Intel® SOA Expressway v2.7.0.4 and Intel® SOA Expressway v2.7.0.4 for Healthcare Security Target

EAL 4+

Document No. 1627-006
Version 1.9, August 30, 2011

Prepared for:
Intel Corporation
1815 South Meyers Road, Suite 150
Oakbrook Terrace, Illinois
60181

Prepared by:
Electronic Warfare Associates-Canada, Ltd.
55 Metcalfe Street, Suite 1600
Ottawa, Ontario
K1P 6L5

AMENDMENT RECORD SHEET

Rev.	Issue Date	Description	Author	Reviewer
0.1	26 March 2009	Initial Release	Steve Jackson	
0.2	15 April 2009	Updated with developer comments (provided on 3 April)	Steve Jackson	Grant Gibbs
0.3	29 May 2009	Updated to further define security functionality	Steve Jackson	
0.4	10 February 2010	- updated to address: ASE-INT-OR-1, ASE-INT-OR-5, ASE-CCL-OR-1 ASE-REQ-OR-1, ASE-REQ-OR-2, ASE-REQ-OR-3, ASE-REQ-OR-4, ASE-REQ-OR-5, ASE-REQ-OR-6, ASE-INT-CR-1, ASE-INT-CR-2, ASE-INT-CR-3, ASE-INT-CR-4, ASE-INT-CR-5, ASE-CCL-CR-1, ASE-CCL-CR-2, ASE-SPD-CR-1, ASE-OBJ-CR-1, and ASE-REQ-CR-1. - other minor corrections.	Steve Jackson	
0.5	3 March 2010	Update to conform to protection profile	Steve Jackson	
0.6	19 March 2010	- updated to address: ASE-CCL-OR-2, and ASE-REQ-OR-4.	Steve Jackson	

0.7	26 March 2010	Updated to address developer comments: - updated to reflect that FPT_STM.1 is addressed by the environment - Removed 'Codeless Design and Development' row in the table in Section 1.5.2 since it referred to the Intel Services Designer which is not part of the TOE - OS command line references were removed since this is not a TOE function (including in Figures 1 and 2) - FTA_SSL.3.1 numbering corrected - updated FDP_IFF.1.1(1) and FDP_IFF.1.1(2) to conform to PP (also changed to Section 1.5.3.5 and Section 6.1.4) - updated FDP_IFF.1.2(1) and FDP_IFF.1.2(2) to match PP wording	Steve Jackson	
0.8	March 29, 2010	Updated to address developer comments: - in 6.1.2 changed "performs and action" to "performs an action" - added the log administrator role (1.5.5.1, 5.1.5.1, 5.1.5.9, 6.1.1) - added footnote to FMT_MOF.1 to reference FIA_ATD.1 where users are linked to roles - changed TOE to software only but delivered as an appliance	Steve Jackson	

0.9	May 3, 2010	FMT_MTD.1.1 - editorial correction and update for consistency with FMT_MOF.1.1	Steve Jackson	
1.0	June 10, 2010	Added a paragraph about one the time password requirement in F.Audit and made the following changes as discussed on May 5 2010: - made changes for supported protocols (HTTP/HTTPS only) in 1.5.2, 1.5.3.5, 5.1.3.4, 5.1.3.5, and 6.1.4 - added reference to components for FAU_SEL.1.1 in 5.1.1.7 - made change regarding log storage (FAU_STG.3.1) in 5.1.1.8 - change unit to node in Table 3, 5.1.6, 5.1.7.1, 5.1.7.3, 5.4.15, 6.1.3	Steve Jackson	
1.1	June 17, 2010	Added Section 1.5.3.1.4 to include PAM into the TOE logical boundary, and made changes to Figure 3: - Authentication Server was connected to Workflow Runtime as it is used for web services - PAM was added and connected to Operation Management as it is used for authentication of administrator of the TOE	Changying Zhou	

1.2	July 9, 2010	Removed extra assumptions and environment security objectives highlighted in bold to meet the requirements of Demonstrable PP Compliance claim. Added OE.IDAUTH as the web services user authentication is done by external Authentication Server. Removed FIA_UID.2 (2) and FIA_UAU.2 (2) as the web services user authentication is done by external Authentication Server. Updated FIA_UAU.5. Added PP Compliance Rationale.	Changying Zhou	
1.3	September 28, 2010	Updated to incorporate comments submitted by Intel	Ben Cuthbert	
1.4	January 21, 2011	Incorporated more comments.	Ben Cuthbert	
1.5	March 02, 2011	Rework to better reflect the TOE and how it matches the requirements.	Ben Cuthbert	
1.6	May 02, 2011	A few more updates incorporated, reinserted FPT_STM.1	Ben Cuthbert	
1.7	May 04, 2011	Updates due to FPT_STM.1	Ben Cuthbert	
1.8	August 24, 2011	Addressed outstanding issues	Teresa MacArthur	
1.9	August 30, 2011	Changed title and addressed outstanding issues	Teresa MacArthur	

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 DOCUMENT ORGANIZATION

This document consists of the following sections:

- Section 1, Introduction, provides the Security Target (ST) reference, the Target of Evaluation (TOE) reference, the TOE overview and the TOE description;
- Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria and Packages. The ST conforms to a Protection Profile;
- Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis;
- Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition;
- Section 5, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the Information Technology (IT) environment;
- Section 6, TOE Summary Specification, describes the security functions and assurance measures that are included in the TOE to enable it to meet the information technology (IT) security functional and assurance requirements; and
- Section 8, Terminology and Acronyms, defines the acronyms and terminology used in this ST.

1.2 SECURITY TARGET REFERENCE

This document, version 1.9, dated August 30, 2011, is the Security Target for the Intel® SOA Expressway Version 2.7.0.4 and Intel® SOA Expressway Version 2.7.0.4 for Healthcare.

1.3 TARGET OF EVALUATION REFERENCE

The TOE is a software only TOE and is supported on Red Hat Enterprise Linux Advanced Server 5.4 (64-bit). The TOE is delivered to the customer as an appliance. The evaluated configuration consists of two variants; SOAE Version 2.7.0.4 Build on 2011-07-15 18:02 and SOAE-H Version 2.7.0.4 Build on 2011-07-15 18:02. The SOAE-H shares the same

underlying SOAE product as SOAE. SOAE-H contains additional Healthcare templates with a common underlying SOAE build. These templates are completely separate distributables. The two variants are described in Section 1.4 and in this ST are referred to as SOAE except where it is required to distinguish between them.

SOAE uses Java Runtime Environment (JRE) 1.6.0_x (also called Java Virtual Machine (JVM), Version 6ux) where x is 1 or greater. The SOAE appliance also includes Intel® Services Designer, an Eclipse based application design environment for modeling service mediation and orchestration. It offers a policy-based modeling approach with a drag and-drop interface thus removing the need of low level coding, further reducing development time. Service Designer allows the SOA architect to design, develop, test and ultimately deploy applications to a single SOAE or a cluster of SOAE instances.

The TOE is administered using a web interface that can be used from any browser that supports Java Script. The web interface is compatible with Mozilla Firefox 1.0 or higher and Internet Explorer 5.5 or higher.

1.4 INTEL® SOA EXPRESSWAY OVERVIEW

The Intel ® Service Oriented Architecture Expressway (SOAE) appliance is a security gateway designed to simplify, accelerate, and secure the Enterprise SOA architecture. The SOAE provides trust enablement and threat prevention by providing a secure gateway between external service providers and internal services. It expedites SOA deployments by addressing common SOA bottlenecks - it accelerates, secures, integrates and routes extensible stylesheet language (XML), web services and legacy data in a single, easy to manage form factor[1]. SOAE is supported in both Windows and Linux environments.

Typical solutions for managing SOA security involve the use of an intermediary to provide service virtualization, trust and threat functions. This model moves security policy deployment to a central place and reduces last-mile security configuration at each service endpoint in the internal network. Until now intermediaries of this type required an expensive, purpose-built hardware appliance with custom operating systems for security functions and often rely on a “security by obscurity” model, even in cases where some aspects of the appliance (such as crypto) have undergone Federal Information Processing Standards (FIPS) certification. SOAE uses standard hardware and operating systems to provide trust enablement, threat prevention, security offload, central security policy deployment and credential mapping but without the traditional drawbacks of a custom hardware appliance, such as high costs, poor upgrade path, and lack of governance.

Intel® SOA Expressway is also offered in a version that is tailored to the healthcare industry. Intel® SOA Expressway for Healthcare (SOAE-H) uniquely offers cost-containment and operational simplicity by providing a high-performance platform-based solution for translating, processing, and connecting multiple data formats across a healthcare

[1] SOAE runs on standard Intel servers.

environment. The Intel SOAE-H combines robust health level 7 (HL7), electronic data interchange (EDI), and health insurance portability and accountability act (HIPAA) support and a unique healthcare environment developer kit (HDK) with a high-performance, codeless workflow engine, native XML acceleration, and appliance manageability. It can be used in a stand-alone manner to construct large multi-site health networks using the HDK, or it can be used as a base platform to augment healthcare vendor product offerings with a modern, high-performance SOA-based architecture. In either case, the goal is the same - to accelerate computable healthcare information across disparate health environments such as hospitals, integrated delivery networks, clinics, payor networks, labs, and pharmaceutical networks.

The SOAE also provides clustering functionality to both improve performance and provide fault tolerance.

1.4.1 Software Supplied by the IT Environment

The TOE is a software-only TOE and is supported on Red Hat Enterprise Linux 5.4. A standard Internet browser is also required for user access to the SOAE Software. An external active directory server is required for authentication.

The following table identifies the software requirements for components provided by the IT Environment:

Component	Minimum Requirement
Operating System	Red Hat Enterprise Linux 5.4
Other software	Mozilla Firefox 1.0 or higher and Internet Explorer 5.5 or higher

Table 1 - Software Requirements for the TOE

1.5 TARGET OF EVALUATION DESCRIPTION

1.5.1 Architecture

The TOE executes on the host operating system and links web services clients to web services servers and web integration servers using administrator defined security rulesets. Data must match a ruleset otherwise it will not be passed through the TOE.

The TOE may be used as a single appliance or increased performance and reliability may be achieved by clustering multiple machines. This ST addresses the single appliance mode of operation and a dual appliance redundant mode. In both instances they must be operated in a protected environment.

Clustering is, for the most part, transparent to the administrator. The administrator simply maintains the cluster from any one of the appliances and any changes made are provided to

other members of the cluster automatically. However, each machine within a cluster can be addressed individually, and its individual status can be determined. A cluster communicates via an Inter-node communication link. Any time a change is made to a node, that change is propagated to all the nodes in the cluster. Changes that are propagated from one node to another consist of[2]:

- Application changes;
- Application configuration changes; and
- Global configuration changes.

The TOE can be administered via a command line prompt provided by a secure shell (SSH) connection, or via a web browser (HTTPS). In the evaluated configuration, the CLI commands are limited to stopping and starting services, user management commands and audit review commands in the evaluated configuration.

1.5.1.1 Single Appliance

When a single appliance is used the environment is as shown in Figure 1 - Single Appliance below:

[2] SOAE software changes can also be transferred between nodes but are excluded from the evaluated configuration.

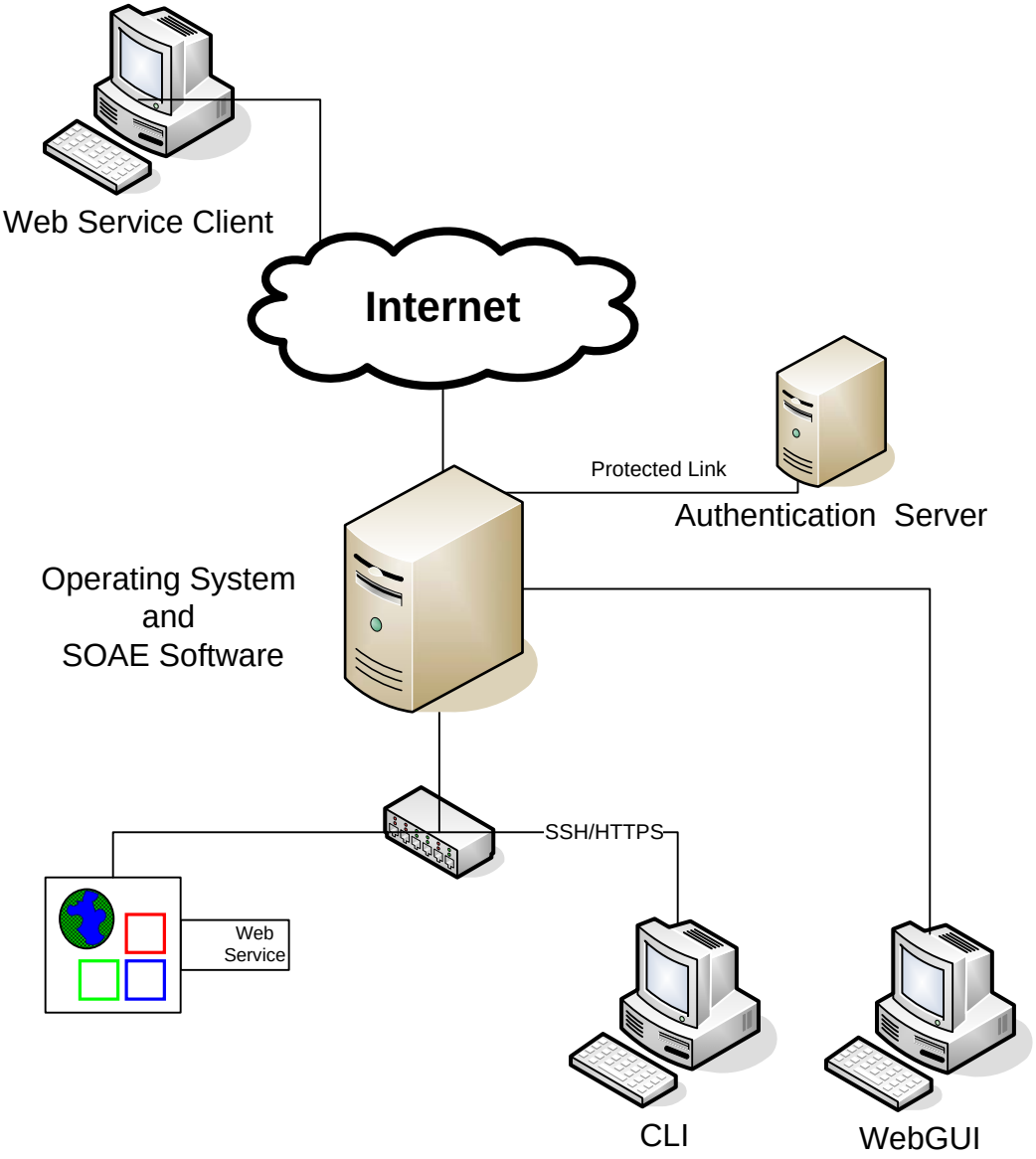

Figure 1 - Single Appliance

The authentication server and administration performed via the CLI must be protected by the TOE. The CLI session is protected by SSH using a FIPS 140-2 validated cryptographic module. The WebGUI session is either directly connected or is located on a private, administrative network on the same subnet as the SOAE server.

1.5.1.2 Dual Appliance

When dual appliances are used the environment is as shown in Figure 2 - below:

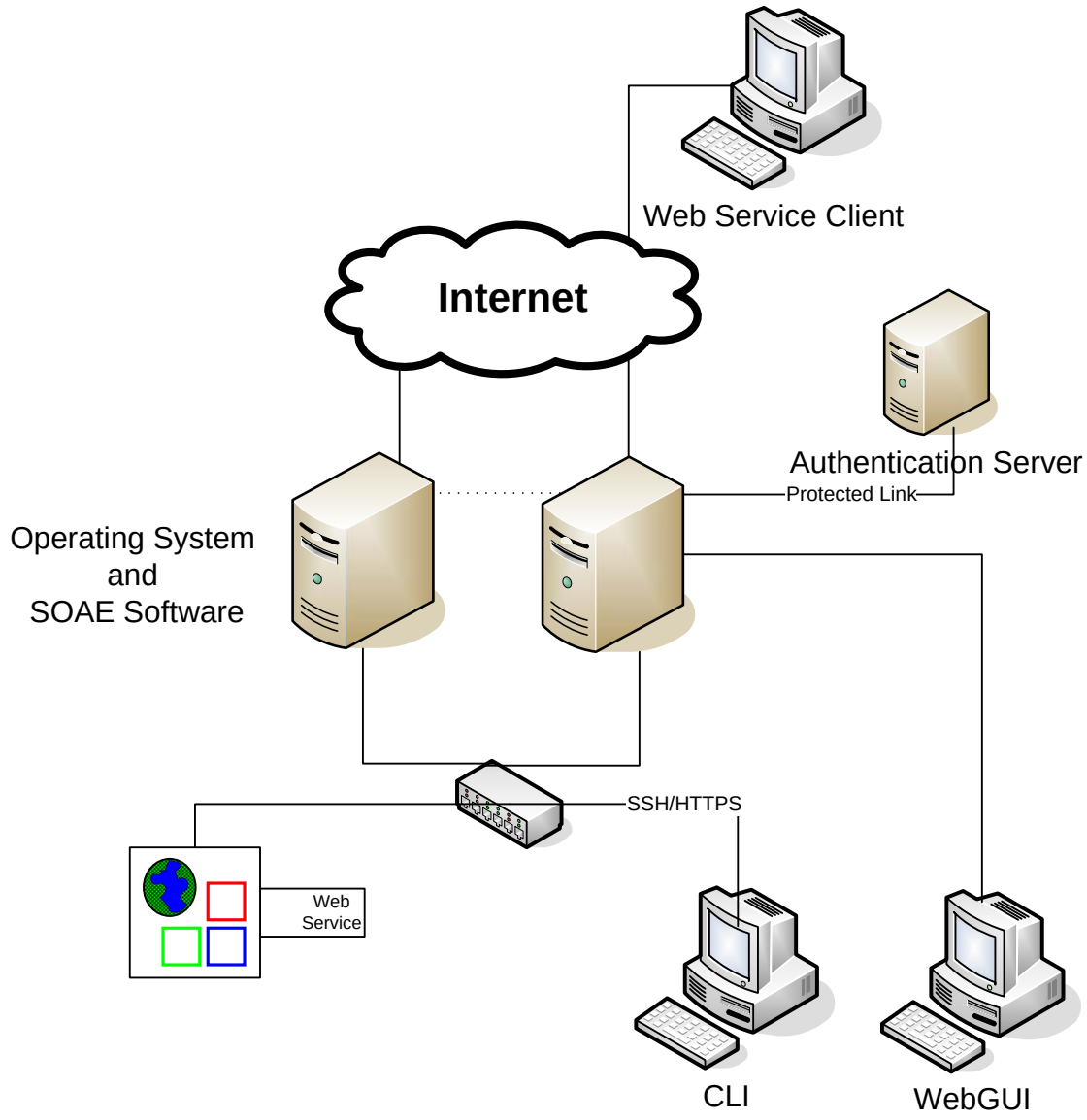

Figure 2 - Dual Appliance

The authentication server must be protected by the environment. The CLI session is protected by SSH. The Inter-node Communication (dashed line between the two servers) is encrypted. The WebGUI session is either directly connected or is located on a private, administrative network on the same subnet as the SOAE server.

1.5.2 Features

Feature	Description
Service Mediation Engine	The TOE includes a high-performance service mediation engine that interprets service based workflows in byte code form for processing SOAP and plain old XML / representational state transfer (POX/REST). This engine binds to the Intel XML core optimization

Feature	Description
	layer that is optimized for Intel® multi-core architecture to accelerate XML processing including XML path language (XPath), schema validation, and transformation operations. SOAE is also capable of processing binary messages but this is not supported in the evaluated configuration.
SOA Message Acceleration	The TOE contains native support for XML acceleration through the use of an efficient binary representation. It achieves wire speed in executing XML operations such as XPath node selection, XSL Transformation (XSLT), schema validation, constraint checking, content routing, and XML security (including canonicalization).
Management	The TOE is managed through a web interface, complete with alarms, alerts, a dashboard and self-healing, self-correcting capabilities. The SOAE can also integrate with management consoles that support simple network management protocol (SNMP) and Java management extensions (JMX) but this is not supported in the evaluated configuration.
Content Conversion	The healthcare variant of the TOE handles non-XML formats including HL7, National Council for Prescription Drug Programs (NCPDP) and HIPAA formats. SOAE also handles EDI, COBOL Copybook but this is not supported in the evaluated configuration.
Platform Extensibility	Though SOAE is extensible and can execute custom services in Axis 2 and Java business integration (JBI) containers, this extensibility is not supported in the evaluated configuration.
Comprehensive Protocol Brokering	The TOE provides protocol brokering for HTTP and HTTPS. SOAE supports additional protocols that are not included in the evaluated configuration. These additional protocols include Java message service (JMS), file transfer protocol (FTP), file, minimal lower layer protocol (MLLP), transport control protocol (TCP) protocols, and Secure File Transfer Protocol (SFTP).
Security Gateway	The TOE supports web services security specification (XML/WS-Security), X.509 Tokens, HTTP Basic Authentication, Username/Password Tokens, X.509 path validation and certificate revocation list (CRL) support. It has full support for secure socket layer / transport layer security (SSL/TLS) origination and termination as well as support for an optional cryptographic accelerator for digital signature, encryption and security token processing. The TOE also offers XML perimeter defense capabilities such as service virtualization, XML limit checking, schema validation, XPath filtering and Denial of Service protection.

1.5.3 Logical Description

Figure 3 - Logical Overview presents a logical overview of the TOE in terms of functional components. Subsequent sections of this document describe these functional components, the TOE boundary, externals, and interfaces.

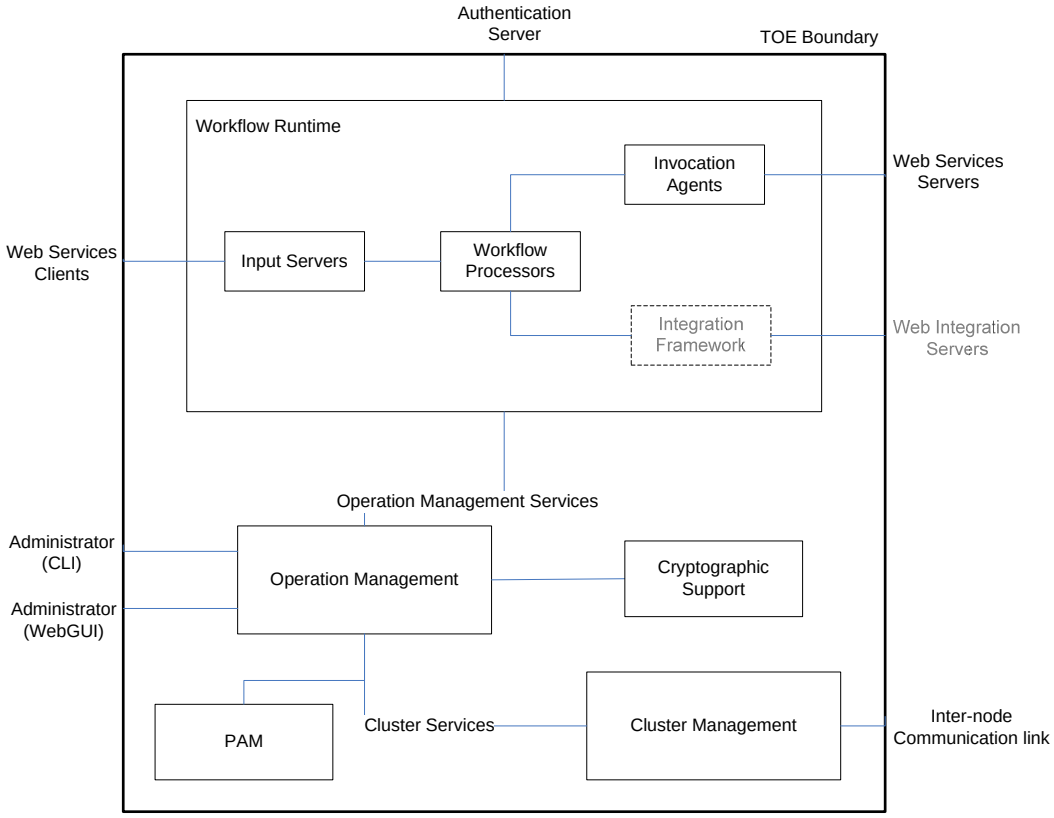

Figure 3 - Logical Overview

The components consisting of the Workflow runtime, Operation Management, Cluster Management, Pluggable Authentication Module (PAM) and Cryptographic Support are described in the following sections. The Integration Framework is in SOAE but is not within the TOE boundary and has not been evaluated.

1.5.3.1 Functional Components

1.5.3.1.1 Workflow Runtime

The workflow runtime implements the security rulesets by performing these functions:

- interprets the application bundle;
- instantiates input servers; and
- handles incoming message events by routing them to local or remote services through invocation agents.

The workflow runtime executes a user-defined workflow and makes dynamic decisions depending on the content of the message and the nature of the service to be invoked. The workflow processor also contains a number of workflow level optimizations that are transparent to the user. It interprets the workflow as byte code and architected with a multi-threaded design that uses Intel® Threading Building Blocks (Intel® TBB) primitives to optimize multiple workflows in a multi-core environment. The workflow engine enables Intel® SOA Expressway to invoke local or remote services in a transparent fashion. Intel® SOA Expressway workflow processor provides built-in local services and nested workflow invocation within a single operating system process to enhance performance.

1.5.3.1.1.1 Input Servers

An input server is an application component that exchanges messages between a client and the TOE. An input server either listens on a specific transport protocol and port, such as HTTP, or pulls messages from a source, such as a JMS queue. The input server forwards normalized client request messages to the Workflow Processor for enforcing policies and processing business logic.

1.5.3.1.1.2 Workflow Processors

Workflow processors execute user-defined workflow and make dynamic decisions depending on the content of the message and the nature of the service to be invoked.
The workflow processor also contains a number of workflow level optimizations that are transparent to the user. The workflow processor processes the workflow as byte code and architected with a multi-threaded design that uses Intel® Threading Building Blocks (Intel® TBB) primitives to optimize multiple workflows in a multi-core environment. The workflow engine enables the TOE to invoke local or remote services in a transparent fashion.

1.5.3.1.1.3 Invocation Agents

An invocation agent is an application component that exchanges messages between the TOE and a back end service (remote service). An invocation agent takes requests from a workflow processor, converts the request to a specific protocol, and sends it to the remote server. It passes the response from the remote server to the workflow processor after it has normalized the message format.

1.5.3.1.2 Operation Management

The operation management component provides functions for configuring the Intel® SOA Expressway either remotely via a command line prompt or a web interface.

1.5.3.1.3 Cluster Management

When appliances are clustered the cluster management component provides the functions for communicating between appliances and managing the cluster.

1.5.3.1.4 PAM

When administrators attempt to login and access the TOE security functionality, they are identified and authenticated by a Pluggable Authentication Module (PAM) in the TOE.

1.5.3.2 Cryptographic Support

The TOE includes the FIPS 140-2 validated cryptographic modules Red Hat Enterprise Linux 5 OpenSSH-Server Cryptographic Module (certificate number 1384) and Red Hat Enterprise Linux 5 OpenSSH Client Cryptographic Module (certificate number 1385). These modules are used by the CLI either locally or remotely. These modules are used to protect an administrative session.

The TOE also includes the Workflow Processor, which uses the Cavium HSM. Included in the TOE is hardware part number CN1620-NFBE1NIC-2.0-FW1.2-G. This part number represents a combination of the Hardware Version CN1620-NFBE1NIC-2.0-G and Firmware Version 1.2, both identified in FIPS 140-2 certificate #1369. The Workflow Processor provides message level encryption and signature processing, HTTP Input Server (SSL), HTTP Invocation Agent (SSL) and the inter-node communication in a cluster (SSL).

1.5.3.3 TOE Boundary

The TOE boundary includes:

- Workflow Runtime;
- Operation Management;
- Cluster Management;
- PAM; and
- Cryptographic Support.

1.5.3.4 Externals

Name	Description
Web Services Clients	The Web Services Clients exchange messages with the Web Services Servers through the intermediary of the SOAE.
Web Services Servers	The Web Services Servers exchange messages with the Web Services Clients through the intermediary of the SOAE.
Administrator (CLI)	The administrator may start and stop the TOE services, perform new user management and perform some audit review using a SSH command line[3].

[3] Though more functionality is available to an administrator, in the evaluated configuration administrator functions are limited.

Name	Description
Administrator (WebGUI)	The administrator may configure the TOE using a web browser.
Inter-node Communication	Inter-node Communication is used in a cluster to transfer application changes, application configuration changes, and global configuration changes between appliance instances.
Authentication Server	The TOE supports lightweight directory access protocol (LDAP) authentication for web services.

1.5.3.5 Interfaces

Interface	Data	Protocol
Web Services Clients[4]	XML requests and messages, mail messages, MQ-series messages, general files	file, HTTP, HTTPS, JMS, MLLP, soae-custom (SOAE-H only), and TCP/IP
Web Services Servers[4]	XML messages, mail messages, general files	file, HTTP, HTTPS, JMS, MLLP, soae-custom (SOAE-H only), soae-local, and TCP/IP
Administrator (CLI)	configuration and status	SSH
Administrator (WebGUI)	configuration and status	HTTPS
Inter-node Communication link	configuration, status, application data	TCP/IP
Authentication Server	username, password, result of authentication request	LDAP

1.5.4 Functions Excluded From the Evaluation

The XSLT and binary data mapping capabilities are excluded from the evaluation. The SOAE Service Design is also excluded from this evaluation.

The SOAE performs authentication via Java authentication and authorization service (JAAS) login modules. The default login module functionality is limited to providing usernames and passwords. Though a more robust JAAS module could be used there was no evaluation of this capability.

In the evaluated configuration, the CLI commands are limited to stopping and starting services, user management commands and audit review commands in the evaluated configuration.

[4] Only the HTTP and HTTPS protocols are supported in the evaluated configuration.

1.5.5 Security Functional Policies

This ST contains three security function policies. One addresses operation management and two cover information flow control. The Protection Profile (PP) defines the UNAUTHENTICATED SFP and the AUTHENTICATED SFP information flow control security function policies. This ST uses more descriptive names for these SFPs which are the Unauthenticated Web Service SFP and the Authenticated Web Service SFP.

1.5.5.1 Operation Management SFP

The TOE imposes an access control requirement on all attempts by a user to perform the Operation Management (OM) process. Access is permitted if the user has a valid username and password and has been assigned a role that permits the performance of the operation. More than one role may be associated with a username.

The TOE implements the following OM roles, listed in order of capability:

- Operations Administrator;
- Log Administrator,
- Configuration Administrator; and
- Security Administrator.

The Operations Administrator can monitor the running SOAE system which includes viewing the dashboard statistics and alerts, checking the components' state, browsing logs, viewing the statistic reports, and performing component health tests. Also included in this role is the ability to manage the running SOAE system: start and stop the components, rotate logs, adjust the logs levels, or restart a specific node or the whole cluster.

The Log Administrator can rotate logs, and adjust the logs levels.

The Configuration Administrator can manage security token/configuration dependencies, edit the cluster configuration, and manage application configurations,

The Security Administrator can manage security tokens within configurations, including creating, modifying and deleting security tokens, and creating configurations to enter security data into them. However, the Security Administrator is not allowed to delete the configurations because they may also contain some non-security data. The Security Administrator may also import and export configurations.

1.5.5.2 Unauthenticated Web Service SFP

The TOE provides a mechanism to configure rulesets to classify unauthenticated incoming HTTP messages to the applications and workflows deployed on the system. The rulesets can be configured based on the content of the incoming HTTP message as well as the message metadata. For example, rulesets can be defined to look for a specific element or attribute tag in the HTTP message. In addition, the rulesets can be defined to classify on the basis of

message metadata attributes such as transport protocol, port, uniform resource identifier (URI) etc.

When the messages match the rulesets, they are accepted for processing by the system and they will be processed by the workflow associated with the matched ruleset. All messages that don't match any of the rulesets defined on the system are rejected.

1.5.5.3 Authenticated Web Service SFP

The TOE provides a mechanism to configure rulesets to classify authenticated incoming HTTP messages to the applications and workflows deployed on the system. Supported authentication methods[5] are XML/WS-Security, X.509 Tokens, HTTP Basic Authentication, Username/Password Tokens, keystore, and LDAP. The rulesets can be configured based on the content of the incoming HTTP message as well as the message metadata. For example, rulesets can be defined to look for a specific element or attribute tag in the HTTP message. In addition, the rulesets can be defined to classify on the basis of message metadata attributes such as transport protocol, port, URI etc.

Provided that authentication is successful, when the messages match the rulesets, they are accepted for processing by the system and they will be processed by the workflow associated with the matched ruleset. All messages that don't match any of the rulesets defined on the system are rejected.

1.5.6 Guidance Documentation

The following guidance documentation is provided with the TOE:

- Intel® SOA Expressway Installation Guide;
- Intel® SOA Expressway Installation Guide for Linux OS;
- Command Line Interface (CLI) Usage Guide;
- Intel® SOA Expressway CLI Guide for Linux OS;
- Intel® SOA Expressway Web Interface System Administrator Guide;
- Intel® SOA Management Console User's Guide for Linux OS;
- Intel® SOA Expressway Security Reference Guide; and
- Setting up the 2.7 Intel® SOA Expressway Hardware Appliance with FIPS option.

[5] The underlying cryptographic protocols are defined outside the TOE and are not evaluated.

2 CONFORMANCE CLAIMS

This ST has been prepared in accordance with the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1R3. The Target of Evaluation (TOE) for this ST is conformant with the functional requirements specified in CC Part 2. The Target of Evaluation (TOE) for this ST, the Intel® SOA Expressway, is therefore conformant with CC Part 2. The TOE for this ST is conformant to the CC Part 3 assurance requirements for EAL 4, augmented with ALC_FLR.1 Basic flaw remediation. Therefore no CC Part 2 or CC Part 3 extended components are in the ST.

The TOE for this ST claims conformance to the Application-Level Firewall Protection Profile for Basic Robustness Environments, Version 1.1, July 25, 2007.

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

The threats discussed below are addressed by the TOE. The threats that are additional to those required by the PP are indicated by bold text. Additionally the PP assumes that threat agents have a **low** attack potential and are assumed to have a moderate level of resources and access to all publicly available information about the TOE and potential methods of attacking the TOE. This ST assumes that threat agents have an **Enhanced-Basic** attack potential.

T.ASPOOF	An unauthorized person on an external network may attempt to by-pass the information flow control policy by disguising authentication data (e.g., spoofing the source address) and masquerading as a legitimate user or entity on an internal network.
T.ATTACK_DATA	The TOE may encounter (process) data that contains malicious code introduced by an authorized user or unauthorized agent in an attempt to disrupt site security operations or the TOE itself.
T.ATTACK_POTENTIAL	An unauthorized person, using obvious vulnerabilities, may attempt to circumvent the TOE security functions.
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.
T.AUDIT_UNDETECTED	An unauthorized person may cause auditable events to go undetected by disabling the audit function.
T.BAD_ADMIN	Authorized users, system or security administrators may unintentionally or intentionally make a security relevant error or take an action that results in inappropriate access to, or modification of, information, or inappropriate utilization of resources.
T.BAD_CREDENTIALS	An unauthorized person may attempt to obtain access to system or network resources using security credentials (e.g., certificate or token) that have been forged, altered, substituted or revoked.
T.CAPTURE	An unauthorized person may eavesdrop, tap into the transmission line, or otherwise capture data being transferred on a communications channel.
T.DENIAL	Authorized persons may make errors or an unauthorized person may deliberately execute commands, send more than

	allowed high priority traffic, or perform other operations that cause undue burden on the network therefore making system resources unavailable to authorized clients (i.e., resulting in service denial). These attacks may be mounted at the TCP, HTTP, XML or SOAP layers. At the XML layer, the attempts may take forms such as: - sending massive numbers of requests that force a system to drop requests; - sending extremely large messages that cause a system to spend most of its time handling them; - sending malformed messages that require a system to waste its limited resources trying to parse them. - SOAP Replay attacks, which use repetitive SOAP messages to force an XML denial-of-service (XDoS), fall into this category.
T.ENHANCEDEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered **Enhanced-Basic**[6].
T.HIJACK	An unauthorized person may intrude on a properly established session in order to access or modify information, or utilize system resources.
T.INTERNAL	An unauthorized internal agent may attempt to compromise the TOE by tampering with its operating system, hardware or operational layers.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
T.MODIFY_ PROTOCOL	An unauthorized person may make unauthorized modifications to, or otherwise manipulate protocols (e.g. routing, signalling, etc.) en-route.
T.NOAUTH	An unauthorized person 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.
T.OLDINF	Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.
T.REMOTE_ATTACK	An unauthorized person may be able to view, modify, and/or delete security-related information that is sent between a

[6] PP specifies low.

	remotely located Authorized Administrator and the TOE.
T.REPEAT	An unauthorized person may repeatedly try to guess authentication data in order to launch an attack against the TOE.
T.REPLAY	An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
T.SERVICE_MISUSE	An unauthorized person on the internal network may try to connect to services other than those expressly permitted.
T.UNAVAILABLE	An unauthorized person may cause the internet, or shared public network to not be available.
T.USAGE	The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons.

3.2 ORGANIZATION SECURITY POLICIES

Federal agencies are required to protect sensitive but unclassified information with cryptography. Products and systems compliant with this Protection Profile are expected to utilize cryptographic modules for remote administration compliant with FIPS PUB 140-2 (level 1).

P.CRYPTO	AES (Advanced Encryption Standard as specified in FIPS 197) encryption (as specified in SP 800-67) must be used to protect remote administration functions, and the associated cryptographic module must comply, at a minimum, with FIPS 140-2 (level 1).

3.3 ASSUMPTIONS

The specific conditions below are assumed to exist in the TOE environment.

A.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
A.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered **low**.
A.NOEVIL	Authorized administrators are non-hostile, and follow all administrator guidance; however, they are capable of error.
A.NOREMO	Human users who are not authorized administrators cannot access the

	TOE remotely from the internal or external networks.
A.PHYSEC	The TOE is physically secure.
A.PUBLIC	The TOE does not host public data.
A.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.
A.SINGEN	Information can not flow between the internal and external networks unless it passes through the TOE.
A.TIME_SOURCE	Network resources are connected to a reliable time source. This is necessary for reliable time for auditing purposes of traffic, performance, and for auditing of user, administrator and security administrator activities.

4 SECURITY OBJECTIVES

This section describes the security objectives for the TOE and the TOE's operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means). The mapping of security objectives to assumptions, threats and organizational security policies along with the rationale for this mapping is found in Section 4.3.

4.1 SECURITY OBJECTIVES FOR THE TOE

This section defines the security objectives that are to be addressed by the TOE and its environment. The objectives that are additional to those required by the PP are indicated by bold text.

O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions.
O.ALARM	The TOE will be capable of analyzing audit logs, event logs, the results of self-tests, and other relevant inputs, according to administrator-selected criteria, and deciding whether or not alarms should be given. The TOE will provide alarming capabilities for notification of security related events, failures or errors.
O.AUDIT	The TOE must provide the means of recording security relevant events, with accurate dates and times, in sufficient detail to help an administrator of the TOE detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
O.CRYPTOGRAPHY	The TOE must protect the confidentiality of configuration data exported to an intermediary for backup purposes or for transfer to a peer TOE in a cluster. The TOE must protect the confidentiality of its dialogue with an authorized administrator or authentication server. In addition, the TOE must provide support for X.509 certificates for authentication and must support XML/WS-Security.
O.EAL	The TOE must be structurally tested and shown to be resistant to obvious vulnerabilities.
O.ENCRYP	The TOE must protect the confidentiality of its dialogue with an

	authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all **administrative** users, before granting a user access to TOE functions or, for certain specified services, to a connected network.
O.LIMEXT	The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.
O.MEDIAT	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, and must ensure that residual information from a previous information flow is not transmitted in any way.
O.ROLE	The TOE must prevent users from gaining access to and performing operations on its resources/objects unless they have been granted access by the resource/object owner or they have been assigned to a role (by an authorized administrator) which permits those operations.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.
O.TOE_AVAILABLE	The TOE will be resilient to denial-of-service attacks.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section defines the security objectives that are to be addressed by the IT domain or by non-technical or procedural means. The objectives that are additional to those required by the PP are indicated by bold text. For clarity the objectives for the environment are labelled with the prefix OE.

OE.ADMTRA	Authorized administrators are trained as to establishment and maintenance of security policies and practices.
OE.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct

	connection (e.g., a console port) if the connection is part of the TOE.
OE.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
OE.IDAUTH	The external Authentication Server must uniquely identify and authenticate the claimed identity of all **authenticated web service** users, before granting a user access, for web services, to a connected network.
OE.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
OE.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
OE.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
OE.NOREMO	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
OE.PHYSEC	The TOE is physically secure.
OE.PUBLIC	The TOE does not host public data.
OE.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
OE.TIME_SOURCE	The IT environment shall provide a reliable time source to which network resources may connect for the purpose of synchronizing their local time. Changes to the time are to be audited. This synchronization ensures reliable time is available across multiple devices in support of audit.

4.3 SECURITY OBJECTIVES RATIONALE

	T.ASPOOF	T.ATTACK_DATA	T.ATTACK_POTENTIAL	T.AUDACC	T.AUDFUL	T.AUDIT_UNDETECTED	T.BAD_ADMIN	T.BAD_CREDENTIALS	T.CAPTURE	T.DENIAL	T.ENHANCEDEXP	T.HIJACK	T.INTERNAL	T.MEDIAT	T.MODIFY_PROTOCOL	T.NOAUTH	T.OLDINF	T.PROCOM	T.REMOTE_ATTACK	T.REPEAT	T.REPLAY	T.SELPRO	T.SERVICE_MISUSE	T.UNAVAILABLE	T.USAGE	A.ACCESS	A.ASSET	A.DIRECT	A.GENPUR	A.LOWEXP	A.NOEVIL	A.NOREMO	A.PHYSEC	A.PUBLIC	A.REMACC	A.SINGEN	A.TIME_SOURCE	P.CRYPTO
O.ACCOUN	X			X				X				X		X		X			X																		
O.ALARM		X					X						X		X				X																		
O.AUDIT					X	X	X												X																		
O.AUDREC				X																																	
O.CRYPTOGRAPHY									X										X			X															X
O.EAL											X																											
O.ENCRYP																X		X																			X
O.IDAUTH	X							X								X				X			X														
O.LIMEXT																X																					
O.MEDIAT	X									X		X		X	X	X	X																				
O.ROLE			X																	X			X														
O.SECFUN		X			X											X			X		X		X														
O.SECSTA																X						X															
O.SELPRO					X											X						X															
O.SINUSE																				X	X																
O.TOE_AVAILABLE		X			X	X				X														X													
OE.ACCESS																										X											
OE.ADMTRA					X																				X						X						
OE.ASSET																											X										
OE.CONSOLE																												X									
OE.DIRECT																												X									
OE.GENPUR																													X								
OE.IDAUTH																X																					
OE.GUIDAN					X																				X						X						
OE.LOWEXP																														X							
OE.NOEVIL																															X						
OE.NOREMO																																X					

	T.ASPOOF	T.ATTACK_DATA	T.ATTACK_POTENTIAL	T.AUDACC	T.AUDFUL	T.AUDIT_UNDETECTED	T.BAD_ADMIN	T.BAD_CREDENTIALS	T.CAPTURE	T.DENIAL	T.ENHANCEDEXP	T.HIJACK	T.INTERNAL	T.MEDIAT	T.MODIFY_PROTOCOL	T.NOAUTH	T.OLDINF	T.PROCOM	T.REMOTE_ATTACK	T.REPEAT	T.REPLAY	T.SELPRO	T.SERVICE_MISUSE	T.UNAVAILABLE	T.USAGE	A.ACCESS	A.ASSET	A.DIRECT	A.GENPUR	A.LOWEXP	A.NOEVIL	A.NOREMO	A.PHYSEC	A.PUBLIC	A.REMACC	A.SINGEN	A.TIME_SOURCE	P.CRYPTO
OE.PHYSCEC																																	X					
OE.PUBLIC																													X					X				
OE.REMACC																																			X			
OE.SINGEN																																				X		
OE.TIME_SOURCE																																					X	

Table 2 - Mapping Between Security Objectives, Threats, and Assumptions

4.3.1 T.ASPOOF

O.ACCOUN requires that users be properly identified and held accountable for their actions (including sending messages) or when they use security functions. O.IDAUTH supports O.ACCOUN by ensuring that the TOE uniquely identifies and authenticates the claimed identity of a user before granting access to TOE functions. O.MEDIAT ensures that the TOE mediates the flow of information in accordance with its security policy.

4.3.2 T.ATTACK_DATA

O.ALARM ensures that alarms are provided for notification of security-related events, failures or errors. O.SECFUN ensures that only authorized administrators can access administrative functionality, thus preventing unauthorized agents from disrupting the TOE through the administrative interface. O.TOE_AVAILABLE ensures that the TOE is resilient to denial of service attacks, which are a common means of attempting to disrupt site operations.

4.3.3 T.ATTACK_POTENTIAL

O.ROLE ensures that users must have been granted access by the resource/object owner or have been assigned to a role, by the authorized administrator, which permits those operations.

4.3.4 T.AUDACC

O.ACCOUN requires that users be properly identified and held accountable for their actions (including sending messages) or when they use security functions. O.AUDREC ensures that the TOE audits security related events and that the records can be searched and sorted.

4.3.5 T.AUDFUL

O.AUDIT ensures that the TOE provides an audit capability, with accurate dates and times, so that lost or missing audit records would be evident O.SECFUN ensures that only authorized administrators can access administrative functionality, thus preventing unauthorized agents from disrupting the TOE through the administrative interface. O.SELPRO ensures that the TOE can not be bypassed or tampered with by unauthorized persons thereby reducing the threat of a full audit record. O.TOE_AVAILABLE ensures that the TOE is resilient to denial of service attacks, which are a common means of attempting to disrupt site operations. OE.GUIDAN also assists in addressing this threat.

4.3.6 T.AUDIT_UNDETECTED

O.AUDIT ensures that the TOE provides an audit capability, with accurate dates and times, so that lost or missing audit records would be evident. O.TOE_AVAILABLE ensures that the TOE is resilient to denial of service attacks, which are a common means of attempting to disrupt site operations.

4.3.7 T.BAD_ADMIN

O.ALARM ensures that the TOE is capable of detecting a failure or error with any component and provides an alarm for notification of security-related events and of a failure or error. This detection and alarming will help to deter authorized users or unauthorized agents from introducing malicious code since, and will provide notice of the introduction at an early stage. O.AUDIT ensures that the TOE provides an audit capability, with accurate dates and times, so that lost or missing audit records would be evident.

4.3.8 T.BAD_CREDENTIALS

O.ACCOUN requires that users be properly identified and held accountable for their actions (including sending messages) or when they use security functions. O.IDAUTH supports O.ACCOUN by ensuring that the TOE uniquely identifies and authenticates the claimed identity of a user before granting access to TOE functions.

4.3.9 T.CAPTURE

O.CRYPTOGRAPHY protects the confidentiality of the dialogue between the TOE and an authorized administrator, thus helping to protect against unauthorized reading of the security-critical TOE configuration data.

4.3.10 T.DENIAL

O.MEDIAT ensures that the TOE mediates the flow of information in accordance with its security policy. O.TOE_AVAILABLE ensures that the TOE is resilient to denial of service attacks, which are a common means of attempting to disrupt site operations.

4.3.11 T.ENHANCEDEXP

O.EAL ensures that the TOE is structurally tested and shown to be resistant to attacks performed by an attacker possessing Enhanced-Basic attack potential.

4.3.12 T.HIJACK

O.ACCOUN requires that users be properly identified and held accountable for their actions (including sending messages) or when they use security functions. O.MEDIAT ensures that the TOE mediates the flow of information in accordance with its security policy.

4.3.13 T.INTERNAL

O.ALARM ensures that the TOE is capable of detecting a failure or error with any component and provides an alarm for notification of security-related events and of a failure or error. This detection and alarming will help to deter authorized users or unauthorized agents from introducing malicious code since the TOE will provide notice of the introduction at an early stage.

4.3.14 T.MEDIAT

O.ACCOUN requires that users be properly identified and held accountable for their actions (including sending messages) or when they use security functions. O.MEDIAT ensures that the TOE mediates the flow of information in accordance with its security policy.

4.3.15 T.MODIFY_PROTOCOL

O.ALARM ensures that the TOE is capable of detecting a failure or error with any component and provides an alarm for notification of security-related events and of a failure or error. This detection and alarming will help to deter authorized users or unauthorized agents from introducing malicious code since the TOE will provide notice of the introduction at an early stage. O.MEDIAT ensures that the TOE mediates the flow of information in accordance with its security policy.

4.3.16 T.NOAUTH

O.ACCOUN requires that users be properly identified and held accountable for their actions (including sending messages) or when they use security functions. O.ENCRYP requires that the TOE protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network. O.IDAUTH ensures that **administrative** users are identified and authenticated. OE.IDAUTH ensures that **authenticated web service** users are identified and authenticated. O.LIMEXT requires that the TOE provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity. O.MEDIAT ensures that the TOE mediates the flow of information in accordance with its security policy. O.SECFUN ensures that only authorized administrators can access administrative functionality, thus preventing unauthorized agents from disrupting the TOE through the administrative interface. O.SECSTA protects the TOE during start-up or recovery. O.SELPRO ensures that the TOE is protected against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

4.3.17 T.OLDINF

O.MEDIAT ensures that the TOE mediates the flow of information in accordance with its security policy.

4.3.18 T.PROCOM

O.ENCRYP requires that the TOE protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.

4.3.19 T.REMOTE_ATTACK

O.ACCOUN requires that users be properly identified and held accountable for their actions (including sending messages) or when they use security functions. O.ALARM ensures that the TOE is capable of detecting a failure or error with any component and provides an alarm for notification of security-related events and of a failure or error. This detection and alarming will help to deter authorized users or unauthorized agents from introducing malicious code since, and will provide notice of the introduction at an early stage. O.AUDIT ensures that the TOE provides an audit capability, with accurate dates and times, so that lost or missing audit records would be evident. O.CRYPTOGRAPHY protects the confidentiality of the dialogue between the TOE and an authorized administrator, thus helping to protect against unauthorized reading of the security-critical TOE configuration data. O.SECFUN ensures that only authorized administrators can access administrative functionality, thus preventing unauthorized agents from disrupting the TOE through the administrative interface. O.SINUSE ensures that the TOE prevents the reuse of authentication data.

4.3.20 T.REPEAT

O.IDAUTH ensures that users are identified. O.ROLE ensures that the TOE prevents users from gaining access to and performing operations on its resources/objects unless they have been granted access by the resource/object owner or they have been assigned to a role (by an authorized administrator) which permits those operations. O.SINUSE ensures that the TOE prevents the reuse of authentication data.

4.3.21 T.REPLAY

O.SECFUN ensures that only authorized administrators can access administrative functionality, thus preventing unauthorized agents from disrupting the TOE through the administrative interface. O.SINUSE ensures that the TOE prevents the reuse of authentication data.

4.3.22 T.SELPRO

O.CRYPTOGRAPHY protects the confidentiality of the dialogue between the TOE and an authorized administrator, thus helping to protect against unauthorized reading of the security-critical TOE configuration data. O.SECSTA protects the TOE during start-up or recovery. O.SELPRO ensures that the TOE is protected against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

4.3.23 T.SERVICE_MISUSE

O.IDAUTH ensures that the TOE uniquely identifies and authenticates the claimed identity of a user before granting access to TOE functions. O.ROLE ensures that the TOE prevents users from gaining access to and performing operations on its resources/objects unless they have been granted access by the resource/object owner or they have been assigned to a role

(by an authorized administrator) which permits those operations. O.SECFUN ensures that only authorized administrators can access administrative functionality.

4.3.24 T.UNAVAILABLE

O.TOE_AVAILABLE ensures that the TOE is resilient to denial of service attacks, which are a common means of attempting to disrupt site operations.

4.3.25 T.USAGE

OE.ADMTRA ensures that authorized administrators are selected and trained in the establishment and maintenance of security policies and practices as defined by the administrator guidance.

4.3.26 A.ACCESS

OE.ACCESS defines rights for users to gain access and perform operations on information in terms of one or more roles that are then granted to the users by the TOE Administrator. These roles accurately reflect the users job function, responsibilities, qualifications, and/or competencies within the enterprise.

4.3.27 A.ASSET

OE.ASSET allows for the storage of assets whose value merits moderately intensive penetration or masquerading attacks on the TOE or in areas that it protects.

4.3.28 A.DIRECT

OE.CONSOLE and OE.DIRECT allow for a direct console connection to the TOE.

4.3.29 A.GENPUR

OE.GENPUR and OE.PUBLIC ensure that the TOE does not host public data.

4.3.30 A.LOWEXP

OE.LOWEXP allows for connections to the Internet or other networks where the threat of malicious attacks aimed at discovering exploitable vulnerabilities is low.

4.3.31 A.NOEVIL

OE.ADMTRA ensures that authorized administrators are selected and trained in the establishment and maintenance of security policies and practices as defined by the administrator guidance. OE.GUIDANCE provides the administrative guidance for delivering, installing, administering, and operating the console in a manner that maintains security. OE.NOEVIL assumes that administrators are trusted.

4.3.32 A.NOREMO

OE.NOREMO ensures that human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.

4.3.33 A.PHYSEC

OE.PHYSEC ensures that the TOE is located within controlled access facilities that prevent unauthorized physical access by outsiders. The TOE is installed so that it is protected from casual contact by employees (e.g., unintentional harm that could be caused by a person knocking into the cables).

4.3.34 A.PUBLIC

OE.PUBLIC ensures that the TOE does not host public data.

4.3.35 A.REMACC

OE.REMACC allows authorized administrators to access the TOE remotely from the internal and external networks.

4.3.36 A.SINGEN

OE.SINGEN ensures that information can not flow between the internal and external networks unless it passes through the TOE.

4.3.37 A.TIME_SOURCE

OE.TIME_SOURCE provides a reliable time source to which network resources may connect for the purpose of synchronizing their local time. This synchronization ensures reliable time is available across multiple devices in support of audit.

4.3.38 P.CRYPTO

O.CRYPTOGRAPHY and O.ENCRYP protect the confidentiality of the dialogue between the TOE and an authorized administrator, thus helping to protect against unauthorized reading of the security-critical TOE configuration data.

5 SECURITY REQUIREMENTS

This section provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC, and an augmented component.

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2 are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item]. To improve readability selections of [none] are generally not shown.

- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*]. To improve readability assignments of [*none*] are generally not shown.

- Refinement: Refined components are identified by underlining additional information, or ~~strikeout~~ for deleted text.

- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_IFC.1(1), Subset information flow control (unauthenticated web service)' and 'FDP_IFC.1(2) Subset information flow control (authenticated web service)'.

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC, summarized in Table 3 - Security Functional Requirements. The requirements that are in addition to the PP requirements are indicated by bold text.

Identifier	Name
FAU_ARP.1	Security alarms
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAA.1	Potential violation analysis
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG.1	Protect audit trail storage
FAU_STG.3	Action in case of possible audit data loss
FAU_STG.4	Prevention of audit data loss
FCS_COP.1	Cryptographic operation

Identifier	Name
FDP_ETC.1	Export of user data without security attributes
FDP_IFC.1(1)	Subset information flow control (unauthenticated web service)
FDP_IFC.1(2)	Subset information flow control (authenticated web service)
FDP_IFF.1(1)	Simple security attributes (unauthenticated web service)
FDP_IFF.1(2)	Simple security attributes (authenticated web service)
FDP_ITC.1	Import of user data without security attributes
FDP_RIP.1	Subset residual information protection
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.2	User authentication before any action
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.7	Protected authentication feedback
FIA_UID.2	User identification before any action
FMT_MOF.1(1)	Management of security functions behavior (1)
FMT_MOF.1(2)	Management of security functions behavior (2)
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_MTD.2	Management of limits on TSF data
FMT_REV.1(1)	Revocation (WebGUI)
FMT_REV.1(2)	Revocation (CLI)
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_FLS.1	Failure with preservation of secure state
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_STM.1	Reliable time stamps
FRU_FLT.2	Limited fault tolerance
FRU_RSA.1	Maximum quotas (transactions)
FTA_SSL.3	TSF-initiated termination

Table 3 - Security Functional Requirements

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_ARP.1 Security alarms

FAU_ARP.1.1 The TSF shall take [*send an email alert to the specified email address*] upon detection of a potential security violation.

5.1.1.2 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. [*the events identified in Table 4*].

Functional Component	**Auditable Event(s)**	**Additional Audit Information**
FAU_ARP.1	notification that potential security violation detected	username that was notified and identification of alert type, count, source
FAU_SAA.1	potential security violation detected	identification of alert type, count, source
FAU_SEL.1	changes to the overall log level or component log level	new level
FAU_STG.3	disk usage reaches 80%	
FCS_COP.1	Success and failure, and the type of cryptographic operation	The identity of the external IT entity attempting to perform the cryptographic operation
FDP_ETC.1	export	the identity of the user performing the function
FDP_IFF.1(1)	all decisions on requests for information flow	presumed source internet protocol (IP) address, presumed destination IP address, workflow runtime rule information, status of flow
FDP_IFF.1(2)	all decisions on requests for information flow	presumed source IP address, presumed destination IP address, workflow runtime rule information, status of flow, username
FDP_ITC.1	import	the identity of the user performing the function
FIA_AFL.1	The reaching of the threshold	The identity of the offending

Functional Component	Auditable Event(s)	Additional Audit Information
	for unsuccessful authentication attempts and the subsequent restoration by the authorized administrator of the user's capability to authenticate	user and the authorized administrator
FIA_ATD.1	changes to user attributes	username and role that was changed
FIA_UAU.2	all use of the authentication mechanism	The user identities provided to the TOE
FIA_UID.2	all use of the authentication mechanism	The user identities provided to the TOE
FIA_UAU.5	all use of the authentication mechanism	The user identities provided to the TOE
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit	The identity of the authorized administrator performing the operation
FMT_MTD.2	none	none
FMT_SMR.1	changes to users assigned to roles	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role
FPT_FLS.1	failure of a node in a cluster	identification of node that failed
FPT_STM.1	Changes to the time	The identity of the authorized administrator performing the operation
FRU_RSA.1	enforcement of quota	transaction limit that has been reached

Table 4 - Additional Audit Information[7]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b. For each audit event type, based on the auditable event definitions of the functional components included in the ST, [*information included in the 'Additional Audit Information' column of Table 4*].

[7] The components in bold are additional to the PP audit requirements.

5.1.1.3 FAU_GEN.2 User identity association

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

5.1.1.4 FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a. Accumulation or combination of [*Configuration Administrator configured interval alerts*] known to indicate a potential security violation; and
b. [*no other rules*].

5.1.1.5 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [*the Operations Administrator*[8]] with the capability to read [*all audit information*[9]] 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.

5.1.1.6 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [*selection/searches and ordering/sorting*[10]] of audit data based on [*user identify, presumed subject address, range of dates, range of times, range of address, and/or search string*].

5.1.1.7 FAU_SEL.1 Selective audit

FAU_SEL.1.1 The TSF shall be able to select the set of audited events from the set of all auditable events based on the following attributes:

a. [none];
b. [*log level, component*[11]].

[8] The PP specifies 'an authorized administrator'. The TOE restricts this function to the operations administrator.
[9] The PP uses the term 'all audit trail data'. This ST uses more common terminology.
[10] The PP uses the term searches and ordering.
[11] Components consist of input server, invocation agent, workflow engine, nested workflow engine, and custom services (more details are in 1.5.3.1 Functional Components and 6.1.2 F.Audit).

5.1.1.8 FAU_STG.1 Protected audit trail storage[12]

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

FAU_STG.1.2 The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in the audit trail.

5.1.1.9 FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TSF shall [*send e-mail notification*] if ~~the audit trail~~ disk usage exceeds [*80% of capacity*].

Note: The administrator can set a limit on audit trail storage by specifying the size of an audit log and the total file system disk space allowed for buffering log files. Provided that disk space is available audit records will not be overwritten until these limits are reached. By checking disk capacity this not only ensures that there is sufficient audit storage available but that there is also sufficient disk space for TOE operation.

5.1.1.10 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall [***overwrite old audit records***] and [*shall limit the number of audit records lost*] if the audit trail is full.

5.1.2 Cryptographic operation (FCS_COP)

5.1.2.1 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 - The TSF shall perform [encryption of remote authorized administrator sessions] in accordance with a specified cryptographic algorithm: [AES (Advanced Encryption Standard as specified in FIPS 197) encryption (as specified in SP 800-67)] and cryptographic key sizes [that are at least 128 binary digits in length] that meet the following: [FIPS PUB 140-2 (Level 1)].

5.1.3 User Data Protection (FDP)

5.1.3.1 FDP_ETC.1 Export of user data without security attributes

FDP_ETC.1.1 The TSF shall enforce the [*Operation Management SFP*] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

[12] This requirement was updated to match the CC text.

Note: Though the administrator's security attributes are not associated with the exported data the data contains a configuration and security portion.

5.1.3.2 FDP_IFC.1(1) Subset information flow control (unauthenticated web service)

FDP_IFC.1.1(1) The TSF shall enforce the [*Unauthenticated Web Service SFP*] on [*Web Services Clients to process data according to administrator defined Workflow Runtime rules and send to Web Services Servers*].

Note: The ST provides more specific source and destination terms while the PP uses the term 'unauthenticated external IT entities'.

5.1.3.3 FDP_IFC.1(2) Subset information flow control (authenticated web service)

FDP_IFC.1.1(2) The TSF shall enforce the [*Authenticated Web Service SFP*] on [*Web Services Clients to process data according to administrator defined Workflow Runtime rules and send to Web Services Servers only after the information flow has been authenticated at the TOE per FIA_UAU.5*].

5.1.3.4 FDP_IFF.1(1) Simple security attributes (unauthenticated web service)

FDP_IFF.1.1(1)[13] The TSF shall enforce the [*Unauthenticated Web Service SFP*] based on the following types of subjects and information security attributes: [

a. subject security attributes:
   - *presumed address*

b. information security attributes:
   - *presumed address of source subject;*
   - *presumed address of destination subject;*
   - *transport layer protocol;*
   - *TOE interface on which traffic arrives and departs;*
   - *service;*
   - *input server consisting of HTTP and HTTPS;*
   - *invocation agent consisting of HTTP and HTTPS; and*
   - *Workflow Runtime Rules*].

FDP_IFF.1.2(1)[14] The TSF shall permit an information flow between a controlled subject and another controlled subject ~~information~~ via a controlled operation if the following rules hold: [

a. the presumed address of the source subject, in the information, translates to an internal network address;

[13] The PP specifies transport layer protocol, TOE interface, and service. These parameters are specified in the ST in more detail by the input server and invocation agent.
[14] The PP uses the terms internal and external network. Since all interfaces are external to the TOE and the concept of internal/external is defined by the Workflow Runtime rules this distinction is not required in the ST.

b. the presumed address of the destination subject, in the information, translates to an address on the other connected network;
c. source IP address is not blocked; and
d. *all the information security attribute values are unambiguously permitted by the Workflow Runtime Rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator*].

FDP_IFF.1.3(1) The TSF shall enforce the [*none*].

FDP_IFF.1.4(1) The TSF shall explicitly authorise an information flow based on the following rules: [*none*].

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow based on the following rules: [

a. *The TOE shall reject requests for access or services where the information arrives on an* external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;
b. The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;
c. The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;
d. The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network;
e. The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject; and
f. *For application protocols supported by the TOE, the TOE shall deny any access or service requests that do not conform to its associated published protocol specification*].

5.1.3.5 FDP_IFF.1(2) Simple security attributes (authenticated web service)

FDP_IFF.1.1(2) The TSF shall enforce the [A*uthenticated Web Service SFP*] based on the following types of subjects and information security attributes: [

a. subject security attributes:
   - *presumed address*
b. information security attributes:
   - *user identity;*
   - *presumed address of source subject;*
   - *presumed address of destination subject;*

- *transport layer protocol;*
- *TOE interface on which traffic arrives and departs;*
- *service;*
- *security-relevant service command;*
- *input server consisting of HTTP and HTTPS;*
- *invocation agent consisting of HTTP and HTTPS; and*
- *Workflow Runtime Rules*].

FDP_IFF.1.2(2) The TSF shall permit an information flow between a controlled subject and another controlled subject ~~information~~ via a controlled operation if the following rules hold: [

a. the information flow has been authenticated at the TOE per FIA_UAU.5;
b. the presumed address of the source subject, in the information, translates to an internal network address;
c. the presumed address of the destination subject, in the information, translates to an address on the other connected network;
d. source IP address is not blocked; and
e. *all the information security attribute values are unambiguously permitted by the Workflow Runtime Rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator*].

FDP_IFF.1.3(2) The TSF shall enforce the [*none*].

FDP_IFF.1.4(2) The TSF shall explicitly authorise an information flow based on the following rules: [*none*].

FDP_IFF.1.5(2) The TSF shall explicitly deny an information flow based on the following rules: [

a. The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;
b. The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;
c. The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;
d. The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network;
e. The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject; and

f. *For application protocols supported by the TOE, the TOE shall deny any access or service requests that do not conform to its associated published protocol specification***]**.

5.1.3.6 FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the [*Operation Management SFP*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*the administrator performing the import can only import the portion (configuration or security) for which they have the appropriate role*].

5.1.3.7 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [allocation of the resource to] the following objects: [*all objects*[15]].

5.1.4 Identification and Authentication (FIA)

5.1.4.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [a Security Administrator configurable positive integer] within [*non-zero*] unsuccessful authentication attempts occur related to [administrator or Web Service authentication].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*prevent the offending user from successfully authenticating until the Security Administrator takes some action to make authentication possible for the user in question*].

5.1.4.2 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*username, password, role*].

[15] PD-0001 states: Objects that are used by the subjects of the TOE to communicate through the TOE to other subjects (e.g., packets) are resources subject to RIP. However, the internal data structures used to implement those resources are not subject to RIP, unless those internal structures are visible.

5.1.4.3 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [*the requirement that administrator passwords be at least 8 characters*].

5.1.4.4 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each administrative user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.4.5 FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [*password and single-use authentication mechanisms*] to support user authentication.

FIA_UAU.5.2 - The TSF shall authenticate any user's claimed identity according to the [*following multiple authentication mechanism rules:*

a. ***Perfect Forward Secrecy mechanisms of the SSL and SSH protocols*** *shall be used for authorized administrators to access the TOE remotely such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator; and*
b. *reusable password mechanism shall be used for authorized administrators to access the TOE via a directly connected terminal such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator*].

5.1.4.6 FIA_UAU.7 Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide ~~only~~ [*no authentication feedback*] to the user while the authentication is in progress.

5.1.4.7 FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each administrative user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.5 Security Management (FMT)

5.1.5.1 FMT_MOF.1 Management of security functions behaviour (1)

FMT_MOF.1.1(1) The TSF shall restrict the ability to [enable, disable] the functions:

a) [*operation of the TOE;*
b) *Multiple use authentication functions described in FIA_UAU.5*] to [*an authorized administrator*].

Application Note: By "Operation of the TOE" in a) above, we mean having the TOE start up (enable operation) and shut down (disable operation). By "Multiple use authentication" in b) above, we mean the management of password and single use authentication mechanisms.

5.1.5.2 FMT_MOF.1 Management of security functions behaviour (2)

FMT_MOF.1.1(2) The TSF shall restrict the ability to [enable, disable, determine and modify the behavior of] the functions:

a) [*audit trail management;*
b) *Backup and restore for TSF data, information flow rules, and audit trail data; and*
c) *Communication of authorized external IT entities with the TOE*] to [*an authorized administrator*].

Application Note: Determine and modify the behavior of element c (communication of authorized external IT entities with the TOE) is intended to cover functionality such as providing a range of addresses from which the authorized external entity can connect.

5.1.5.3 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [*Unauthenticated Web Service SPF and Authenticated Web Service SFP*] to restrict the ability to [change_default, query, modify, delete] the security attributes [*defined in FDP_IFF.1(1), FDP_IFF.1(2)*] to [*the authorised administrator*].

5.1.5.4 FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [*Operation Management SFP, Unauthenticated Web Service SFP, Authenticated Web Service SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

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

5.1.5.5 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [*perform the actions identified in Table 5 - Management of TSF Data*] the [*on the data identified in Table 5 - Management of TSF Data*] to [*the administrator identified in Table 5 - Management of TSF Data*].

Action	**Data**	**Administrator**
query, modify, delete, assign	user attributes defined in FIA_ATD.1.1	Security Administrator
change_default, query, modify, delete, clear	security portion of configuration data	Security Administrator

set	Time and date used to form the timestamps in FPT_STM.1.1	Security Administrator

Table 5 - Management of TSF Data

5.1.5.6 FMT_MTD.2 Management of limits on TSF data

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [*the number of authentication failures*] to [*the Security Administrator*].

FMT_MTD.2.2 - The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [*actions specified in FIA_AFL.1.2*].

5.1.5.7 FMT_REV.1(1) Revocation (WebGUI)

FMT_REV.1.1(1) The TSF shall restrict the ability to revoke [*security attributes*] associated with the [*WebGUI administrators*] under the control of the TSF to [*authorized administrators*].

FMT_REV.1.2(1) The TSF shall enforce the rules [

a. *a WebGUI administrator who is logged in when the account is revoked is logged out; although the browser may not display a message until the administrator attempts another operation; and the account is removed from the system and cannot be used to log in again; and*
b. *a WebGUI administrator who is logged in when the user role assignment changes is logged out and the changes take effect immediately*].

5.1.5.8 FMT_REV.1(2) Revocation (CLI)

FMT_REV.1.1(2) The TSF shall restrict the ability to revoke [*security attributes*] associated with the [*non-root CLI administrators*] under the control of the TSF to [*authorized administrators*].

FMT_REV.1.2(2) The TSF shall enforce the rules [

a. *a non-root CLI administrator who is logged in when the account is revoked is logged out and the account is removed from the system and cannot be used to log in again; and*
b. *a non-root CLI administrator who is logged in when the user role assignment changes is logged out and the changes take effect immediately*].

5.1.5.9 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*list of management functions listed in Table 6 - Security Management Functions*].

Functional Component	Management Function
FAU_ARP.1	the management (addition, removal, or modification) of actions
FAU_SAA.1	maintenance (deletion, modification, addition) of the subset of system events
FAU_SAR.1	maintenance (deletion, modification, addition) of the group of users with read access right to the audit records
FAU_SAR.3	maintenance (deletion, modification, addition) of the group of users with read access right to the audit records
FAU_SEL.1	changing the log level
FDP_ETC.1	export
FDP_IFF.1(1)	managing the attributes used to make explicit access based decisions
FDP_IFF.1(2)	managing the attributes used to make explicit access based decisions
FIA_AFL.1	changes to authentication failure handling
FIA_ATD.1	assigning users to roles
FMT_MOF.1(1)	enable/disable TOE and multiple use authentication
FMT_MOF.1(2)	enable/disable/determine/modify audit trail, backup/restore, and communication
FMT_MSA.1	control Unauthenticated Web Service SFP and Authenticated Web Service SFP
FMT_MSA.3	alternative initial values for security attributes
FMT_MTD.1	change configuration, operational, and security data
FMT_MTD.2	changes to authentication failure handling
FMT_REV.1(1)	revocation of security attributes
FMT_REV.1(2)	revocation of security attributes
FPT_STM.1	changes to the time
FRU_FLT.2	cluster configuration
FRU_RSA.1	changing quotas
FTA_SSL.3	changing the session termination time

Table 6 - Security Management Functions

5.1.5.10 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [*configuration administrator, log administrator, operation administrator, and security administrator*].

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

5.1.6 Protection of the TSF (FPT)

5.1.6.1 FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [*failure of a node in a cluster*].

Note: This applies to the HA or clustered configuration only.

5.1.6.2 FPT_ITT.1 Basic internal TSF data transfer protection

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

5.1.6.3 FPT_STM.1 Reliable time stamps

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

5.1.7 Resource Utilisation (FRU)

5.1.7.1 FRU_FLT.2 Limited fault tolerance

FRU_FLT.2.1 The TSF shall ensure the operation of all of the TOE's capabilities when the following failures occur: [*failure of a node in a cluster*].

Note: This applies to the HA or clustered configuration only.

5.1.7.2 FRU_RSA.1 Maximum quotas (transactions)

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [*simultaneous transactions*] that [an application in a workflow] can use [over a specified period of time].

5.1.8 TOE Access (FTA)

5.1.8.1 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [*security administrator specified time interval of user inactivity*].

5.2 DEPENDENCY RATIONALE

Table 7 - Functional Requirement Dependencies identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency. Notes are provided for those cases where the dependencies are satisfied by components which are hierarchical to the specified dependency.

SFR	Dependencies	Dependency Satisfied?	Notes
FAU_ARP.1	FAU_SAA.1	Yes	
FAU_GEN.1	FPT_STM.1	Yes	
FAU_GEN.2	FAU_GEN.1 , FIA_UID.1	Yes	ST includes FIA_UID.2 which is hierarchical to FIA_UID.1
FAU_SAA.1	FAU_GEN.1	Yes	
FAU_SAR.1	FAU_GEN.1	Yes	
FAU_SAR.3	FAU_SAR.1	Yes	
FAU_SEL.1	FAU_GEN.1, FMT_MTD.1	Yes	
FAU_STG.1	FAU_GEN.1	Yes	
FAU_STG.3	FAU_STG.1	Yes	
FAU_STG.4	FAU_STG.1	Yes	
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4		ST includes FDP_IFC.1. FCS_CKM.4 is not required since cryptography is not the main purpose of the TOE and the TOE uses a FIPS 140-2 validated cryptographic module.
FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	Yes	ST includes FDP_IFC.1

SFR	Dependencies	Dependency Satisfied?	Notes
FDP_IFC.1	FDP_IFF.1	Yes	
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	Yes	
FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.3		ST includes FDP_IFC.1, FMT_MSA.3
FDP_RIP.1	No dependencies	Yes	
FIA_AFL.1	FIA_UAU.1	Yes	ST includes FIA_UAU.2 which is hierarchical to FIA_UAU.1
FIA_ATD.1	No dependencies	Yes	
FIA_SOS.1	No dependencies	Yes	
FIA_UAU.2	FIA_UID.1	Yes	ST includes FIA_UID.2 which is hierarchical to FIA_UID.1
FIA_UAU.5			
FIA_UAU.7	FIA_UAU.1	Yes	ST includes FIA_UAU.2 which is hierarchical to FIA_UAU.1
FIA_UID.2	No dependencies	Yes	
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	Yes	
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1, FMT_SMR.1	Yes	ST includes FDP_IFC.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	Yes	
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	Yes	
FMT_MTD.2	FMT_MTD.1, FMT_SMR.1	Yes	
FMT_REV.1	FMT_SMR.1	Yes	
FMT_SMF.1	No dependencies	Yes	
FMT_SMR.1	FIA_UID.1	Yes	ST includes FIA_UID.2 which is hierarchical to FIA_UID.1
FPT_FLS.1	No dependencies	Yes	

SFR	Dependencies	Dependency Satisfied?	Notes
FPT_ITT.1	No dependencies	Yes	
FPT_STM.1	No dependencies	Yes	
FRU_FLT.2	FPT_FLS.1	Yes	
FRU_RSA.1	No dependencies	Yes	
FTA_SSL.3	No dependencies	Yes	

Table 7 - Functional Requirement Dependencies

5.3 TOE SECURITY ASSURANCE REQUIREMENTS

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 4 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw Reporting Procedures (ALC_FLR.2). EAL 4 was chosen for competitive reasons. The developer is claiming the ALC_FLR.1 augmentation since there are a number of areas where current Intel practices and procedures exceed the minimum requirements for EAL 4.

The assurance requirements are summarized in the Table 8 - EAL 4 Assurance Requirements below.

Assurance Class	Identifier	Name
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures

Assurance Class	Identifier	Name
	ALC_FLR.2[16]	Flaw reporting procedures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.3	Focused vulnerability analysis

Table 8 - EAL 4 Assurance Requirements

5.4 SECURITY REQUIREMENTS RATIONALE

The following table maps the SFRs to the security objectives for the TOE.

[16] ALR_FLR.2 is an augmentation to the EAL 4 assurance requirements.

	O.ACCOUN	O.ALARM	O.AUDIT	O.AUDREC	O.CRYPTOGRAPHY	O.ENCRYP	O.IDAUTH	O.LIMEXT	O.MEDIAT	O.ROLE	O.SECFUN	O.SECSTA	O.SELPRO	O.SINUSE	O.TOE_AVAILABLE
FAU_ARP.1		X	X												
FAU_GEN.1	X		X	X											
FAU_GEN.2		X													
FAU_SAA.1		X													
FAU_SAR.1			X	X								X			
FAU_SAR.3			X	X								X			
FAU_SEL.1			X									X			
FAU_STG.1			X								X	X	X		X
FAU_STG.3															X
FAU_STG.4											X	X	X		X
FCS_COP.1					X	X								X	
FDP_ETC.1												X			
FDP_IFC.1(1)									X						
FDP_IFC.1(2)									X						
FDP_IFF.1(1)									X						
FDP_IFF.1(2)									X						
FDP_ITC.1												X			
FDP_RIP.1									X						
FIA_AFL.1													X		
FIA_ATD.1							X			X	X	X			
FIA_SOS.1							X			X					
FIA_UAU.2	X						X			X		X			
FIA_UAU.5							X							X	
FIA_UAU.7										X					
FIA_UID.2	X	X					X			X		X			
FMT_MOF.1(1)	X						X	X	X		X	X			
FMT_MOF.1(2)	X						X	X	X		X	X			
FMT_MSA.1	X						X		X		X	X			
FMT_MSA.3	X						X		X		X	X			
FMT_MTD.1							X				X				
FMT_MTD.2											X				
FMT_REV.1(1)							X					X			
FMT_REV.1(2)							X					X			
FMT_SMF.1										X		X			
FMT_SMR.1							X			X	X				
FPT_FLS.1															X
FPT_ITT.1					X										
FPT_STM.1				X											
FRU_FLT.2															X
FRU_RSA.1									X						X

	O.ACCOUN	O.ALARM	O.AUDIT	O.AUDREC	O.CRYPTOGRAPHY	O.ENCRYP	O.IDAUTH	O.LIMEXT	O.MEDIAT	O.ROLE	O.SECFUN	O.SECSTA	O.SELPRO	O.SINUSE	O.TOE_AVAILABLE
FTA_SSL.3	X														

Table 9 - Mapping Between SFRs and Security Objectives for the TOE

5.4.1 O.ACCOUN

O.ACCOUNT requires that the TOE provide user accountability for information flows through the TOE and for authorized administrator use of security functions. The audit generation, identification/authentication, and management SFRs FAU_GEN.1, FIA_UAU.2, FIA_UID.2, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MSA.1, FMT_MSA.3, and FTA_SSL.3 address this objective.

5.4.2 O.ALARM

FAU_ARP.1and FAU_SAA.1 provide for alarm capabilities while FAU_GEN.2 ensures that audit events are associated with users. FIA_UID.2 ensure that users are identified. FAU_GEN.1 ensures that there is an audit record of actions.

5.4.3 O.AUDIT

This objective is met by the auditing related SFRs FAU_GEN.1, FAU_SAR.1, FAU_SAR.3, FAU_SEL.1, FAU_STG.1 and FAU_ARP.1 which notifies the administrator of security violations.

5.4.4 O.AUDREC

This objective is met by the auditing related SFRs FAU_GEN.1, FAU_SAR.1, FAU_SAR.3, and FPT_STM.1.

5.4.5 O.CRYPTOGRAPHY

This objective is met by FCS_COP.1 which specifies the requirements for a FIPS 140-2 validated cryptographic module. FPT_ITT.1 provides for the protection of data transferred within a cluster.

5.4.6 O.ENCRYP

This objective is met by FCS_COP.1 which specifies the requirements for a FIPS 140-2 validated cryptographic module.

5.4.7 O.IDAUTH

This objective is met through a combination of SFRs consisting of FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.5, FIA_UID.2, FMT_MOF.1(1), FMT_MOF(2), FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_REV.1(1), FMT_REV.1(2), and FMT_SMR.1 which provide for identification, authentication, management, revoking of rights, and user roles.

5.4.8 O.LIMEXT

This objective is addressed by FMT_MOF.1(1) and FMT_MOF.1(2), which restricts access to administrative functions.

5.4.9 O.MEDIAT

The objective O.MEDIAT is met by FDP_IFC.1(1), FDP_IFF.1(2), FDP_IFF.1(1), FDP_IFF.1(2), FDP_RIP.1, and FRU_RSA.1 which mediate information flow through the TOE. The SFRs FMT_MOF.1(1), FMT_MOF.1(2), FMT_MSA.1, and FMT_MSA.3 address the related management functions.

5.4.10 O.ROLE

O.ROLE is met by a combination of FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FMT_SMF.1, and FMT_SMR.1 which provide for user identification, authentication, and management of roles.

5.4.11 O.SECFUN

This objective is addressed through a combination of the audit, identification and authentication, and management functions consisting of FAU_STG.1, FAU_STG.4, FIA_ATD.1, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, and FMT_SMR.1.

5.4.12 O.SECSTA

This objective requires that the provide functions to enable authorized administrators to effectively manage and maintain the TOE and its security functions. The audit, identification/authentication and management SFRs FAU_SAR.1, FAU_SAR.3, FAU_SEL.1, FAU_STG.1, FAU_STG.4, FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_REV.1(1), FMT_REV.1(2), and FMT_SMF.1 contribute to meeting this objective. FMT_REV.1(1) and FMT_REV.1(2) ensures that an administrator can revoke

previously granted rights immediately. FDP_ETC.1 and FDP_ITC.1 ensure that the SOAE configuration data can be saved and restored.

5.4.13 O.SELPRO

FAU_STG.1, FAU_STG.4, and FIA_AFL.1 contribute to this objective by ensuring that audit information is available and that brute force authentication attempts are prevented.

5.4.14 O.SINUSE

FCS_COP.1 and FIA_UAU.5 ensure that authentication credentials are not compromised thereby fulfilling this objective.

5.4.15 O.TOE_AVAILABLE

FRU_RSA.1 contributes to this objective by reducing the likelihood of a successful denial-of-service attack. FAU_STG.1 provides for protected audit trail storage while FAU_STG.3 and FAU_STG.4 ensure that the administrator is notified before disk storage is limited and that auditing continues when the audit trail is full. FPT_FLS.1 allows for the preservation of a secure state when an appliance in a cluster fails and FRU_FLT.2 ensures that the TOE continues to operate when a node in a cluster fails. FRU_RSA.1 contribute to this objective by reducing the likelihood of a TOE component failing due to excessive traffic.

6 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements. Table 10 - Mapping Between SFRs and Security Functions provides the mapping between the SFRs and the security functions.

	F.Admin	F.Audit	F.Protect	F.WebService
FAU_ARP.1		X		
FAU_GEN.1		X		
FAU_GEN.2		X		
FAU_SAA.1		X		
FAU_SAR.1		X		
FAU_SAR.3		X		
FAU_SEL.1		X		
FAU_STG.1		X		
FAU_STG.3		X		
FAU_STG.4		X		
FCS_COP.1			X	
FDP_ETC.1	X			
FDP_IFC.1(1)				X
FDP_IFC.1(2)				X
FDP_IFF.1(1)				X
FDP_IFF.1(2)				X
FDP_ITC.1	X			
FDP_RIP.1			X	
FIA_AFL.1	X			
FIA_ATD.1	X			
FIA_SOS.1	X			
FIA_UAU.2	X			
FIA_UAU.5	X			
FIA_UAU.7	X			
FIA_UID.2	X			
FMT_MOF.1(1)	X			
FMT_MOF.1(2)	X			
FMT_MSA.1	X			
FMT_MSA.3	X			
FMT_MTD.1	X			

	F.Admin	F.Audit	F.Protect	F.WebService
FMT_MTD.2	X			
FMT_REV.1(1)	X			
FMT_REV.1(2)	X			
FMT_SMF.1	X			
FMT_SMR.1	X			
FPT_FLS.1			X	
FPT_ITT.1			X	
FPT_STM.1		X		
FRU_FLT.2			X	
FRU_RSA.1			X	
FTA_SSL.3	X			

Table 10 - Mapping Between SFRs and Security Functions

6.1 TOE SECURITY FUNCTIONS

A description of each of the TOE security functions follows.

6.1.1 F.Admin

The TOE provides for the ability to administer the appliance from a web browser interface or from a command line. Some administrative actions can be performed from the Web GUI interface within the browser. The command line is accessible via SSH. From the command line, the evaluated configuration restricts the administrator to stopping and starting services, user management commands and audit review commands. The TOE enforces an authentication failure limit for the administrator and will prevent further login attempts for the offending user. Changes to the limit and re-enabling of an account are restricted to the Security Administrator.

No action is possible prior to identification and authentication. The TOE does not provide feedback while authentication is in progress. Web GUI and SSH command shell sessions are terminated after an administrator specified period of inactivity.

Remote administration sessions are established using Perfect Forward Secrecy (PFS) mechanisms of the SSL and SSH protocols in order to demonstrably meet the intent of the protection profile requirement for a single-use authentication mechanism.

Administrator user attributes consist of username, password, and role. Passwords must be at least eight characters in length. The system has three administrator users which are assigned to mutually exclusive roles. These roles are the Configuration Administrator, Log Administrator, Operations Administrator, and Security Administrator. Additional accounts can be created by the Security Administrator. Changes to user role assignments are immediate. Through the use of SSH or HTTPS the TOE enforces a single-use authentication mechanism.

The root user account is used for performing administrator actions via the SSH command shell. The root is not assigned a SOAE role, but all the functionality that can be performed by the Security Administrator is applicable to the root user.

By default the TOE does not pass traffic and traffic only flows via the Unauthenticated Web Service SFP and Authenticated Web Service SFP when rules have been configured by the administrator. When an administrator account is created there is no pre-assigned default role.

The administrator can save the configuration data to a file and subsequently restore the configuration. The exported file contains a configuration portion and a security portion. When the configuration data is imported an administrator can only import the portion(s) applicable to their assigned role(s).

6.1.2 F.Audit

The TOE provides administrator configurable alerts upon detection of a potential security violation and can notify an administrator via email. Audit records are generated for the events specified in FAU_GEN.1 and where applicable are associated with an administrator, workflow, and user for an authenticated information flow. The timestamp for the audit log is provided by the TOE.

The administrator is provided with an interface to read all audit information and is able to perform searches and ordering. Searches can be based on time, or strings within the audit records.

The set of events that is audited can be changed based on log level and component. Components consist of input server, invocation agent, workflow engine, nested workflow engine, and custom services. Log levels consist of fatal, trace, error, warning, info, verbose, and debug. A log level of fatal means that only most critical error messages are logged thereby minimizing the logging output and achieving maximum system performance. A level of trace would result in every message created by the TOE being logged. The other levels fall in between fatal and trace. For HTTP traffic the log level can also be specified for an IP address and/or netmask.

Audit records are protected from unauthorized deletion and are protected from modification. The interface presented to the administrator provides the ability to maintain the logs meaning that they can be read but no modification ability is provided. The IT environment is required

to prevent access to the logs, except to an authorized administrator using the TOE's interfaces.

The TOE limits the size of log files and will notify the administrator if disk usage exceeds 80% of capacity. By checking disk capacity this not only ensures that there is sufficient audit storage available but that there is also sufficient disk space for TOE operation.

6.1.3 F.Protect

The TOE uses a FIPS 140-2 validated cryptographic module to protect administrator SSH sessions, the inter-node communication link for the dual appliance configuration, and configuration data that is exported to an intermediary for backup purposes. The TOE clears memory prior to use to protect residual information.

The TOE provides the ability to limit the simultaneous transactions that an application can use over a specified period of time for workflows defined by the Web Service SFPs.

The TOE provides the ability to configure multiple appliances in a cluster. This can be done to improve performance or provide for fault tolerance. Clustering is, for the most part, transparent to the administrative user since administration is performed on the cluster using either appliance. However, each appliance within a cluster can be addressed individually, and its individual status can be determined. Appliances communicate via an Inter-node communication link. Any time a change is made to a node, that change is propagated to all the nodes in the cluster. Changes that are propagated from one node to another are:

- Application changes
- Application configuration changes
- Global configuration changes

When a node fails in a cluster the other node will take over. Each node performs its own logging or audit generation and consequently logs from a failed node would not be available.

6.1.4 F.WebService

The TOE mediates access between sources and destinations of web data based on rules defined by the administrator. Rulesets are created by the Operation Management process and stored for use by the Workflow Runtime. The Workflow Runtime is required to allow or deny transfer of the message from source to destination based on the ruleset. The default information flow security policy for the SOAE is that message transfers are denied unless explicitly allowed by the ruleset. A blank ruleset thus forbids all message transfer. The ruleset is traversed from top to bottom and all applicable rules must be obeyed before the message is allowed to pass. Rulesets address denial of service rules, allowed protocols and protection mechanisms, such as the use of SSL[17]. The ruleset may require successful

[17] The underlying cryptographic protocols are defined outside the TOE and are not evaluated.

authentication before the transfer is allowed. By default, authentication is not required. The authentication can be locally, to a LDAP server, using a X.509 certificate, username and password stored in HTTP header. The authentication for web services is provided by the Authentication Server, which is not part of the TOE. The ruleset may be over-ridden by IP filters, which have the ability to block specific IP addresses.

Information flow is controlled by workflow rules which work in conjunction with input servers and invocation agents. The TOE includes pre-defined input servers consisting of file, HTTP, HTTPS, JMS, MLLP, and TCP/IP (only HTTP and HTTPS are supported in the evaluated configuration). Additionally there is the soae-custom input server (SOAE-H only) that allows administrators to define input servers. The SOAE-H TOE variant includes custom input servers to allow HL7, EDI, and HIPAA support. Invocation agents include support for file, HTTP, HTTPS, JMS, MLLP, soae-local, and TCP/IP (only HTTP and HTTPS are supported in the evaluated configuration). Additionally there is the soae-custom invocation agent (SOAE-H only) that allows administrators to define invocation agents. The SOAE-H TOE variant includes custom invocation agents to allow HL7, EDI, and HIPAA support.

7 PP COMPLIANCE RATIONALE

This section is intended to explain any difference between the ST and the PP to which conformance is claimed in Section 2. It demonstrates why the ST is equivalent or more restrictive than the claimed PP, and rationalizes any changes in the ST which are deemed not equivalent or more restrictive than the claimed PP.

The ST states a conformance claim to the U. S. Department of Defense Application-Level Firewall Protection Profile for Basic Robustness Environments 25 July 2007, which allows demonstrable-PP conformance as defined in CC section D3 of part 1 (i.e., "STs claiming conformance with the PP must offer a solution to the generic security problem described in the PP, but can do so in any way that is equivalent or more restrictive to that described in the PP.").

Additional Threats The following threats, which are addressed by the TOE, are added: T.ATTACK_DATA, T.ATTACK_POTENTIAL, T.AUDIT_UNDETECTED, T.BAD_ADMIN, T.BAD_CREDENTIALS, T.CAPTURE, T.DENIAL, T.HIJACK, T.INTERNAL, T.MODIFY_PROTOCOL, T.REMOTE_ATTACK, T.SERVICE_MISUSE, and T.UNAVAILABLE. Such a change makes the ST more restrictive than the claimed PP.

Additional TOE Security Objectives The following TOE security objectives are added: O.ALARM, O.AUDIT, O.CRYPTOGRAPHY, O.ROLE, and O.TOE_AVAILABLE. Such a change makes the ST more restrictive than the claimed PP.

Resistant to Attack of Enhanced-Basic attack potential T.LOWEXP is replaced with T.ENHANCEDEXP, which considers malicious attacks of Enhanced-Basic attack potential. Such a change makes the ST more restrictive than the claimed PP.

Reliable Time Stamp The A.TIME_SOURCE is added to the assumptions on operational environment, and OE.TIME_SOURCE is added to the operational environment security objectives. The time and date provided by the operational environment are used to form the timestamps in FPT_STM.1.1. The TOE ensures that the audit trail data is stamped when recorded with a dependable date and time received from the OE (operating system). In this manner, accurate time and date is maintained on the TOE.

Modification of FAU_STG.4 FAU_STG.4 is changed according to interpretation of the U.S. Government Traffic-filter and Application-level Firewall PPs for Medium Robustness Environments (9 Jan 2006). It allowed the Security Administrator the option of overwriting "old" audit records rather than preventing auditable events, which would protect against denial-of-service attacks. U.S. Department of Defense Application-Level Firewall Protection Profile for Basic Robustness Environments 25 July 2007 requires that the TSF prevent auditable events (i.e., the TOE shuts down) and therefore is susceptible to the DoS threat. In this case the Intel SOAE ST offers an "equivalent" and more "restrictive" solution in terms of countering an additional DoS threat by rolling over log files and not shutting down when the

audit log is full. SOAE can also throttle log entries for the same type of DoS attack events. It can log every nth instance of the same type of DoS Attack. The DoS attacks are categorized as interval alerts and SOAE can group the repetitive instances of alerts into a single log entry.

Single-use Authentication Mechanism for Remote Administration FIA_UAU.5 is changed to use Perfect Forward Secrecy (PFS) mechanisms of the SSL and SSH protocols for remote administration sessions in order to demonstrably meet the intent of the protection profile requirement for a single-use authentication mechanism.

Single-use Authentication Mechanism for FTP and Telnet The FTP and Telnet are not supported by the TOE, thus, the requirement of using single-use authentication mechanism for human users sending or receiving information through the TOE using FTP or Telnet is not applicable. Hence, the FIA_UAU.5 is changed by removing such a requirement, and section 5.1.3.3 (FDP_IFC.1(2) Subset information flow control (authenticated web service)) has been changed to reflect authenticated web service instead of FTP/Telnet services.

Authentication of Web Services The authentication of web services users is done by external LDAP based Authentication Server. After successful authentication, web services users are allowed to pass through the TOE, but they are unable to access TOE's security functionality. Hence, OE.IDAUTH is added to the operational environment security objectives to counter the threat of T.NOAUTH. The FIA_UAU.5 is changed by removing the requirement of using single-use authentication mechanism for authorized external IT entities accessing the TOE. The PD-0115 has been used as guidance for interpreting the claimed PP.

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY AND ACRONYMS

CLI	Command Line Interface
COBOL	COmmon Business-Oriented Language
CRL	Certificate Revocation List
EDI	Electronic Data Interchange
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
HDK	Healthcare Environment Developer Kit
HIPAA	Health Insurance Portability and Accountability Act
HL7	Health Level 7
HTTP	Hyper-Text Transfer Protocol
HTTPS	Secure Hyper-Text Transfer Protocol
IP	Internet Protocol
IT	Information Technology
JAAS	Java authentication and authorization service
JBI	Java Business Integration
JMS	Java Message Service
JMX	Java Management Extensions
JRE	Java Runtime Environment
JVM	Java Virtual Machine
LDAP	Lightweight Directory Access Protocol
MLLP	Minimal Lower Layer Protocol
NCPDP	National Council for Prescription Drug Programs
OM	Operation Management
OS	Operating System
POX	Plain Old XML
PP	Protection Profile
REST	Representational State Transfer
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SOAE	Service Oriented Architecture Expressway
SOAP	Simple Object Access Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TBB	Threading Building Blocks
TCP	Transport Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
URI	Uniform Resource Identifier

XDoS	XML denial-of-service
XML	Extensible Markup Language
XML/WS-Security	Web Services Security Specification
XPath	XML Path Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformation