1. Introduction

1.1. PP Reference

PP Title:	Geographical Information System (GIS) Security Target
PP Version:	v0.1
PP Release Date:	03 September 2013
TOE Identification:	Geographical Information System Application Protection Profile
CC Identification:	Common Criteria for Information Technology Security Evaluations, Version 3.1R4
Keywords:	GIS, PROTECTION PROFILE, MIS, GEOCODING, GEOSPATIAL

1.2. Conventions

In this Protection Profile some notations and conventions which are taken from the Common Criteria v3.1R4 have been used in order to guide the reader.

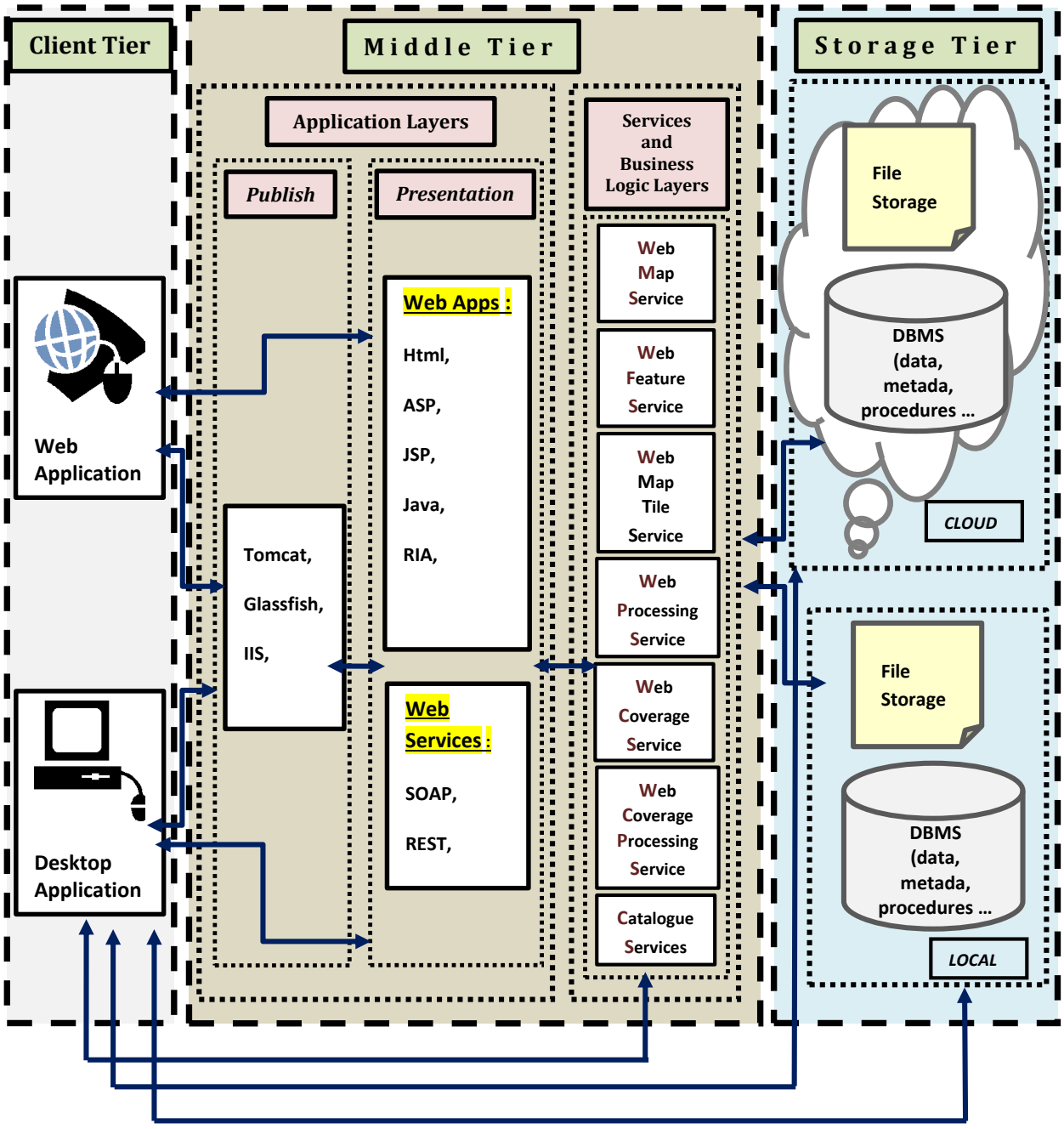
During the specification of the functional requirements under the Section 4, the functional components are interpreted according to the “assignment” and “selection” operations.

- The outcome of the assignment operations is shown with **bold** and identified between “[**brackets**]”.
- The outcome of the selection operations is shown with **bold** and **underlined** and identified between “[**brackets**]”.
- The iterated components are shown **ComponentID/”IterationLabel”.**

1.3. Terminology

1.4. TOE Overview

1.4.1. TOE Description


Client Tier
Middle Tier
Storage Tier
Application Layers
Services and Business Logic Layers
Publish
Presentation
Web Apps :
Html,
ASP,
JSP,
Java,
RIA,
Web Map Service
Web Feature Service
Web Map Tile Service
Web Processing Service
Web Coverage Service
Web Coverage Processing Service
Catalogue Services
Tomcat,
Glassfish,
IIS,
Web Services :
SOAP,
REST,
Web Application
Desktop Application
File Storage
DBMS (data, metada, procedures ...
CLOUD
File Storage
DBMS (data, metada, procedures ...
LOCAL

1.4.2. Usage and Major Security Features

The following features are the major security functionality of the TOE;

Audit: TOE will generate audit logs in order to provide accountability for the administrators and system users. The assigned roles have the capability to review the audit logs.

Identification and Authentication: TOE will sucessfully identify and authenticate its users.

Data Protection: TOE provides confidentiality and integrity of user and TSF data during import/export of data to the or from third parties.

Security Management: TOE will manage the security attributes and user roles.

1.4.3. TOE Type

TOE is a software solution which provides GIS services to third party IT solutions and/or users.

1.4.4. Non-TOE Hardware/Software/Firmware

#	Requirements	Descriptions	Version & Specifications
1	Hardware		
2	Software		

2. Conformance Claims

2.1. CC Conformance Claim

The Protection Profile is based upon

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 4, CCMB-2012-09-001, [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 2, CCMB-2012-09-002, [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 2, CCMB-2012-09-003, [3]

referenced hereafter as [CC].

2.2. PP Claim

This Protection Profile claims the following CC conformance:

- part 2 conformant
- part 3 conformant
- evaluation assurance level (EAL) 3

2.3. Conformance Rationale

EAL3 is accepted as the highest required assurance level according to the sensitivity of the operational environment and the data protected by the TOE.

2.4. Conformance Statement

Security targets or other PPs wishing to claim conformance to this PP can do so as;

“Strict PP conformance. Demonstrable PP conformance is not allowed for this PP”

3. Security Problem Definition

3.1. Threats

T.Accountability: Administrators may not held accountable for their actions.

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

T.Confidentiality: An unauthorized external IT entity may access TSF Data by intercepting it while it is in transmitted accross a network.

3.2. Organizational Security Policies

None.

3.3. Assumptions

A.Manage: There will be one or more competent employees assigned to manage the TOE and the securtiy of the information.

A.Time: The environment will provide a reliable time stamp for use by the TOE.

A.Physical: The TOE will be located within controlled access facilities which will prevent unauthorized physical access.

A.Access: An access control mechanism will be provided by the environment to support identification and authentication of administrative and user accounts.

4. Security Objectives

4.1. Security Objectives for the TOE

O.Admin Authentication: TOE will verify the claimed identity of administrators

O.Admin Identification: TOE will uniquely identify administrators

O.Audit: TOE will provide the capability to create audit records of security relevant events associated with users and allow capability to review audit information.

O.Manage: TOE will allow administrators to effectively manage the TOE and its security functions and must ensure that only authorized administrators are able to access such functionality.

O.Data Protection: TOE will protect the confidentiality and integrity of TSF data during transmission to other trusted IT entities.

4.2. Security Objectives for the Operational Environment

OE.Time: The environment will provide reliable time stamps for use by the TOE.

OE.PhysicalProtection: The TOE will be located within controlled access facilities.

OE.Manage: Competent employees will be assigned to manage TOE and the security of the information it contains.

4.3. Security Objectives Rationale

5. Extended Components Definition

There is not any extended components definition within this Protection Profile.

6. Security Requirements

6.1. Security Functional Requirements

6.1.1. FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [**minimum**] level of audit; and

c) [assignment: other specifically defined auditable events].

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,[assignment: other audit relevant information].

6.1.2. FAU_GEN.1 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.

6.1.3. FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [assignment: authorised users] with the capability to read [assignment: list of audit information] 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.

6.1.4. FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [assignment: methods of selection and/or ordering] of audit data based on [assignment: criteria with logical relations].

6.1.5. FCS_COP

6.1.6. FCS_CKM

6.1.7. FDP_IFC.1 Subset information flow control

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

6.1.8. FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: 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: [assignment: 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 [assignment: additional information flow control SFP rules].

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

6.1.9. FDP_ITC.2 Import of User Data with Security Attributes

FDP_ITC.2.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: additional importation control rules].

6.1.10. FDP_ETC.2 Export of User Data with Security Attributes

FDP_ETC.2.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] when exporting user data, controlledunder the SFP(s), outside of the TOE.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE: [assignment: additional exportation control rules].

6.1.11. FIA_ATD.1 User attribute Definition

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

6.1.12. FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: a defined quality metric].

6.1.13. FIA_UAU.1 Timing of Authentication

FIA_UAU.1.1 The TSF shall allow [assignment: 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.

6.1.14. FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow [assignment: 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.

6.1.15. FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: determine the behaviour of, disable, enable, modify the behaviour of] the functions [assignment: list of functions] to [assignment: the authorised identified roles].

6.1.16. FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the [assignment: access control SFP(s), information flow control SFP(s)] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorised identified roles].

6.1.17. FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [assignment: access control SFP, information flow control SFP] to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP.

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

6.1.18. FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorised identified roles].

6.1.19. FMT_SMF.1 Specification of Management Functions

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

6.1.20. FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: the authorised identified roles].

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

6.2. Security Assurance Requirements

Assurance Class	Assurance Component
ADV: Development	ADV_ARC.1 – Security architecture description
	ADV_FSP.3 – Functional Specification with complete summary
	ADV_TDS.2 – Architectural Design
AGD: Guidance Documents	AGD_OPE.1 – Operational user guidance
	AGD_PRE.1 – Preparative procedures
ALC: Life-cycle Support	ALC_CMC.3 – Authorization controls
	ALC_CMS.3– Implementation representation CM coverage
	ALC_DEL.1 – Delivery procedures
	ALC_DVS.1 – Identification of security measures

Assurance Class	Assurance Component
	ALC_LCD.1 – Development defined life-cycle model
ASE: 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
ATE: Test	ATE_COV.2 – Analysis of coverage
	ATE_DPT.1 – Testing: basic design
	ATE_FUN.1 – Functional testing
	ATE_IND.2 – Independent testing – sample
AVA: Vulnerability Assessment	AVA_VAN.2 –Vulnerability analysis

6.3. Security Requirements Rationale