HMA-T/G-POD Gateway
System Requirements
Document
Terradue
<table>
<thead>
<tr>
<th>Short Title</th>
<th>HMA-T/G-POD Gateway System Requirements Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepared by</td>
<td>Terradue</td>
</tr>
<tr>
<td>Approved by</td>
<td>-</td>
</tr>
<tr>
<td>Reference</td>
<td>T2-ESA-HMAT-RS-08-022</td>
</tr>
<tr>
<td>External Reference</td>
<td>HMAT-SRD-0002-T2</td>
</tr>
<tr>
<td>Issue</td>
<td>0</td>
</tr>
<tr>
<td>Revision</td>
<td>2</td>
</tr>
<tr>
<td>Date of issue</td>
<td>N/A</td>
</tr>
<tr>
<td>Status</td>
<td>DRAFT</td>
</tr>
<tr>
<td>Document type</td>
<td>System Requirements Document</td>
</tr>
<tr>
<td>Distribution</td>
<td>ESA, SPACEBEL</td>
</tr>
<tr>
<td>Category</td>
<td>HMA-T, GPOD</td>
</tr>
<tr>
<td>Keywords</td>
<td></td>
</tr>
<tr>
<td>Comments</td>
<td></td>
</tr>
</tbody>
</table>
### Approval

<table>
<thead>
<tr>
<th>title</th>
<th>HMA-T/G-POD Gateway System Requirements Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>issue</td>
<td>1</td>
</tr>
<tr>
<td>revision</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>author</th>
<th>Terradue</th>
</tr>
</thead>
<tbody>
<tr>
<td>date</td>
<td>2008-09-30</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>approved by</th>
<th>Fabrice Brito</th>
</tr>
</thead>
<tbody>
<tr>
<td>date</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Change Log

<table>
<thead>
<tr>
<th>reason for change</th>
<th>issue</th>
<th>revision</th>
<th>date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial version</td>
<td>0</td>
<td>1</td>
<td>2008-07-20</td>
</tr>
<tr>
<td>Updated</td>
<td>0</td>
<td>2</td>
<td>2008-09-30</td>
</tr>
</tbody>
</table>
# Table of Contents

1 Introduction .................................................................................................................. 1  
1.1 Purpose of the document ......................................................................................... 1  
1.2 Objectives ................................................................................................................ 1  
1.3 Content Overview .................................................................................................. 1  
2 Applicable and Reference Documents ...................................................................... 2  
2.1 Applicable Documents ............................................................................................ 2  
2.2 Reference Documents ............................................................................................. 2  
3 Terms, Definitions and Abbreviated Terms ............................................................... 3  
3.1 Definition of Terms .................................................................................................. 3  
3.2 Abbreviated Terms ................................................................................................. 3  
4 General Description ...................................................................................................... 5  
4.1 Project Background ................................................................................................. 5  
4.2 HMA-T Gateway Product Perspective ................................................................. 8  
4.3 General capabilities ............................................................................................... 9  
4.4 Use Case Diagrams ................................................................................................ 9  
4.5 Sequence Diagram ................................................................................................ 12  
4.6 General constraints .............................................................................................. 13  
4.7 Operational environment ....................................................................................... 13  
4.7.1 Hardware and Software Environment ............................................................. 13  
4.7.2 Networking Environment and External Interfaces ........................................... 13  
4.7.3 Client Interfaces ............................................................................................... 13  
4.8 Assumptions and dependencies ............................................................................ 13  
5 Specific Requirements ................................................................................................. 14  
5.1 General ................................................................................................................ 14  
5.2 Capabilities Requirements ................................................................................... 14  
5.3 System Interface Requirements ............................................................................ 14  
5.4 Computer Resources Requirements ...................................................................... 15  
5.5 Safety Requirements ............................................................................................. 15  
5.6 Reliability Requirements ...................................................................................... 15  
5.7 Quality Requirements .......................................................................................... 15  
5.8 Design Requirements and Constraints .................................................................. 16  
5.9 Software Operations Requirements ....................................................................... 16  
5.10 Software Maintenance Requirements ................................................................. 16
5.11 Software Performance Requirements ........................................... 16

6 Validation Approach And Requirements ........................................ 17
  6.1 Validation approach ........................................................................ 17
  6.2 Validation requirements................................................................. 17
  6.3 Requirement to Validation-Method Correlation Table ....................... 17

7 Traceability ......................................................................................... 18
  7.1 Statement of Work to Software System Specification Requirements Traceability Matrix ................................................................. 18
  7.2 Software System Specification Requirements to Statement of Work Traceability Matrix ................................................................. 18
List of Tables
Table 1 Test Method Definition ................................................................. 17
Table 2 Test Method per Requirement ......................................................... 17
Table 3 SoW to SSS Requirements Traceability Matrix .................................. 18
Table 4 SSS to SoW Requirements Traceability Matrix .................................. 18

List of Figures
Figure 1 G-POD Job Submission Web Service flow ..................................... 7
Figure 2 Client - Gateway use case ............................................................. 10
Figure 3 Gateway - G-POD Web service use case ....................................... 11
Figure 4: System sequence diagram ............................................................ 12
1 Introduction

1.1 Purpose of the document

This document contains the HMA-T/G-POD Gateway System requirements document. It provides in detail the capabilities and services that the prototype system shall provide during the HMA-T project for the harmonization of the authentication between HMA and G-POD.

1.2 Objectives

This document is part of the Requirement Baseline (RB) and is one of the main inputs of the Critical Design Review (CDR).

1.3 Content Overview

Section 1
This section.
Section 2
This section gives the list of all documents applicable to this System Software Specification document and the list of the project document used as reference.
Section 3
This section list all abbreviation and terms used throughout the document.
Section 4
This section gives a general description of the project from a system point of view.
Section 5
This section lists all the requirements identified for the system during the requirement definition phase.
Section 6
This section describes the validation approach selected for this project by Terradue and RAL.
Section 7
This section provided the traceability matrices from and to the Statement of Work requirements.
2 Applicable and Reference Documents

2.1 Applicable Documents

<table>
<thead>
<tr>
<th>Document Code</th>
<th>Description</th>
<th>Standard</th>
<th>Date</th>
</tr>
</thead>
</table>

2.2 Reference Documents

<table>
<thead>
<tr>
<th>Document Code</th>
<th>Description</th>
<th>Code</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>[R1]</td>
<td>SoW For HMA Testbed HMA-T Phase 2</td>
<td>SPB-HMA-T-SOW-002</td>
<td>31-01-2008</td>
</tr>
</tbody>
</table>
3 Terms, Definitions and Abbreviated Terms

3.1 Definition of Terms

This document and its appendices use the terms:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>To confirm a system entity’s asserted principal identity with a specified, or understood, level of confidence.</td>
</tr>
<tr>
<td>Circle of trust</td>
<td>A federation of service providers and identity providers within which service providers accept the authentication asserted by the identity provider.</td>
</tr>
<tr>
<td>Client</td>
<td>Software component that can invoke an operation from a server</td>
</tr>
<tr>
<td>Interface</td>
<td>Named set of operations that characterise the behaviour of an entity</td>
</tr>
<tr>
<td>Operation</td>
<td>Specification of a transformation or query that an object may be called to execute</td>
</tr>
<tr>
<td>Parameter</td>
<td>Variable whose name and value are included in an operation request or response</td>
</tr>
<tr>
<td>Request</td>
<td>Invocation of an operation by a client</td>
</tr>
<tr>
<td>Response</td>
<td>Result of an operation, returned from a server to a client</td>
</tr>
<tr>
<td>The Prime Contractor</td>
<td>Spacebel is the ESA appointed Prime Contractor for the project Heterogeneous Missions Accessibility Testbed “HMA Testbed” (HMA-T). In the following Spacebel is referred to as the “Prime Contractor”.</td>
</tr>
<tr>
<td>The Agency</td>
<td>To indicate the European Space Agency (ESA)</td>
</tr>
<tr>
<td>Service</td>
<td>Capability which a service provider entity makes available to a service user entity at the interface between those entities</td>
</tr>
<tr>
<td>Service Interface</td>
<td>Shared boundary between an automated system or human being and another automated system or human being</td>
</tr>
<tr>
<td>Service Provider</td>
<td>A role donned by a system entity where the system entity provides services to principals or other system entities.</td>
</tr>
<tr>
<td>Shall</td>
<td>To indicate a firm requirement</td>
</tr>
<tr>
<td>Should</td>
<td>To indicate a highly desirable requirement</td>
</tr>
<tr>
<td>TBD</td>
<td>To be defined by the Agency, or in agreement with the Agency</td>
</tr>
<tr>
<td>TBC</td>
<td>To be conformed by the Agency, or in agreement with the Agency</td>
</tr>
</tbody>
</table>

3.2 Abbreviated Terms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDR</td>
<td>Critical Design Review</td>
</tr>
<tr>
<td>CERN</td>
<td>Conseil Européen pour la Recherche Nucléaire</td>
</tr>
<tr>
<td>CITE</td>
<td>OGC Compliance &amp; Interoperability Testing &amp; Evaluation</td>
</tr>
<tr>
<td>EO</td>
<td>Earth Observation</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>ESA</td>
<td>European Space Agency</td>
</tr>
<tr>
<td>ESRIN</td>
<td>European Space Research Institute</td>
</tr>
<tr>
<td>G-POD</td>
<td>Grid Processing on-Demand</td>
</tr>
<tr>
<td>HMA</td>
<td>Heterogeneous Mission Accessibility</td>
</tr>
<tr>
<td>HW</td>
<td>Hardware</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>OGC</td>
<td>Open Geospatial Consortium</td>
</tr>
<tr>
<td>PAC</td>
<td>Processing and Archiving Centre</td>
</tr>
<tr>
<td>PEP</td>
<td>Policy Enforcement Point</td>
</tr>
<tr>
<td>RB</td>
<td>Requirements Baseline</td>
</tr>
<tr>
<td>SAML</td>
<td>Security Assertion Markup Language</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>SP</td>
<td>Service Provider</td>
</tr>
<tr>
<td>SW</td>
<td>Software</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
</tbody>
</table>
4 General Description

4.1 Project Background

The validation of earth remote sensing satellite data, and associated algorithms, often requires a large amount of processing resources and highly interactive access to the large amount of satellite data. On the other-hand, the cost of the necessary computing infrastructure coupled with the access to large volumes of satellite data is often too high to motivate local investments. As such, providing a common shared infrastructure accessible to science users is a very valuable and cost effective approach to support EO science and application development. Grid Processing on-Demand, an ESA initiated project and then industrialized by Terradue provides a “user-segment” putting EO data and processors together.

ESA G-POD is a generic GRID-based operational environment for Earth Observation applications where specific data handling applications can be seamlessly plugged into system. Coupled with high-performance and sizeable computing resources managed by GRID technologies, it provides the necessary flexibility for building an application virtual environment with quick accessibility to data, computing resources and results.

The gridify web portal component used in G-POD delivers a flexible, secure, generic and distributed platform where the user can easily manage all its tasks. From the creation of a new task to the result publication, passing by the data selection and the job monitoring, the user goes through a friendly and intuitive interface accessible from everywhere. Using this infrastructure, ESA also delivers a regular sustained opportunity available to scientists. This opportunity, referred to as the "G-POD CAT-1", creates a partnership opportunity for conducting Earth Science research activities through grid technology. Within this framework, ESA offers on-line access to data, together with the G-POD attached computing infrastructure to host and run the partner’s applications.

The grid model has proven to overcome known problems that haunt Earth observations services with the paradigm change in the data and application flows. This paradigm change reduces the strain on the network, optimizes the use processing resources, reduces substantially or eliminates completely data access time delays and shipping issues and provides a framework for IPR enforcement and management. By reducing or overcoming these obstacles, the G-POD model is currently enthusiastically accepted by the research community. The adoption of the HMA will allow a more widely use for Earth observation services and expand its research user community.

In conclusion, the G-POD Web Service acts as a Earth Observation service provider.

The G-POD security model is based on the Grid Security Infrastructure (GSI). Basically, the principal motivations behind the GSI are:

1. The necessity of establishing for secure communications between elements of a computational Grid.
2. The need to support security across organizational boundaries, thus prohibiting a centrally managed security system.
3. The need to support "single sign-on" for users of the Grid, including
delegation of credentials for computations that involve multiple resources
and/or sites.

The certificate is a central concept in GSI authentication. Every user and service
on the Grid is identified via a certificate, which contains information vital to
authenticating the user or service.

A GSI certificate includes four primary pieces of information:

1. A subject name, which identifies the person or object that the certificate
   represents.
2. A public key belonging to the subject.
3. The identity of a Certificate Authority (CA) that has signed the certificate.
   This certifies that the public key and the identity both belong to the
   subject.
4. The digital signature of the named CA.

A third party (a CA) is used to certify the link between the public key and the
subject in the certificate. In order to trust the certificate and its contents, the
CA’s certificate must be trusted. The link between the CA and its certificate must
be established via some non-cryptographic means, or else the system is not
trustworthy. GSI certificates are encoded in the X.509 certificate format, a
standard data format for certificates established by the Internet Engineering Task
Force (IETF). These certificates can be shared with other public key-based
software, including commercial web browsers from Microsoft Internet Explorer
and Firefox.

Derived from the user’s certificates, G-POD uses proxy certificates to authenticate
the job execution on the grid. The proxy certificate is a digital certificate created
on the fly and digitally signed with the user’s private key; generally it has a
shorter lifetime than your personal certificate (typically days or weeks).

To achieve this, the G-POD infrastructure uses a MyProxy server acting as a
repository for Grid users’ proxy certificates. MyProxy¹ is an open source software
for managing X.509 Public Key Infrastructure (PKI) security credentials
(certificates and private keys) developed by the University of Illinois’ National
Center for Supercomputing Applications (NCSA). MyProxy combines an online
credential repository with an online certificate authority to allow users to securely
obtain credentials when and where needed.

Whenever the user logs into the G-POD Portal, it automatically tries to retrieve
the user’s proxy certificate from the MyProxy repository and uses it to log into the
Grid. It’s the user responsibility to create and upload a valid proxy certificate to
the MyProxy server using the Portal user preferences web page.

However, this only covers the user’s authentication action. To provide
authorisation, the G-POD portal has a membership management section defined
where all users and services are registered and to each element is given a group
with a given set of attributes describing their role and capabilities.

¹ http://grid.ncsa.uiuc.edu/myproxy/
The main module of this component is an Attribute Authority Service. It asserts the requesting individual’s attributes and validates the authorization rights of the request. This means that after validating the requester identity, it must also validate its right to access the information to a given service (be it a data or service resource). The identity database stores the information as a structured collection of information pertaining to a given user or service. Typically, it includes name, address, email address, affiliation, and its electronic identifiers (the Distinguished Name or Certificate Subject). Both of the electronic identifiers are string representations that uniquely identify users, services or organizations together with the ownership of a given certificate and the authority that issued the certificate.

In parallel to the G-POD portal pages published in HTML, the G-POD Web Service high-level functions and services are published via a job-control interface implemented using SOAP. This Wed Service interface allows the remote job submission and control of G-POD services. The G-POD Soap interface is generic and its interface briefly described in this section. Its transport layer is implemented as a set of SOAP RPC style services published on a G-POD portal computer (e.g. http://eogrid.esrin.esa.int) via HTTP.

G-POD WS service invocation follows a well-defined protocol sequence summarized here and depicted in Figure 1:

- First the client initializes a session with the G-POD WS server and authenticate itself;
- Then, the G-POD WS application services available to the authenticated client may be triggered and monitored independently;
- Finally, the client optionally releases its active session with the server.

![Figure 1 G-POD Job Submission Web Service flow](image)

For each invoked service process, status monitoring is accomplished via either of two methods, or both in parallel:

- Asynchronous status queries triggered by the client;
- Explicit status notification triggered by the server back to the client notification server.
In the current implementation, the session initialization is performed via a SOAP service call to the *ifyService* port on the WS server requiring user authentication. In other terms, the client connection defined in the connection call is a registered account on G-POD based on a username and password.

The *Connect* call returns a session-token back to the client, to be used as reference in all subsequent calls to the interface within the defined session. The session token must be used as SOAP header defined as a *SessionKeyType* in any subsequently call to the G-POD WS. The validity and certification of the token is made in the actual subsequent requests (in other terms, a session token does not guarantee the ability to perform any service execution, just identifies the user).

The other methods are briefly described below:

- **SetVariable** - Defines session states variables to enhance the job submission. The possible values for the Name variable are:
  - CE: defines the default CE (hostname) to launch all session’s tasks. This will be discarded if the service is configures to a single CE.
  - PRIORITY: Defines the priority to launch all the session’s tasks.

- **GetVariable** - Retrieves the session states variables. The possible values for the Name variable are:
  - CE: defines the default CE (hostname) to launch all session’s tasks. This will be discarded if the service is configures to a single CE.
  - PRIORITY: Defines the priority to launch all the session’s tasks.

- **SubmitExt** - The SubmitExt operation creates a task of the ServiceName type and submits it for execution. A unique task identifier (taskToken) is returned on submission success, otherwise a SOAP exception is returned.

- **Status** - Returns the current status of the service process referred by the value returned by the SubmitExt function. The keyword “DONE” is returned on task successful completion.

- **GetTaskMetadata** – This operation lists in a key name value pair array all the task parameters classified as metadata by the actual G-POD service being accessed.

- **DescribeService** – This operation lists in an array of feature type the necessary parameters for a given service and their actual meaning.

- **Results** - Returns an array of strings with the URL to access the results published on the portal associated to this task. If the results were published on external server the array will be empty.

## 4.2 HMA-T Gateway Product Perspective

Within the HMA-T project, the role of the HMA-T/G-POD Gateway (HGG) is to serve as a link between the G-POD Web Service and the clients already authenticated by an HMA Identity Provider (IdP). This will ensure that clients authenticated by the IdP have access through the HGG to the G-POD processing Web services exposed.
The authentication at the IdP is out of scope of the HHG as it should be a service provided by HMA.

HGG will nevertheless be able to contact and query the G-POD Policy Enforcement Point (G-POD PEP) and verify the SAML assertion including the attributes of the given user according to the OGC 07-118r1 specification for User Management.

With HGG, the harmonization of users’ authentication between G-POD and HMA is enhanced.

### 4.3 General capabilities

The HMA-T/G-POD Gateway shall:

- Authenticate users on G-POD Web Service;
- Authorize users on G-POD Web-Service;
- Handle Web service requests coming from G-POD Web Service clients;
- Handle Web service responses coming from G-POD Web Service;
- Verify the SAML token in the SOAP header of the Web service requests coming from authenticated Web Service Clients;
- Accept service requests only via “policy enforcement point”.

### 4.4 Use Case Diagrams

The HMA-T/G-POD Gateway use case contemplates the interaction with the client and with the G-POD Web Service. The first interaction is depicted in Figure 2 while the second in Figure 3.
**Figure 2 Client - Gateway use case**

In the first diagram, the "Client" entity refers to authenticated clients (with a valid SAML assertion) and invoking the HGG Web Service operations exposed.
Figure 3 Gateway - G-POD Web service use case

In the second diagram, the HGG communicates with the G-POD Web Service and forwards the client requests previously verified.
4.5 Sequence Diagram

The typical use case for the system is depicted the sequence diagram in Figure 4.

Figure 4: System sequence diagram

1. The client sends an authentication request to the IdP PEP.
2. The client receives the authentication response containing the SAML token.
3. The client sends a first service request to the G-POD PEP with the SAML token.
4. The HGG PEP send and authentication request to the HGG User Registry.
5. The HGG User Registry sends an authentication request to the G-POD User Registry.
6. The G-POD User Registry sends and authentication response to the HGG User Registry.
7. The HGG User Registry sends the authentication response to the HGG PEP.
8. The service request is sent to the G-POD Web Service.
9. The G-POD Web Service sends the response to the G-POD PEP.
10. The HGG PEP sends the response to the Client.

The subsequent requests are handled:
1. The client sends a service request to the G-POD PEP with the SAML token.
2. The HGG PEP send and authentication request to the HGG User Registry.
3. The HGG User Registry sends the authentication response to the HGG PEP.
4. The service request is sent to the G-POD Web Service.
5. The G-POD Web Service sends the response to the G-POD PEP.
6. The HGG PEP sends the response to the Client.

4.6 General constraints

• It shall be possible to run the HMA-T/G-POD Gateway on a *nix environment (Unix, Linux or Mac OS X);
• The HMA-T/G-POD Gateway shall use SOAP messaging (via HTTP/POST or HTTPS/POST) with document/literal style to communicate with the Authenticated Client.
• The HMA-T/G-POD Gateway shall use RPC encoded SOAP messaging (via HTTP/POST or HTTPS/POST) to communicate with the G-POD Web Service.
• All the authentication tokens shall be in the header of the SOAP envelope.

4.7 Operational environment

• The HMA-T/G-POD Gateway shall be installed at Terradue premises.

4.7.1 Hardware and Software Environment

• The HMA-T/G-POD Gateway shall be installed on a G-POD reference platform.

4.7.2 Networking Environment and External Interfaces

• The HMA-T/G-POD Gateway shall be connected outside Terradue corporate firewall.

4.7.3 Client Interfaces

• The HMA-T/G-POD Gateway shall publish its service to the Authenticated Clients via SOAP messaging (via HTTP/POST or HTTPS/POST) with document/literal style. The messages shall be conform to SOAP 1.2.
• The HMA-T/G-POD Gateway shall publish its service to the G-POD Web service using RPC encoded SOAP messaging (via HTTP/POST or HTTPS/POST).

4.8 Assumptions and dependencies

• It is assumed that the HMA-T/G-POD Gateway will only process requests to the G-POD Web Service from Authenticated Clients.
5 Specific Requirements

5.1 General

The following requirements have been derived from the careful analysis of the specific intended use of the HMA-T/G-POD Gateway system. These requirements take into account and consolidate the technical requirements extracted from the SoW and analysis of the OGC 07-118r1 specification.

Each requirement is identified using the following convention:

<table>
<thead>
<tr>
<th>System</th>
<th>HGG (HMA-T/GPOD Gateway)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement Type</td>
<td>REQ (Technical Requirement)</td>
</tr>
<tr>
<td></td>
<td>VAL (Validation Requirement)</td>
</tr>
<tr>
<td>Incremental Counter</td>
<td>2 digits</td>
</tr>
</tbody>
</table>

Traceability from the SoW Requirements and OGC specification is provided in Section 7.

5.2 Capabilities Requirements

**HGG-REQ-01.** The HMA-T/G-POD Gateway shall be able to communicate with Clients.

**HGG-REQ-02.** The HMA-T/G-POD Gateway shall be able to communicate with G-POD Web Service.

**HGG-REQ-03.** The HMA-T/G-POD Gateway shall be able to verify the SAML assertion against the G-POD User Registry.

**HGG-REQ-04.** The HMA-T/G-POD Gateway shall be return errors for invalid SAML assertions.

**HGG-REQ-05.** The HMA-T/G-POD Gateway shall only pass requests to the G-POD Web Service from verified client request SAML assertion.

5.3 System Interface Requirements

**HGG-REQ-06.** The HMA-T/G-POD Gateway shall provide an interface to Clients.

**HGG-REQ-07.** The HMA-T/G-POD Gateway shall provide an interface to G-POD Web Service.

**HGG-REQ-08.** The HMA-T/G-POD Gateway interface to Clients shall contain the methods SetVariable, GetVariable, SubmitExt, Status, GetTaskMetadata, DescribeService and Results.
HGG-REQ-09. The HMA-T/G-POD Gateway interface to G-POD WebService shall contain the methods Connect, Disconnect, SetVariable, GetVariable, SubmitExt, Status, GetTaskMetadata, DescribeService and Results.

HGG-REQ-10. The HMA-T/G-POD Gateway shall be accessible from SSE if a compatible client exists within SSE.

HGG-REQ-11. The HMA-T/G-POD Gateway operations shall support the embedding of requests and responses in SOAP messages.

HGG-REQ-12. The HMA-T/G-POD Gateway messaging shall be via HTTP/POS or HTTPS/POST.


HGG-REQ-14. The HMA-T/G-POD Gateway SOAP messages for the Client interface shall be conform to SOAP 1.2.

HGG-REQ-15. The HMA-T/G-POD Gateway message payload for the Client interface shall be in the body of the SOAP envelope.

HGG-REQ-16. All HMA-T/G-POD Gateway authentication tokens shall be in the header of the SOAP envelope.

5.4 Computer Resources Requirements

HGG-REQ-17. The HMA-T/G-POD Gateway shall be installed on a dedicated platform hosted at Terradue premises.

HGG-REQ-18. The HMA-T/G-POD Gateway shall be deployed on a Apple Mac OS X server running Apache 2.2.

HGG-REQ-19. The HMA-T/G-POD Gateway shall able to run with Microsoft Internet Information Services version 6.0 web server.

5.5 Safety Requirements

HGG-REQ-20. The HMA-T/G-POD Gateway shall be protected from Viruses and external malicious attacks.

5.6 Reliability Requirements

HGG-REQ-21. The HMA-T/G-POD Gateway is not an operational system but it expected to be tolerant to system failure.

5.7 Quality Requirements

HGG-REQ-22. The HMA-T/G-POD Gateway shall serve each client managing requests separately, with no interference between several user parallel requests.

HGG-REQ-23. The HMA-T/G-POD Gateway shall serve each client requests providing feedback whenever the requests cannot be served.

HGG-REQ-24. The HMA-T/G-POD Gateway shall clean up all temporary resource allocated on the system for each Internet Authorized User session of session ending.
**HGG-REQ-25.** The HMA/G-POD Gateway shall log events to facilitate system failure investigation.

### 5.8 Design Requirements and Constraints

**HGG-REQ-26.** The HMA-T/G-POD Gateway development process shall be based on ECSS-40-1B.

### 5.9 Software Operations Requirements

**HGG-REQ-27.** The HMA-T/G-POD Gateway shall be reliable so as to provide at least 98% availability for client requests.

**HGG-REQ-28.** The HMA-T/G-POD Gateway shall be designed such that no hardware or software resource is used beyond 80% of its capacity on average.

**HGG-REQ-29.** The HMA-T/G-POD Gateway shall be able to serve at least 20 Internet Authorized User sessions in parallel.

### 5.10 Software Maintenance Requirements

**HGG-REQ-30.** The HMA-T/G-POD Gateway is not an operational system. It will nevertheless be maintained during the HMA-T project duration.

**HGG-REQ-31.** The HMA-T/G-POD Gateway is not an operational system. It will nevertheless be maintained on a best-effort basis after the conclusion of the HMA-T project.

### 5.11 Software Performance Requirements

**HGG-REQ-32.** The HMA-T/G-POD Gateway shall ensure that any client request (within the limit of the 20 users connected simultaneously) is served.
6 Validation Approach And Requirements

6.1 Validation approach

This section summarizes the validation approach to be utilized to validate all the HMA-T/G-POD Gateway requirements stated in Section 5 and to ensure the requirements are met.

The HMA-T/G-POD shall be validated by specific test cases.

Performance requirements shall be validated by system stress tests (TBD: Multi-session simulations), and analysis.

The other requirement areas will be validated by specific test cases, code inspection, or a combination of methods as more appropriate.

6.2 Validation requirements

HGG-VAL-01. The validation shall require a Service Invoker to invoke the HMA-T/G-POD Gateway exposed methods.

HGG-VAL-02. TBC

6.3 Requirement to Validation-Method Correlation Table

The following table provides the validation baseline, associating a validation method to each system requirement.

The validation methods are given in Table 1.

Table 1 Test Method Definition

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSPECTION</td>
<td>Visual check</td>
</tr>
<tr>
<td>TEST</td>
<td>Specific test</td>
</tr>
<tr>
<td>ANALYSIS</td>
<td>Analysis of the system design / Code inspection</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Validation Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>HGG-REQ-01</td>
<td>INSPECTION</td>
</tr>
<tr>
<td>HGG-REQ-01</td>
<td>INSPECTION/TEST</td>
</tr>
<tr>
<td>TBC</td>
<td>TBC</td>
</tr>
</tbody>
</table>
7 Traceability

7.1 Statement of Work to Software System Specification Requirements Traceability Matrix

Table 3 provides the link between all technical requirements defined in the Statement of Work and the System Requirement defined in this document.

<table>
<thead>
<tr>
<th>SoW Requirement</th>
<th>SSS Requirement</th>
<th>Compliancy</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>I9</td>
<td>All</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>I9.1</td>
<td>HGG-REQ-01</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>I9.1.5</td>
<td>HGG-REQ-01</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>I10</td>
<td>Not traced</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>I11</td>
<td>Not traced</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>I12</td>
<td>All</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>I13</td>
<td>TBD</td>
<td>N/A</td>
<td>No compliance tests for specification 07-118r1</td>
</tr>
<tr>
<td>I14</td>
<td>Not traced</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>I15</td>
<td>Not traced</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>I17</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I18</td>
<td>TBD</td>
<td>N/A</td>
<td>No compliance tests for specification 07-118r1</td>
</tr>
</tbody>
</table>

7.2 Software System Specification Requirements to Statement of Work Traceability Matrix

Table 4 provides the link between all the System Requirement defined in this document and the technical requirements defined in the Statement of Work.

<table>
<thead>
<tr>
<th>SSS Requirement</th>
<th>SoW Requirement</th>
<th>Compliancy</th>
<th>Comments</th>
</tr>
</thead>
</table>