COMMON CRITERIA PROTECTION PROFILE

For

SECURITY OF WEB SERVICES

Version 1.0

TURKISH STANDARDS INSTITUTION

CONTENTS

1. PP INTRODUCTION

This Protection Profile defines these items below;

- Target of Evaluation(TOE) and related components,
- Critical security and functional features
- TOE Types
- TOE Conformance Claims
- Security problem definition that re defined in TOE scope(Assets, Roles, Threats and Assumptions)
- Security Objectives
- External Component Definition
- In the scope of the Security Functions and Requirements (Select, Assign, Refinement and Iteration operations) and relations between them.
- Acronym and Synonym that included in the PP
- Sources and References that are used by the PP

1.1 PP Reference

PP Title:	Security of Web Services
Sponsor:	**TURKISH STANDARDS INSTITUTION**
Editor(s):	**TURKISH STANDARDS INSTITUTION**
CC Version:	Version 3.1 Revision 4
Evaluation Level:	Evaluation Level of the PP İS EAL Level 2.
Version Number:	1.0
Keywords:	Web Service, Security, Web Service Functions, Audit

Notes: You can easily find the Acronym and Synonym definitions at Part 7.

1.2 TOE Overview

The term Web services describes a standardized way of integrating Web-based applications using the XML, SOAP, WSDL and UDDI open standardsover an Internet protocol backbone. XML is used to tag the data, SOAP is used to transfer the data, WSDL is used for describing the services available and UDDI is used for listing what services are available. Used primarily as a means for businesses to communicate with each other and with clients, Web services allow organizations to communicate data without intimate knowledge of each other's IT systems behind the firewall.

When all major platforms could access the Web using Web browsers, different platforms couldn't interact. For these platforms to work together, Web-applications were developed. Web-applications are simply applications that run on the web. These are built around the Web browser standards and can be used by any browser on any platform. By using Web services, your application can publish its function or message to the rest of the world.

According to the information above, Web Services are summarized like;

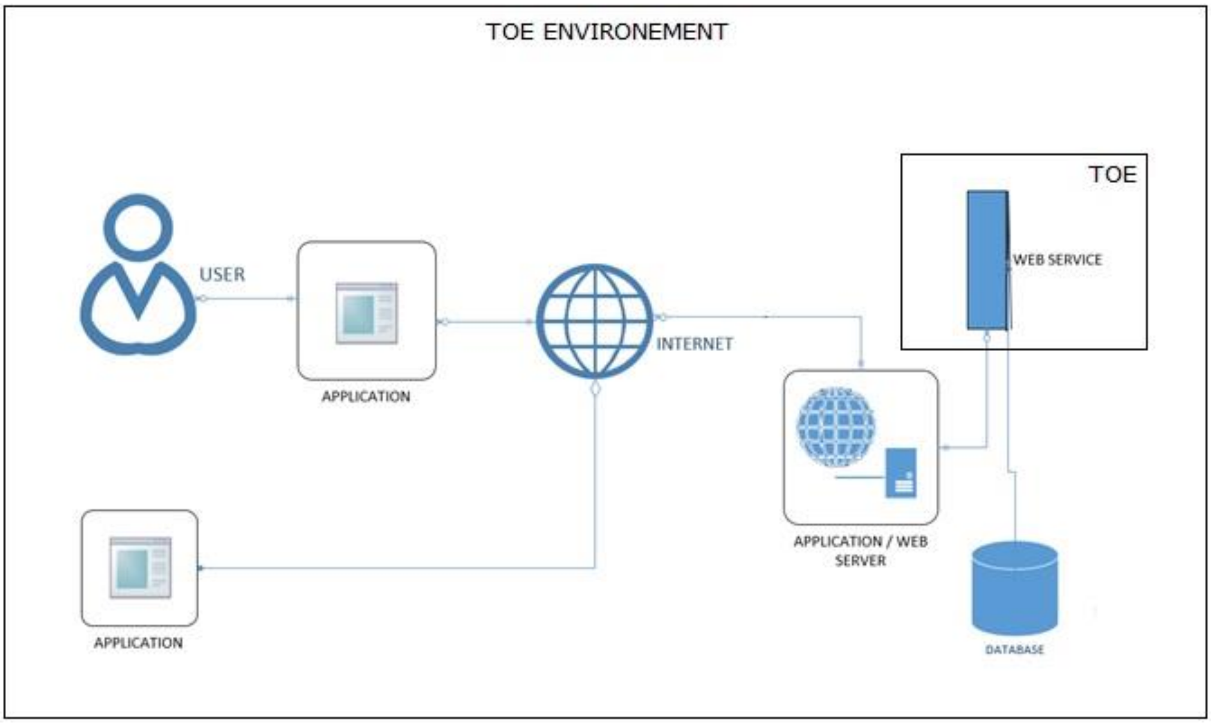
- **Software Language Independence:** With the help of the common standard, web services are developed in many type of software language(C, Java, Php, etc…). It shows platform and Software Language Independence. In this way, making rapid application development and service are increased.
- **Platform-Independent:** Web Services works on the different platforms because of it' s platform-independent properties. That's why, operating system, framework, language and platform can be different. There is a common standard for Web Services to work in different type of platforms. For example; There is a web service that was written in C# language in Windows operating system with MSSQL Database. It was used by the application that was developed in Php language in Linux operating system with MySQL Database.
- **Ease of Integration:** Integration of one application with another application are easily provided by Web Services.
- **Ease of Access:** Web Services works on the http protocols. That's why it is easy to access.

Along with the benefits of the Web Services above, they also face with different threats. Because of this reason, this protection profile have been published for protection and security reason.

This TOE addresses the Protection Profile that is prepared for security of the Web Services.

1.2.1 General overview of the TOE and related components

General structure of the TOE are shown in the Figure 1. According to Figure 1, there are two types of connection for web services. First one, user reach the web service on web browser that consists of working application. At the second scenario, there is application which uses web service directly reach the system.



- Figure1-

1.2.2 Required Non-TOE Hardware/Software

Required Non-TOE Hardware and Software are defined below;

1.2.2.1 Software Environment of TOE

TOE is using the software components that belows;

Operating System: TOE works on the operating system. Web Services also works on the any kind of operating systems. It is platform-independent(Linux, Microsoft Windows, etc...).

Application Server / Web Server: TOE works on the any kind of Application Servers for response of requests and ensure the provision of services(IIS, Apache, WebSephire, etc…).

Database Server: According to the incoming requests, TOE makes optional interactions with Database and send query result. It works on the any kind of Database Servers(Oracle, MSSQL, MySQL, Sysbase, etc…).

1.2.2.2 Hardware Environment of TOE

TOE is using the hardware components that belows;

Because of the Platform-Independent Structure of TOE, and accordance with the characteristics of the selected platform, it depends on any server configuration.

1.2.3 Major security and functional features

Critical Security and Functional Features of TOE are described below.

1.2.3.1 TOE Functional Features

TOE Functional Features consists of the specifications below;

- TOE should always be on active status and should correspond the requests.
- Requests via TOE should always be filtered (IP, Time, etc…). Requests that are not proper for filtering should always reject.
- TOE should always check the requests (Schematic, Content, Parameter, Data Type) and reject the requests that are not proper.
- At the correspond time of request, TOE should not give redundant response. (Error Message Simplification and coding in a proper format).
- TOE should be controlled according to capacity of defined request message and over capacity messages should be rejected.
- TOE should discover virüs in the request message or containing offensive content message. According to this situations, necessary security prevention should be taken by TOE.
- Requests and Responses that are coming to TOE should be done on XML Format type.
- Web services do not require the use of browsers or HTML.

1.2.3.2 TOE Security Features

TOE Security Features consists of the specifications below;

- Connection with TOE should be established in a secure environment
- Validation mechanism should be applied on the Processes about TOE Scope
- Authorization mechanism should be applied on the Processes about TOE Scope
- TOE should provide message integrity of incoming requests
- Making requests should be recorded by TOE

1.2.4 TOE Type

The TOE Type is Web Service.

1.3 Document Conventions

The notation formatting and conventions used in this Protection Profile are consistent with those used in Version 3.1 Revision 4 of the Common Criteria. Selected section choices are discussed here to aid the Protection Profile reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in part 2 of the Common Criteria are selection and assignment.

- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *[italicized text]*.
- The assignment operation is used to assign a specific volue to an unspecified parameter to a component element. Assignments are denoted by [Blue-Colored Text]

2. CONFORMANCE CLAIMS

2.1 CC Conformance Claim

This protection profile claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 4, September 2012
- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 4, September 2012

2.2 PP Claim

This PP does not claim conformance to any protection profile.

2.3 Package Claim

The current PP is conformant to the following security requirements package:

- Assurance package EAL2 conformant to CC, part 3.

2.4 Conformance Claim Rationale

Since this PP does not claim conformance to any protection profile, this section is not applicable.

2.5 Conformance Statement

This PP requires demonstrable conformance of any ST or PP claiming conformance to this PP.

3. SECURITY PROBLEM DEFINITION

3.1 Introduction

3.1.1 Roles

Web Service Client User: Authorized user to access web service that was published by institution.

Web Service Client Application: Authorized client application to access web service that was published by institution.

Attacker: People who want to reach web service and it's functions illegally. Because he/she does not has enough permission to access functions of the service. He/She also wants to blocked the accessability and functionality of the services and use these service informations of the institutions in a bad way outside the jurisdiction.

System Admin: Person who is providing security and configuration of the web service. He/She allows configuration of all hardware and software components during the publishment of the web service.

Designer: Person who designs the publishment of the web service and it's functions.

Developer: Person who develops the publishment of the web service and it's functions.

3.1.2 Assets

Corporate Information

Held by the organization, and only authorized users access to this information.

Corporate Service

Services offered to the organization stakeholders by organization.

XML Message

It consists of the requests and response XML format data information that was taken and send by web service.

3.2 Threats

This section defines the threats that can occur on the TOE. In this situation, relations between threats and protected assets of the TOE.

T.ACCESS CONTROL - T.ACCSCON: Unauthorized user or application access to the web service and it’s functions.

Threat: A result of unauthorized access to corporate information disclosure

Asset: Corporate Information

T.AUTHORITY DEFINITION - T.DEFIN: Outside the defined authority, user access the web service and it’s functions.

Threat: A result of unauthorized access to corporate information disclosure

Asset: Corporate Information

T.DATA MANIPULATION - T.DATAMANIP: During the use of web service, modifying the content of XML Format Message**.**

Threat: Changing XML Format message content of web service, that’s why it gives wrong data or reach different data sources.

Asset: Corporate Information, XML Message

T.BLOCK THE ACCESS - T.BLOCKACC: Preventing the access of the web service that reached by authorized user and/or application. The attack against the web service to stop the services.

Threat: The prevention of the services offered by the institution.

Asset: Corporate Service

T.WRONG USAGE AND CONFIGURATION - T.WRONGUSANDCONFIG: After unauthorized and untrained user usage and configuration, the web service is unable to serve and the authorization system remains ineffective.

Threat: Access to web service by unauthorized person and stay unsufficent for publishment of web service.

Asset: Corporate Service and Information

T.LOSS OF DATA - T.DATALOSS: Attacker gives harm and damage to the Corporate Informations so, it is not possible to make the Corporate Service.

Threat:	Damage and destruction of Corporate Information causes Corporate Service interruption.
Asset:	Corporate Service and Information

T.RECORDS - T.RECORDS: Due to the lack of the records and analyzing, attacker undetected access to the web service and it's functions.

Threat:	Corporate Information Disclosure.
Asset:	Corporate Information

3.3 OSP

This section defines the Organizational Security Policy that can be applied on the TOE.

P.SECURITY - P.SECURE: There should be personal or application-based authorization control. Access to web services that are run within the scope of the TOE must be restricted to only authorized sources. In this context, all necessary components (Switch, Router, Firewall, etc…) and necessary settings (security rules, security configurations) should be done. There should be all kinds of physical and logical security measures should be taken.

P.SECURE COMMUNICATION - P.SECCOMM: Communication with the published web service should be ensured safely. In this context, communication to be performed on the SSL/TLS protocols. Web Service Provider should be ensured, communication should be done on Server Certificate that revoked and annulled(not time expired). During each use of the Web Service Certificate provided by the Web Service Provider and then the web service requests must be authenticated. Secure communication protocol is used to communicate with the Web service must also be provided.

P.FILTERING - P.FILTER: Filters should be applied to a variety of communications within the scope of the Web Service. These filters can be used interchangeably or simultaneously. That can be two types of filter; Time Filter and IP Filter.

- Time Filter provides access to the web service or it's functions in a specified time frames.
- IP Filter provides access to the web service or it's functions in the specified and defined IP Blocks.

P.SCHEMA VALIDATION - P.SCHEMAVALID: XML based message for the web service communication should checked for XML Schema validation. Schema validation of requests that fail should not be considered.

P.VALIDATION AND AUTHENTICATION - P.VALIDANDAUTH: Web services to access and use the corresponding functions previously defined by the Authentication and Authorization mechanism, should be checked and prevented from unauthorized access.

P.ACCESSIBILITY - P.ACCESSIBILITY: If intensive use of Web services in order to ensure the availability of the necessary infrastructure must be installed on the service. In accordance with requests from the load must be balanced and continuous access to web services.

P.MESSAGE CAPACITY - P.MESSAGECAP: Capacity size of the Request and Response Message that is XML formatted message should be determined according to general terms and/or web service's functions. If the message exceeds the capacity, web service requests should be rejected. Messages should be sent to prevent over capacity (Paging, different access methods to use for file transfer (FTP), etc…).

P.SCANNER MECHANISM - P.SCANNER: There should be Scanner mechanism to control against any malicious software and code for any threat. It also be screened and rejected if requests with malicious content.

P.LOG RECORDS - P.RECLOG: All kinds of access to the web service, should be recorded(Access by IP, Time, Accessed Function, Access Performed User, etc…).

P.MAINTENANCE - P.MAINTENANCE: Web services technology is constantly changing and needs to be checked. Necessary security updates should be done according to needs. Received logs (P.RECLOG) should be examined and detect unauthorized access. After detection, necessary safety precautions should be increased. In addition, authorization of new added web service and functions should be checked and each user definition should also be controlled. Similarly, the functions have been canceled and revoked by the user should also be controlled and, necessary security updates should be applied.

3.4 Assumptions

This section defines the Assumptions on the TOE.

A.DESIGNER SECURITY - A.DESIGNERSEC: Design structure of the Web Service which works on the TOE should be designed by trustable designer. Designer must be careful at the designing phase, there must be no backdoor or vulnerability on the design. It is assumed that designer designs the structure of TOE according to security requirements. Designer must also be meet the web service designing features.

A.DEVELOPER SECURTIY - A.DEVELOPERSEC: Development structure of the Web Service which works on the TOE should be developed by trustable developer. Developer must be careful at the coding phase, there must be no backdoor or vulnerability on the development. It is assumed that developer develops the structure of TOE according to security requirements. Developer must also be meet the web service development features.

A.ENVIRONMENT SECURITY - A.ENVSEC: It is assumed latest security settings of operating system, database, application server, web server and other components are complated that TOE will operate on. All security vulnerabilities are closed and taken all the necessary security measures against potential threats is also assumed.

A.PHYSICAL PROTECTION - A.PHYSICALPROTECT: Work environment of TOE and, the software and hardware components that are physically protected to prevent access by unauthorized persons. That's why it is assumed that, environment security are taken and it is unavailable for the unauthorized access.

A.PERSONEL TRAINING - A.TRAINEDPERS: Software and hardware components that will work within the scope of the TOE to be configured, operated and actions that will be taken to protect the authority and have received the necessary training on the subject is assumed to be by authorized person.

4. SECURITY OBJECTIVES

4.1 Security objectives for the TOE

This section defines the Security Objectives for the TOE.

O.ACCESS CONTROL - O.ACCONTROL: The TOE must control access to web services and functions.

O.VALIDATION AND AUTHENTICATION - O. VALAUTH: Validation and authentication mechanism must operated by TOE.

O.INTEGRITY - O.INTEGRITY: The TOE must ensure the integrity of the XML messages.

O.RECORDS - O.RECORDS: The TOE must record all access.

O.AUTHORIZE - O.AUTHORIZE: Within the scope of the TOE, physical and logical configuration of all types of software and hardware components must be performed by an authorized person.

4.2 Securtity objectives for the Operational Environment

This section defines the Security Objectives for the Operational Environment.

OE.PHYSICAL PROTECTION - OE. PHYSPRTC: The TOE should be in a secure physical environment that must be preserved and accessible. Only authorized person should be in the environment.

OE.PERSONEL TRUST - OE. TRUSTPER: The TOE must be not only designed by the reliable staff, but also developed, updated and configured. Then, there should be configuration and continuity of the service provided.

OE.TRAINING - OE. TRAINING: Necessary training should be given to the reliable person in the TOE scope.

OE.ENVIRONMENT SECURITY - OE. SECENV: Environment of the TOE should be in a secure. Unauthorized access, service interruption and message damage should be prevented by the taken environment precautions. Necessary configuration must be also provided by qualified person for trustworthy environment.

OE.DEVELOPMENT - OE. DEVLP: Developer and Designer should be ensure that there is no vulnerability while developing and designing of the TOE. Necessary controls are also be provided by them for the information security at the development phase.

4.3 Security Objective Rationale

4.3.1 Rationale for Security Threats to the TOE

THREAT	RATIONALE
T.ACCSCON	This threat is completely countered by • O.ACCCONTROL which ensures the TOE must control access to web services and functions
T.DEFIN	This threat is completely countered by • O.VALAUTH which ensures the validation and authentication mechanism that operated by TOE.
T.DATAMANIP	This threat is completely countered by • O.INTEGRITY requires that the TOE must ensure the integrity of the XML messages.
T.BLOCKACC	This threat is completely countered by • OE.SECENV which ensures the environment of the TOE should be in a secure. Unauthorized access, service interruption and message damage should be prevented by the taken environment precautions. Necessary configuration must be also provided by qualified person for trustworthy environment
T.WRONGUSANDCONFIG	This threat is completely countered by • O.RECORDS which ensures the The TOE must record all access. • OE.TRAINING which ensures nnecessary training should be given to the reliable person in the TOE scope.

T.DATALOSS	This threat is completely countered by • O.INTEGRITY requires that the TOE must ensure the integrity of the XML messages. • O.AUTHORIZE which ensures within the scope of the TOE, physical and logical configuration of all types of software and hardware components must be performed by an authorized person
T.RECORDS	This threat is completely countered by • O.ACCCONTROL which ensures the TOE must control access to web services and functions • O.VALAUTH which ensures the validation and authentication mechanism that operated by TOE. • O.RECORDS which ensures the The TOE must record all access. • O.AUTHORIZE which ensures within the scope of the TOE, physical and logical configuration of all types of software and hardware components must be performed by an authorized person • OE.TRUSTPER which ensures the TOE must be not only designed by the reliable staff, but also developed, updated and configured. Then, there should be configuration and continuity of the service provided. • OE.TRAINING which ensures nnecessary training should be given to the reliable person in the TOE scope.

4.3.2 Rationale for Organizational Security Policy to the TOE

OSP	RATIONALE
P.SECURE	This threat is completely countered by • O.ACCCONTROL which ensures the TOE must control access to web services and functions • O.VALAUTH which ensures the validation and authentication mechanism that operated by TOE. • OE.PHYSPRTC which ensures the TOE should be in a secure physical environment that must be preserved and accessible. Only authorized person should be in the environment. • OE.TRAINING which ensures nnecessary training should be given to the reliable person in the TOE scope. • OE.SECENV which ensures the environment of the TOE should be in a secure. Unauthorized access, service interruption and message damage should be prevented by the taken environment precautions. Necessary configuration must be also provided by qualified person for trustworthy environment

P.SECCOMM	This threat is completely countered by • O.ACCCONTROL which ensures the TOE must control access to web services and functions • O.INTEGRITY requires that the TOE must ensure the integrity of the XML messages. • OE.SECENV which ensures the environment of the TOE should be in a secure. Unauthorized access, service interruption and message damage should be prevented by the taken environment precautions. Necessary configuration must be also provided by qualified person for trustworthy environment
P.FILTER	This threat is completely countered by • O.ACCCONTROL which ensures the TOE must control access to web services and functions • O.VALAUTH which ensures the validation and authentication mechanism that operated by TOE.
P.SCHEMAVALID	This threat is completely countered by • O.INTEGRITY requires that the TOE must ensure the integrity of the XML messages.
P.VALIDANDAUTH	This threat is completely countered by • O.VALAUTH which ensures the validation and authentication mechanism that operated by TOE.
P.ACCESSABILITY	This threat is completely countered by • O.ACCCONTROL which ensures the TOE must control access to web services and functions • OE.SECENV which ensures the environment of the TOE should be in a secure. Unauthorized access, service interruption and message damage should be prevented by the taken environment precautions. Necessary configuration must be also provided by qualified person for trustworthy environment
P.MESSAGECAP	This threat is completely countered by • O.INTEGRITY requires that the TOE must ensure the integrity of the XML messages.
P.SCANNER	This threat is completely countered by • O.INTEGRITY requires that the TOE must ensure the integrity of the XML messages.
P.RECLOG	This threat is completely countered by • O.ACCCONTROL which ensures the TOE must control access to web services and functions • O.VALAUTH which ensures the validation and authentication mechanism that operated by TOE. • O.RECORDS which ensures the The TOE must record all access. • OE.TRUSTPER which ensures the TOE must be not only designed by the reliable staff, but also developed, updated and configured. Then, there should be configuration and continuity of the service provided.

P.MAINTENANCE	This threat is completely countered by • O.ACCCONTROL which ensures the TOE must control access to web services and functions • O.VALAUTH which ensures the validation and authentication mechanism that operated by TOE. • O.RECORDS which ensures the The TOE must record all access. • O.AUTHORIZE which ensures within the scope of the TOE, physical and logical configuration of all types of software and hardware components must be performed by an authorized person • OE.TRUSTPER which ensures the TOE must be not only designed by the reliable staff, but also developed, updated and configured. Then, there should be configuration and continuity of the service provided. • OE.TRAINING which ensures nnecessary training should be given to the reliable person in the TOE scope.

4.3.3 Rationale for Assumptions to the TOE

ASSUMPTIONS	RATIONALE
A.DESIGNERSEC	This threat is completely countered by • O.AUTHORIZE which ensures within the scope of the TOE, physical and logical configuration of all types of software and hardware components must be performed by an authorized person • OE.TRUSTPER which ensures the TOE must be not only designed by the reliable staff, but also developed, updated and configured. Then, there should be configuration and continuity of the service provided. • OE.TRAINING which ensures nnecessary training should be given to the reliable person in the TOE scope. • OE.DEVLP requires that Developer and Designer should be ensure that there is no vulnerability while developing and designing of the TOE. Necessary controls are also be provided by them for the information security at the development phase.
A.DEVELOPERSEC	This threat is completely countered by • O.AUTHORIZE which ensures within the scope of the TOE, physical and logical configuration of all types of software and hardware components must be performed by an authorized person • OE.TRUSTPER which ensures the TOE must be not only designed by the reliable staff, but also developed, updated and configured. Then, there should be configuration and continuity of the service provided. • OE.TRAINING which ensures nnecessary training should be given to the reliable person in the TOE scope. • OE.DEVLP requires that Developer and Designer should be ensure that there is no vulnerability while developing and designing of the TOE. Necessary controls are also be provided by them for the information security at the development phase.

A.ENVSEC	This threat is completely countered by • O.AUTHORIZE which ensures within the scope of the TOE, physical and logical configuration of all types of software and hardware components must be performed by an authorized person • OE.PHYSPRTC which ensures the TOE should be in a secure physical environment that must be preserved and accessible. Only authorized person should be in the environment. • OE.SECENV which ensures the environment of the TOE should be in a secure. Unauthorized access, service interruption and message damage should be prevented by the taken environment precautions. Necessary configuration must be also provided by qualified person for trustworthy environment
A.PHYSICALPROTECT	This threat is completely countered by • O.AUTHORIZE which ensures within the scope of the TOE, physical and logical configuration of all types of software and hardware components must be performed by an authorized person • OE.PHYSPRTC which ensures the TOE should be in a secure physical environment that must be preserved and accessible. Only authorized person should be in the environment. • OE.SECENV which ensures the environment of the TOE should be in a secure. Unauthorized access, service interruption and message damage should be prevented by the taken environment precautions. Necessary configuration must be also provided by qualified person for trustworthy environment.
A.TRAINEDPERS	This threat is completely countered by • O.AUTHORIZE which ensures within the scope of the TOE, physical and logical configuration of all types of software and hardware components must be performed by an authorized person • OE.TRUSTPER which ensures the TOE must be not only designed by the reliable staff, but also developed, updated and configured. Then, there should be configuration and continuity of the service provided. • OE.TRAINING which ensures nnecessary training should be given to the reliable person in the TOE scope. • OE.DEVLP requires that Developer and Designer should be ensure that there is no vulnerability while developing and designing of the TOE. Necessary controls are also be provided by them for the information security at the development phase.

		THREATS							ORGANIZATIONAL SECURITY POLICIES										ASSUMPTIONS				
		T.ACCSCON	T.DEFIN	T.DATAMANIP	T.BLOCKACC	T.WRONGUSANDCONFIG	T.DATALOSS	T.RECORDS	P.SECURE	P.SECCOMM	P.FILTER	P.SCHEMAVALID	P.VALIDANDAUTH	P.ACCESSABILITY	P.MESSAGECAP	P.SCANNER	P.RECLOG	P.MAINTENANCE	A.DESIGNERSEC	A.DEVELOPERSEC	A.ENVSEC	A.PHYSICALPROTECT	A.TRAINEDPERS
SECURITY OBJECTIVES	O.ACCONTROL	X						X	X	X	X			X			X	X					
	O.VALAUTH		X					X	X		X		X				X	X					
	O.INTEGRITY			X			X			X		X			X	X							
	O.RECORDS					X		X									X	X					
	O.AUTHORIZE						X	X										X	X	X	X	X	X
OPERATIONAL ENVIRONMENT	OE. PHYSPRTC								X												X	X	
	OE. TRUSTPER					X		X									X	X	X	X			X
	OE. TRAINING					X		X	X									X	X	X			X
	OE. SECENV				X	X			X	X				X							X	X	
	OE. DEVLP																		X	X			X

5. EXTENDED COMPONENTS DEFINITION

Since this PP has a conformance claim to CC part 2 and 3, there is no need of any additional and extended components.

6. SECURITY REQUIREMENTS

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE. It also shoes the Security Requirements Rationale.

6.1 Security Functional Requirements for the TOE

CLASS	CLASS FAMILY	DESCRIPTION	SELECT	ASSIGN	REFINE	ITERATE
Security Audit	FAU_GEN.1	Audit Data Generation	x	x		
	FAU_GEN.2	User identity association				
	FAU_SAR.1	Audit review		x		
	FAU_SEL.1	Selective audit	x	x		
	FAU_STG.1	Protected audit trail storage	x			
Communication	FCO_NRO.1	Selective proof of origin	x	x		
	FCO_NRR.1	Selective proof of receipt	x	x		
User Data Protection	FDP_ACC.1	Subset Access Control		x		
	FDP_ACF.1	Security attribute based access control		x		
	FDP_DAU.1	Basic Data Authentication		x		
	FDP_IFC.1	Subset information flow control		x		
	FDP_IFF.1	Simple security attributes		x		
Identification and Authentication	FIA_AFL.1	Authentication failure handling	x	x		
	FIA_ATD.1	User attribute definition		x		
	FIA_SOS.1	Verification of Secrets		x		
	FIA_SOS.2	TSF Generation of secrets		x		
	FIA_UAU.1	Timing of authentication		x		
	FIA_UAU.6	Re-authenticating		x		
	FIA_UID.1	Timing of identification		x		

Security Management	FMT_MOF.1	Management of security functions behaviour	x	x		
	FMT_MSA.1	Management of Security Attributes	x	x		
	FMT_MSA.3		x	x		
	FMT_MTD.1	Management of TSF Data	x	x		
	FMT_SAE.1	Time-limited authorization		x		
	FMT_SMF.1	Specification of Management Functions		x		
	FMT_SMR.1	Security roles		x		
Protection of the TSF	FPT_STM.1	Reliable time stamps				
Resource Utilization	FRU_RSA.1	Maximum quotas	x	x		
Trusted Path / Channels	FTP_ITC.1	Inter-TSF trusted channel	x	x		
	FTP_TRP.1	Trusted path	x	x		

6.1.1 Class Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit data generation

Description: Audit data generation defines the level of auditable events, and specifies the list of data that shall be recorded in each record

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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[*basic*] level of audit; and

c) [User Identification and Authorization, Access to Web Service and Functions].

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

a) Date and time of the event, type of event, subject identity (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 PP/ST, [Username, Datetime ,Source IP and Web Service Functions].

FAU_GEN.2 User identity association

Description: User identity association, the TSF shall associate auditable events to individual user identities.

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

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.

The following are examples of the types of the events that should be defined as auditable within each PP functional component:

- **a.** Introduction of objects within the control of the TSF into a subject's address space;
- **b.** Deletion of objects;
- **c.** Changes to subject or object security attributes;
- **d.** Use of Identification and Authentication functions;

SFR	Auditable Events	Extra Informations
FAU_SAR.1	Read data from auditable events	Access Logs, Database logs, Firewall logs, Application and Web Server logs
FAU_SEL.1	User Identification information and web service access events	Web Service Client User information
FAU_STG.1	Protected Audit Trial Storage	Unauthorized deletion and modification audit trails
FDP_ACF.1	Security attribute based SFP access control events	İdentification information of SFP objects
FIA_UID.1	Authorization and authentication information about TSF actions	User Identification informations
FMT_MOF.1	Disable, enable or modify the behaviour of the functions	Web Service and Identification
FMT_MSA.1	Security attributes and actions	Defined access logs and information flow controls
FMT_MTD.1	TSF Data Management events	
FMT_SMF.1	Management functions specifications	List of management functions
FMT_SMR.1	Security roles	
FPT_STM.1	Reliable Time Stamps	
FTP_ITC.1	Providing communication trusted channel	
FTP_TRP.1	Provided communication path	

6.1.1.2 FAU_SAR.1 Audit review

Description: Audit review, provides the capability to read information from the audit records

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [System Admin] with the capability to read [access logs, database logs, firewall logs and application and web server logs] 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.

6.1.1.3 FAU_SEL.1 Selective audit

Description: Selective audit, requires the ability to select the set of events to be audited from the set of all auditable events, identified in FAU_GEN.1 Audit data generation, based upon attributes to be specified by the PP/ST author.

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FMT_MTD.1 Management of TSF data

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

a) [O*bject Identity, User Identity, Host Identity and Event Type*]

b) [Web Service Functions, Web Service Client User, Web Service Client Application(Host), Web Service Access, User Identification and Authorization]

6.1.1.4 FAU_STG.1 Protected audit trail storage

Description: Protected audit trail storage, requirements are placed on the audit trail. It will be protected from unauthorized deletion and/or modification

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

FAU_STG.1.2 The TSF shall be able to [*detect*] unauthorized modifications to the stored audit records in the audit trail.

6.1.2 Class Communication(FCO)

6.1.2.1 FCO_NRO.1 Selective proof of origin

Description: Selective proof of origin, requires the TSF to provide subjects with the capability to request evidence of the origin of information

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for transmitted [Web Service Client User and Web Service Client Application] at the request of the [*originator*].

FCO_NRO.1.2 The TSF shall be able to relate the [IP Address, Username and Password] of the originator of the information, and the [Web Service Functions] of the information to which the evidence applies.

FCO_NRO.1.3 The TSF shall provide a capability to verify the evidence of origin of information to [*originator*] given [limitations on the evidence of origin].

6.1.2.2 FCO_NRR.1 Selective proof of receipt

Description: Selective proof of receipt, requires the TSF to provide subjects with a capability to request evidence of the receipt of information

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FCO_NRR.1.1 The TSF shall be able to generate evidence of receipt for received [Web Service Client User and Web Service Client Application] at the request of the [*originator*].

FCO_NRR.1.2 The TSF shall be able to relate the [IP Address, Username and Password] of the recipient of the information, and the [Web Service Functions] of the information to which the evidence applies.

FCO_NRR.1.3 The TSF shall provide a capability to verify the evidence of receipt of information to [*originator*] given [limitations on the evidence of origin].

6.1.3 Class User Data Protection (FDP)

6.1.3.1 FDP_ACC.1 Subset access control

Description: Subset access control, requires that each identified access control SFP be in place for a subset of the possible operations on a subset of the objects in the TOE

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [access control SFP] on [access the Web Service Functions].

6.1.3.2 FDP_ACF.1 Security attribute based access control

Description: Security attribute based access control allows the TSF to enforce access based upon security attributes and named groups of attributes. Furthermore, the TSF may have the ability to explicitly authorise or deny access to an object based upon security attributes.

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [access control SFP] to objects based on the following: [list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

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

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [rules, based on security attributes, that explicitly authorise access of subjects to objects].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [rules, based on security attributes, that explicitly deny access of subjects to objects].

6.1.3.3 FDP_DAU.1 Basic Data Authentication

Description: Basic Data Authentication, requires that the TSF is capable of generating a guarantee of authenticity of the information content of objects

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [Web Service Client User and Web Service Client Application].

FDP_DAU.1.2 The TSF shall provide [Web Service Access] with the ability to verify evidence of the validity of the indicated information.

6.1.3.4 FDP_IFC.1 Subset information flow control

Description: Subset information flow control, requires that each identified information flow control SFPs be in place for a subset of the possible operations on a subset of information flows in the TOE

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [information flow control SFP] on [list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

6.1.3.5 FDP_IFF.1 Simple security attributes

Description: Simple security attributes, requires security attributes on information, and on subjects that cause that information to flow and on subjects that act as recipients of that information. It specifies the rules that must be enforced by the function, and describes how security attributes are derived by the function.

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [information flow control SFP] based on the following types of subject and information security attributes: [list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

FDP_IFF.1.3 The TSF shall enforce the [additional information flow control SFP rules].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [based on security attributes, that explicitly authorise information flows].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [based on security attributes, that explicitly deny information flows].

6.1.4 Class Identification and Authentication (FIA)

6.1.4.1 FIA_AFL.1 Authentication failure handling

Description: Authentication failure handling, requires that the TSF be able to terminate the session establishment process after a specified number of unsuccessful user authentication attempts. It also requires that, after termination of the session establishment process, the TSF be able to disable the user account or the point of entry (e.g. workstation) from which the attempts were made until an administrator-defined condition occurs

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [*an administrator configurable positive integer within* [3-5]] unsuccessful authentication attempts occur related to [User Identification and Authorization].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*surpassed*], the TSF shall [User Account Passive or Disable].

6.1.4.2 FIA_ATD.1 User attribute definition

Description: User attribute definition, allows user security attributes for each user to be maintained individually.

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [Username and Password, Host IP, Working Time Range].

6.1.4.3 FIA_SOS.1 Verification of secrets

Description: Verification of secrets, requires the TSF to verify that secrets meet defined quality metrics

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [defined quality metric (Defined Time-out Value)].

FIA_SOS.2 TSF Generation of secrets

Description: TSF Generation of secrets, requires the TSF to be able to generate secrets that meet defined quality metrics

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet [defined quality metric (Defined Time-out Value)].

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for [FIA_UAU and FIA_UID].

6.1.4.4 FIA_UAU.1 Timing of authentication

Description: Timing of authentication, allows a user to perform certain actions prior to the authentication of the user's identity.

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.6 Re-authenticating

Description: Re-authenticating, requires the ability to specify events for which the user needs to be re-authenticated

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [FIA_SOS.2 generated message when it is an invalid].

6.1.4.5 FIA_UID.1 Timing of identification

Description: Timing of identification, allows users to perform certain actions before being identified by the TSF

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [list of TSF-mediated actions] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.5 Class Security Management (FMT)

6.1.5.1 FMT_MOF.1 Management of security functions behaviour

Description: Management of security functions behaviour allows the authorised users (roles) to manage the behaviour of functions in the TSF that use rules or have specified conditions that may be manageable.

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [*disable, enable or modify the behaviour of*] the functions [Web Service Access and Identification] to [System Admin].

6.1.5.2 FMT_MSA.1 Management of security attributes

Description: Management of security attributes allows authorised users (roles) to manage the specified security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [FDP_ACC.1 defined access control(s) and FDP_IFC.1 information flow control(s)] to restrict the ability to [*query*] the security attributes [FAU_GEN.1 generated logs] to [System Admin].

FMT_MSA.3 Static attribute initialisation

Description: Static attribute initialisation ensures that the default values of security attributes are appropriately either permissive or restrictive in nature

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [access control SFP, information flow control 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 [System Admin] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.3 FMT_MTD.1 Management of TSF data

Description: Management of TSF data allows authorised users to manage TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [*query*] the [FAU_GEN.1 generated logs] to [System Admin].

6.1.5.4 FMT_SAE.1 Time-limited authorization

Description: Time-limited authorization provides the capability for an authorised user to specify an expiration time on specified security attributes

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FPT_STM.1 Reliable time stamps

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [FIA_SOS.2 generated message] to [System Admin].

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [User Re-Authenticate] after the expiration time for the indicated security attribute has passed.

6.1.5.5 FMT_SMF.1 Specification of Management Functions

Description: Specification of Management Functions requires that the TSF provide specific management functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [list of management functions to be provided by the TSF].

6.1.5.6 FMT_SMR.1 Security roles

Description: Security roles specifies the roles with respect to security that the TSF recognises

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [System Admin].

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

SFR	Management Events	Extra Informations
FMT_MOF.1	Disable, enable or modify the behaviour of the functions	Web Service and Identification
FMT_MSA.1	Security attributes and actions	Defined access logs and information flow controls
FMT_MSA.3	Static attribute initialisation events	Specify alternative initial values
FMT_MTD.1	TSF Data Management events	
FMT_SAE.1	Timi limited authorization	FIA_SOS.2 generated message
FMT_SMF.1	Management functions specifications	List of management functions
FMT_SMR.1	Security roles	

6.1.6 Class Protection of the TSF (FPT)

6.1.6.1 FPT_STM.1 Reliable time stamps

Description: Reliable time stamps, which requires that the TSF provide reliable time stamps for TSF functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.1.7 Class Resource Utilization (FRU)

6.1.7.1 FRU_RSA.1 Maximum quotas

Description: Maximum quotas, provides requirements for quota mechanisms that ensure that users and subjects will not monopolise a controlled resource

Hierarchical to: No other components.

Dependencies: No dependencies.

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [XML Message] that [*Web Service Functions*] can use [*simultaneously*].

6.1.8 Class Trusted Path/Channels (FTP)

6.1.8.1 FTP_ITC.1 Inter-TSF trusted channel

Description: Inter-TSF trusted channel, requires that the TSF provide a trusted communication channel between itself and another trusted IT product

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [*the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [User Identification and Authorization and Web Service Access].

6.1.8.2 FTP_TRP.1 Trusted path

Description: Trusted path, requires that a trusted path between the TSF and a user be provided for a set of events defined by a PP/ST author. The user and/or the TSF may have the ability to initiate the trusted path.

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [*local and remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [*disclosure*]

FTP_TRP.1.2 The TSF shall permit [*local users and remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [*initial user authentication* [Web Service Access]].

6.2 Security Assurance Requirements for the TOE

The assurance requirements for the evaluation of the TOE and for its development and operating environment are chosen as the predefined assurance package EAL2.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

		O.ACCONTROL	O.VALAUTH	O.INTEGRITY	O.RECORDS	O.AUTHORIZE
SECURITY AUDIT	FAU_GEN.1				X	
	FAU_GEN.2	X			X	X
	FAU_SAR.1	X			X	X
	FAU_SEL.1	X			X	X
	FAU_STG.1				X	X
COMMUNICATION	FCO_NRO.1		X	X		
	FCO_NRR.1		X	X		
USER DATA PROTECTION	FDP_ACC.1	X				
	FDP_ACF.1	X	X			X
	FDP_DAU.1		X			X
	FDP_IFC.1		X	X	X	
	FDP_IFF.1		X	X	X	
IDENTIFICATION AND AUTHENTICATION	FIA_AFL.1					X
	FIA_ATD.1					X
	FIA_SOS.1		X			
	FIA_SOS.2		X	X		
	FIA_UAU.1					X
	FIA_UAU.6		X			X
	FIA_UID.1					X
SECURITY MANAGEMENT	FMT_MOF.1	X	X			X
	FMT_MSA.1					X
	FMT_MSA.3	X				X
	FMT_MTD.1	X	X			X
	FMT_SAE.1	X	X			
	FMT_SMF.1	X				
	FMT_SMR.1		X			X
PROTECTION OF THE TSF	FPT_STM.1				X	
RESOURCE UTILIZATION	FRU_RSA.1	X		X		
TRUSTED PATH / CHANNELS	FTP_ITC.1			X		X
	FTP_TRP.1					X

SECURITY OBJECTIVES	SECURITY FUNCTIONAL REQUIREMENTS	
O.ACCONTROL	FAU_GEN.2	Provides user identity association
	FAU_SAR.1	Provides the capability to read information from the audit records
	FAU_SEL.1	Requires the ability to select the set of events to be audited from the set of all auditable events
	FDP_ACC.1	Provides security functional policy for functions and data
	FDP_ACF.1	Allows the TSF to enforce access based upon security attributes and named groups of attributes
	FMT_MOF.1	Management of security functions behaviour allows the authorised users (roles) to manage the behaviour of functions in the TSF that use rules or have specified conditions that may be manageable
	FMT_MSA.3	Static attribute initialisation ensures that the default values of security attributes are appropriately either permissive or restrictive in nature
	FMT_MTD.1	Provides authorised processing of sales data and event data
	FMT_SAE.1	Provides the capability for an authorised user to specify an expiration time on specified security attributes
	FMT_SMF.1	Performing all operations being allowed only in the maintenance mode
	FRU_RSA.1	Provides requirements for quota mechanisms that ensure that users and subjects will not monopolise a controlled resource
O.VALAUTH	FCO_NRO.1	Selective proof of origin, requires the TSF to provide subjects with the capability to request evidence of the origin of information
	FCO_NRR.1	Selective proof of receipt, requires the TSF to provide subjects with a capability to request evidence of the receipt of information
	FDP_ACF.1	Allows the TSF to enforce access based upon security attributes and named groups of attributes
	FDP_DAU.1	Requires that the TSF is capable of generating a guarantee of authenticity of the information content of objects
	FDP_IFC.1	Provides information flow control for sales data and event data
	FDP_IFF.1	Provides information flow control policy for data
	FIA_SOS.1	Requires the TSF to verify that secrets meet defined quality metrics
	FIA_SOS.2	Requires the TSF to be able to generate secrets that meet defined quality metrics
	FIA_UAU.6	Requires the ability to specify events for which the user needs to be re-authenticated
	FMT_MOF.1	Management of security functions behaviour allows the authorised users (roles) to manage the behaviour of functions in the TSF that use rules or have specified conditions that may be manageable
	FMT_MTD.1	Provides authorised processing of sales data and event data
	FMT_SAE.1	Provides the capability for an authorised user to specify an expiration time on specified security attributes

	FMT_SMR.1	Security roles specifies the roles with respect to security that the TSF recognises
O.INTEGRITY	FCO_NRO.1	Selective proof of origin, requires the TSF to provide subjects with the capability to request evidence of the origin of information
	FCO_NRR.1	Selective proof of receipt, requires the TSF to provide subjects with a capability to request evidence of the receipt of information
	FDP_IFC.1	Requires each identified information flow control SFPs be in place for a subset of the possible operations on a subset of information flows in the TOE
	FDP_IFF.1	Provides information flow control policy for data
	FIA_SOS.2	Requires the TSF to be able to generate secrets that meet defined quality metrics
	FRU_RSA.1	Provides requirements for quota mechanisms that ensure that users and subjects will not monopolise a controlled resource
	FTP_ITC.1	Requires that the TSF provide a trusted communication channel between itself and another trusted IT product
O.AUTHORIZE	FAU_GEN.2	Provides user identity association
	FAU_SAR.1	Allows users to read audit records
	FAU_SEL.1	Requires the ability to select the set of events to be audited from the set of all auditable events
	FAU_STG.1	Protects stored audit data from unauthorized deletion
	FDP_ACF.1	Allows the TSF to enforce access based upon security attributes and named groups of attributes
	FDP_DAU.1	Requires that the TSF is capable of generating a guarantee of authenticity of the information content of objects
	FIA_AFL.1	Detects and records authentication failure events
	FIA_ATD.1	Allows user security attributes for each user to be maintained individually
	FIA_UAU.1	Defines user authentication before any action
	FIA_UAU.6	Requires the ability to specify events for which the user needs to be re-authenticated
	FIA_UID.1	No allowed actions before identification
	FMT_MOF.1	Management of security functions behaviour allows the authorised users (roles) to manage the behaviour of functions in the TSF that use rules or have specified conditions that may be manageable
	FMT_MSA.1	Provides the functions to restrict the ability to modify the security attributes to FCR Authorised User
	FMT_MSA.3	Static attribute initialisation ensures that the default values of security attributes are appropriately either permissive or restrictive in nature
	FMT_MTD.1	Provides authorised processing of sales data and event data
	FMT_SMR.1	Security roles specifies the roles with respect to security that the TSF recognises
	FTP_ITC.1	Requires that the TSF provide a trusted communication channel between itself and another trusted IT product
	FTP_TRP.1	Requires that a trusted path between the TSF and a user be provided for a set of events defined by a PP/ST author

O.RECORDS	FAU_GEN.1	Generates correct audit events
	FAU_GEN.2	Provides user identity association
	FAU_SAR.1	Allows users to read audit records
	FAU_SEL.1	Requires the ability to select the set of events to be audited from the set of all auditable events
	FAU_STG.1	Protects stored audit data from unauthorized deletion
	FDP_IFC.1	Requires each identified information flow control SFPs be in place for a subset of the possible operations on a subset of information flows in the TOE
	FDP_IFF.1	Provides information flow control policy for data
	FPT_STM.1	Provides accurate time for logging events

6.3.2 Security Assurance Requirements Rationale

The current assurance package was chosen based on the pre-defined assurance packet EAL2. EAL2 is chosen because the threats that were chosen are consistent with an attacker of basic attack potential and there is also different techniques for developing Web Service Technology.

6.3.3 Security Requirements- Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together forms an internally consistent whole.

The assurance package EAL2 is a pre-defined set of internally consistent assurance requirements. The assurance requirements are internally consistent as all (additional) dependencies are satisfied and no inconsistency appears. Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met. So, there are no inconsistencies between the goals of these two groups of security requirements.

7. ACRONYMS

CC	Common Criteria
EAL	Evaulation Assurance Level
IT	Information Technology
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirements
SFR	Security Functional Requirements
SSL	Secure Sockets Layer
TOE	Target of Evaulation
TSF	TOE Security Functionality

8. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 4, September 2012

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 4, September 2012

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 4, September 2012

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 4, September 2012

[5] SANS, XML Web Services Security and Web based Application Security, Chris Kwabi, GIAC Security Essentials Certification Practical Assignment Version 1.4b, Website URL: http://www.sans.org/reading-room/whitepapers/securecode/xml-web-services-security-web-based-application-security-1201

[6] OWASP, Web Services Architecture and Security, Website URL: https://www.owasp.org/index.php/Web_Services_Architecture_and_Security

[7] OWASP**,** Web Service Security Cheat Sheet, Website URL: https://www.owasp.org/index.php/Web_Service_Security_Cheat_Sheet