TIBCO Enterprise Message Service™ Version 4.3.0 Security Target

Version 1.0
12/08/06

Prepared for:
TIBCO Software Inc.

3303 Hillview Avenue
Palo Alto, CA 94304

Prepared By:
Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

1. SECURITY TARGET INTRODUCTION 1

1.1 SECURITY TARGET, TOE AND CC IDENTIFICATION 1
1.2 CONFORMANCE CLAIMS 1
1.3 CONVENTIONS 2

2. TOE DESCRIPTION 3

2.1 TOE OVERVIEW 3
2.2 TOE ARCHITECTURE 3
2.2.1 Physical Boundaries 4
2.2.2 Logical Boundaries 4
2.3 TOE DOCUMENTATION 5

3. SECURITY ENVIRONMENT 6

3.1 THREATS 6
3.2 ASSUMPTIONS 6

4. SECURITY OBJECTIVES 6

4.1 SECURITY OBJECTIVES FOR THE TOE 6
4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT 6
4.3 SECURITY OBJECTIVES FOR THE NON-IT ENVIRONMENT 7

5. IT SECURITY REQUIREMENTS 8

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 8
5.1.1 Security audit (FAU) 8
5.1.2 Cryptographic support (FCS) 9
5.1.3 User data protection (FDP) 9
5.1.4 Identification and authentication (FIA) 10
5.1.5 Security management (FMT) 10
5.1.6 Protection of the TSF (FPT) 11
5.1.7 Protection of the TSF (FPT) 11
5.2 IT ENVIRONMENT SECURITY FUNCTIONAL REQUIREMENTS 11
5.2.1 Security audit (FAU) 11
5.2.2 Identification and authentication (FIA) 12
5.3 TOE SECURITY ASSURANCE REQUIREMENTS 12
5.3.1 Configuration management (ACM) 13
5.3.2 Delivery and operation (ADO) 13
5.3.3 Development (ADV) 14
5.3.4 Guidance documents (AGD) 14
5.3.5 Tests (ATE) 15
5.3.6 Vulnerability assessment (AVA) 16

6. TOE SUMMARY SPECIFICATION 17

6.1 TOE SECURITY FUNCTIONS 17
6.1.1 Security audit 17
6.1.2 Cryptographic support 18
6.1.3 User data protection 18
6.1.4 Identification and authentication 19
6.1.5 Security management 20
6.1.6 Protection of the TSF 21
6.2 TOE SECURITY ASSURANCE MEASURES 22
6.2.1 Configuration management 22
6.2.2 Delivery and operation 22
6.2.3 Development 22
6.2.4 Guidance documents 23

6.2.5 Tests *23*
6.2.6 Vulnerability assessment *23*

7. PROTECTION PROFILE CLAIMS **25**

8. RATIONALE **26**

8.1 SECURITY OBJECTIVES RATIONALE 26
8.1.1 Security Objectives Rationale for the TOE and Environment *26*
8.2 SECURITY REQUIREMENTS RATIONALE 28
8.2.1 Security Functional Requirements Rationale *28*
8.3 SECURITY ASSURANCE REQUIREMENTS RATIONALE 31
8.4 STRENGTH OF FUNCTIONS RATIONALE 31
8.5 REQUIREMENT DEPENDENCY RATIONALE 33
8.6 EXPLICITLY STATED REQUIREMENTS RATIONALE 33
8.7 TOE SUMMARY SPECIFICATION RATIONALE 33
8.8 PP CLAIMS RATIONALE 35

LIST OF TABLES

Table 1 Security Functional Components 8
Table 2 EAL 2 Assurance Components 13
Table 3 Environment to Objective Correspondence 26
Table 4 Objective to Requirement Correspondence 29
Table 5 Security Functions vs. Requirements Mapping 35

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 Enterprise Message Service™ provided by TIBCO Software Inc. TIBCO Enterprise Message Service™ 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 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 IT environment, and the organizational policy that the TOE must fulfill.
- Section 4 – TOE Security Objectives
  This section details the security objectives of the TOE and IT environment.
- Section 5 – IT Security Requirements
  The section presents the security functional requirements (SFR) for the TOE and IT Environment that supports the TOE, and details the assurance requirements for EAL2.
- 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 Enterprise Message Service™ Version 4.3.0 Security Target

ST Version – Version 1.0

ST Date – 12/08/06

TOE Identification – TIBCO Enterprise Message Service™ Version 4.3.0

TOE Developer – TIBCO Software Inc.

Evaluation Sponsor – TIBCO Software Inc.

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

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005.
  - Part 2 Extended

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

1.3 Conventions

The following conventions have been applied in this document:

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

2. TOE Description

The Target of Evaluation (TOE) is TIBCO Software Inc. Enterprise Message Service™ Version 4.3.0.

EMS is a Java Messaging Service (JMS) version 1.1 provider (server), which is a messaging system server application that provides both JMS interfaces and administrative console interfaces. The TOE provides a uniform messaging interface between applications in the IT environment according to the JMS specification that these applications can use to communicate with each other.

The remainder of this section summarizes the TOE architecture.

2.1 TOE Overview

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).

2.2 TOE Architecture

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 Java APIs 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.

The TOE can be managed using either using the command-line EMS Administration Tool application or by creating an application that calls the EMS Administrator API. Messages are sent by message senders and receivers in the IT environment using messaging type objects that are instantiated on the EMS Server, not by the EMS Message APIs or within the calling application. The TOE provides administrators with interfaces that can be used to manage topics and queues, as well as to manage users.

2.2.1 Physical Boundaries

The components that make up the TOE are:

- EMS Server application
- EMS Message APIs (both C and Java language)
- EMS Administrator API
- EMS Administration Tool application

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

There is no distinction between the product and the TOE. The above-listed TOE components are all installed for each instance of the TOE. The TOE installation process does not give the user an opportunity to install components individually.

2.2.2 Logical Boundaries

This section summarizes the security functions provided by TIBCO Enterprise Message Service™:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Self protection

2.2.2.1 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.

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

2.2.2.2 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).

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

2.2.2.3 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.

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

2.2.2.4 Identification and authentication

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.

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

2.2.2.5 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.

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

2.2.2.6 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.

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

2.3 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.

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) also serves as an indicator of whether the TOE would be suitable for a given environment.

3.1 Threats

T. ACCOUNTABILITY	A user may not be held accountable for their actions within the TOE.
T. ADMIN_ERROR	An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms
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. UNAUTH_ACCESS	A user may gain unauthorized access (view, modify, delete) to user data

3.2 Assumptions

A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.NO_EVIL	The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation.

4. Security Objectives

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

4.1 Security Objectives for the TOE

O.ACCESS	The TOE will ensure that users gain only authorized access to it and to the resources that it controls.
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security relevant events associated with users.
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.PROTECT	The TOE will protect itself and its assets from external interference or tampering.
O.USER_AUTHENTICATION	The TOE will verify the claimed identity of users.
O.USER_IDENTIFICATION	The TOE will uniquely identify users.

4.2 Security Objectives for the Environment

OE.TIME	The IT environment will provide a time source that provides reliable time stamps.
OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.

OE.AUDIT_REVIEW	The IT environment will provide the capability to view audit information, and alert the authorized administrator of identified potential security violations.
OE.PROTECT	The IT environment will protect TOE network communication from external interference or tampering.
OE.USER_AUTHENTICATION	The IT Environment will verify the claimed identity of users.
OE.USER_IDENTIFICATION	The IT Environment will uniquely identify users.

4.3 Security Objectives for the Non-IT Environment

OE.CONFIG	The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation.
OE.PHYCAL	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

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. All of the requirements have been copied from version 2.3 of the applicable Common Criteria documents.

5.1 TOE Security Functional Requirements

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit data generation
FCS: Cryptographic support	FCS_COP.1a: Cryptographic operation
	FCS_COP.1b: Cryptographic operation
FDP: User data protection	FDP_ACC.2: Complete access control
	FDP_ACF.1: Security attribute based access control
FIA: Identification and authentication	FIA_ATD.1a: User attribute definition
	FIA_UAU_EXP.2: User authentication by the TOE or IT Environment
	FIA_UID.2a: User identification before any action
FMT: Security management	FMT_MSA.1a: Management of security attributes
	FMT_MSA.1b: Management of security attributes
	FMT_MSA.3: Static attribute initialization
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_ITT.1: Basic internal TSF data transfer protection
	FPT_RVM.1: Non-bypassability of the TSP

Table 1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 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 following events:**

- **unsuccessful use of the authentication mechanism**
- **all requests to send a message using a topic or a queue**
- **use of the management functions**

].

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, 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, [**no additional information**].

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic operation (FCS_COP.1a)

FCS_COP.1a.1 The TSF shall perform [**digital signature verification**] in accordance with a specified cryptographic algorithm [**RSA digital signature**] and cryptographic key sizes [**1024**] that meet the following: [**ANSI X9.31**].

5.1.2.2 Cryptographic operation (FCS_COP.1b)

FCS_COP.1b.1 The TSF shall perform [**data encryption**] in accordance with a specified cryptographic algorithm [**AES-CBC**] and cryptographic key sizes [**256**] that meet the following: [**FIPS 197**].

5.1.3 User data protection (FDP)

5.1.3.1 Complete access control (FDP_ACC.2)

FDP_ACC.2.1 The TSF shall enforce the [**Messaging Access Control Policy**] on [**the following subjects and objects:**

- **subjects: users**
- **objects: topics and queues**].

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

5.1.3.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the **[Messaging Access Control Policy]** to objects based on the following: **[security attributes:**

a.) **subject security attributes:**
- **user identity**
- **permissions**
- **group membership**

b.) **object security attributes:**
- **access control list (ACL)**

]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

a.) **the requested access is allowed if:**
- **if the user identity is equal to the object owner; and**
- **if the user possesses the necessary messaging permission to perform the requested operation**

b.) **the requested access is allowed if:**
- **if the user identity is a member of a messaging user group and the ACL grants the group the requested access; and**
- **if the messaging user group possesses the necessary messaging permission to perform the requested operation**

c.) **otherwise access is denied, unless access is explicitly authorized in accordance with the rules specified in FDP_ACF.1.3**

]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [

a.) **the requested access is allowed if:**
- **if the user is member of the administrative user group; or**

- **if the user possesses the necessary administrative permission to perform the requested operation and the user possesses the necessary protection permission to perform the requested operation**

]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the **[there are no explicit access denial rules**].

5.1.4 Identification and authentication (FIA)

5.1.4.1 User attribute definition (FIA_ATD.1a)

FIA_ATD.1a.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

a.) **user identity**
b.) **authentication data**
c.) **group memberships**
d.) **permissions**

].

5.1.4.2 User authentication by the TOE or IT Environment (FIA_UAU_EXP.2)

FIA_UAU_EXP.2 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.

5.1.4.3 User identification before any action (FIA_UID.2a)

FIA_UID.2a.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.5 Security management (FMT)

5.1.5.1 Management of security attributes (FMT_MSA.1a)

FMT_MSA.1a.1 The TSF shall enforce the **[Messaging Access Control Policy]** to restrict the ability to [***modify***] the security attributes [**object ACLs**] to [**administrators or users that have been granted the necessary administrative permission**].

5.1.5.2 Management of security attributes (FMT_MSA.1b)

FMT_MSA.1b.1 The TSF shall enforce the **[Messaging Access Control Policy]** to restrict the ability to [***manage***] the security attributes [**of messaging users**] to [**administrators or users that have been granted the necessary administrative permission**].

5.1.5.3 Static attribute initialization (FMT_MSA.3)

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

FMT_MSA.3.2 The TSF shall allow the **[administrators or users that have been granted the necessary administrative permission]** to specify alternative initial values to override the default values when an object or information is created.

5.1.5.4 Specification of Management Functions (FMT_SMF.1)

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

a.) **manage topics and queues**
b.) **manage users**

].

5.1.5.5 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [
a.) **user**
b.) **administrator**
].

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

5.1.6 Protection of the TSF (FPT)

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

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

5.1.7 Protection of the TSF (FPT)

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

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

5.2 IT Environment Security Functional Requirements

The following table describes the SFRs that to be satisfied by the IT environment in which the TOE operates.

Requirement Class	Requirement Component
FAU: Security audit	FAU_SAR.1: Audit review
	FAU_STG.1: Protected audit trail storage
FCS: Cryptographic support	FCS_COP.1c: Cryptographic operation
	FCS_COP.1d: Cryptographic operation
FIA: Identification and authentication	FIA_ATD.1b: User attribute definition
	FIA_SUP_EXP.1: User authentication at the request of the TOE
	FIA_UID.2b: User identification before any action
FPT: Protection of the TSF	FPT_SEP.1: TSF domain separation
	FPT_STM.1: Reliable time stamps

5.2.1 Security audit (FAU)

5.2.1.1 Audit review (FAU_SAR.1)

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

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

5.2.1.2 Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1 The ~~TSF~~ **IT Environment** shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 The ~~TSF~~ **IT Environment** shall be able to **[*prevent*]** unauthorised modifications to the audit records in the audit trail.

5.2.2 Cryptographic support (FCS)

5.2.2.1 Cryptographic operation (FCS_COP.1c)

FCS_COP.1c.1 The ~~TSF~~ **IT Environment** shall perform [**digital signature verification**] in accordance with a specified cryptographic algorithm [**RSA digital signature**] and cryptographic key sizes [**1024**] that meet the following: [**ANSI X9.31**].

5.2.2.2 Cryptographic operation (FCS_COP.1d)

FCS_COP.1d.1 The ~~TSF~~ **IT Environment** shall perform [**data encryption**] in accordance with a specified cryptographic algorithm [**AES-CBC**] and cryptographic key sizes [**256**] that meet the following: [**FIPS 197**].

5.2.3 Identification and authentication (FIA)

FIA_ATD.1b.1 The ~~TSF~~ **IT Environment** shall maintain the following list of security attributes belonging to individual users: [

a.) **user identity**

b.) **authentication data**

].

5.2.3.1 User authentication at the request of the TOE (FIA_SUP_EXP.1)

FIA_SUP_EXP.1 The IT environment shall require each user to be successfully authenticated at the request of the TOE.

5.2.3.2 User identification before any action (FIA_UID.2b)

FIA_UID.2b.1 The ~~TSF~~ **IT Environment** shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.2.3.3 TSF domain separation (FPT_SEP.1)

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

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

5.2.3.4 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1 The ~~TSF~~ **IT Environment** shall be able to provide reliable time stamps for its own **and TOE** use.

5.3 TOE Security Assurance Requirements

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

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.2: Configuration items
ADO: Delivery and operation	ADO_DEL.1: Delivery procedures
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.1: Descriptive high-level design
	ADV_RCR.1: Informal correspondence demonstration

AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

Table 2 EAL 2 Assurance Components

5.3.1 Configuration management (ACM)

5.3.1.1 Configuration items (ACM_CAP.2)

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

5.3.2 Delivery and operation (ADO)

5.3.2.1 Delivery procedures (ADO_DEL.1)

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

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

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

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.
ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.1.2c The functional specification shall be internally consistent.
ADV_FSP.1.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.
ADV_FSP.1.4c The functional specification shall completely represent the TSF.
ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Descriptive high-level design (ADV_HLD.1)

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

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

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

5.3.4 Guidance documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.
AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.
AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.
AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.
AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.
AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.
AGD_ADM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 User guidance (AGD_USR.1)

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

5.3.5 Tests (ATE)

5.3.5.1 Evidence of coverage (ATE_COV.1)

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

5.3.5.2 Functional testing (ATE_FUN.1)

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

5.3.5.3 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.
ATE_IND.2.1c The TOE shall be suitable for testing.
ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.6 Vulnerability assessment (AVA)

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

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.
AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.
AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.3.6.2 Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.
AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.
AVA_VLA.1.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.
AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.
AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.
AVA_VLA.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 Security audit

The TOE generates audit records for start-up and shutdown of the audit functions, as well as an unspecified level of audit. The TOE writes audit records to a text file stored in the IT environment. The auditable events include:

- start-up and shutdown of the audit function
- unsuccessful use of the authentication mechanism, including:
  - Use of TOE username/password mechanism
  - Use of the LDAP server in the IT environment
- all requests to send a message using a topic or a queue, including:
  - messages received by a destination
  - messages sent to consumers
  - messages imported or exported to/from an external system
  - messages acknowledged
- use of the management functions, including:
  - Use of the EMS Administrator API
  - Use of the Administration Tool application

Each audit record includes date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. The TOE allows administrators to define auditable events by configuring what are called tracing options. Tracing options are defined for types of events such as use of the management functions. Administrators can also specify the name and location of the audit trail file in the file system in the operating system in the IT environment. The following tracing options are required in the evaluated configuration:

Trace option	**Corresponding event types**
ACL	• all requests to send a message using a topic or a queue
ADMIN	• use of the management functions
AUTH	• unsuccessful use of the authentication mechanism
CONNECT_ERROR	• all requests to send a message using a topic or a queue
DEFAULT	• start-up and shutdown of the audit function
LDAP_DEBUG	• unsuccessful use of the authentication mechanism
MESSAGE	• all requests to send a message using a topic or a queue

SSL	• all requests to send a message using a topic or a queue
SSL_DEBUG	• all requests to send a message using a topic or a queue

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

- 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. 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.

6.1.2 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). The cryptomodule performs cryptographic operations as follows:

- certificate-based authentication – the engine is used to verify the signature of the certificate that is presented across an SSL connection as well as those used to build a path from the trust anchor in order to determine the validity of the certificate that is presented.
- message encrypting – the engine is used to encrypt and decrypt messages across an SSL connection

Only the administrator has the ability to configure cryptographic operation settings in general, including configuring root certificates (i.e. trust anchors).

The Cryptographic support function is designed to satisfy the following security functional requirements:

- FCS_COP.1a: The TOE provides its own FIPS-evaluated cryptographic engine which performs digital signature verification of certificates across an SSL connection. The TOE may be configured to use a FIPS-evaluated cryptomodule provided by the IT environment which performs digital signature verification of certificates across an SSL connection.
- FCS_COP.1b: The TOE provides its own FIPS-evaluated cryptographic engine which performs symmetric encryption and decryption of messages across an SSL connection. The TOE may be configured to use a FIPS-evaluated cryptomodule provided by the IT environment which performs symmetric encryption and decryption of messages across an SSL connection.

6.1.3 User data protection

The TOE implements an access control policy called the Messaging Access Control Policy that can control access to topics and queues based on:

- user identity
- permissions
- group membership
- access control list (ACL)

The EMS Server 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.

There are four protection permissions (“protect1”, “protect2”, “protect3”, and “protect4”) that support the creation of up to four groups of administrators in the evaluated configuration. Protection permissions do not apply to the single admin user or users in the $admin group, these users can perform any action on any user regardless of protection permissions. Protection permissions can be granted to a set of messaging users (either individually, or to a defined group(s)) by a member of the $admin group in the evaluated configuration. The same protection permission is then granted (also by a member of the $admin group in the evaluated configuration) to a user who has also been granted the “admin” administrative permission that can perform actions on those users.

In a publish and subscribe JMS messaging service model, producers address messages to a topic. In this model, the producer is known as a publisher and the consumer is known as a subscriber. Many publishers can publish to the same topic, and a message from a single publisher can be received by many subscribers. Subscribers subscribe to topics, and all messages published to the topic are received by all subscribers to the topic. This type of message protocol is also known as broadcast messaging because messages are sent over the network and received by all interested subscribers, similar to how radio or television signals are broadcast and received. Each message consumer subscribes to a topic. When a message is published to that topic, all subscribed consumers receive the message. There can be a time dependency in the publish and subscribe model. By default, subscribers only receive messages when they are active. If messages are delivered when the subscriber is not available, the subscriber does not receive those messages. JMS specifies a way to remove part of the timing dependency by allowing subscribers to create durable subscriptions. Messages for durable subscriptions are stored on the server until the message expires or the storage limit is reached. Subscribers can receive messages from a durable subscription even if the subscriber was not available when the message was originally delivered.

The point-to-point JMS messaging service model has one producer and one consumer per message. This style of messaging uses a queue to store messages until they are received. The message producer sends the message to the queue; the message consumer retrieves messages from the queue and sends acknowledgement that the message was received. More than one producer can send messages to the same queue, and more than one consumer can retrieve messages from the same queue. The queue can be configured to be exclusive, if desired. If the queue is exclusive, then all queue messages can only be retrieved by the first consumer specified for the queue. Exclusive queues are useful when you want only one application to receive messages for a specific queue. If the queue is not exclusive, any number of receivers can retrieve messages from the queue. Non-exclusive queues are useful for balancing the load of incoming messages across multiple receivers. Regardless of whether the queue is exclusive or not, only one consumer can ever retrieve each message that is placed on the queue. Each message consumer receives a message from the queue and acknowledges receipt of the message. The message is taken off the queue so that no other consumer can receive it.

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. Permissions stored in the access control list determine the actions a user can perform on a destination. A user’s permissions are the union of the permissions granted explicitly to that user along with any permissions the user receives by belonging to a group. Permissions can only be granted by administrators. When granting permissions, the administrator specifies the user or group to whom to grant the permission, the name of the destination, and the permission(s) to grant. Administrators can specify either explicit destination names or wildcard destination names. Topics and queues each have associated permissions, i.e. there are a set of permissions that are specific to queues, and a set of permissions that are specific to topics.

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

- FDP_ACC.2, FDP_ACF.1: All messaging users are subject to the Messaging Access Control Policy for all available operations on topics and queues that are used to send and receive publish/subscribe and point-to-point messages, respectively.

6.1.4 Identification and authentication

The TOE defines users in terms of:

- user identities
- authentication data (passwords)

- group membership
- permissions (messaging and administrative types)

The TOE provides its own username and password authentication mechanism that is always used to authenticate administrative users. Similarly, when a user accesses the TOE using its certificate-based authentication mechanism, a valid certificate for which a certificate path can be found from the trust anchor that the TOE has been configured with must be entered before accessing any other TOE interfaces. Either the TOE password or certificate mechanism, or an LDAP server in the IT environment, can be used to authenticate messaging users, depending on TOE configuration.

The TOE can be configured to combine TOE and IT Environment authentication mechanisms. In such a configuration TOE configuration files provide interfaces to specify which one of the authentication mechanisms to attempt first. Both TOE and IT Environment authentication mechanisms can be enabled such that one mechanism can be attempted before the other in the case that authentication using the first mechanism fails. If the second authentication mechanism fails then the user is not allowed any access to the TOE.

In order for an administrator to access the TOE, a user account including a username, password, and membership in the single administrative group must be created for the user. In order for a messaging user to access the TOE, if the TOE has been configured to use its password or certificate mechanism to authenticate messaging users, a username, password or certificate respectively, and optionally membership in an administrator-defined messaging user group must be created for the user. In order for a messaging user to access the TOE, if the TOE has been configured to use LDAP to authenticate messaging users, a username and optionally membership in an administrator-defined messaging user group must be created for the user.

Groups can be used to create classes of messaging users. Groups can be used to grant and revoke permissions to large numbers of users with a single operation on the group. Messaging users may belong to more than one group. A messaging user's permissions are the union of the permissions of the groups the user belongs to, in addition to any permissions granted to the user directly.

Messaging permissions (compared to administrative type permissions) determine the type of operations that users or groups may perform on topics or queues. Topics and queues each have associated messaging permissions, i.e. there are a set of messaging permissions that are specific to queues, and a set of messaging permissions that are specific to topics. Administrative message type permissions are described in the Security Management security function description below.

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

- FIA_ATD.1a: The TOE defines users in terms of user identity, authentication data, group memberships, and permissions.
- FIA_UAU_EXP.2: 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. Note that the password mechanism can meet or exceed SOF-basic using password length and other composition rules.
- FIA_UID.2a: The TOE offers no TSF-mediated functions until the user is identified.

6.1.5 Security management

The TOE defines the following roles:

- user
- administrator

Users who are who are not a member of any administrator-defined messaging user groups, or who are a member of one or more administrator-defined messaging user groups, are considered users, also referred to as messaging users. Users who are a member of the single administrative user group called "$admin" are considered administrators.

Individual users who are not a member of any administrator-defined messaging user groups, as well as users who are a member of one or more administrator-defined messaging user groups, may send and receive messages using topics and queues according the Message Access Control Policy.

Individual users who are a member of the single administrative user group can perform any administrative action. While there is a pre-defined user called “admin” that also can perform any administrative action, this user account is only used during initial installation and configuration, members of the group $admin are used to manage TOE functions during operation.

Individual users who are not a member of the single administrative user group may be able to perform an administrative action if they have been granted an administrative permission to do so by a member of the administrative user group. Administrative permissions are not the same as permissions stored in the access control list. Administrative permissions can be granted and revoked by members of the administrative user group using “grant” and “revoke” commands for individual administrative permissions. Any member of the administrative user group may grant or revoke any administrative permissions granted to any user who is not a member of the administrative user group. Administrative permissions include global permissions, destination-level permissions, and protection permissions. Global permissions can be used to perform global actions, such as creating users or viewing all queues. Destination-level permissions can be used to control the administration functions a user can perform on a specific destination (i.e. topic or queue). Protection permissions allow grouping users into administrative domains so that users with a given set of protection permissions can only perform actions within their domain, for example only performing administrative operations on a user that has the same protection permission as the user.

The TOE provides administrator console interfaces to perform the following:

- manage topics and queues
- manage users

The TOE administrator console interfaces consist of command-line EMS Administration Tool application interfaces and programmatic interfaces provided by the EMS Administrator API. Connections 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 are protected from disclosure and from modification using SSL. The TOE ensures that the trust anchors can be modified only by members of the administrative user group and the private key for the server can only be activated by the members of the administrative user group.

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

- FMT_MSA.1a: The ability to manage topic and queue ACLs is limited to administrators or users that have been granted the necessary administrative permission by restricting access to interfaces.
- FMT_MSA.1b: The ability to manage message user security attributes is limited to administrators or users that have been granted the necessary administrative permission by restricting access to interfaces.
- FMT_MSA.3: By default, after the TOE has been installed and configured into its evaluated configuration, access to topics and queues must be explicitly granted by administrators or users that have been granted the necessary administrative permission using restricted interfaces.
- FMT_SMF.1: The TOE provides administrative interfaces to manage topics and queues, and users.
- FMT_SMR.1: The TOE supports administrator-defined messaging user groups and a single administrative user group. Users who are members of the administrative group are considered administrators, all others are simply considered “users”, even if they have been granted one or more administrative permissions.

6.1.6 Protection of the TSF

The EMS Server JMS provider implementation requires authenticated messaging message senders and message receivers in the evaluated configuration. Authenticated messaging users are required for both publish and subscribe and point-to-point messaging models, as well as for the hybrid messaging model that supports sending the same message to both a topic and a queue. The EMS Server controls messages until they are delivered. The EMS Server for example creates and manages the threads that it uses to listen for and establish network connections with

producers and consumers. In addition, the TOE requires administrators log into its API and command-line administrative interfaces.

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

- FPT_ITT.1: The TOE uses SSL to protect network connections 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.
- FPT_RVM.1: The TOE prevents users from bypassing implicit and explicit policies that it enforces by mediating messages sent and received using its interfaces between producers and consumers, and requiring authenticated messaging users. The TOE also requires administrators log into its API and command-line administrative interfaces.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by TIBCO ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, life-cycle documentation, vulnerability analysis documentation, and configuration management documentation.

These activities are documented in:

- TIBCO - Configuration Management Plan

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

- ACM_CAP.2

6.2.2 Delivery and operation

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

These activities are documented in:

- TIBCO - Installation and Delivery Guide

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

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

TIBCO has numerous documents describing all facets of the design of the TOE. In particular, they have a functional specification that describes the accessible TOE interfaces; a high-level design that decomposes the TOE architecture into subsystems and describes each subsystem and their interfaces; and, correspondence documentation that explains how each of the design abstractions correspond from the TOE summary specification in the Security Target to the subsystems.

These activities are documented in:

- TIBCO - Functional Specification
- TIBCO - High-level Design

- TIBCO - Design Correspondence

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

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

6.2.4 Guidance documents

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

These activities are documented in:

- TIBCO – Installation Manual
- TIBCO – Administration Guide
- TIBCO – Content Server User's Guide
- TIBCO – Content Server Reference Manual

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

- AGD_ADM.1
- AGD_USR.1

6.2.5 Tests

TIBCO has a test plan that describes how each of the necessary security functions is tested, along with the expected test results. TIBCO has documented each test as well as an analysis of test coverage and depth demonstrating that the security aspects of the design evident from the functional specification and high-level design are appropriately tested. Actual test results are also provided to demonstrate that the tests have been applied and that the TOE operates as designed.

These activities are documented in:

- TIBCO - Test Plan
- TIBCO - Test Coverage Analysis
- TIBCO - Test

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

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

6.2.6 Vulnerability assessment

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

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

These activities are documented in:

- TIBCO - Vulnerability Analysis Report

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

- AVA_SOF.1
- AVA_VLA.1

7. Protection Profile Claims

There is no Protection Profile claim in this Security Target.

8. Rationale

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

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

8.1 Security Objectives Rationale

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

8.1.1 Security Objectives Rationale for the TOE and Environment

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

	O.ACCESS	O.AUDIT_GENERATION	O.MANAGE	O.PROTECT	O.USER_AUTHENTICATION	O.USER_IDENTIFICATION	OE.AUDIT_PROTECTION	OE.AUDIT_REVIEW	OE.PROTECT	OE.TIME	OE.USER_AUTHENTICATION	OE.CONFIG	OE.PHYCAL
T.ACCOUNTABILITY		x					x	x		x			
T.ADMIN_ERROR			x										
T.MASQERADE					x	x					x		
T.UNAUTH_ACCESS	x			x					x				
A.LOCATE													x
A.NO_EVIL												x	

Table 3 Environment to Objective Correspondence

8.1.1.1 T.ACCOUNTABILITY

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

This Threat is satisfied by ensuring that:

- O.AUDIT_GENERATION: The TOE will provide the capability to detect and create records of security relevant events associated with users.
- OE.AUDIT_PROTECTION: The IT Environment will provide the capability to protect audit information.
- OE.AUDIT_REVIEW: The IT environment will provide the capability to view audit information, and alert the authorized administrator of identified potential security violations.
- OE.TIME: The IT environment will provide a time source that provides reliable time stamps.

8.1.1.2 T.ADMIN_ERROR

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

This Threat is satisfied by ensuring that:

- 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.

8.1.1.3 T.MASQUERADE

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

This Threat is countered by ensuring that:

- O.USER_AUTHENTICATION: The TOE will verify the claimed identity of users.
- O.USER_IDENTIFICATION: The TOE will uniquely identify users.
- OE.USER_AUTHENTICATION: The IT Environment will verify the claimed identity of users.

8.1.1.4 T.UNAUTH_ACCESS

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

This Threat is countered by ensuring that:

- O.ACCESS: The TOE will ensure that users gain only authorized access to it and to the resources that it controls.
- O.PROTECT: The TOE will protect itself and its assets from external interference or tampering.
- OE.PROTECT: The IT Environment will protect itself and its assets from external interference or tampering.

8.1.1.5 A. LOCATE

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

This Assumption is satisfied by ensuring that:

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

8.1.1.6 A. NO_EVIL

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

This Assumption is satisfied by ensuring that:

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

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.ACCESS	O.AUDIT_GENERATION	O.MANAGE	O.PROTECT	O.USER_AUTHENTICATION	O.USER_IDENTIFICATION	OE.AUDIT_PROTECTION	OE.AUDIT_REVIEW	OE.PROTECT	OE.TIME	OE.USER_AUTHENTICATION	OE.USER_IDENTIFICATION
FAU_GEN.1		x										
FAU_SAR.1								x				
FAU_STG.1							x					
FCS_COP.1a					x							
FCS_COP.1b				x								
FCS_COP.1c											x	
FCS_COP.1d									x			
FDP_ACC.2	x											
FDP_ACF.1	x											
FIA_ATD.1a						x						
FIA_ATD.1b												x
FIA_UAU_EXP.2					x							
FIA_SUP_EXP.1											x	
FIA_UAU.5					x							
FIA_UID.2a						x						
FIA_UID.2b												x
FMT_MSA.1a			x									
FMT_MSA.1b			x									
FMT_MSA.3			x									

FMT_SMF.1			x									
FMT_SMR.1			x									
FPT_ITT.1				x								
FPT_RVM.1				x								
FPT_SEP.1									x			
FPT_STM.1		x								x		

Table 4 Objective to Requirement Correspondence

8.2.1.1 O.ACCESS

The TOE will ensure that users gain only authorized access to it and to the resources that it controls.

This TOE Security Objective is satisfied by ensuring that:

- FDP_ACC.2, FDP_ACF.1: All messaging users are subject to the Messaging Access Control Policy for all available operations on topics and queues that are used to send and receive publish/subscribe and point-to-point messages, respectively.

8.2.1.2 O.AUDIT_GENERATION

The TOE will provide the capability to detect and create records of security relevant events associated with users.

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.
- FPT_STM.1: Reliable time stamps are assumed to be provided by the IT environment.

8.2.1.3 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.1a: The ability to manage topic and queue ACLs is limited to administrators or users that have been granted the necessary administrative permission by restricting access to interfaces.
- FMT_MSA.1b: The ability to manage message user security attributes is limited to administrators or users that have been granted the necessary administrative permission by restricting access to interfaces.
- FMT_MSA.3: By default, after the TOE has been installed and configured into its evaluated configuration, access to topics and queues must be explicitly granted by administrators or users that have been granted the necessary administrative permission using restricted interfaces.
- FMT_SMF.1: The TOE provides administrative interfaces to manage topics and queues, and users.
- FMT_SMR.1: The TOE supports administrator-defined messaging user groups and a single administrative user group. Users who are members of the administrative group are considered administrators, all others are simply considered “users”, even if they have been granted one or more administrative permissions.

8.2.1.4 O.PROTECT

The TOE will protect itself and its assets from external interference or tampering.

This TOE Security Objective is satisfied by ensuring that:

- FCS_COP.1b: The TOE provides its own FIPS-evaluated cryptographic engine which performs symmetric encryption and decryption of messages across an SSL connection.
- FPT_ITT.1: The TOE uses SSL to protect network connections 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.
- FPT_RVM.1: The TOE prevents users from bypassing implicit and explicit policies that it enforces by mediating messages sent and received using its interfaces between producers and consumers, and requiring authenticated messaging users. The TOE also requires administrators log into its API and command-line administrative interfaces.

8.2.1.5 O.USER_AUTHENTICATION

The TOE will verify the claimed identity of users.

This TOE Security Objective is satisfied by ensuring that:

- FCS_COP.1a: The TOE provides its own FIPS-evaluated cryptographic engine which performs digital signature verification of certificates across an SSL connection.
- FIA_UAU_EXP.2: 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.

8.2.1.6 O.USER_IDENTIFICATION

The TOE will uniquely identify users.

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1a: The TOE defines users in terms of user identity, authentication data, group memberships, and permissions.
- FIA_UID.2a: The TOE offers no TSF-mediated functions until the user is identified.

8.2.1.7 OE.AUDIT_PROTECTION

The IT Environment will provide the capability to protect audit information.

This IT Environment Security Objective is satisfied by ensuring that:

- FAU_STG.1: The IT environment is relied on to protect the audit trail.

8.2.1.8 OE.AUDIT_REVIEW

The IT environment will provide the capability to view audit information, and alert the authorized administrator of identified potential security violations.

This IT Environment Security Objective is satisfied by ensuring that:

- FAU_SAR.1: The IT environment is relied on to provide the ability to review audit trail contents.

8.2.1.9 OE.PROTECT

The IT Environment will protect itself and its assets from external interference or tampering.

This IT Environment Security Objective is satisfied by ensuring that:

- FCS_COP.1d: The TOE may be configured to use a FIPS-evaluated cryptographic engine provided by the IT environment which performs symmetric encryption and decryption of messages across an SSL connection.
- FPT_SEP.1: The IT Environment is relied on to provide a secure domain.

8.2.1.10 OE.TIME

The IT environment will provide a time source that provides reliable time stamps.

This IT Environment Security Objective is satisfied by ensuring that:

- FPT_STM.1: Reliable time stamps are assumed to be provided by the IT environment.

8.2.1.11 OE.USER_AUTHENTICATION

The IT Environment will verify the claimed identity of users.

This IT Environment Security Objective is satisfied by ensuring that:

- FIA_SUP_EXP.1: The TOE authenticates messaging users using either its username/password mechanism or uses an LDAP server in the IT environment to authenticate users, depending on configuration.
- FCS_COP.1c: The TOE may be configured to use a FIPS-evaluated cryptographic engine provided by the IT environment which performs digital signature verification of certificates across an SSL connection.

8.2.1.12 OE.USER_IDENTIFICATION

The IT Environment will uniquely identify users.

This IT Environment Security Objective is satisfied by ensuring that:

- FIA_ATD.1b: The IT Environment defines users in terms of user identity and authentication data.
- FIA_UID.2b: The IT Environment offers no TSF-mediated functions until the user is identified

8.3 Security Assurance Requirements Rationale

EAL2 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. 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, EAL2 is appropriate to provide the assurance necessary to counter the limited potential for attack.

8.4 Strength of Functions Rationale

The overall strength of function claim of SOF-Basic is believed to be commensurate with the overall assurance claim of EAL 2. The only applicable security function is Identification and Authentication where passwords are used by users as evidence of their claimed identities. The intent is that the password mechanism meets or exceeds basic.

The list of relevant security functions and security functional requirements includes:

- Identification and Authentication
    - FIA_UAU.2a – User Authentication before any Action

Users are required to enter a valid password during login for authentication when using any Administration application (Administration Tool, or application written with the Java-based Administration APIs) or when using any Client Messaging application.

Users (both Administration and Client messaging users) can be authenticated via the TOE either locally or using an LDAP Server in the IT environment. Users of the Administration Tool must authenticate with the TOE or using an LDAP Server in the IT environment.

The password space is calculated as follows:

- Passwords must be at least eight characters.
- Each password must have at least one upper case character, at least one numeric character, and at least one special character.
- The 72 valid alphanumeric characters include:
  - 52 alphabetic characters (uppercase and lowercase)
  - 10 numerals
  - 10 special characters (!, @, #, $, %, ^, &, *, (,))
- Each password must differ from the user's User ID and any reverse or circular shift of that User ID.
- New passwords must differ from the old password by at least three characters.
- Users must avoid using consecutive sequences, dictionary words, or other easily guessed passwords.
- Users must never write down or share your passwords.

This is a reasonable assumption, since the guidelines (Security Features User Guide for TIBCO EMS 4.3.0) state users are not to choose easily guessable passwords, consecutive sequences, or dictionary words. In addition the guidance states that the password must differ form the user ID that includes any reverse or circular shift. Furthermore, the guidance states the new password must differ from the old password by at least three characters.

Patterns of human usage are important considerations that can influence the approach to searching a password space, and thus affect SOF. The most vulnerable scenario is that in which a user chooses a password with the smallest length of six characters, giving N6 as the number of possible passwords (where N is the number of characters available in the character set), the number of password permutations is:

52 alpha characters (upper and lower)
10 digits
+ 10 special characters (!, @, #, $, %, ^, &, *, (,))
72 possible values

72^8 = (72*72*72*72*72*72*72*72) = 722,204,136,308,736

The amount of time it takes to manually type a password given that authentication can only occur based upon manual input is 7 seconds. An attacker can at best attempt (60 / 7= 8.6 password entries every minute, or 514 password entries every hour.

On average, an attacker would have to enter (722,204,136,308,736 / 2 = 361,102,068,154,368) passwords, over (361,102,068,154,368 / 514) 702,533,206,526.01 hours, before entering the correct password. The average successful attack would, as a result, occur in slightly less than:

(702,533,206,526.01 / 24 / 365 =) 80,197,854.63 years

In accordance with annex B.3 in the CEM, the elapse time of attack is not practical and thus results in a High strength of function rating, which exceeds SOF-Basic.

8.5 Requirement Dependency Rationale

The following table demonstrates that all dependencies among the claimed security requirements are satsified and 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_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FCS_COP.1a	FDP_ITC.1 or FCS_CKM.1) and FCS_CKM.4 and FMT_MSA.2	The TOE includes an instance of a FIPS-evaluated cryptomodule. Dependencies will have been satisfied in becoming FIPS compliant.
FCS_COP.1b	FDP_ITC.1 or FCS_CKM.1) and FCS_CKM.4 and FMT_MSA.2	The TOE includes an instance of a FIPS-evaluated cryptomodule. Dependencies will have been satisfied in becoming FIPS compliant.
FCS_COP.1c	FDP_ITC.1 or FCS_CKM.1) and FCS_CKM.4 and FMT_MSA.2	The TOE may be configured to use a FIPS-evaluated cryptomodule provided by the IT environment. Dependencies will have been satisfied in becoming FIPS compliant.
FCS_COP.1d	FDP_ITC.1 or FCS_CKM.1) and FCS_CKM.4 and FMT_MSA.2	The TOE may be configured to use a FIPS-evaluated cryptomodule provided by the IT environment. Dependencies will have been satisfied in becoming FIPS compliant.
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.2 and FMT_MSA.3
FIA_ATD.1a	none	none
FIA_ATD.1b	none	none
FIA_UAU_EXP.2	FIA_UID.2	FIA_UID.2
FIA_SUP_EXP.1	FIA_UID.2	FIA_UID.2
FIA_UID.2a	none	none
FIA_UID.2b	none	none
FMT_MSA.1a	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_ACC.2
FMT_MSA.1b	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_ACC.2
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1 and FMT_SMR.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_ITT.1	none	none
FPT_RVM.1	none	none
FPT_SEP.1	none	none
FPT_STM.1	none	none
ACM_CAP.2	none	none
ADO_DEL.1	none	none
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1	ADV_RCR.1
ADV_HLD.1	ADV_FSP.1 and ADV_RCR.1	ADV_FSP.1 and ADV_RCR.1
ADV_RCR.1	none	none
AGD_ADM.1	ADV_FSP.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1	ADV_FSP.1
ATE_COV.1	ADV_FSP.1 and ATE_FUN.1	ADV_FSP.1 and ATE_FUN.1
ATE_FUN.1	none	none
ATE_IND.2	ADV_FSP.1 and AGD_ADM.1 and	ADV_FSP.1 and AGD_ADM.1 and

	AGD_USR.1 and ATE_FUN.1	AGD_USR.1 and ATE_FUN.1
AVA_SOF.1	ADV_FSP.1 and ADV_HLD.1	ADV_FSP.1 and ADV_HLD.1
AVA_VLA.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1

8.6 Explicitly Stated Requirements Rationale

A set of FIA requirements was created to specifically address TOE password authentication mechanisms. The I&A family of the CC (FIA) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of TOE authentication mechanisms and provide for requirements about same. These requirements both are dependent on FIA_UID.2.

8.7 TOE Summary Specification Rationale

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

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 5 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Security audit	**Cryptographic support**	**User data protection**	**Identification and authentication**	**Security management**	**Self protection**
FAU_GEN.1	x					
FCS_COP.1a		x				
FCS_COP.1b		x				
FDP_ACC.2			x			
FDP_ACF.1			x			
FIA_ATD.1a				x		
FIA_UAU_EXP.2				x		
FIA_UID.2a				x		
FMT_MSA.1a					x	
FMT_MSA.1b					x	
FMT_MSA.3					x	
FMT_SMF.1					x	

FMT_SMR.1					x	
FPT_ITT.1						x
FPT_RVM.1						x

Table 5 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.