Actional Corporation
XML Web Services Management and XML Firewall Security Solution

Actional Security Gateway
Security Target

Document Version 1.0
FINAL

Prepared for:

Actional Corporate Headquarters
800 W. El Camino Real, Suite 120
Mountain View, CA 94040 USA
Tel: (650) 210-0700
Fax: (650) 210-8855

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
(703) 267-6050

DISCLAIMER:

Westbridge Technologies, Inc. has merged with Actional Corporation Inc.

The product formerly known as:
"Westbridge Technology, Inc
XML Web Services Management and XML Firewall Security Solution
XML Message Server Version 3.1"

is known by the new product name:
"Actional Corporation, Inc
XML Web Services Management and XML Firewall Security Solution
Actional Security Gateway Version 3.1"

The product functionality has not changed in any way and remains the same. Only the naming conventions used to reflect the company merger have changed to reflect the product in accordance with the new company. Any mention of the company's former name, "Westbridge Technologies, Inc", or the product's former name, "Westbridge XML Message Server Version 3.1", will strictly adhere to the naming convention outlined above.

Table of Contents

List of Tables

List of Figures

1 Security Target Introduction

The Security Target (ST) introduction section presents introductory information on the Security Target, the Target of Evaluation (TOE) referenced in this Security Target, and a basic introduction to the TOE. It also contains document management information.

1.1 Security Target and TOE Identification

Table 1 – ST and TOE Identification

ST Title	Actional Corporation, Inc. XML Web Services Management and XML Firewall Security Solution Actional Security Gateway Security Target
ST Version	1.0
Author	Corsec Security, Inc.
TOE Identification	"Actional Security Gateway Version 3.1.2.5"
Common Criteria (CC) Identification	Common Criteria for Information Technology Security Evaluation (CC), Version 2.1, August 1999 (**aligned with ISO 15408)**; Parts 2 and 3; the Common Criteria Interpretations Management Board (CCIMB) as of June 4, 2004.
PP Identification	This ST claims no conformance to any Protection Profile.
Assurance Level	Evaluation Assurance Level (EAL) 2 augmented with Examination of guidance (AVA_MSU.1), Flaw reporting procedures (ALC_FLR.2), and an Informal TOE security policy model (ADV_SPM.1).
Keywords	XML, XML Server, XML Firewall, Security Target, Web Services Management (WSM), Web Services Management Platform (WSMP), XML Proxy, XML Security, Web Services Security, SOAP Proxy, SOAP Security, Application Firewall, Web Services middleware, Enterprise Service Bus, SOAP Firewall, Security Gateway, Web Service Broker, SOAP Broker, XML Broker, Web Service Manager, XML middleware, XML Message Server, Actional Security Gateway, Actional Gateway

1.2 Security Target Overview

The Target of Evaluation is the Actional Security Gateway (ASG) version 3.1.2.5, the product formally known as: "Westbridge XML Message Server (XMS) version 3.1.2.5". The ASG is infrastructure software (available also as an appliance) that provides security and management for XML Web Services networks. The ASG provides interoperability with existing and future standards and leverages existing infrastructure to provide support for XML networks.

This ST describes the requirements for the ASG and specifies how the TOE meets those requirements. This ST does not claim conformance to any Protection Profile.

This ST contains the following sections to provide mapping of the Security Environment to the Security Requirements that the ASG product meets in order to mitigate the defined threats:

- Security Target Introduction– Provides a brief summary of the content of the ST and describes the organization of other sections of this document.

- TOE Description– Provides an overview of the TOE security functions and describes the physical and logical boundaries for the TOE.
- TOE Security Environment– Describes the threats and assumptions that pertain to the TOE and the TOE environment.
- Security Objectives– Identifies the security objectives that are satisfied by the TOE and its supporting environment.
- TOE Security Functional Requirements– Presents the Security Functional Requirements (SFRs) met by the TOE.
- TOE Environment Security Requirements– Presents the Security Functional Requirements (SFRs) met by the TOE environment.
- TOE Security Assurance Requirements– Presents the Security Assurance Requirements (SARs) met by the TOE.
- TOE Summary Specification– Describes the security functions provided by the TOE to satisfy the security requirements and objectives.
- ST Rationale– Presents the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.
- Glossary of Terms– Defines the terms and acronyms used within this ST.

1.3 Common Criteria (CC) Conformance Claims

This ST conforms to the Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 (as aligned with ISO 15408) Part 2 and Part 3; specifically CC Part 2 extended and CC Part 3 augmented including interpretations as of June 04, 2004. Additionally, the TOE claims augmentation to the Evaluation Assurance Level 2 augmented with AVA_MSU.1, ALC_FLR.2, ADV_SPM.1 package. Interpretations used in this ST are as follows:

- FAU_GEN.1-INTERP-202
- FAU_STG.1-INTERP-141
- FDP_ACF.1-INTERP-103
- FDP_IFF.1-INTERP-104
- FIA_AFL.1-INTERP-111
- FIA_USB.1-INTERP-137
- FMT_MOF.1-INTERP-065
- FMT_MSA.1-INTERP-065
- FMT_MSA.3-INTERP-201
- FMT_MSA.3-INTERP-202
- FMT_SMF.1-INTERP-065
- ACM_CAP.2-INTERP-003
- ADO_IGS.1-INTERP-051
- ADO_VLA.1-INTERP-051

1.4 Conventions and Terminology

1.4.1 Conventions

There are several font variations within this ST. Selected presentation choices are discussed here to aid the Security Target user.

The CC allows several operations to be performed on security requirements; *assignment*, *refinement*, *selection* and *iteration*. Three of these operations are used in this ST.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment_value].

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text.**

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by underlined text.

The **iteration** operation is used when a component is repeated with varying operations. Iterations are noted by the inclusion of parenthesis, followed by a numeral, following the requirement.

2 TOE Description

The TOE description provides context for the evaluation. It describes the TOE as an aid to understanding the general capabilities and security requirements for the TOE.

The Actional Security Gateway is a product which contains the following: Actional Security Gateway v3.1.2.5 (inclusive of the ASG Manager and Actional Security Gateway), HSQLDBv1.7, OpenLDAP, and administrative/user guidance documentation. The TOE is the Actional Security Gateway version 3.1.2.5 (i.e. "ASG"). ASG is a subset of the product which secures and manages Web Services networks. Web Services networks typically are application-application communication networks that use XML-based messages for communication. Additional standards that may be used for Web Services networks include SOAP (simple object access protocol), WSDL and UDDI. ASG provides support for these XML and Web Services-based environments.

ASG is a communications infrastructure that provides enterprises with centralized security, monitoring, brokering, reliability, and management for XML Web Services[1] networks. The ASG product architecture consists of two major components: the Actional Security Gateway and the ASG Manager.

The ASG Manager comprises a ASG web based User Interface (UI) which facilitates all the management functions of the Actional Security Gateway. The ASG Manager manages one or more Actional Security Gateways. Moreover, the ASG Manager is both logically and physically separate from the Actional Security Gateway. The ASG Manager performs all policy rule-sets for the Actional Security Gateway to enforce.

The Actional Security Gateway includes security capabilities that are typically described as XML firewall functionality. XML application firewalls are similar to network firewalls in that they are focused on securing and monitoring a network; however, unlike network firewalls, they operate at the application level using an in-depth knowledge of the Web Services, service requestors, and message content. Moreover, the XML firewall functionality contained in the TOE consists of XML message filtering mechanisms. The ASG provides unified protection and control, even across decentralized, heterogeneous Web Service implementations and frameworks.

Due to the gateway architecture of ASG, the ASG can be implemented without requiring changes to the underlying service interfaces. IT and security professionals will be able to monitor, audit, and secure an XML Web Service network. The ASG provides a security infrastructure for accessing any XML-based Web Service, regardless of the specific messaging protocol (e.g., MQ, JMS, SSL, HTTP, etc.) used by the given service.

The ASG has various capabilities which enable users to connect, secure, and manage an XML network. For example:

Table 2 –ASG v3.1 Capabilities

Key Capability	Description
XML Firewall Application level security	The ASG provides authentication, access control, encryption, signature, malicious attack protection and deep packet inspection (content filtering).
Service Tracking,	The ASG provides monitoring, reporting (via the System Log Viewer option in the ASG Manager), auditing and alerting capabilities for users to manage their XML Web Services network for requirements such as service level agreement

[1] XML Web Services is a term referring to a set of related standards that enable program-to-program communication.

	(SLA) enforcement, business activity monitoring, exception handling and audit compliance. The ASG enables users to create customized triggers to capture the information users want for the specific events users wish to capture and provide both real-time and log information for effective visibility and control of the network.
XML Brokering	The ASG provides interoperability among different systems, including transport mediation (JMS, MQ, HTTP, HTTPS), data transformation and credential mapping. It also performs dynamic routing of messages according to defined rules.
Flexible Rule Engine	At the heart of the ASG is a flexible, extendable Rule Execution Engine which enables administrators to create coarse- and fine-grained security policies based on Boolean logic and a rich set of available variables (such as content of message, service requestor, web service operations and dozens more.)
Service Management	The ability to create Service Views, which are logical virtual web services that provide an abstraction layer for back end services, also exists. The ASG provides a workflow for publishing and deployment of XML Web Services from testing, staging, and production environments. A centralized directory of available services is provided to users as well.

2.1 Basic ASG Concepts

The following presents a discussion of basic concepts related to the ASG and its general functionality.

2.1.1 Policies

A **policy** is conceptually a set of Processing Steps, which in turn are comprised of condition-action pairs and actions that determine how the ASG will deal with a given situation. Policies can be used across a wide range of ASG functionality including data logging and exception handling. Policies may sometimes refer to "Rule Groups" within the ASG.

2.1.2 Services and Operations

Services are XML Web Services that are generally described via a Web Service Definition Language (WSDL) file and use SOAP as the standard for message exchange. **Operations** are functions made available by the service. A service may have one or more operations. Oftentimes operations are described as method calls or callable procedures for the service.

2.1.3 Service Views

A **Service View** consists of a group of operations associated with an XML Web Service that is being republished via the ASG to make available, under defined security constraints, to Service Requestors. The Service View is the central conceptual structure and key organizing principle within the ASG. To it are associated services, operations, roles (user groups and privileges), Processing Steps, and rules.

The Service View can be considered an abstraction layer, a proxied version or a virtual representation of the actual Web Service. The Service View can be created from multiple different services and multiple Service Views can be published from the same service. Each Service View may have its own characteristics, standards that are supported, and policies attached to it.

2.1.4 Service Requestor Roles

A **Service Requestor Role** is a group of Service Requestors who have permission to access a given Operation Group. In general, Service Requestor Roles can be based on business constraints. Service requestor roles can be created across different directories and different types of directories as well. The ASG can leverage the attributes within the directory for determining Service Requestor Roles.

2.1.5 Admin Roles

In an administration context, a **role** is a privilege or level of access to perform certain tasks within the ASG. Each role is constructed from a set of permissions.

2.1.6 Admin Permissions

Admin Permissions are the low-level building blocks of admin roles, determining what activities the admin role is allowed to perform. Basically, permissions can be grouped together in order to create admin roles.

2.1.7 Authentication Directories

An **Authentication Directory** provides the infrastructure for user authentication. An Authentication Directory may be implemented using one of the commonly available directory access protocols, such as Lightweight Directory Access Protocol (LDAP). A custom directory can also be set up using another format (e.g., a plain text flat-file database). Other authentication directories include X.509 certificates. The ASG can authenticate each Web Service message according to the authentication requirements.

2.1.8 Processing Steps

A **Processing Step** is an ASG system capability that a message encounters as it moves through the message pipeline. Examples of Processing Steps are Authenticate Requestor and Validate IP. Each Processing Step can be enabled to execute sequentially as a message passes through the message pipeline, and each consists of a set of rules.

2.1.9 Rules

A **rule** consists of the aggregate of conditions and actions associated with a Processing Step. These conditions and actions determine whether and how a given Processing Step will be executed.

2.2 ASG v3.1 Architecture Context

Figure 1: Deployment of the below illustrates an example of a configured ASG system.

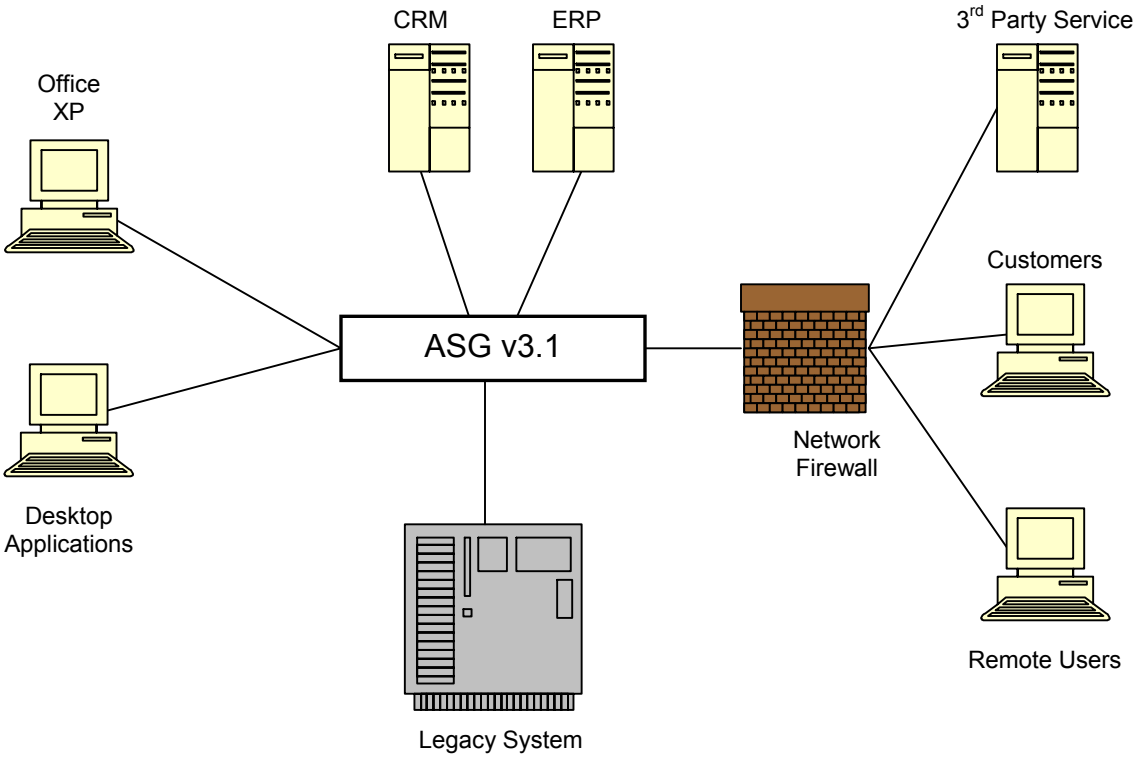

Figure 1: Deployment of the ASG

The ASG is designed to provide centralized security, reliability and manageability for heterogeneous XML Web Services networks. The ASG may be deployed in a variety of ways:

- As a single ASG;
- As load-balanced ASGs for scalability and failover; and
- As separate ASGs – for example, in a corporation where policies differ by department.

The ASG can be located within the DMZ, behind the network firewall, or at each Web Service depending upon the configuration desired and it provides security for traffic within and across network firewalls. Similarly ASG can be located between business systems (such as CRMs and ERPs) and legacy systems. CRM, Customer Relationship Management, systems provide customized business data management system specifically tailored to storing business processes and resources. An ERP, Enterprise Resource Planning, is a system which manages all enterprise product development activity. Of these systems, many leverage XML technology. ASG serves to perform validation of XML messages these systems generate.

The Westbridge architecture includes an ASG Manager which is the administrative console for managing policies and viewing reports. The Actional Security Gateways deployments are the policy enforcement points which actually intercept and process the messages. Using the centralized ASG Manager User Interface (UI), an authorized administrator is able to monitor the environment of Actional Security Gateway(s) and create reports. Additionally, an authorized administrator can configure the TOE through the ASG Manager UI console via a web browser using Secure Sockets Layer (SSL).

The ASG Manager can control one or many Actional Security Gateway(s). Multiple ASG Managers may exist in an organization; they control their own policy and rule-sets. Each ASG Manager has its own configuration which may be transmitted or pushed to any number of Actional Security Gateways. The ASG ServiceGate is a deployment option for the Actional Security Gateway where the Actional Security Gateway code is installed at the Web Service endpoint.

Each Actional Security Gateway maintains a log which may be transmitted or pulled to any ASG Manager. Configurations and logs may also be merged at the specified ASG Manager pull time. The implementation of multiple Actional Security Gateways enhances processing speed and provides redundancy.

The ASG has a parallel architecture that distributes and balances load as necessary, handling any throughput requirements. With a message processing engine, the ASG can receive, process, and forward messages.

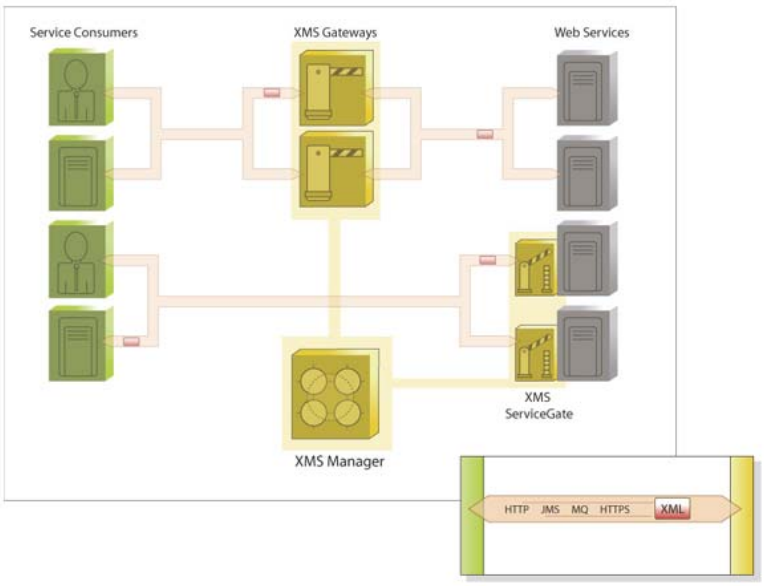

Figure 2: ASG v3.1 Architecture

The purpose of the TOE is to provide a solution to connect, secure, and manage Web Services across an organization's diverse range of applications and audiences. The ASG v3.1 is functionally a combination of an XML firewall, a Service Tracker, an XML Broker, and a Service Manager. These capabilities are fully integrated within the ASG.

The Actional Security Gateway implements XML Firewall enforcement mechanisms. The XML Firewall capability enables a user to deploy Web Services securely.

The ASG Manager employs Service Tracker mechanisms. The Service Tracker capability provides visibility and insight into business transactions and enables users to perform active exception handling when network problems occur.

The ASG Manager and Gateway employ XML Brokering functionality. The XML Broker functionality enables interoperability without the need to add any code into the network. XML Brokering includes transport mediation, data transformation, credential mapping, dynamic routing, and failover. Administration of the ASG Manager determines credential mapping resources as well as dynamic routing

strategies. The Actional Security Gateway employs the identified resources and furthermore facilitates transport mediation, data transformation, credential mapping, dynamic routing, and failover.

The ASG Manager and Gateway collectively manage services. The Service Manager capability enables administrators to control the publishing of interfaces and manages the Service Views, which enables users to upgrade their services and present the appropriate service interface to the correct service consumer. The ASG Manager defines which services are to be published while the Actional Security Gateway enforces the ASG Manager's predefined Service View ruleset.

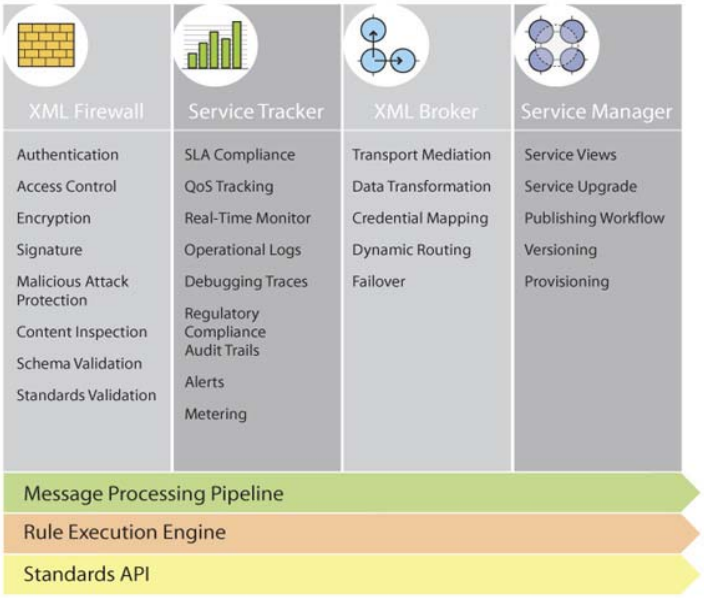

Figure 3: ASG v3.1 Functions

Note that the physical hardware and operating system of the appliance are out of scope of this evaluation. Actional Security Gateways can also sit behind a commercial load balancer for scalability and redundancy.

2.3 Product Type

The TOE is a XML web services security server which enforces security policies in a web services network. A web services security server is an application which enforces security mechanisms on the applicable web services network. A web services security server protects sensitive information by applying a combination of cryptographic algorithms and access controls. The access controls employed are determined by a set of rules specified by the TOE's administrator. The cryptographic support mechanisms are invoked by the web services network.

2.4 TOE Scope and Boundary

The boundary of the TOE encompasses all of the components that are encompassed by the red line in Figure 4 below. The two logical components of distinction that lie within the TOE boundary are the ASG Manager and the Actional Security Gateway (both are software components).

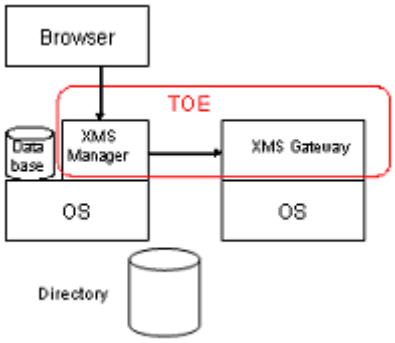

Figure 4: TOE Boundary and Logical Interaction between the ASG and External Components

The ASG comes bundled with the HSQLDB (formerly known as Hypersonic SQL) but can also be used with other databases such as Microsoft SQL Server 7+ or Oracle 8+. Note that regardless of the database used, the database lies outside of the TOE boundary and instead is part of the TOE's operating environment (although it resides on a Trusted network).

2.4.1 Physical Scope and Boundaries

The physical scope of ASG is subdivided by two major TOE components: the ASG Manager and the Actional Security Gateway. The physical boundary includes the ASG Manager and the Actional Security Gateway. The TOE contains two physically distinct components;

- The Actional Security Gateway, which serves as the web services environment policy enforcer.
- The ASG Manager, which establishes and maintains the policy for the Actional Security Gateway(s).

Table 3: ASG Physical Scope Configuration

PHYSICAL COMPONENT	HARDWARE CONFIGURATION	SOFTWARE CONFIGURATION
ASG Manager	**Microprocessor:** x86 machine with a processor speed of at least 1 GHz. **Hard Drive:** At least 30GB of hard disk space. **Memory:** At least 1GB of RAM.	**Authentication Directory:** LDAP Directory **Database:** HSQLDB1.7x **Operating System:** Windows XP Professional or EnGarde Secure Linux v1.5: Standard Edition or Solaris 8 (SunOS 2.8) **Interpretor:** Java Virtual Machine **ASG Manager Software:** ASG v3.1 Manager
Actional Security Gateway	**Microprocessor:** x86 machine with a processor speed of at least 1 GHz. **Hard Drive:** At least 30GB of hard disk space. **Memory:** At least 1 GB of RAM.	**Operating System:** Windows XP Professional or EnGarde Secure Linux v1.5: Standard Edition or Solaris 8 (SunOS 2.8) **Interpretor:** Java Virtual Machine **Actional Security Gateway Software:** ASG v3.1 Gateway

The table above outlines and describes the physical distinctions of the TOE components and the associated hardware and software configuration. Please note: for the purposes of this documentation, the evaluated configuration is defined in the above table. The following diagram further illustrates the TOE in regards to its physical boundary.

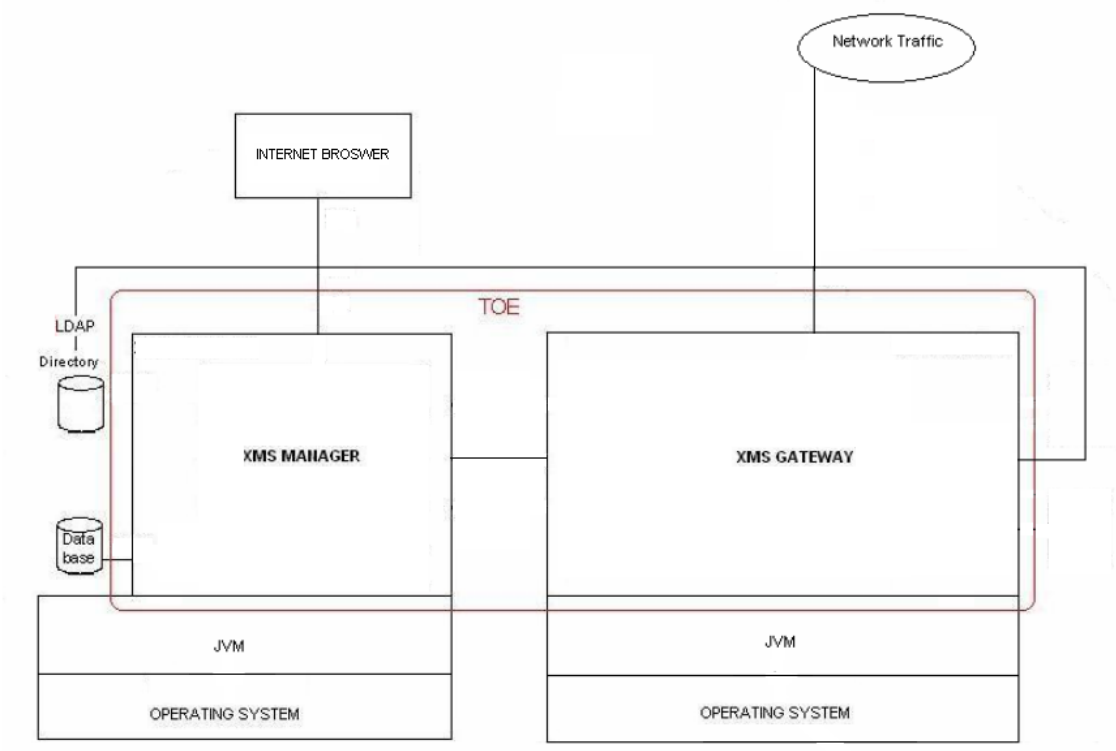

Figure 5: Physical Scope

2.4.2 Logical Scope and Boundaries

The logical boundary of the TOE encompasses all of the ASGv3.1 application components that reside within the physical boundary of the TOE. The TOE's logical boundary includes the ASG Manager and Actional Security Gateway. The evaluated secure configuration contains the same physical and logical isolation.

The TOE consists of two logically distinct components: the ASG Manager and the Actional Security Gateway. The ASG Manager is the policy decision point of the Actional Security Gateway. The ASG Manager facilitates the administration of the Actional Security Gateway. The ASG Manager provides the capabilities to view and query logs generated by the Actional Security Gateway. The ASG Manager provides access control of the management functions on the ASG Manager. The ASG Manager enforces authentication mechanisms on administrators accessing ASG's management functions. The ASG Manager communicates with authentication directories for Actional Security Gateway credential mapping. The ASG Manager provides management of user roles and associated permissions. The ASG Manager establishes which services can be viewed.

The Actional Security Gateway is resident on a local network server. The Actional Security Gateway is the policy enforcement point. The Actional Security Gateway provides multi-standard support. The Actional Security Gateway publishes viewable service views (as established by the ASG Manager). The Actional Security Gateway provides credential mapping of services against the applicable authentication directory (i.e. LDAP). The Actional Security Gateway also provides XML validation (DTD and schema) and malicious message scanning. All components of the TOE are resident on third party operating systems and hardware.

The TOE interacts with 5 major IT Environment components: the Authentication Directory, the Database, the Operating System, the Internet Browser, and the Java Virtual Machine. The following segments briefly outline, describe, and define the IT Environment components with regards to the logical scope.

Authentication Directory	The Authentication Directory is accessed by the TOE to perform authentication on the message stream from the network. While the Authentication Directory is physically resident on the ASG Manager, it is logically accessed and applied by the Actional Security Gateway.
Database	The Database is accessed by the TOE to store ASG audit logs and Administrator credentials.
Operating System	The Operating Systems is used by the TOE to provide a functional operating environment for the ASG v3.1 Manager and Gateway.
Internet Browser	The Internet Browser is used by the TOE to provide Administrators with a viewer for the ASG Manager's Graphical User Interface.
Java Virtual Machine	ASG is implemented in the Java Object Oriented language. The Java Virtual Machine is used by the TOE to provide the applicable Operating System with a Java interpreter.

2.5 TOE Documentation

The following lists the documentation for the Actional Security Gateway version 3.1. Note that ASG version 3.1 document names reflect the Westbridge Technology product name and branding.

- Getting Started with XMS: Advanced Topics Version 3.1.1
- Getting Started with XMS: Basic Administration Version 3.1.1
- The XML Message Server Reference Guide Version 3.1.1
- The XML Message Server Installation Guide Version 3.1
- The XMS Appliance Installation Guide Version 3.1
- The XMS Release Notes Guide Version 3.1
- The XMS Administrative Guidance Supplement Version 3.1

3 TOE Security Environment

This section describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

Table 4: TOE ASSUMPTIONS

ASSUMPTION CLASSIFICATION	ASSUMPTIONS
Intended Usage	A.GENPUR A.PUBLIC
Personnel	A.MANAGE A.NOEVIL A.NOTRST
Environmental	A.DBPROT A.SECSTR A.TIME
Physical	A.PROTCT A.LOCATE

3.1.1 Intended Usage Assumptions

A.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or application) on the machine on which the TOE resides.

A.PUBLIC The machine on which the TOE resides does not host public data.

3.1.2 Personnel Assumptions

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

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

A.NOTRST The TOE can only be accessed by authorized users.

3.1.3 Environmental Assumptions

A.DBPROT The database used by the TOE for ASG Manager audit storage will be located on a trusted network to prevent unauthorized tampering and modification of audit records.

A.SECSTR The key store used by the TOE for x.509 certificate and key storage will be placed within the trusted network to protect certificates and keys from tampering.

A.TIME The operating environment of the TOE will provide a reliable timestamp.

3.1.4 Physical Assumptions

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

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

3.2 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The assumed level of expertise of the attacker for all threats is unsophisticated.

Threat agents are individuals (authorized users and/or unauthorized users) that are capable of posing a threat to the TOE and the assets being protected by the TOE. The threat agents have a low attack potential. The resources and motivations of the threat agents are low to moderate.

Table 5: TOE Threats

THREAT LOCATION	ASSUMPTIONS
TOE	T.NOAUTH T.ATKPOT T.BRUTEF T.MASQUE T.REMATK T.FACCNT T.COMINT T.LOSSOF T.NOHALT T.IMPCON T.GOTHRU T.NOVALD
ENVIRONMENT	T.AUDFUL

3.2.1 Threats Addressed by the TOE

T.NOAUTH An unauthorized user may attempt to bypass the security (identification and authentication) of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

T.ATKPOT An unauthorized user may attempt to circumvent TOE security functions using obvious vulnerabilities.

T.BRUTEF An unauthorized user may attempt a brute force attack in which authentication data may be repeatedly guessed in order to gain access to the TOE and/or its data.

T.MASQUE An unauthorized user may attempt to capture identification and authentication data to use for the purpose of masquerading as an authorized administrator of the TOE.

T.REMATK An unauthorized user may attempt to view, modify, and/or delete sensitive and/or security-related information that is sent between a remotely located authorized administrator and the TOE.

T.FACCNT	An unauthorized user may attempt to access TSFs invoking security functions that may go undetected.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.LOSSOF	An unauthorized user may attempt to remove, destroy, or corrupt data stored by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the TOE's functions by halting execution of the TOE.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.GOTHRU	An unauthorized user may attempt to distribute malicious information or messages to pass through the TOE.
T.NOVALD	An unauthorized user may cause the XML messages passing through the TOE to not be checked for well formed structure validation.

3.2.2 Threats Addressed by the Environment

T.AUDFUL	An unauthorized user may attempt to exhaust storage capacity in effort to lose audit records and prevent future audit records from being recorded.

4 Security Objectives

This section identifies the security objectives for the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

O.EADMIN	The TOE shall include a set of functions that allow effective management (inclusive of audit) and maintenance of its functions and data by authorized users and administrators.
O.ACCESS	The TOE shall allow authorized users to access only TOE functions and data that are allowed per each user's assigned role.
O.IDAUTH	The TOE shall be able to identify and authenticate the claimed identity of all users prior to allowing access to TOE functions and data.
O.REMATK	The TOE shall be able to protect against unauthorized access to data transmitted.
O.NOCONF	The TOE shall allow only authorized users to alter TOE execution and/or TOE configuration.
O.AUDITS	The TOE shall provide a means to accurately detect, record, review, analyze, and act upon events in audit records.
O.SECFUN	The TOE shall provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality
O.SELPRO	The TOE shall protect itself against unauthorized modifications and attempts by unauthorized users to bypass, modify, deactivate, circumvent, or tamper with TOE security functions.
O.SANITZ	The TOE shall be able to block and/or sanitize messages in the XML message stream to protect against malicious attacks.
O.MSGVAL	The TOE shall be able to perform message validations, including message integrity validation and schema validation checks.
O.SUPPOR	The TOE shall support multiple authentication standards for the XML Message Stream.
O.CRYPTSD	The TOE must provide a choice of cryptographic algorithms and strengths based on key sizes with which to protect data.
O.CRYKEY	The TOE shall ensure appropriate protection for cryptographic keys covering generation and destruction.
O.COMM	The TOE shall provide secure session establishment between the system components and remote systems using encryption functions.

4.2 Security Objectives for the Environment

The TOE's operating environment must satisfy the following objectives.

4.2.1 Non-IT Security Objectives

O.INSTAL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

O.PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

O.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.

O.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE and are not careless, willfully negligent, or hostile and follow instructions provided by the TOE documentation.

O.SECSTR The key store used by the TOE for x.509 certificate and key storage shall be securely stored within a trusted network to protect certificates and keys from tampering.

4.2.2 IT Security Objectives

O.DBPROT The database used by the TOE for audit storage will be located on a trusted network to prevent unauthorized tampering and modification of audit records.

O. TIME The host operating system shall provide a reliable timestamp the TOE can use for accurately tracking audit events.

5 TOE Security Functional Requirements

This section defines the functional requirements for the TOE. Functional requirements in this ST were drawn from Part 2 of the CC and CCIMB Interpretations. These requirements are relevant to supporting the secure operation of the TOE. This Security Target also responds to explicitly stated requirements that were created to address additional security-relevant functions of the TOE that are unique to the TOE's product type. These new requirements contain the text (EXP) in the title.

Table 6 – Functional Requirements for the TOE Mapped to ST Operations

Functional Component	Description	ST Operation
FAU_GEN.1	Audit data generation	Assignment and Selection
FAU_SAR.1	Audit Review	Assignment
FAU_SAR.3	Selectable Audit Review	None
FCS_CKM.1(1)	Cryptographic key generation	Assignment
FCS_CKM.1(2)	Cryptographic key generation	Assignment
FCS_CKM.1(3)	Cryptographic key generation	Assignment
FCS_CKM.1(4)	Cryptographic key generation	Assignment
FCS_CKM.4	Cryptographic key destruction	Assignment
FCS_COP.1(1)	Cryptographic operation	Assignment
FCS_COP.1(2)	Cryptographic operation	Assignment
FCS_COP.1(3)	Cryptographic operation	Assignment
FCS_COP.1(4)	Cryptographic operation	Assignment
FCS_COP.1(5)	Cryptographic operation	Assignment
FCS_COP.1(6)	Cryptographic operation	Assignment
FCS_COP.1(7)	Cryptographic operation	Assignment
FCS_COP.1(8)	Cryptographic operation	Assignment
FDP_ACC.1	Subset access control	Assignment
FDP_ACF.1	Security attribute based access control	Assignment
FDP_IFC.1	Subset information flow control	Assignment
FDP_IFF.1	Simple security attributes	Assignment
FIA_UAU.2	User authentication before any action	None
FIA_UID.2	User identification before any action	None
FIA_ATD.1	User attribute definition	Assignment
FIA_AFL.1 (1)	Authentication failure handling	Assignment and Selection
FIA_AFL.1 (2)	Authentication failure handling	Assignment and Selection
FIA_USB.1	User-subject binding	None
FMT_MSA.1 (1)	Management of security attributes	Assignment and Selection
FMT_MSA.1 (2)	Management of security attributes	Assignment and Selection
FMT_MSA.2	Secure security attributes	None
FMT_MSA.3 (1)	Static attribute initialization	Assignment and Selection
FMT_MSA.3 (2)	Static attribute initialization	Assignment and Selection
FMT_MOF.1	Management of security functions behavior	Assignment and Selection
FMT_MTD.1	Management of TSF data	Assignment and Selection
FMT_SMF.1	Specification of management functions	Assignment
FMT_SMR.1	Security roles	Assignment
FPT_RVM.1	Non-bypassability of the TSP	None
XMS_VEW.1	Service views	Assignment
XMS_SUP.1	Support for many standards	Assignment
XMS_MAP.1	Credential mapping	Assignment

The following sections present the IT Security Functional Requirements (SFRs) with any ST operations performed on them (identified using the notation described in Section 1.4.1).

5.1 SECURITY AUDIT (FAU)

The security audit (FAU) class is formally defined in CC as recognizing, recording, storing, and analyzing information regarding security relevant activities. This section outlines, describes, and defines the security functional requirements in the FAU class which are implemented in the TOE. This section categorizes the security functional components in regards to their respective family. The TOE employs the audit data generation family and the security audit event selection family. The following table outlines the FAU class, families, and components in regards to the TOE.

5.1.1 FAU_GEN.1 Audit data generation

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) [Unsuccessful login attempts, successful login attempts (access to TOE), user locks out, successful add/delete/modify of TOE configuration changes of TOE objects and successful add/modify/delete of user accounts]

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 ST [Name, Object Type].

5.1.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [certain default roles[Root Administrator and Security Administrator or any role with AuditTrail permission] with the capability to read [all ASG Manager audit data] from the audit records.

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

5.1.3 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform ordering of audit data based on [the following fields: Name, Object Type, Action (event type), Changed By (subject identity), and Date/Time].

5.2 Cryptographic Support

The cryptographic support (FCS) class is formally defined in CC as cryptographic functions which perform the following: identification and authentication, non-repudiation, trusted path, trusted channel and data separation. This section outlines, describes, and defines the security functional requirements in the FCS class which are implemented in the TOE. This section categorizes the security functional components in regards to their respective family. The TOE employs the cryptographic key generation family and the cryptographic key destruction family. The following table outlines the FCS class, families, and components in regards to the TOE.

5.2.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [DES key generation algorithm] and specified cryptographic key sizes [64 bits] that meet the following [none].

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Triple-DES(3DES) key generation algorithm] and specified cryptographic key sizes [3x64 bits] that meet the following [none].

FCS_CKM.1.1(3) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [AES key generation algorithm] and specified cryptographic key sizes [128 bits] that meet the following [none].

FCS_CKM.1.1(4) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA key generation algorithm] and specified cryptographic key sizes [1024 bits] that meet the following [none].

5.2.2 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall be able to destroy cryptographic keys in accordance with a specified cryptographic key destruction method [deletion of the keys] that meets the following: [none].

5.2.3 FCS_COP.1 Cryptographic Operation

FCS_COP.1.1(1) The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [DES] and cryptographic key sizes [64 bits] that must meet the following: [none].

FCS_COP.1.1(2) The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [Triple-DES] and cryptographic key sizes [64x3 bits] that must meet the following: [none].

FCS_COP.1.1(3) The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [128 bits] that must meet the following: [none].

FCS_COP.1.1(4) The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [RSA] and cryptographic key sizes [1024 bits] that must meet the following: [none].

FCS_COP.1.1(5) The TSF shall perform [signing] in accordance with a specified cryptographic algorithm [RSA] and cryptographic key sizes [1024 bits] that must meet the following: [none].

FCS_COP.1.1(6) The TSF shall perform [signing] in accordance with a specified cryptographic algorithm [DSA] and cryptographic key sizes [1024 bits] that must meet the following: [none].

FCS_COP.1.1(7) The TSF shall perform [hashing computation and verification] in accordance with a specified cryptographic algorithm [HMAC SHA-1] and cryptographic key sizes [none] that must meet the following: [none].

FCS_COP.1.1(8) The TSF shall perform [checksum computation and verification] in accordance with a specified cryptographic algorithm [SHA-1] and cryptographic key sizes [none] that must meet the following: [none].

5.3 USER DATA PROTECTION (FDP)

The user data protection (FDP) class is formally defined in CC as protection of user data. This section outlines, describes, and defines the security functional requirements in the FDP class which are implemented in the TOE. This section categorizes the security functional components in regards to their respective family. The TOE employs the following families: subset access control, access control functions, export to outside the TSF control, import of user data with security attributes, basic rollback and stored data integrity monitoring and action. The following table outlines the FDP class, families, and components in regards to the TOE.

Table 7: RBAC Security Functional Policy

Objects	**Subjects**					
	Root Admin.	**Publisher**	**Sec. Admin.**	**Gateway Admin.**	**Console Admin.**	**Console User Admin**
Admin Roles	Create Edit Delete Assign					Create Edit Delete Assign
Admin Users	Create Edit Delete					Create Edit Delete
Auth. Directories.	Create Edit Delete Enable Disable		Create Edit Delete Enable Disable			
Base Operations	Create Edit Delete Enable Disable	Create Edit Delete Enable Disable	Enable Disable			
Base Services	Create Edit Delete Enable Disable	Create Edit Delete Enable Disable	Enable Disable			
Data Stores	Create Edit Delete	Create Edit Delete				
Data Store Entries	Create Edit Delete	Create Edit Delete				
Gateways	Create Edit Delete Push Pull Monitor Clear Start Stop			Create Edit Delete Push Pull Monitor Clear Start Stop		

Objects	Subjects					
	Root Admin.	**Publisher**	**Sec. Admin.**	**Gateway Admin.**	**Console Admin.**	**Console User Admin**
Published Operations	Create Edit Delete Enable Disable	Create Edit Delete Enable Disable	Enable Disable			
Published Ports	Create Edit Delete Enable Disable	Create Edit Delete Enable Disable	Enable Disable			
Published Service Views	Create Edit Delete Enable Disable	Create Edit Delete Enable Disable	Enable Disable			
Reports	Create Edit Delete View		Create Edit Delete View	View		
Shared Rule Groups	Create Edit Delete Use	Use	Create Edit Delete Use			
Op-specific Rule Groups	Create Edit Delete Use	Create Edit Delete Use				
Rules	Create Edit Delete Change State	Create Edit Delete Change State	Create Edit Delete Change state			
System-defined Rule Groups	Use	Use	Use			
Scheduled Jobs/Task	Create Edit Delete Execute			Create Edit Delete Execute		
Tasks	Create Edit Delete			Create Edit Delete		
Scheduled Job	Start Stop			Start Stop		
Service Requestor Roles	Create Edit Delete		Create Edit Delete			

5.3.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the [RBAC SFP] on [the subjects listed in row 1 of Table 7, the objects listed in column 1 of Table 7, and the operations listed in the cells of columns 2 through 8 of Table 7].

5.3.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [RBAC SFP as outlined in Table 7] to objects based on the following: [subjects and objects as listed in Table 7 *controlled under the* RBAC SFP*, and for each* permission associated with the subject and object].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [subjects can only perform operations on objects based on their permissions].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [no additional access rules].

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

5.3.3 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [Information Flow Control SFP] on [Service Requestor, base web services; XML and SOAP messages; and requested service operations].

5.3.4 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [Information Flow Control SFP] based on the following types of subject and information security attributes: [Service Requestor and base web services controlled under the Information Flow Control SFP, and for each, the presumed address of the source/destination subject as appropriate, content of SOAP message, permissions inherited from the Service Requestor's role, and the requested service operation].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled destination via a controlled operation if the following rules configured for that operation hold: [Messages flow through the TOE between service requestors and base web services is permitted if: the address of source/destination subject is allowed, XML Digital signature verification/application succeeds, XML encryption/decryption succeeds, the requestor is succesfully authenticated, and authorization for that user is confirmed].

FDP_IFF.1.3 The TSF shall enforce the [none].

FDP_IFF.1.4 The TSF shall provide the following [schema validations, DTD validations, and malicious or restricted content inspection and sanitation, of the XML and SOAP messages].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [Users and/or IP addresses blacklisted due to a previous policy violation, or traffic to any address for any protocol not specifically configured as a valid destination.].

5.4 IDENTIFICATION AND AUTHENTICATION (FIA)

5.4.1 FIA_AFL.1 Authentication failure handling

The user authentication (FIA) class is formally defined in CC as the conditions under which users shall be required to identify themselves before performing any other actions that are to be mediated by the TSF and which require user protection. This section outlines, describes, and defines the security functional requirements in FIA class which are relevant to the TOE. This section categorizes the security functional components in regards to their respective family. The TOE employs the timing of authentication family and the timing of identification family. The following table outlines the FIA class, families, and components in regards to the TOE.

FIA_AFL.1.1(1) The TSF shall detect when [3] unsuccessful authentication attempts occur related to [ASG Administrators (Root Administrator, Publisher, Security Administrator, Gateway Administrator, Console Adminstrator, Console User Administrator) attempting to authenticate to the ASG Manager].

FIA_AFL.1.2 (1) When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the offending external entity from accessing the TOE's functionality by locking out the applicable account until an authorized administrator enables the release of the locked account].

FIA_AFL.1.1(2) The TSF shall detect when [3] unsuccessful authentication attempts occur related to [external service consumers (Service Requestor) attempting to authenticate to Web Service].

FIA_AFL.1.2(2) When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [disable the service requestor account until it is removed from the blacklist by an authorized administrator].

5.4.2 FIA_ATD.1 User attribute definition

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

1) The admin role of the user
2) Username
3) Password
4) Account status

5.4.3 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated **using a password based authentication mechanism** before allowing **any other TSF-mediated actions** on behalf of that user.

5.4.4 FIA_UID.2 User identification before any action

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

5.4.5 FIA_USB.1 User-subject binding

FIA_USB.1.1: The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [role of the user].

FIA_USB.1.2: The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [the subject will inherit the exact set of privileges associated with the role of the user that the subject is acting on behalf of].

FIA_USB.1.3: The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [none].

5.5 SECURITY MANAGEMENT (FMT)

5.5.1 FMT_MOF.1 Management of security functions behavior

The security management (FMT) class is formally defined in CC as the allocation of authorized users to control the management functions in the TSF. This section outlines, describes, and defines the security functional requirements in the FMT class which are relevant to the TOE. This section categorizes the security functional components in regards to their respective family. The TOE employs the management of security functions behavior family and the revocation family. The following table outlines the FMT class, families, and components in regards to the TOE.

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behavior of, disable, enable the following functions in regards to the following authorized identified roles: [

Table 8: Functions and Authorized Identified Roles

FUNCTIONS	AUTHORIZED IDENTIFIED ROLES					
	Root Administrator	Publisher	Security Administrator	Gateway Administrator	Console Administrator	Console User Administrator
Modify the behavior of administrative role	X					X
Enable assignment of user to administrative role	X					X
Modify behavior of/Enable/Disable authentication directory	X		X			
Modify behavior of data store	X	X				
Modify behavior of data store entry	X	X				
Modify behavior of gateway administration functionality	X			X		
Enable release of locked account	X					X
Enable/Disable published operation	X	X	X			
Enable/Disable published port	X	X	X			
Create/Edit/Delete published service view	X	X				
Enable/Disable published service view	X	X	X			
Modify behavior of shared rule group	X		X			
Modify behavior of operation-specific rule group	X	X				
Modify behavior of/Enable/Disable rules	X	X	X			
Modify behavior of service requestor role	X		X			
Enable a push configuration from manager to gateway	X	X[2]		X		
Enable a pull log retrieval from gateway	X			X		
Enable a configuration pull from gateway to manager	X			X		

].

5.5.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1(1) The TSF shall enforce the [RBAC SFP] to restrict the ability to modify the security attributes [permissions] to [Root Administrator, Console User Administrator].

FMT_MSA.1.1(2) The TSF shall enforce the [information flow control SFP] to restrict the ability to modify the security attributes [permissions] to [Root Administrator, Security Administrator, Gateway Administrator and Publisher].

5.5.3 FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

[2] Publisher can only push configurations to non-production Gateways. Root Admin and Gateway Admin can push configuration to non-production and production Gateways.

5.5.4 FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1(1) The TSF shall enforce the [RBAC SFP] to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1) The TSF shall allow the [Root Administrator and Console User Administrator] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3.1(2) The TSF shall enforce the [information flow control SFP] to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) The TSF shall allow the [Root Administrator, Publisher, Gateway Administrator, and Security Administrator] to specify alternative initial values to override the default values when an object or information is created.

5.5.5 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to query the [audit data] to [ASG Administrators (Root Administrator, Security Administrator) who are authorized to access audit data].

5.5.6 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [management of security attributes as indicated in FMT_MSA, management of audit data as indicated in FMT_MTD, and management configuration of security functionality as indicated in FMT_MOF].

5.5.7 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [Root Administrator, Publisher, Security Administrator, Gateway Administrator, Console Administrator, and Console User Administrator].

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

5.6 PROTECTION OF THE TOE SECURITY FUNCTIONS (FPT)

The protection of the TSF (FPT) class is formally defined in CC as functional requirements which relate to the integrity and management of the mechanisms that provide the TSF and to the integrity of the TSF data. This section outlines, describes, and defines the security functional requirements in the protection of the TSF class which are implemented in the TOE. This section categorizes the security functional components in regards to their respective family. The TOE employs the following families: abstract machine testing, inter-TSF confidentiality during transmission, inter-TSF detection of modification, basic internal TSF data transfer protection, and basic non-bypassability of the TSP. The following table outlines the FPT class, families, and components in regards to the TOE.

5.6.1 FPT_RVM.1 Non-bypassability of the TSP

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.

5.7 XML MESSAGE SERVER REQUIREMENTS (XMS)

The EXP notation following the ASG functional requirements indicates that the ASG ST is explicitly stating these requirements.

5.7.1 XMS_VEW.1 Service views (EXP)

XMS_VEW.1.1 The TSF shall enable an authorized user to hide backed resources, URLs, Web Services operations from the Service Requestor. (EXP)

5.7.2 XMS_SUP.1 Multi-standard support (EXP)

XMS_SUP.1.1 The TSF shall enable the acceptance of XML messages in the following formats SOAP, WSDL, XML Encryption, SAML, WS-Security, XKMS, XML Schema, XPath, and XSLT for the ASG Message Stream. (EXP)

XMS_SUP.1.2 The TSF shall enable the acceptance of protocols in the format of HTTP, HTTPS (SSL), and/or HTTP-based authentication, for the ASG Message Stream. (EXP)

XMS_SUP.1.3 The TSF shall enable the acceptance of PKI technologies in the format of X.509 certificates, OCSP, and the Public Key Infrastructures (PKCS#7, #10, #11, #12.

5.7.3 XMS_MAP.1 Credential mapping (EXP)

XMS_MAP.1.1 The TSF shall enable the mapping of credentials of a Service Requestor into a username and password combination for the base service. (EXP)

6 TOE Environment Security Requirements

This section defines the functional requirements for the TOE's environment. Functional requirements in this ST were drawn from Part 2 of the CC. These requirements are relevant to supporting the secure operation of the TOE.

Table 9 – – List of Functional Components

Functional Component	Description	ST Operation
FAU_STG.1	Protected audit trail storage	Selection
FPT_STM.1	Reliable time stamps	None

6.1 Security Audit

6.1.1 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to prevent unauthorized modifications to the audit records in the audit trail.

6.2 Protection of TSF

6.2.1 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

7 TOE Security Assurance Requirements

This section specifies the Security Assurance Requirements (SARs) for the TOE. Table 10 – Security Assurance Requirements for the TOE below provides a complete listing of the Assurance Requirements for the TOE at EAL 2 augmented with Examination of guidance (AVA_MSU.1), Flaw reporting procedures (ALC_FLR.2), and Informal TOE security policy model (ADV_SPM.1). Assurance requirements are taken from the CC Part 3.

Table 10 – Security Assurance Requirements for the TOE

Assurance Class	Assurance Components	
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
	ADV_SPM.1	Informal TOE security policy model
AGD: Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
ALC: Life Cycle Support	ALC_FLR.2	Flaw reporting procedures
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.1	Examination of guidance
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

7.1 Configuration Management (ACM)

CONFIGURATION ITEMS (ACM_CAP.2)
[CCIMB 003]

Developer Action elements:

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.

Content and Presentation of Evidence Elements:

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labeled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.2.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.6C The CM system shall uniquely identify all configuration items.

Evaluator Action elements:

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

7.2 Delivery and Operation (ADO)

DELIVERY PROCEDURES (ADO_DEL.1)

Developer Action Elements:

ADO_DEL.1.1D The developer shall document procedures for the delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and Presentation of Evidence Elements:

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.

Evaluator Action Elements:

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

INSTALLATION, GENERATION, & START-UP PROCEDURES (ADO_IGS.1)
[CCIMB 051]

Developer Action Elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and Presentation of Evidence Elements:

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.

Evaluator Action Elements:

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.

7.3 Development (ADV)

INFORMAL FUNCTIONAL SPECIFICATION (ADV_FSP.1)

Developer Action Elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and Presentation of Evidence Elements:

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.

Evaluator Action Elements:

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.

DESCRIPTIVE HIGH-LEVEL DESIGN (ADV_HLD.1)

Developer Action Elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and Presentation of Evidence Elements:

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 of the subsystems of the TSF are externally visible.

Evaluator action elements

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.

INFORMAL CORRESPONDENCE DEMONSTRATION (ADV_RCR.1)

Developer Action Elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and Presentation of Evidence Elements:

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.

Evaluator Action Elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence**.**

7.4 Guidance Documents (AGD)

ADMINISTRATOR GUIDANCE (AGD_ADM.1)

Developer Action Elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and Presentation of Evidence Elements:

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 behavior 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.

Evaluator Action Elements:

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

USER GUIDANCE (AGD_USR.1)

Developer Action Elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and Presentation of Evidence Elements:

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 behavior 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.

Evaluator Action Elements:

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

7.5 Life Cycle Support (ALC)

FLAW REPORTING PROCEDURES (ALC_FLR.2)

Developer action elements:

ALC_FLR.2.1D The developer shall provide flaw remediation procedures addressed to TOE developers.

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

ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users.

Content and presentation of evidence elements:

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

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

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

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

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

ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

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

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

Evaluator action elements:

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

7.6 Tests (ATE)

EVIDENCE OF COVERAGE (ATE_COV.1)

Developer Action Elements:

ATE_COV.1.1D The developer shall provide evidence of test coverage.

Content and Presentation of Evidence Elements:

ATE_COV.1.1C The evidence of test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator Action Elements:

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

FUNCTIONAL TESTING (ATE_FUN.1)

Developer Action Elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and Presentation of Evidence Elements:

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.

Evaluator Action Elements:

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

INDEPENDENT TESTING – SAMPLE (ATE_IND.2)

Developer Action Elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and Presentation of Evidence Elements:

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.

Evaluator Action Elements:

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.

7.7 Vulnerability Assessment (AVA)

EXAMINATION OF GUIDANCE (AVA_MSU.1)

Developer action elements:

AVA_MSU.1.1D The developer shall provide guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.1.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.1.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.1.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.1.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

Evaluator action elements:

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

AVA_MSU.1.2E The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.1.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

STRENGTH OF TOE SECURITY FUNCTION EVALUATION (AVA_SOF.1)
[CCIMB 051]

Developer Action Elements:

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.

Content and Presentation of Evidence Elements:

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.

Evaluator Action Elements:

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.

DEVELOPER VULERABILITY ANALYSIS (AVA_VLA.1)

Developer Action Elements:

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

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

Content and Presentation of Evidence Elements:

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.

Evaluator Action Elements:

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.

.

8 TOE Summary Specification

The TOE Summary Specification TSS presents a high level, and non-proprietary, look at how the product meets the functional and assurance requirements described in the previous sections.

8.1 TOE Security Functions

8.1.1 Security Audit (FAU)

The ASG records the following events: the startup-shutdown of TOE functions, all TOE transactions as specified by the SFP including accessing ASG via ASG Management GUI, successful TOE configuration changes, addition/deletion/modification of user accounts, unsuccessful login attempts, and the lockout of user accounts.

The ASG generates three different types of logs: system logs, application logs, and a configuration audit log, which is a specific type of application log. **System logs** list system messages and log the low level system actions (e.g., starting up, shutting down, handled exceptions, etc.) that are related to ASG maintenance, but that are not security relevant.

System logs may be accessed via the Monitor/Reports interface reporting functionality. The system logs report on system activities and maintenance such as starting up, shutting down, loading configuration, etc. show the following parameters:

- Date and time of the event
- Type of event (category or activity occurring)
- Action performed
- Success or error messages

Application logs handle events gathered from the Actional Security Gateway(s) and are applicable only to the Information Flow Control FSP. This includes application security-related message processing events (e.g., request encrypted, failed to authenticate requestor, response received, etc). Authorized administrators can configure auditable event actions to fire when processing messages between Service Requestors and Web Services. Application logs show the following parameters (which meet the security functional requirements addressed by the generation of audit records):

- LogEvent Name – a unique name for the given LogEvent action;
- Level – critical, error, warning, info, debug, or trace;
- Message – a user-readable text message; and
- Properties – the context properties associated by default with the given LogEvent action.

The outcome attribute within Application logs is determined by the content of the audit records themselves.

An application log starts out as an *active log*[3], with its specifications defined in the *xmsrt.properties* file for the given Actional Security Gateway. A given Gateway's active log files will be rotated[4] either when reaching the specified log file size or on demand from an ASG Manager. At that point the log file will be copied to another file. The active log file is emptied and is then ready to receive new data.

When a user request to *pull*[5] a log file is issued (manually or via a scheduled job), the log file is transferred to a log repository which is stored and maintained on the operating environment of the ASG Manager. Actional Security Gateway logs are written to the ASG Manager upon the *pull* request. Prior to the *pull* request, log files remain resident on the Actional Security Gateway. Application logs may then be accessed via the Monitor/Report interface;

[3] An active log is a temporary log in the process of being written to an Actional Security Gateway.
[4] A rotated log is a permanent log file that has been copied from the active log.
[5] A pulled log is a rotated log that has been moved to a log repository, from which it can be accessed via the ASG Manager.

The configuration audit logs contain information on administration actions performed on the ASG Manager. It tracks and displays activites such as: unsuccessful login attempts, successful login attempts (access to TOE), user locks out, successful add/delete/modify of TOE configuration changes of TOE objects and successful add/modify/delete of user accounts. For each audit event it lists:

- Name of object modified, created, deleted
- Type of object modified, created, deleted
- The action performed on the object
- Identity of user who performed the auditable event
- Date and time of auditable event

The Root Administrator and Security Administrator can review audit logs in the ASG Manager. When a request is made to the ASG to view an audit log, a report is made by the ASG Manager and displayed to the administrator in a human-readable text format (i.e., a report in the form of a formatted Web page). The audit review feature can be used to order the ASG Manager System audit records.

Audit logs are viewable by authorized administrators of the ASG.

Audit data records are stored on a database that is located outside of the TOE boundary. System logs, recording ASG Manager events and configuration changes, are stored in a relational database. The database is an SQL database that communicates with the ASG Manager through the use of SQL commands. Although the database is external to the TOE, it is located on the same trusted network on which the TOE resides. Application logs, which store audit records relevant to the examination of the ASG message stream, are stored in flat files in the file system.

Meets Functional Requirements: FAU_GEN.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.1

8.1.2 Cryptographic Support (FCS)

The ASG verifies signatures by performing XML digital signature verification using DSA/RSA key information provided in the signature and XML Encryption using DES/3DES/AES/RSA.Cryptography is implemented by ASG on the Actional Security Gateway. The Actional Security Gateway manages (generation, distribution, recovery, and rotation) keys for the ASG system. Component cryptographic key destruction is implemented by the Actional Security Gateway. The Actional Security Gateway only encrypts messages upon request. The Actional Security Gateway decrypts all relevant XML encrypted files by default.

The ASG Manager manages the relationships between encryption/decryption/signing entities. The ASG Manager maintains a directory listing of keystores which house Java Key Stores and/or XKMS keystores. The ASG Manager maintains a directory listing of keystores and their location, while the Actional Security Gateway uses the keys identified in the directory listing. The ASG Manager *pushes* configuration (i.e. wsdl.xml) settings (inclusive of keystore directory listings) to the Actional Security Gateway. The Actional Security Gateway retrieves applicable configuration information and applies encryption/decryption/signing as specified.

The Actional Security Gateway generates cryptographic keys by leveraging the Java Cryptography Extension (JCE). JCE is resident within the Actional Security Gateway both physically and logically. Within JCE, several key generation, distribution, recovery, and rotation components exist to facilitate the key management system. JCE uses the following algorithms to generate keys: AES (128 bits), DES (64 bits), 3DES (3x64 bits). Algorithm type for key generation is specified by the administrator and in accordance with the organizational security policy.

The Actional Security Gateway leverages memory dumping aspects of Java technologies to perform key destruction. JCE facilitates the destruction of keys. When the respective application server completes its usage of the keys, all keys in memory are deleted by Java's garbage collector.

JCE supports encryption and decryption security functionality by generating public (AES, 3DES, DES) and private (RSA) keys. JCE supports cryptographic checksum computation and verification by employing the SHA-1 cryptographic algorithm. JCE supports secure hash computation and verification by employing the HMAC SHA-1 cryptographic algorithm.

Meets Functional Requirements: FCS_CKM.1, FCS_CKM.4, FCS_COP.1

8.1.3 User Data Protection (FDP)

In order to gain access to the administrative functions of the ASG, the RBAC SFP is enforced. A user must authenticate to the ASG before they are able to perform any administrative action. Based on the user's authentication credentials and the RBAC SFP, ASG explicitly denies/allows access of the users to certain ASG functions.

Access control to the ASG is accomplished through role based access control which utilizes authentication mechanisms to identify the role of the user as described in section 8.1.5 below. Roles are created with permissions to certain objects (i.e. the ASG Manager and Actional Security Gateway) within the ASG system, and only users with the proper authorization and permissions will be allowed to access certain parts of the ASG.

Meets Functional Requirements: FDP_ACC.1, FDP_ACF.1

8.1.4 Identification and Authentication (FIA)

ASG usernames, passwords, and the role of the ASG Administrators are maintained by the ASG Manager (stored in a database). Usernames and passwords are associated to the user as an identification mechanism. A user is identified to the ASG Manager through the use of an ASG username. Combined with a password, this information is used to identify and authenticate each user before allowing any other action to be taken regarding managing the ASG on behalf of the user.

The role of the user is the user-subject binding that is associated with the subject acting on behalf of the user. A user logs into the ASG Manager providing a username and password. The authentication credentials are mapped to what is stored in the database and if the mapping is valid, a subject is created which acts on behalf of the authenticated user and is granted access to operations/views within the ASG based on the role the user is assuming. The permissions associated with the authenticated user's role are inherited by child processes of the initial process.

Before any security-relevant action can be performed, the user attempting the action must successfully identify and authenticate to the ASG Manager. If the identification and authentication credentials provided by the user do not match a user account in the authentication directory, the user will not be allowed access to the ASG Manager. If the user is able to authenticate to the ASG Manager successfully, he will be allowed access to the functions permitted to him by the role(s) and specific permissions configuration that he is assuming.

A user is permitted a specified fixed number of successive unsuccessful authentication attempts; this limit is set by an authorized ASG Administrator (Root Administrator or Console User Administrator) who is administering the machine on which the ASG Manager is installed. The capability of the authorized Administrator to alter the limit of successive unsuccessful authentication attempts is handled during the installation of the TOE and requires a re-boot of the TOE to take effect. This is a global lockout parameter that applies to all users of the ASG Manager. Once this limit is reached, the ASG Manager will no longer accept identification and authentication attempts for that username; the account is locked out. After an account has been locked it will not be accessible until a different authorized ASG Administrator unlocks the account.

For Service Requestor to Web Service traffic, administrators can require authentication and set limits on the number of failed authentication attempts. If the information flow FSP requires authentication and limits the number of unsuccessful attempts, the service requestor will be required to authenticate. If the number of unsuccessful attempts is reached, the account is disabled on the gateway (blacklisted). Removal from the blacklist requires an authorized TOE administrator.

Meets Functional Requirement: FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FIA_USB.1

8.1.5 Security Management (FMT)

Actional has implemented a flexible permissioning system in the ASG Manager that is based on roles. An unlimited number of roles can be defined with each role having its own set of permissions attached to it. Six types of users exist on the ASG: Root Administrator, Publisher, Security Administrator, Gateway Administrator, Console Administrator, Console User Administrator. An ASG account is already set up when the system is delivered to the customer. The account has the role of Root Administrator which is the highest level of administrator for the ASG and has access to all ASG functions. By definition, this individual has the highest level of privileges/permissions. Through the use the Root Administrator, other user accounts may be created that have administrative access to certain parts of the ASG; these are the ASG Admins[6]. All other ASG Administrators (i.e., anyone who has authorized access to the ASG Manager) function under the admin roles (level of privilege) defined for them by the Root Administrator.

In addition to the Root Administrator, the following preconfigured admin roles are on the ASG by default:

- Publisher;
- Security Administrator;
- Gateway Administrator;
- Console Administrator; and
- Console User Administrator.

Management of the ASG is role-based. A role is a set of rules that either gives or denies access to certain ASG management functions. When a user account is created, it is associated with a role that provides the permissions and is also associated with a user who is able to access the ASG Manager with that user account. User's may be associated with one or more role(s). The basic building blocks of admin roles are *permissions* – that is, actions performed by the admin role. Any permissions (from the ASG Manager's list of all available permissions) may be added to, or deleted from, the initial preconfigured Admin Roles or to whatever new Admin Roles are created.

When a role is created, the ASG Administrator creating the role will either restrict or allow access to functions used to modify audit data generation and other ASG configuration and administration activities.

The TSF is capable of performing access control, authentication, and audit control. Authentication to the ASG Manager is handled through the use matching user credentials (username and password) against the database. Access control is provided through the use of this authentication mechanism. If a user is not authenticated, they are not capable of accessing the ASG Manager. Audit control is enforced by privileges that are assigned to a specific user.

The ASG system comes with several pre-defined roles that are ready to be assigned to users of the system.

The Admin category contains the Root Administrator which is the highest level of administrator. The Root Administrator has complete control over all aspects of the ASG. The following table lists the other pre-defined administrator roles and each role's corresponding responsibilities.

[6] In Westbridge terminology, any authorized user who is not assigned to the role of Superuser is referred to as an ASG Administrator.

Table 11 – Pre-Defined Administrator Roles

Pre-Defined Role	Responsibilities
Publisher	The Publisher Administrator Role is responsible for publishing services and operations within the ASG: • Push configurations to non-production Gateways. • Create Operation Groups • Edit, enable, and change states
Security Administrator	The Security Administrator Role is responsible for maintaining and checking security within the ASG: • Viewing the audit trail • Creating, deleting, editing, enabling, and disabling authentication directories • Creating, deleting, editing Keystores • Editing, enabling, and disabling processing steps • Creating, deleting, editing, enabling, disabling, and reordering rules • Creating, deleting, editing, enabling, and disabling service requestor roles • Release lock
Gateway Administrator	The Gateway Administrator Role is responsible for maintaining and working with Actional Security Gateways (runtime servers) • Creating, deleting, editing monitoring enabling, and disabling Actional Security Gateway • Push configuration to non-production / production Actional Security Gateways • Pull configuration changes from the Actional Security Gateway into ASG Manager • Pull/View system logs • Clear Actional Security Gateway statistics • Edit, delete, enable, disable scheduled job • Create, edit, delete task • Start/Stop scheduler
Console Administrator	• Save ASG Manager configuration to disk at the distribution of the configuration • Restore console configuration from disk
Console User Administrator	• Create, edit, delete administrator role • Assign user to role • Create, edit, delete administrator user • Release Lock

Actional has implemented a Service Requestor role, . An authorized administrator can define Service Requestor roles which are groups of external service consumers who have permission to access a given set of base web service views and operations. A service requestor is a person or a service requesting a web service. If a service requestor fails authentication or authorization, the request is rejected and an appropriate error message is returned to the service requestor.

The ability to query the ASG audit records is restricted by the TSF to authorized administrators or admin roles (root administrator and security administrator).

Meets Functional Requirements: FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

8.1.6 Protection of the TOE Security Functions (FPT)

The log timestamp used by the TOE for audit data generation is system-generated and is not directly user-readable. The ASG software retrieves the time from the operating system and uses this to time-stamp audit records.

When a user authenticates to the ASG Manager, they assume the role that has been assigned to their account. Their role has certain permissions regarding functions that the ASG can execute. If a user attempts to access a functionality that is beyond the permissions that are granted to the user through the role they are assuming, they will not be permitted to execute the function.

As network traffic enter and exit the Actional Security Gateway through the network interface, there are rules being applied to packets. When an incoming packet is scanned and an associated rule matches the packet which a rule applies to, the rule is enforced before the packet can proceed past the Actional Security Gateway.

Meets Functional Requirements: FPT_RVM.1, FPT_STM.1

8.1.7 XML Message Server Requirements (XMS)

Messages can be checked for well-formedness, content and for malicious attacks. Messages can be blocked or transformed to remove malicious content or remove other parts of the message based on the findings of the message checks.

The ASG performs four different types of validations on all messages being sent throught the ASG. They are: schema validations, DTD validations, signature verification, and content inspection. Setting up the ASG to perform schema validations can be done manually or automatically. Document Type Definition (DTD) has been replaced by SOAP and XML schema; however, there are some legacy servers that still require this type of authentication. In order to maintain complete robustness across the industry, the ASG also provides DTD validation. The ASG verifies signatures by performing XML digital signature verification using DSA/RSA key information provided in the signature. The ASG encrypts messages by performing XML encryption using DES/3DES/AES/RSA.

Additionally, the ASG can check that certain elements that require a signature were signed. If the ASG is unable to validate the signature or a signature is required but not included, the message can be rejected by the ASG, alerts can be sent to the appropriate destination, or other actions can be performed.

The ASG is able to create an abstraction layer for each Web service for manageability and usability purposes that can be used to match requirements of a Web Service consumer calling that Web Service. For the sake of security, the ASG has the ability to hide URLs and backed resources from a service requestor. The determination to hide information from a particular requestor is made by an administrator. Parts of the URLs can be modified to ensure publishing control of the URLs to the Service consumer. Another Service View function is that an ASG Administrator can opt to present only selected operations that are pertinent to the requesting service consumer, thus hiding any sensitive services from that consumer's view.

The ASG has been designed to handle many different standards for traffic on the XML Message Stream. The following table lists the different types of standards and the specific standards the ASG supports.

Meets Functional Requirements: FDP_IFF.1, XMS_VEW.1, XMS_SUP.1, XMS_MAP.1, FDP_IFC.1

Table 12 – Standards Supported by the ASG

Type of Standard	Specific Standard
Services	XML SOAP WSDL UDDI

Type of Standard	Specific Standard
Transport	HTTP HTTPS (SSL) JMS MQ
Signature	XML Signature RSA-SHA1 DSA-SHA1
Encryption	XML Encryption 3DES, AES, RSA using 128/192/256 bit keys
Authentication/Access Control	SAML LDAP HTTP based authentication Active Directory X.509 Certificates
PKI Support	XKMS OCSP PKCS #7, #10, #11, #12 CRL
Other	WS-Security 1.0 XML Schema 1.0 XPath 1.0 XSLT

The ASG is capable of mapping credentials to a username and password from the following Authentication Services: Username/Password, LDAP, Active Directory, and X.509 Certificates to a username/password. Credentials are mapped to provide authentication on service requestors in the ASG deployed environment. Service requestor credentials are stored in authentication directories. Each time a service requestor requests a service on the ASG deployed environment, that service requestor must be identified and authenticated. If null/invalid credentials are supplied by the service requestor, the service requestor is denied access to the requested service. No additional code needs to be added for this mapping to be performed. If an incoming XML message contains certain credentials, they can be compared to either of the four authentication mechanisms compatible with the ASG and mapped to a username/password credential.

Meets Functional Requirements: XMS_SAN.1.1, XMS_CHK.1.1, XMS_CHK.1.2, XMS_SUP.1.1, XMS_VEW.1.1, XMS_MAP.1.1

8.2 TOE Security Assurance Measures

This section of the ST maps the assurance requirements for a CC EAL 2 augmented to the assurance measures used for the development and maintenance of the TOE. Table 13 provides a mapping of the appropriate documentation to the assurance requirements.

The TOE was developed with the following security assurance measures in place, which constitute a CC EAL 2 augmented level of assurance:

- Configuration Management
- Delivery and Operation
- Development
- Guidance Documentation
- Testing
- Vulnerability Assessment

Table 13 – Assurance Measures Mapping to Security Assurance Requirements (SARs)

CC Assurance Components	Actional Assurance Measures
ACM_CAP.2 Configuration items	XML Web Services Management and Security Solution XML Message Server Configuration Management
ADO_DEL.1 Delivery procedures	XML Web Services Management and Security Solution XML Message Server Secure Delivery and Installation
ADO_IGS.1 Installation, generation, and start-up procedures	XML Web Services Management and Security Solution XML Message Server The XML Message Server Installation Guide Version 3.1 The XMS Appliance Installation Guide Version 3.1 XMS Release Notes Guide Version 3.1
ADV_FSP.1 Informal functional specification	XML Web Services Management and Security Solution XML Message Server Functional Specification
ADV_HLD.1 Descriptive high-level design	XML Web Services Management and Security Solution XML Message Server High-Level Design
ADV_RCR.1 Informal correspondence demonstration	XML Web Services Management and Security Solution XML Message Server Informal Correspondence Analysis
ADV_SPM.1 Informal TOE security policy model	XML Web Services Management and Security Solution XML Message Server Informal TOE Security Policy Model
AGD_ADM.1 Administrator guidance	Getting Started with XMS: Advanced Topics Version 3.1 Getting Started with XMS: Basic Administration Version 3.1.1 The XMS Administrative Guidance Supplement Version 3.1 The XMS Message Server Reference Guide Version 3.1.1
AGD_USR.1 User guidance	The XMS Release Notes Guide Version 3.1
ALC_FLR.2 Flaw reporting procedures	Actional Corporation. XML Web Services Management and Security Solution XML Message Server Flaw Remediation Procedures
ATE_COV.1 Evidence of coverage	XML Web Services Management and Security Solution XML Message Server XML Message Server Test Plan

CC Assurance Components	Actional Assurance Measures
ATE_FUN.1 Functional testing	. XML Web Services Management and Security Solution XML Message Server Westbridge XMS Test Procedures: per Test Procedure: GEN1, SAR3, IFC1, IFF1, AFL1, COP1, ATD1, UAU2, UID2, MOF1, MSA3, MTD1, SMR1, RVM1, VEW1, SUP1, MAP1
ATE_IND.1 Independent testing	Evaluation Laboratory Test Report
AVA_MSU.1 Examination of guidance	
AVA_SOF.1 Strength of TOE security function evaluation	XML Web Services Management and Security Solution XML Message Server XML Message Server Vulnerability Assessment
AVA_VLA.1 Developer vulnerability analysis	XML Web Services Management and Security Solution XML Message Server XML Message Server Vulnerability Assessment

8.3 TOE Strength of Function Claims

"The TOE requires that the minimum password length used to authenticate an entity acting in the Superuser role be a minimum of 5 alpha characters (case sensitive) and 1 numeric character. The Superuser can set password requirements for other XMS Manager users but, for the purposes of this evaluation, none of those requirements should be weaker than those imposed on the Superuser."

9 Rationale

This section provides the rationale for the selection of the security requirements, objectives, assumptions, and threats. In particular, it shows that the security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

9.1 RATIONALE FOR IT SECURITY OBJECTIVES

This section provides a rationale for the existence of each assumption and threat that compose this ST. Table 14 demonstrates the mapping between the assumptions and threats to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption and threat.

A.DBPROT The database used by the TOE for ASG Manager audit storage will be located on a Trusted network to prevent unauthorized tampering and modification of audit records.

The O.DBPROT objective ensures that the database used by the TOE for audit storage will be located on a trusted network to prevent unauthorized tampering and modification of audit records.

A.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or application) on the machine on which the TOE resides.

The O.INSTAL and O.PERSON objectives ensure that those responsible for the TOE are trained in proper IT security procedures and policies and will install, manage, and operate the TOE in a manner that is consisted with those procedures and policies.

A.PUBLIC The machine on which the TOE resides does not host public data.

The O.INSTAL and O.PERSON objectives ensure that those responsible for the TOE are trained in proper IT security procedures and policies and will install, manage, and operate the TOE in a manner that is consisted with those procedures and policies.

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

The O.PHYCAL provides for the physical protection of the TOE hardware and software.

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

The O.PHYCAL provides for the physical protection of the TOE.

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

The O.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

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

The O.INSTAL objective ensures that the TOE is properly installed and operated. The O.PERSON objective ensures that authorized administrators are not careless, willfully negligent, or hostile and follow instructions provided by the TOE documentation.

A.NOTRST The TOE can only be accessed by authorized users.

The O.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.

A.TIME The operating environment of the TOE will provide a reliable timestamp.

The O.TIME objective provides a reliable time stamp for the TOE.

A.SECSTR The key store used by the TOE for x.509 certificate and key storage will be placed within the trusted network to protect certificates and keys from tampering.

The O.SECSTR objective ensures that the key store used by the TOE for x.509 certificate and key storage will be located on a trusted network to prevent unauthorized tampering and modification.

T.NOAUTH An unauthorized user may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

The O.IDAUTH objective removes this threat by providing a means for authentication, effectively mitigating against bypassability. The O.ACCESS objective provides access control enforcement by allowing only users with applicable access to the requested TOE functions. The O.SELPRO objective also counters this threat by requiring that the TOE be able to protect itself against bypass attempts by unauthorized users. The O.SECFUN also provides for only authorized administrators being able to access security-relevant functions of the TOE. The O.CRYPTSTD, O.CRYKEY, O.COMM, and O.SUPPOR objectives provide additional PKI authentication technologies.

T.ATKPOT An unauthorized user may attempt to circumvent TOE security functions using obvious vulnerabilities.

The O.SELPRO objective mitigates this threat by ensuring that the security functions of the TOE are not capable of being circumnavigated.

T.AUDFUL An unauthorized user may attempt to exhaust storage capacity in effort to lose audit records and prevent future audit records from being recorded.

The O.PERSON objective mitigates this threat by ensuring that, if audit storage capacity is exhausted, a trained, authorized administrator will take appropriate actions to restore audit storage capability.

T.BRUTEF An unauthorized user may attempt a brute force attack in which authentication data may be repeatedly guessed in order to gain access to the TOE and/or its data.

The O.SELPRO objective diminishes this threat by providing that the TOE can protect itself against attempts by unauthorized users to bypass, modify, deactivate, circumvent, or tamper with TOE security functions (e.g., by locking out a user account after three unsuccessful identification and authentication attempts has been reached). The O.AUDITS objective provides that the TOE will create an audit log to store number of unsuccessful logins. The O.IDAUTH objective ensures that successful authentication is necessary to access TOE data. The O.SUPPOR objective by provides the (PKI) authentication mechanisms to authenticate against.

T.MASQUE An unauthorized user may attempt to capture identification and authentication data to use for the purpose of masquerading as an authorized administrator of the TOE.

The O.SUPPOR objective effectively removes this threat by providing PKI authentication and encryption technologies which effectively prohibit capture of identification and authentication data

for the use of administrator spoofing. The O.AUDITS objective removes this threat ensures that all events are audited. Effective management and review of these audit records by trained authorized administrators is covered by the O.EADMIN objective.

T.REMATK An unauthorized user may attempt to view, modify, and/or delete sensitive and/or security-related information that is sent between a remotely located authorized administrator and the TOE.

The O.REMATK objective removes this threat by ensuring that transmitted data is protected from unauthorized users.

T.FACCNT An unauthorized user may attempt to access TSFs invoking security functions that may go undetected.

The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.

T.COMINT An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

O.CRYPTSD objective mitigates this threat by ensuring the integrity of audit specific data via authentication encryption mechanisms. The O.CRYKEY, O.COMM, and O.SUPPOR objectives provides additional PKI encryption and authentication technologies which verify the integrity of data. The O.IDAUTH objective mitigates this threat by providing the authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.SELPRO objective addresses this threat by providing TOE self- protection.

T.LOSSOF An unauthorized user may attempt to remove, destroy, or corrupt data stored by the TOE.

O.CRYPTSD objective mitigates this threat by ensuring the integrity of audit specific data via authentication encryption mechanisms. The O.IDAUTH objective removes this threat by providing for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.SELPRO objective addresses this threat by providing TOE self- protection. The O.CRYKEY, O.COMM, and O.SUPPOR objectives provide additional PKI encryption technologies which prevent corruption of data.

T.NOHALT An unauthorized user may attempt to compromise the continuity of the TOE's functions by halting execution of the TOE.

The O.IDAUTH objective removes this threat by prohibiting access of TOE functions when unsuccessful authentication occurs. The O.ACCESS objective accompanies O.IDAUTH by allowing for only authorized users to access TOE functions. The O.NOCONF objective provides that only authorized users may alter TOE execution.

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

The O.IDAUTH objective removes this threat by prohibiting access of TOE functions when unsuccessful authentication occurs. The O.NOCONF objective further mitigates this threat by providing that only authorized users may edit the TOE configuration. The O.PHYCAL objective ensures the physical protection against unauthorized physical configuration.

T.GOTHRU An unauthorized user may attempt to distribute malicious information or messages to pass through the TOE.

The O.SANITZ objective mitigates this threat by ensuring that malicious information is detected and messages are appropriately sanitized or handled.

T.NOVALD An unauthorized user may cause the XML messages passing through the TOE to not be checked for well formed structure validation.

The O.MSGVAL objective removes this threat by ensuring that the TOE can perform multiple types of message validations.

Table 14– Relationship of Security Environment to Objectives

– Relationship of Security Environment to Objectives

	O.EADMIN	O.ACCESS	O.IDAUTH	O.AUDITS	O.SECFUN	O.SELPRO	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.SANITZ	O.SECSTR	O.MSGVAL	O.REMATK	O.NOCONF	O.DBPROT	O.COMM	O.CRYKEY	O.CRYPTSD	O.TIME	O.SUPPOR
A.GENPUR							X			X											
A.PUBLIC							X			X											
A.PROTCT								X													
A.LOCATE								X													
A.MANAGE										X											
A.NOEVIL							X			X											
A.NOTRST								X	X												
A.DBPROT																X					
A.TIME																				X	
A.SECSTR												X									
T.NOAUTH		X	X		X	X											X	X	X		X
T.ATKPOT						X															
T.AUDFUL										X											
T.BRUTEF			X	X		X															X
T.MASQUE	X			X																	X
T.REMATK														X							
T.FACCNT				X																	
T.COMINT		X	X			X											X	X	X		X
T.LOSSOF		X	X			X											X	X	X		X
T.NOHALT		X	X												X						
T.IMPCON			X					X							X						
T.GOTHRU											X										
T.NOVALD													X								

9.2 RATIONALE FOR SECURITY OBJECTIVES FOR THE ENVIRONMENT

The purpose for the environmental objectives is to provide protection for the TOE that cannot be addressed through IT measures. The defined objectives provide for physical protection of the TOE, proper management of the TOE, and interoperability requirements on the TOE. Together with the IT security objectives, these environmental objectives provide a complete description of the responsibilities of TOE in meeting security needs.

Because several of the security objectives for the environment are not IT in nature, they need only be mapped to security assurance requirements (SARs). They do not need to be mapped to security functional requirements (SFRs). Security objectives for the environment that are not IT in nature are:

O.INSTAL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

O.PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

O.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.

O.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE and are not careless, willfully negligent, or hostile and follow instructions provided by the TOE documentation.

These objectives are satisfied by procedural or administrative measures. Thereby, each of these objectives is addressed by the TOE installation, administrator and user guidance (ADO_IGS, AGD_ADM, and AGD_USR) .

9.3 RATIONALE FOR SECURITY REQUIREMENTS

This section demonstrates that the functional components selected for this ST provide complete coverage of the defined security IT objectives. The mapping of components to security IT objectives is depicted in the following table. Please note: of the environment objectives only IT environment objectives are mapped to SFRs.

This table assumes that for functional requirements with iterations, that unless explicitly noted, that all iterations within a functional requirement map to the same IT objectives.

Table 15 – Mapping of Functional Requirements to IT Objectives

	O.EADMIN	O.ACCESS	O.IDAUTH	O.AUDITS	O.SECFUN	O.SELPRO	O.SANITZ	O.MSGVAL	O.DBPROT	O.REMATK	O.NOCONF	O.TIME	O.COMM	O.CRYKEY	O.CRYPTSD	O.SUPPOR
FAU_GEN.1	X			X												
FAU_SAR.1				X												
FAU_SAR.3	X			X												
FAU_STG.1									X							
FCS_CKM.1													X	X	X	
FCS_CKM.4													X	X		

	O.EADMIN	O.ACCESS	O.IDAUTH	O.AUDITS	O.SECFUN	O.SELPRO	O.SANITZ	O.MSGVAL	O.DBPROT	O.REMATK	O.NOCONF	O.TIME	O.COMM	O.CRYKEY	O.CRYPTSD	O.SUPPOR
FCS_COP.1										X			X		X	
FDP_ACC.1		X									X					
FDP_ACF.1		X														
FDP_IFF.1							X	X								
FDP_IFC.1							X	X								
FIA_AFL.1						X										
FIA_ATD.1			X								X					
FIA_UAU.2		X	X			X										
FIA_UID.2		X	X			X										
FIA_USB.1	X	X	X		X	X					X					
FMT_MOF.1	X	X			X	X					X					
FMT_MSA.1(1)		X			X						X					
FMT_MSA.1(2)		X			X											
FMT_MSA.2														X	X	
FMT_MSA.3(1)					X	X					X					
FMT_MSA.3(2)					X	X										
FMT_MTD.1	X	X														
FMT_SMF.1	X															
FMT_SMR.1		X			X	X										
FPT_RVM.1	X					X							X			
FPT_STM.1				X								X				
XMS_VEW.1	X															
XMS_MAP.1								X								
XMS_SUP.1																X

The following discussion provides detailed evidence of coverage for each security objective.

O.EADMIN The TOE shall include a set of functions that allow effective management (inclusive of audit) and maintenance of its functions and data by authorized users and administrators.

The TOE contains a set of functions which must be manually configured to generate audit records. Audit mechanisms are manually configured by a TOE administrator. Based upon the security functional policy, audit mechanisms will return the specified logged security function events. The central audit configuration mechanism is the ASG Manager. Configuration of audit includes the pulling of logs from the Actional Security Gateway and the customization of reports to facilitate sorting and viewing of audit data. This functionality is invoked within the ASG Manager. [**FAU_GEN.1**]. Query and review functionality of audit records is restricted to authorized administrators [**FMT_MTD.1**]. The TOE provides management of security attributes, audit data, and configuration of security functionality which are managed by a TOE administrator in accordance with the security functional policy [**FMT_SMF.1]**. TOE audit data can be ordered from the ASG Manager (via the ASG Management GUI) facilitating the review and management of audit data [**FAU_SAR.3**]. Moreover, security functional behavior of the TOE is restricted to authorized administrators [**FMT_MOF.1**]. Authorized administrators' ability to perform functionality within the TOE is restricted to the permissions defined by their specific user role. These permissions are associated with the admin user's role and are inherited by child processes of the initial process within the TOE. [**FIA_USB.1**]. Enforcement functions (e.g. identification & authentication procedures) are invoked and succeed before prior to User data protection. User data protection is invoked and succeeded prior to Security Management. Security Management is invoked before any other function is allowed to proceed [**FPT_RVM.1**] The TOE also provides

authorized users to block specified web services and resources lower-level users (i.e., service requestors) [**XMS_VEW.1**].

O.ACCESS The TOE shall allow authorized users to access only TOE functions and data that are allowed per each user's assigned role.

Users authorized to access the TOE are defined using an identification and authentication process and only users who successfully complete the identification and authentication process may access any security functions of the TOE [**FIA_UAU.2, FIA_UID.2**]. The TOE is required to provide and enforce the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE. The notion of roles in the TOE further ensures that users of the TOE may only access those functions that area accessible to that user's assigned role [**FMT_MOF.1, FMT_MTD.1**]. Moreover, administrative roles are predefined by the TOE to provide enhanced enforcement of access control to TOE functions [**FMT_SMR.1**]. The RBAC SFP is enforced on all users attempting to access administrator-level activities and all other activities based on User Role [**FDP_ACC.1, FDP_ACF.1**]. The User role is the security attribute associated with subjects acting on behalf of users [**FIA_USB.1**]. The TOE enforces the RBAC SFP and the information flow control FSP to restrict the ability to modify the permissions to a subset of authorized administrators. [**FMT_MSA.1**]. Furthermore, the TSF enforces the RBAC SFP to restrict modifications of security attributes and set default values for security attributes.

O.IDAUTH The TOE shall be able to identify and authenticate the claimed identity of all users prior to allowing access to TOE functions and data.

Attributes are maintained for each user of the TOE; these include the role of the user, the authentication mechanism required for the user to authenticate, and whether the login for the user is currently permitted [**FIA_ATD.1**]. The role of the user is the security attribute associated with subjects acting on behalf of users [**FIA_USB.1**]. The TSF requires that each user be successfully identified and authenticated before any TSF-mediated actions can be performed [**FIA_UAU.2, FIA_UID.2**].

O.REMATK The TOE shall be able to protect against unauthorized access to data transmitted.

Data transmitted to and from the TOE is protected by encryption. [**FCS_COP.1**]

O.NOCONF The TOE shall allow only authorized users to alter execution and/or TOE configuration.

The TOE requires each user to be successfully authenticated to verify their authorization [**FIA_UAU.2**]. Moreover, the TOE enforces the RBAC SFP [**FDP_ACC.1**] allowing only specified users to alter TOE execution and/or configuration [**FMT_MOF.1**]. The specification of the user is defined by the user role, where the subject inherits the exact set of privileges associated with the role of the user that the subject is acting on behalf of [**FIA_USB.1**] The TOE enforces the RBAC SFP to restrict the ability to modify the role permissions to a subset of authorized administrators. [**FMT_MSA.1(1)**]. Only authorized administrators are able to specify alternative initial values to override the default values when an object or information is created. [**FMT_MSA.3(1)**].

O.AUDITS The TOE shall provide a means to accurately detect, record, review, analyze, and act upon events in audit records.

Security-relevant events are defined and audited by the TOE [**FAU_GEN.1**]. The TOE generates audit logs for all TOE events. Moreover, invoking of any TOE security function is recorded as according to the security functional requirement. These audit logs are stored in a database and used for further analysis and review. Only authorized users of the TOE are permitted to access audit records, which are presented in a user-readable format [**FAU_SAR.1**]. These records can

also be ordered based on defined criteria for ease of review [**FAU_SAR.3**]. The TOE retrieves a reliable time stamp from the operating environment and applies that timestamp to audit records [**FPT_STM.1**].

O.SECFUN The TOE shall provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

TOE Administrative roles (ASG Root Administrator, ASG Publisher, ASG Security Administrator, Actional Security Gateway Administrator, ASG Console Administrator, and ASG Console User Administrator)are defined within the ASG and each role had a defined set of actions with users assigned to that role are authorized to perform [**FMT_SMR.1, FIA_USB.1**]. The defined set of actions ASG users are authorized to perform are restricted RBAC SFP [**FMT_MOF.1**]. The TOE enforces the RBAC SFP and information flow control SFP to restrict the ability to modify the permissions to a subset of authorized administrators. [**FMT_MSA.1**]. Only authorized administrators are able to specify alternative initial values to override the default values when an object or information is created. [**FMT_MSA.3**].

O.SELPRO The TOE shall protect itself against unauthorized modifications and attempts by unauthorized users to bypass, modify, deactivate, circumvent, or tamper with TOE security functions.

The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [**FMT_MOF.1**]. TOE Security Functions are enforced by the RBAC SFP to provide restrictive default values for security attributes. Additionally, only authorized administrators are able to specify alternative initial values to override the default values when an object or information is created. [**FMT_MSA.3**]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [**FPT_RVM.1**]. The TOE will also prevent a user, entity, and/or unauthorized administrator from accessing the TOE if the TOE determines that a number of unsuccessful login attempts in series indicates a possible brute force attack [**FIA_AFL.1**]. The O.SELPRO objected is further supported in that all users must successfully identify and authenticate themselves to the TOE before they are allowed to proceed with any other action and the TSF maintains roles that are associated with individual users as well as authorized functions [**FIA_UAU.2, FIA_UID.2, FMT_SMR.1, FIA_USB.1**].

O.SANITZ The TOE shall be able to block and/or sanitize messages in the XML message stream to protect against malicious attacks.

Messages are sanitized by the TOE by scanning the messages for potential malicious information [**FDP_IFC.1**, **FDP_IFF.1**].

O.MSGVAL The TOE shall be able to perform message validations, including message integrity validation and schema validation checks.

Multiple validations are performed by the TOE on messages received: schema validations, DTD validations, and signature verification [**FDP_IFC.1**, **FDP_IFF.1**]. Username and password fields supplied within the message are validated that they are correctly formed and are mapped for the service requestor as messages pass through the TOE. Authentication of the service requestor to view/perform operations is determined based upon the credential combination (username/password) supplied by service requestor requesting access to a base service [**XMS_MAP.1**].

O.SUPPOR The TOE shall support multiple authentication standards for the XML Message Stream.

The TOE supports the following authentication standards: LDAP, X.509, Active Directory. HTTP Authentication, and PKI [**XMS_SUP.1**].

O.CRYPTSD The TOE must provide a choice of cryptographic algorithms and strengths based on key sizes with which to protect data.

The TOE provides encryption, decryption, and signs xml messages. The TOE uses RSA key exchange to facility the establishment of secure sessions [**FCS_COP.1**]. The TOE houses keys in an encrypted data store [**FMT_MSA.2**]. The TOE generates AES, DES, and 3DES keys [**FCS_CKM.1**].

O.CRYKEY The TOE shall ensure appropriate protection for cryptographic keys throughout their lifecycle, covering generation and destruction.

The destruction of keys is performed within the TOE by deleting them [**FCS_CKM.4**]. The TOE generates AES, DES, RSA, and 3DES keys [**FCS_CKM.1**]. The TSF protects all key values, which are used to protect security attributes [**FMT_MSA.2**].

O.COMM The TOE shall provide secure session establishment between the system components and remote systems using encryption functions.

The TOE uses RSA key exchange to facility the establishment of secure sessions. The TSFs provide encryption and decryption by facilitating the generation and destruction of cryptographic keys [**FCS_CKM.1**, **FCS_CKM.4**]. Additionally, the TOE provides a secure communication channel between itself and external TOE components utilizing SSL/TLS [**FCS_COP.1]**.

O.DBPROT The database used by the TOE for audit storage will be located on a trusted network to prevent unauthorized tampering and modification of audit records.

TOE audit records are stored in the database and protected from modification [**FAU_STG.1**].

O.TIME The host operating system shall provide a reliable timestamp the TOE can use for accurately tracking audit events.

The operating system provides reliable time stamps [**FPT_STM.1**].

9.4 RATIONALE FOR THE TOE SUMMARY SPECIFICATION

The following table represents a mapping between the security functions in this ST to their related TOE security functional requirements and provides a rationale for how each security function meets the corresponding security functional requirement.

This table assumes that for functional requirements with iterations, that unless explicitly noted, that all iterations within a functional requirement map to the same rationale.

Table 16 – Mapping of Security Functional Requirements to TOE Security Functions

SFR	Security function	Rationale
Functional Requirements for the TOE		
FAU_GEN.1	Security Audit	This SFR supports security audit by providing audit data generation for the ASG message stream as well as the ASG Manager.
FAU_SAR.1	Security Audit	This SFR supports security audit by providing the capability for ASG Administrators to view audit data from ASG. Further more, capability exists to define what audit information users are permitted to read, in the ASG Manager, and requiring that this information be presented in a manner that is conducive to the reader's interpretation. ASG Audit Review is generated by administration of the auditing configuration selection in the ASG Management GUI.
FAU_SAR.3	Security Audit	This SFR supports security audit by providing ordering capability of the audit data, in the ASG Manager, based on defined criteria for ease of management and use. ASG Selectable Audit Review is generated by administration of the auditing configuration selection in the ASG Management GUI.
FAU_STG.1	Security Audit	This SFR supports security audit by providing database protection of audit records ensuring that the IT Environment protects stored audit records from unauthorized deletion and prevent modifications to the audit records.
FCS_CKM.1	Cryptographic Support	This SFR supports cryptographic support by providing key generation, key destruction, and implemented key operation mechanisms.
FCS_COP.1	Cryptographic Support	This SFR supports cryptographic support by providing secure operations (encryption/decryption/signing) necessary for the establishment of secure sessions.
FDP_ACC.1	User Data Protection	This SFR supports user data protection by enforcing the access control policy within Table 7 (Access Control Policy) on the authentication directories, base operations, base services, data stores, reports, and all operations performed by ASG Administrators.
FDP_ACF.1	User Data Protection	This SFR supports user data protection by enforcing the access control policy within Table 7 (Access Control Policy) for the ASG Administrator based upon an authenticated user's associated role.
FDP_IFC.1	XML Message Server Requirements	This SFR supports user data protection by enforcing the Information Flow Control SFP on service requestors, messages and base services.
FDP_IFF.1	XML Message Server Requirements	This SFR supports user data protection by allowing the TOE to sanitize and validate messages through various means. The TOE performs several types of validations on all messages received and take appropriate actions (as defined) if a message is determined to not comply with set standards.
FIA_AFL.1	Identification and Authentication	This SFR supports identification and authentication by tracking the number of successive unsuccessful authentication attempts a user has tallied and, if this number reaches a pre-set limit, locking out this account until it is unlocked by an authorized administrator. This function is implemented by the Release Lock option in the ASG Management GUI.

SFR	Security function	Rationale
FIA_ATD.1	Identification and Authentication	This SFR supports identification and authentication by requiring that the TSF maintain security attributes (role of the user, authentication mechanism required for the user to authenticate, and whether the login for the user is currently permitted) that belong to individual users of the TOE. User Attributes are maintained by the database.
FIA_UAU.2	Identification and Authentication	This SFR supports identification and authentication by requiring the TSF to ensure that each user has successfully authenticated to the TOE before a user is allowed to perform any TSF-mediated action(s).
FIA_UID.2	Identification and Authentication	This SFR supports identification and authentication by requiring each user to be successfully identified before allowing the user to perform any other action.
FIA_USB.1	Identification and Authentication	This SFR supports identification and authentication by requiring that the TSF be able to associate user security attributes with subjects acting on behalf of a particular user.
FMT_MOF.1	Security Management	This SFR supports security management by restricting access to modify the behavior of or change the configurations of the security functions for the applicable ASG Administrator, and by restricting access to modify administrator accounts and the audit log of the ASG to the Root administrator..
FMT_MSA.1	Security Management	This SFR supports security management by restricting ability to modify the security attributes that effect the SFPs to the applicable ASG Administrator.
FMT_MSA.2	Security Management	This SFR supports security management by providing secure values for security attributes.
FMT_MSA.3	Security Management	This SFR supports security management by configuring the ASG Manager settings for the SFPs defined for the TOE.
FMT_MTD.1	Security Management	This SFR supports security management by restricting that management of the audit records to the applicable ASG Administrators.
FMT_SMF.1	Security Management	This SFR supports security management by providing mechanisms to enforce the restrictions stated in FMT_MOF.1, FMT_MSA.1 and FMT_MTD.1.
FMT_SMR.1	Security Management	This SFR supports security management by providing user and administrator roles (ASG Root Administrator, ASG Publisher, Actional Security Gateway Administrator, ASG Security Administrator, ASG Console Administrator, and ASG Console User Administrator)and associating each user with one of these pre-defined roles.
FPT_RVM.1	Protection of the TOE Security Functions	This SFR supports protection of the TOE security functions by ensuring that TSP enforcement functions (e.g. identification & authentication procedures) are invoked and succeed before any other function is allowed to proceed. Identification and Authentication is invoked before TOE access is allowed and more specifically TSF's of the TOE is allowed.
FPT_STM.1	Protection of the TOE Security Functions	This SFR supports protection of the TOE security functions by ensuring that the IT Environment be able to provide reliable time stamps for its own use (e.g., to time stamp audit records). Reliable time stamps are retrieved from the Java Virtual Machine and used principly for auditing functions.
Explicitly Stated Requirements for the TOE		

SFR	Security function	Rationale
XMS_VEW.1	XML Message Server Requirements	This SFR supports xml message server requirements by enabling an authorized user to hide information from the service requestor, if desired and to control the publishing of URL's
XMS_SUP.1	XML Message Server Requirements	This SFR supports xml message server requirements by supporting LDAP, Active Directory, X.509, HTTP authentication, and PKI standards.
XMS_MAP.1	XML Message Server Requirements	This SFR supports xml message server requirements by ensuring that the TOE can map credentials from Username/Password, LDAP, Active Directory, and X.509 certificates to Username/Password without adding additional code.

9.5 RATIONALE FOR ASSURANCE REQUIREMENTS

EAL2 augmented was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. At EAL2 augmented, the ASG will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The chosen assurance level was also selected to meet the vendor's customer requirements.

Configuration Management – The Configuration Management documentation provides a description of automation tools used to control the configuration items and how they are used at the Actional and vendor support development facilities. The documentation provides a complete configuration item list and a unique reference for each item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

Corresponding CC Assurance Components:

- Configuration Items

Delivery and Operation – The Delivery and Operation documentation provides a description of the secure delivery procedures implemented by Actional to protect against TOE modification during product delivery. The Installation Documentation provided by Actional details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the administrator on the TOE configuration parameters and how they affect the TSF.

Corresponding CC Assurance Components:

- Delivery Procedures
- Installation, Generation and Start-Up Procedures

Development – The XMS v3.1 Design documentation consist of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and errors message for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design

identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.

- The Correspondence Analysis demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the High-Level Design.
- The Informal TOE Security Policy Model provides additional assurance that the security functions in the Functional Specification enforce the policies in the TSP.

Corresponding CC Assurance Components:

- Informal Functional Specification
- Descriptive High-Level Design
- Informal Correspondence Demonstration
- Informal TOE Security Policy Model

Guidance Documentation – The Westbridge Technology Guidance documentation provides administrator and user guidance on how to securely operate the TOE. The Administrator Guidance provides descriptions of the security functions provided by the TOE. Additionally it provides detailed accurate information on how to administer the TOE in a secure manner and how to effectively use the TSF privileges and protective functions. The User Guidance provided directs users on how to operate the TOE in a secure manner. Additionally, User Guidance explains the user-visible security functions and how they are to be used and explains the user's role in maintaining the TOE's Security. Actional provides single versions of documents which address the Administrator Guidance and User Guidance; there are not separate guidance documents specifically for non-administrator users of the TOE.

Corresponding CC Assurance Components:

- Administrator Guidance
- User Guidance

Tests – There are a number of components that make up the Test documentation. The Coverage Analysis demonstrates the testing performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. Westbridge Technology's Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided. Westbridge Technology's Test Plans and Test Procedures provide expected and actual results satisfying the assurance level.

Corresponding CC Assurance Components:

- Evidence of Coverage
- Functional Testing

Lifecycle Support – Support is provided as part of the EAL 2 augmentation assurance package. The Flaw Reporting Procedures illustrates how TOE users should handle corrective fixes found and how to compile a security flaw report to be sent to the right person within the development team. The developer is provided with procedures to act appropriately upon security flaw reports submitted from TOE users.

Corresponding CC Assurance Components:

- Flaw Reporting Procedures

Vulnerability and TOE Strength of Function Analyses – A Vulnerability Analysis is provided to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, the document provides evidence of how the TOE is resistant to obvious attacks. The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions

within the TOE and how they exceed the minimum SOF requirements. The Examination of Guidance is provided as a part of the EAL 2 augmentation assurance package. The Examination of Guidance provides additional insight to ensure that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed.

Corresponding CC Assurance Components:

- Strength of TOE Security Function evaluation
- Developer Vulnerability Analysis
- Examination of Guidance

9.6 RATIONALE FOR EXPLICITLY STATED REQUIREMENTS

A family of ASG requirements was created to specifically address some of the security-relevant tasks performed by ASG. The purpose of this family of requirements is to address the unique functions of the ASG and provide requirements to describe the manner in which the ASG handles the XML message stream that it is examining. These requirements have no dependencies since the stated requirements embody all of the necessary security functions.

9.7 RATIONALE FOR STRENGTH OF FUNCTION

The TOE minimum strength of function is SOF-basic. The evaluated TOE is intended to operate in commercial and DoD low robustness environments processing unclassified information. This security function is in turn consistent with the security objectives described in Section 4.

9.8 RATIONALE FOR DEPENDENCIES

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 17 lists each functional requirement to which the TOE claims conformance with its dependency or dependencies and indicates whether the dependent requirement was included.

This table assumes that for functional requirements with iterations, that unless explicitly noted, that all iterations within a functional requirement map to the same dependencies.

Table 17 – Functional Requirements Dependencies

Functional Component	Dependency	Included
FAU_GEN.1	FPT_STM.1	Yes
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.3	FAU_SAR.1	Yes
FAU_STG.1	FAU_GEN.1	Yes
FCS_CKM.1	FCS_COP.1, FCS_CKM.4, FMT_MSA.2	Yes
FCS_CKM.4	FDP_ITC.1, FCS_CKM.1, FMT_MSA.2	Yes
FCS_COP.1	FDP_ITC.1, FCS_CKM.1, FMT_MSA.2	Yes
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	Yes
FDP_IFC.1	FDP_IFF.1	Yes
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	Yes
FIA_AFL.1	FIA_UAU.1	Yes
FIA_ATD.1	None	N/A
FIA_UAU.1	FIA_UID.1	FIA_UAU.1 is required by a dependency but was not included in this ST as this dependency

Functional Component	Dependency	Included
		is satisfied by the inclusion of its hierarchical component (FIA_UAU.2).
FIA_UAU.2	FIA_UID.1	Yes
FIA_UID.1	None	FIA_UID.1 is required by a dependency but was not included in this ST as this dependency is satisfied by the inclusion of its hierarchical component (FIA_UID.2).
FIA_UID.2	None	N/A
FIA_USB.1	FIA_ATD.1	Yes
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	Yes
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1, FMT_SMR.1, FMT_SMF.1	Yes
FMT_MSA.2	ADV_SPM.1, FDP_ACC.1 or FDP_IFC.1, FMT_MSA.1, FMT_SMR.1	Yes
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	Yes
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	Yes
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	Yes
FPT_RVM.1	None	N/A
FPT_STM.1	None	N/A
XMS_VEW.1	None	N/A
XMS_SUP.1	None	N/A
XMS_MAP.1	None	N/A

10 Glossary of Terms

3DES	Triple data encryption standard
AES	Advanced encryption standard
CC	Common Criteria
CEM	Common Evaluation Methodology
CM	Configuration management
CRL	Certificate revocation list
CRM	Customer relationship management
DES	Data encryption standard
DMZ	Demilitarized zone
EAL	Evaluation assurance level
ERP	Enterprise resource planning
HSQLDB	Hypersonic SQL database
HTTP	Hypertext transfer protocol
HTTPS	Secure hypertext transfer protocol
JMS	Java message service
LDAP	Lightweight directory access protocol
OCSP	Online certificate status protocol
OS	Operating system
PKCS #7	Public key cryptography standard - Cryptographic message syntax standard
PKCS #10	Public key cryptography standard - Certification request syntax standard
PKCS #11	Public key cryptography standard - Cryptographic token interface standard
PKCS #12	Public key cryptography standard - Personal information exchange syntax standard
PKI	Public key infrastructure
SAML	Security assertion markup language
SAR	Security Assurance Requirement
SFR	Security Functional Requirement

SLA	Service level agreement
SMTP	Simple mail transfer protocol
SNMP	Simple network management protocol
SOAP	Simple object access protocol
SSL	Secure sockets layer
ST	Security Target
TCP	Transmission control protocol
TOE	Target of Evaluation
TSF	Target of Evaluation (TOE) security function
TSP	Target of Evaluation (TOE) security policy
UI	User interface
WS-Security	Web Services Security
WSDL	Web service definition language
XKMS	XML key management specification
XML	Extensible markup language
ASG	Actional Security Gateway v3.1
XPath	XML Path Language
XSLT	Extensible stylesheet language transformations