – Any one of: Java Runtime Environment (JRE) JRE 1.3

Cryptographic libraries – Entrust SSL v6.1

In addition, there is one expectation on the TOE environment for the evaluated configuration:

- The TOE can retrieve Authentication information using its embedded LDAP client which communicates with an LDAP server provided by the TOE environment. The connection between the TOE LDAP client and the IT LDAP server may be configured as a TLS/SSL encrypted link, or must be deployed in an internal communication link within a trusted network. CRLs (Certificate Revocation Lists) are retrieved from a named directory path only (not a directory service like LDAP).

9 Results of the Evaluation

The Evaluation Team conducted the evaluation based on the Common Criteria (CC) Version 2.3 and the Common Evaluation Methodology (CEM) Version 2.3 and all applicable National and International Interpretations in effect.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Verdicts were not assigned to assurance classes.

Section 6, Conclusions, in the Evaluation Team's ETR, Part 1, states:

> "Each verdict for each CEM work unit in the ASE ETR is a "PASS". Therefore, the TIBCO Enterprise Message Service™ Version 4.3.0 Security Target is a CC compliant ST."

In addition,

> "The verdicts for each CEM work unit in the ETR sections included in Section 15 are each "PASS". Therefore, when configured according to the following guidance documentation:
>
> *TIBCO Enterprise Message Service™ Installation Software Release 4.3 and the Security Features User's Guide For TIBCO Enterprise Message Service™ 4.3*

The TIBCO Enterprise Message Service™ Version 4.3.0 TOE (see product identification below) satisfies the TIBCO Enterprise Message Service™ Version 4.3.0 Security Target, Version 1.0, 8 December 2006. "

The rationale supporting each CEM work unit verdict is recorded in the *Evaluation Technical Report for TIBCO Enterprise Message Service™ Version 4.3.0, Part 2,* which is considered proprietary.

The validation team followed the procedures outlined in the *Common Criteria Evaluation and Validation Scheme (CCEVS) Publication # 3* for Technical Oversight and Validation Procedures. The validation team has observed the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the

CCEVS. The validation team therefore concludes that the evaluation and its results of pass are complete.

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 subset of the vendor test suites, the independent tests, and the penetration test also demonstrates the accuracy of the claims in the ST.

10 Validator Comments/Recommendations

The Evaluation Team worked with the vendor to enable the TOE to meet CCEVS Policy Letter 9, Crypto in Common Criteria Evaluations. The TOE provides its own FIPS-evaluated cryptographic engine (an instance of OpenSSL 0.9.7i) which performs symmetric encryption and decryption of messages and digital signature verification of certificates. The TOE may also be configured to use a FIPS-evaluated cryptomodule in the IT environment (Entrust SSL v6.1). Both possible configurations were tested by the Evaluation Team during Independent Team Testing and verified to work as expected in the evaluated configuration.

The ST includes an extended SFR for Identification and Authentication, FIA_UAU_EXP.2. This SFR states, "The TSF shall require each user to be successfully authenticated by either the TOE or its environment before allowing any other TSF-mediated actions on behalf of that user." In other words, the TOE can be configured to authenticate users using its password mechanism or an LDAP authentication mechanism provided by the IT environment. Use of each authentication method, including processing of CRLs when certificates were used, was tested during the Independent Team Testing effort, and each method was verified to work as expected in the evaluated configuration.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *TIBCO Enterprise Message Service™ Version 4.3.0 Version 1.0, 8 December 2006*. The document identifies the security functional requirements (SFRs) necessary to implement the TOE security policies. These include TOE SFRs and IT Environment SFRs. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 2.

13 Glossary

The following definitions are used throughout this document:

Hardware: the physical equipment used to process programs.

Software: the programs and associated data that can be dynamically written and modified.

Target of Evaluation (TOE) - An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

14 Bibliography

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

- *Common Criteria for Information Technology Security Evaluation* Part 1: Introduction and general model, Version 2.3, August 2005
- *Common Criteria for Information Technology Security Evaluation* Part 2: Security Functional Requirements, Version 2.3, August 2005
- *Common Criteria for Information Technology Security Evaluation* Part 3: Security Assurance Requirements, Version 2.3, August 2005
- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005
- Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.
- *TIBCO Enterprise Message Service™ Version 4.3.0 Version 1.0, 8 December 2006*.
- *Evaluation Technical Report for TIBCO Enterprise Message Service™ Version 4.3.0, Part 1* (Non-Proprietary), Version 4.0, 30 January 2007.
- *Evaluation Technical Report for TIBCO Enterprise Message Service™ Version 4.3.0, Part 2(SAIC and TIBCO Proprietary)*, Version 1.0, 14 December 2006
- *Evaluation Team Test Plan for TIBCO Enterprise Message Service™ Version 4.3.0, Part 2 Supplement (SAIC and TIBCO Proprietary),* Version 1.0, 15 December 2006.