

VGISC

Central Europe

Statement of Work Software Development VGISC

Version 1.5



Version for distribution by the WMO Secretariat

Revision history

Date	Version	Author	Modification
4 th April 2008	0.1	Duncan Jeffery	Template created.
9 th May 2008	0.2	Duncan Jeffery	Additional heading levels added.
9 th May 2008	0.3	Peter Piotrowski	First chapters integrated
10 th May 2008	0.4	Peter Piotrowski	Additional chapters integrated
10 th May 2008	0.5	Peter Piotrowski	Reading Status without tech. requirements
10 th May 2008	0.6	Peter Piotrowski	Reading Status with tech. Requirements included
13. May 2008	0.7	Peter Piotrowski	Included J. Roumilhac contributions chapter. 4.6 "Collect observations" plus references
13. May 2008	0.8	Peter Piotrowski	Included J. Roumilhac "Test and Verification und H. Heene "Development & Delivery
14. May 2008	0.81	Peter Piotrowski	Including Use Cases J. Roumilhac
14. May 2008	0.81	Peter Piotrowski	Use Cases, Change H.Heene
16. May 2008	0.83	Peter Piotrowski	Included C. Little A.7 and A.3, Authorize & Authenticate A2 (M. Gutierrez)
18. May 2008	0.84	Peter Piotrowski	Software contributions
18. May 2008	0.85	Peter Piotrowski	Software contributions GTS/SIMDAT
18. May 2008	0.86	Peter Piotrowski	Formatting
19. May 2008	0.88A	Peter Piotrowski	H.Heene und contribution Jeffery Duncan
20 May 2008	0.89	Karla Schöttler-Jansen	Various edits
21 May 2008	0.90	Eliot Christian	Various edits
5. June 2008	0.91	Peter Piotrowski	Formatting corrected, contributions from Mr. Little, Li Xiang and B. Garcia added, resp. corrected
12 June 2008	0.92	Duncan Jeffery	Update of requirements following cross-checking.
16 June 2008	0.93	Duncan Jeffery	Renumber requirements following Langen meeting.
16 June 2008	0.94	Peter Piotrowski Karla Schöttler-Jansen	Removed Use Cases to an attachment Extracted requirements of chap. 2 Added changes of the chairman in chap.1
17 June 2008	0.95	Duncan Jeffery, Peter Piotrowski	All changes discussed during telco Added to chap. 2.3 contr. Of Mr. Little
18 June 2008	0.96	Jeffery, Gutierrez, Garcia & Godøy	Update DCPC Use Cases, abbreviations and glossary.
19 June 2008	0.97	Peter Piotrowski	Change of references, Fig.2.1 modified according to steering group's request (M.Heene)
20 June 2008	0.98	Jeffery, Garcia & Little	Include comments from Beatriz Garcia. Tweaked Glossary
22 June 2008	0.99	Peter Piotrowski	Chapter 2, Requirement, small corrections regarding numbering
23 June 2008	0.991	Duncan Jeffery	Remove duplicate requirements.
23 June 2008	1.0	Peter Piotrowski	Errata von Mrs. Garcia, Formatting of DWD
11 July 2008	1.1	Chris Little	Agreed changes from Langen 9-10 July 2008
14 July 2008	1.1.1	Chris Little	Plus items from matrix
15 July 2008	1.1.2	Duncan Jeffery	Review Use Cases
15 July 2008	1.1.3	Little & Garcia	Update following Teleconference
17 July 2008	1.1.4	Duncan Jeffery	Including VGISC contribution from Météo-France
17 July 2008	1.1.5	Little & Aubagnac	Included discussion point for metadata generation
31 July 2008	1.1.6	Duncan Jeffery	Remove reference to Non-Functional Requirements document by Fred Branski.
07 October 08	1.1.7	Peter Piotrowski	Interim Version, added questions to req. of bidders

			and answers for chapter 3.5 & 3.6
09 October 08	1.2	Peter Piotrowski	Version with all available information as up to day
14 October 08		Siegfried Fechner	Draft Chapter: 3.5 Function A5
17 October 08	1.21	M.Gutierrez	Draft Chapter: 3.3Function A2&A4 (Pio)
18 October 08	1.21	Peter Piotrowski	Logo EUMETSAT replaced
20 October 08	1.22	Peter Piotrowski, Karla Schöttler-Jansen	Version with contributions of Mr. Heene (chapter 2) added
20 October 08	1.23	Duncan Jeffery	Version with contributions of Mr. Chamberlain (chapter 3) added
20 October 08	1.24& 1.25	Peter Piotrowski	Interim versions: Changes of E.Christian included to chapter 1, Chapter A1 partially corrected
21 October 08	1.26	Duncan Jeffery	Chapter A6 reworked
22 October 08	1.27	Peter Piotrowski	Chapter A1 nearly completed (J. Roumilhac)
23 October 08	1.28	Peter Piotrowski	Chapter A2&A4, A3,A7, A6,A5 integriert, A1 completed
24 October 08	1.29	Duncan Jeffery	Correction to section 3.1.1 and rewording of clarification for some requirements in section 3.6
26 October	1.35	Peter Piotrowski	Close to V 1.4
5 November 08	1.36	Duncan Jeffery	Includes modifications from D Jeffery and E Christian.
17 Nov 2008	1.37	Little, Gutierrez	Corrections from Marta and Chris
18 Nov 2008	1.38	Christian	Meteoalarm reference added
27 Nov 2008	1,40	Little	No new changes received. All clarifications inserted
08 Dec 2008	1.50	Heinrich Knottenberg	WMO-Delivery Version

Table of Contents

1	Introduction.....	7
1.1	General remarks	7
1.2	Description of the Undertaking	7
1.3	Short description of the technical work packages.....	9
2	Development and delivery requirement	13
2.1	Project Management.....	13
2.2	Collaboration Infrastructure	21
2.3	List of Deliverables and Documentation.....	22
3	Technical Requirements.....	24
3.1	Introduction to WIS Architectural Requirements.....	24
3.2	Function A1 - Collect Observations, Create Products and Archive Information.....	28
3.3	Function A2 and A4 – Authenticate and Authorize Users	34
3.4	Function A3 - Maintain and Expose Catalogue of Services and Information.....	41
3.5	Function A5 - Deliver Information to Users.....	48
3.6	Function A6 - Manage System Performance.....	51
3.7	Function A7 – Web Interface.....	64
4	Use Cases.....	67
4.1	Introduction.....	67
4.2	GISC Use Cases.....	68
4.3	VGISC Use Cases	68
4.4	DCPC Use Cases	69
5	Software Contributions	70
5.1	Introduction.....	70
5.2	EFTS_Agents.....	70
5.3	FIMEX	73
5.4	GEMS/SMART	75
5.5	METAMOD 2.x.....	79
5.6	SIMDAT.....	81
5.7	GTS Modules contributed to SIMDAT: Metadata Creation.....	84
5.8	GTS modules contributed to SIMDAT: ingestion / retrieve / feeding.....	86
5.9	WEBWERDIS.....	88
5.10	Summary table: Potential Use of Software contributions within VGISC.....	90
6	Test and Verification Procedures	91
6.1	Introduction.....	91

6.2	Mission Statement.....	91
6.3	Test Conditions.....	91
6.4	Test Requirements	92
6.5	Design Review.....	95
6.6	Prototype Review	95
6.7	System Test.....	96
6.8	Test at the CSO (UAT Phase I).....	97
6.9	Test at each partner site (UAT Phase II)	99
6.10	Test at all partner sites in parallel (UAT Phase III)	100
6.11	Testing for release version.....	100
7	Maintenance and Training	102
7.1	Definition	102
7.2	General Requirements.....	102
8	Standards	103
	Appendix A - Glossary of Terms.....	104
	Appendix B - Abbreviations	107
	Appendix C - References.....	109
	Appendix D – Special Clarifications	110
	Appendix E - User Roles	113
E.1	Collect Observations, Create Products and Archive Information	113
E.2	Manage System Performance	113
E.3	Maintain and Expose Catalogue of Services and Information	113
E.4	Deliver Information to Users	113
E.5	Web Interface.....	114
	Appendix F - Detailed Description of Use Cases	115
F.1	GIS Use Cases.....	115
F.2	VGISC Use Cases.....	125
F.3	Internal DCPC Use Cases.....	144
F.4	External DCPC Use Cases.....	157

1 Introduction

1.1 General remarks

The World Meteorological Organisation (WMO) contributes to the safety and well-being of people throughout the world and to the economic benefit of all nations, by providing world leadership in expertise and international cooperation in weather, climate, hydrology, water resources, and related environmental issues. The mission of WMO includes, among other activities: facilitating worldwide cooperation in the establishment of networks of stations for making meteorological, hydrological and other geophysical observations; promoting the establishment and maintenance of centres charged with the provision of meteorological and related services; promoting the establishment and maintenance of systems for the rapid exchange of meteorological and related information; and promoting standardization of meteorological and related observations.

In 2003, the World Meteorological Congress (Cg XIV) formally adopted the concept of a WMO Information System (WIS), stating that an overarching approach was required for solving data management problems for all WMO and related international programmes. According to the formal report of Cg XIV, WIS will:

- Be used for the collection and sharing of information for all WMO and related international programmes;
- Provide a flexible and extensible structure that will allow the participating centres to enhance their capabilities as their national and international responsibilities grow;
- Build upon the most successful components of existing WMO information systems in an evolutionary process;
- Pay special attention to a smooth and coordinated transition from existing systems;
- Build on the WMO Global Telecommunications System (GTS) for highly reliable delivery of time critical data and products and base its core communication network on the Improved Main Telecommunication Network of the GTS;
- Utilise international industry standards for protocols, hardware and software.

From a systems design perspective, WIS is leveraging "Service Oriented Architecture" concepts to enhance interoperability among WMO systems and with external systems that interact with WMO systems. This approach entails defining how system components must interoperate with each other at their common interfaces. By focusing on interfaces, WIS minimizes the impact on the many component systems of WIS, which are often built and managed independently. A document describing the technical specifications for these interfaces was recently drafted for consideration by the Inter-Commission Coordination Group on WIS ("WIS Compliance Specifications of GISC, DCPC, and NC", online at <ftp://ftp.wmo.int/Documents/wis/WIS-TechnicalSpecification-v1-0.doc>, [Ref 1]).

1.2 Description of the Undertaking

Existing centres within WMO Member States that comply with the required WIS functions and technical specifications will be designated as one of the three types of centres forming the core infrastructure of WIS: Global Information System Centres (GISCs), Data Collection or Production Centres (DCPCs) and National Centres (NCs).

GISCs have a key role in WIS because of their requirement to hold and distribute copies for at least 24 hours of current WMO data and products intended for global distribution, in addition to disseminating information from NCs and DCPCs within their area of responsibility. GISCs also host a Discovery, Access and Retrieval (DAR) facility. The

DAR facility will allow users of WIS to find data and products globally by searching a comprehensive catalogue using subject keywords, geographic extent, or temporal range. The user would then choose from a set of catalogue records describing relevant items. Once the user's authorization for delivery of the data or product is checked against the user's role, WIS would facilitate delivery through any of a broad range of online and offline options, including subscription services.

DCPCs collect, disseminate, add value to, and archive regional or programme-specific data and products. DCPCs also produce regional or specialised information, and provide related data and products for international exchange. Similar to GISCs, DCPCs maintain catalogues of their holdings and services, and appropriate parts of these catalogues are used to update the WIS DAR catalogue.

Existing National Meteorological Centres, as defined in the WMO Manual on the Global Telecommunication System (GTS), are expected to become WIS NCs. Every WIS NC must comply with the requirement to supply metadata for their data and products.

Given the new functionality that WIS needs to deliver, development of a GISC for Europe was initiated by Deutsche Wetterdienst (DWD), Météo-France and, United Kingdom Met Office. This development of a pilot system, known as the "Virtual GISC" or VGISC, is supported by a partnership including also the Norwegian Meteorological Institute, the European Centre for Medium-Range Weather Forecasting (ECMWF) and, the European Organisation for the Exploitation of Meteorological Satellites (EUMETSAT) as candidates for DCPCs. Within this document, these organizations are referred to as "the partners". The VGISC will look and behave to the outside world as a single GISC, while consisting of a collection of components amongst the partners.

Initial development of the VGISC was partly done in the framework of a European research project known as SIMDAT. The VGISC pilot was based on interconnected nodes able to act either as a GISC or as a DCPC. Through a portal, each node provides access to data held in one or more data repositories and offers cataloguing services. The SIMDAT software was designed to be non-intrusive so that any already existing data repository (archives, relational databases or simply collections of files) could be integrated. The catalogues held at the various nodes are synchronised through SIMDAT so that data available on any of the nodes can be discovered and retrieved from any of the portals.

Actual organizations can have multiple roles from a functional perspective. For instance, functions of a VGISC node, a DCPC, and a NC will be performed by organizations such as the UK Met Office, Meteo France, and Deutsche Wetterdienst. Accordingly, VGISC software must be configurable to support distinct functions, such as "VGISC node".

The use of trusted relationships within the VGISC system necessitates the distinction between an "internal DCPC" and an "external DCPC". An internal DCPC must be able to acknowledge VGISC users based on a trusted relationship. This allows an internal DCPC to serve requests originating remotely from any of the VGISC nodes or other internal DCPCs, without further authentication (via single sign-on). An external DCPC does not have this ability to recognise VGISC users based on a trusted relationship. An external DCPC would therefore require a full user registration in order to permit access to data that is subject to authorization.

Both internal and external DCPCs may provide, to the VGISC nodes, data for global distribution and its associated metadata. Metadata for other data and products will be

provided to VGISC nodes, but the actual data and products will not be copied to the VGISC node. Its location for retrieval purposes will be referenced within its metadata.

The partners need to finalise the VGISC development and have identified additional software components necessary for operational deployment of the VGISC. Accordingly, the partners intend to issue an Invitation to Tender (ITT) for software that implements the functions of a GISC and multiple DCPCs. The procurement is under the direction of DWD, and technical specifications are aligned with the specifications and objectives of WIS as defined by WMO.

Given the significant investments in SIMDAT software already made by the partners, prospective suppliers must provide explicit rationale in any case where a required function is proposed to be satisfied without using the corresponding SIMDAT software module. Prospective suppliers are also encouraged to make use of various other software modules that implement various WIS functions and are freely available. For example, WebWerdis and associated software available from DWD provides automated support for WIS data dissemination.

The contract resulting from the VGISC ITT will encompass software, its subsequent maintenance, and enhancements as requested by the partners only. That delivered software will be tested for acceptance, integrated with other components as necessary, and run in production on computer systems operated by the partners. This procurement will not encompass acquisition of hardware, telecommunications, operations, nor other products or services. The scope of the software to be acquired is limited to the software functions described in the WIS Compliance Specifications. For example, the scope does not include functions supporting the sale of data or products, the original acquisition of data, nor DCPC functions such as data collection and product creation.

The partner's preferred outcome is to own the Intellectual Property Rights (IPR) of the developed software, but other approaches might be considered.

Three of the VGISC partner sites (DWD, Météo-France and UKMO) each operate a Message Switching System (MSS) that is connected to the GTS. The VGISC as implemented by these partners must interface to these MSSs in order to ingest and cache data and metadata, to handle subscription and GTS link information, maintain control lists, and provide failover support as necessary. However, among these three partner sites there are neither identical MSS control procedures nor a common interface. The VGISC software acquired through this ITT will provide such an interface, and each of the three partners is responsible to adapt to that common interface.

1.3 Short description of the technical work packages

The following sections summarize the functionality required to build a GISC, DCPC and coordinated interactions within the VGISC.

1.3.1 Collect Observations, Create Products, and Archive Information

The system shall offer the capacity to collect information and create new products in a flexible design and in compliance with existing systems.

It has the responsibility to associate Discovery Access and Retrieve (DAR) metadata to every collected or created product or data. The DAR metadata shall be homogeneous in form (in majority ISO 19115 or WMO Core Profile of the ISO 19115 compliant) and in content.

Metadata shall either be:

- Collected from the data / product producer (batch mode),
- Automatically generated from existing reference catalogues,
- Manually edited and validated via a web based interface provided by the system,
- Possibly built on the fly during the data ingestion.

The system shall provide a common interface with existing Message Switching Systems (MSS) for the collection of Global Telecommunication System (GTS) products. In the VGISC framework, the system is required to provide a strategy to maintain this collection function in the event of a failure of the MSS at one site or a failure of the collecting node. The system shall be able to collect information from the WWW WMO programme from the appropriate WIS nodes and from other WMO programmes in a variety of standard formats and in a variety of protocols.

Local production at a DCPC shall be able to insert new products into the system. As a DCPC, the system shall be able to unpack and pack bulletins and files. As a GISC, the system shall also share DAR metadata among GISC nodes and manage the replication of cached essential data.

1.3.2 Assign user role, Authorise access to information by users.

The VGISC system will tackle security scenarios to be covered by several functions:

- Authentication: Identifying who the user is.
- Authorisation: Identifying what the user is allowed to.
- Trust: Definition of trust relationships among the interacting parties to cover the levels of trust in a distributed environment.

The VGISC system must provide administrative functions for management of user, role and trust relationships together with the monitoring of user activity and control activities over management functions.

Finally, the VGISC system must provide back-up scenarios where one of the involved parties will take over the responsibilities of other party in case of failure. In this context, the acknowledgement of users from a trusted remote site must be supported.

Security will be a cross-cutting activity affecting to all the metadata, data and services that will require protected access.

1.3.3 Maintain and Expose Catalogue of Services and Information

Any GISC must establish and operate the following services for data and products:

- Discovery;
- View;
- Delivery.

It is envisaged that at least three logical metadata catalogues must be implemented in a GISC:

Discovery, Access and Retrieval (DAR) catalogue

The DAR catalogue enables the organisation and management of data and products for discovery, access and retrieval, and allows the discovery of resource information from diverse sources. It will also provide a means of locating, retrieving and storing the resources indexed by the catalogue.

International standards ISO 19115 and ISO 19139 (XML schema implementation) will be used for the description of discovery metadata. The protocol specification of ISO 23950 must be used for the metadata discovery/search service.

The SRU (Search and Retrieve via URL) profile of the ISO 23950 standard, and its predecessor ANSI Z39.50, are widely implemented worldwide, in libraries especially. The OGC CSW search interface standard is based on ISO 23950, and can be readily supported with gateway technology.

Metadata for any data or product available from a DCPC or GISC is created or updated in the DAR Catalogue of the DCPC or GISC, before the data or product is available.

The DAR catalogue of a GISC will have a synchronous part which will be synchronised with other external GISCs. In a VGISC, there will be a non-synchronous part, as well as the synchronous part, both of which have to be synchronized among the VGISC component nodes.

Service catalogue

A service catalogue will hold entries which combine data and services and a recognised standard must be used for service metadata.

Dissemination catalogue

Metadata concerning the delivery details of subscriptions to data and products from a DCPC or GISC are created or updated in the Dissemination Metadata Catalogue.

DCPCs and NCs must ensure that metadata are created for their data and products, and that those metadata are kept up to date. The interactions amongst the nodes of a VGISC, between GISCs, and between a GISC and its associated DCPCs and NCs, which are needed for the maintenance and the exposure of catalogues, must be implemented with respect to relevant international standards. Relevant international standards include the regulations of WMO, current practices in stakeholder communities, and recommendations of relevant European initiatives such as Inspire.

GISCs must maintain data and catalogues entries for at least 24 hours worth of data agreed for global exchange, whereas the VGISC system must also internally coordinate some aspects of the service and dissemination catalogues.

1.3.4 Deliver Information to Users

The VGISC system must deliver the data, products, and metadata intended for global distribution to authorized end-users and to other GISCs, in conformance with the WIS Compliance Specifications. In addition to the VGISC role the software has also to cover the data-delivery requested by the DCPC-components operated by partners. The routine delivery service and the ad hoc request service must be fully integrated into the VGISC failover requirement, and this must be supported by the DAR and dissemination metadata design. In the event of a VGISC node failure, each other VGISC node shall have the capability of backing up the routine delivery service, although this should be manually initiated. The VGISC system must provide a web-based interface for authorized users to manage and schedule the routine delivery service, and access to the management functions must be configurable. The VGISC system must also provide for ad hoc requests through a web-based interface for authorized users.

1.3.5 Manage System Performance

The system shall take into account the complexities of managing the VGISC using diversely located nodes. In the event of a VGISC node failure, the system must be able to manage the migration of data and metadata flows and DAR functionality to backup nodes within the VGISC.

The system shall provide Web-based user interfaces for monitoring, reporting and controlling, for all VGISC components. For each of them, several administration and monitoring levels shall be defined: Local administration / monitoring, global administration / monitoring with different level of responsibilities. The visibility of the database elements shall be user dependant.

The monitoring function shall log all remarkable events that each system shall send, to inform the monitoring agent that an unusual event has occurred. Each VGISC component shall write all their events in log files with a specific format in a way that this information can be processed by all standard monitoring tools (e.g. HP OpenView, Big Brother, Tivoli). The system shall be able to follow a new product from its arrival in the VGISC to its dissemination.

The reporting function shall be able to produce reports based on a define action or event, on request or as defined by a schedule. The reporting interface shall be configurable.

The controlling function shall able to associate logs/events with corresponding actions. The controlling interface shall generate control actions for output to all other system functions, and to operators and users. The controlling user interface shall enable manual and automatic control of the data flow, metadata flow and system performance.

1.3.6 Web Interface (Internet Portals (external, internal))

The system will have to interface to a variety of existing Web interfaces at the partners' sites. These existing interfaces support a variety of functions, including monitoring, management and dissemination. Some will be used by internal users and some by authenticated external users.

2 Development and delivery requirement

2.1 Project Management

The following chapter describes the operational structure of VGISC and the general requirements for project management.

2.1.1 VGISC Operational structure and Contact persons

The technical contact person for the execution of this Contract is given in the contractual section.

The structural model of the entire VGISC organisation is described in detail in the document (see Appendix C, Ref. 5)

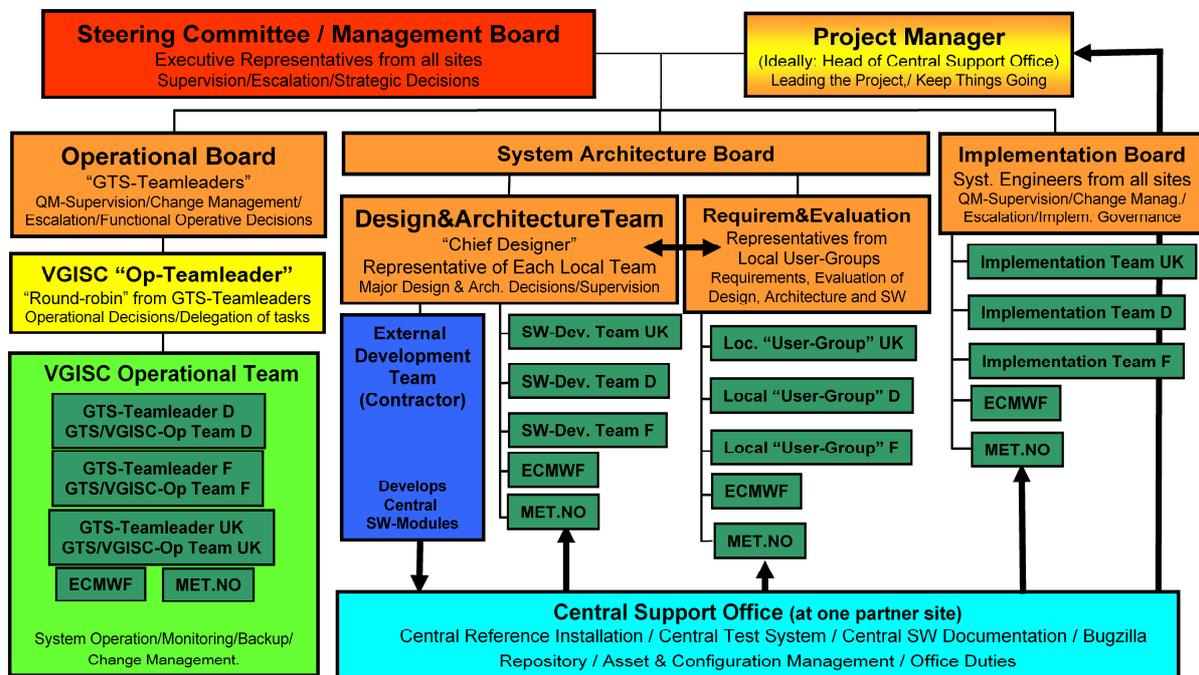


Figure 2.1 Structural Organisation for VGISC

Figure 2.1 provides a first overview of the organisational structure of VGISC (the contractor is reflected by the blue box). During the operation, development & evaluation, and implementation phase of VGISC the Central Support Office shall be the main contact point for the contractor.

2.1.2 Definition of Requirements

Requirements define the baseline that the system has to be designed against. Vendors MUST address each and every requirement given in this ITT. The requirements are identified by the prefix REQ. All mandatory requirements contain the word MUST. All other requirements are considered optional and are characterised as DESIRABLE or HIGHLY DESIRABLE.

The purpose and roles of the National Centres (NCs), Data Collection or Production Centres (DCPCs) and Global Information System Centres (GISCs) are defined at the highest level by

the document: WMO Information System Compliance Specifications of GISC, DCPC and NC, Version 1.0 [Ref 1]. “VGISC” refers to a specific implementation of such a GISC in Europe.

Unless explicitly indicated by a scope statement, it is assumed that the technical requirements apply to all components of the system. In some requirements, the exact scope still needs clarification and this is annotated by “tbd” (“to be developed”)

The terminology “VGISC” is used when the separate, “virtualised” nodes and their (internal) functionality are emphasised. The terminology “GISC” is used to emphasise the function of all the nodes acting as a single system, such as for external interfaces.

Three of the VGISC nodes (MF, UK Met Office, DWD) act collectively as the single "Central European GISC". In addition to its role as a VGISC, each of these VGISC nodes must be capable of acting alone as the Central European GISC if ever both other VGISC nodes are out of operation.

Details of how the transition would occur in this situation must be clarified during the dialogue phase.

2.1.3 Project management approach for the development phase

- REQ-2.01 The vendor **MUST** describe the method and approach to the overall project management and communication with the customer. Clarification. No particular model is requested. The vendor should describe which model they suggest to use for this project.
- REQ-2.02 It is **DESIRABLE** that the vendor provides evidence of any current external certification of their project management practices
- REQ-2.03 The description **MUST** at least contain the following items:
- Project structure and organisation
 - Project phases and Milestones
 - Project plan including PERT and GANNT charts
 - Roles and responsibilities
 - Work package descriptions
 - Reporting procedures
 - Escalation procedures
 - Risk Management Plan
 - Quality Management Plan
 - Training Plan

REQ-2.04 The major milestones shall be:

- M0: Acceptance of Bid and Kick-Off Meeting
- M1: Specification (including redefined use cases, system architecture, functions)
- M2: Design document (including software and system design, Entity Relationship Diagrams, Interfaces, etc.)
- M3: Delivery of Prototype (first verification of software and system architecture, gap-analysis of use cases and test cases)
- M4: Functional test of the MSS interface as provided by the vendor
- M5: Final Version for User Acceptance Test
 - M5a IT verification and functional validation and Performance Tests at Central Support Office
 - M5b External interfaces, security and backup/restore features Tests at local centres
 - M5c Failover and reliability features Tests at all partner sites in parallel
- M6: Closing

The main objective of the Milestone M1 Specification is to review all detailed use cases and definitions of the functional requirements of the system (including operational environment, software, and documentation). It also details the performance, interfaces, operational, verification and quality assurance requirements. At Milestone M1 the Contractor shall also present a preliminary user interface description for review, which shall be reflected in the more detailed design documentation.

The main objective of the Milestone M2 Design is to review the Architectural Design Document, which defines the architectural design of the complete software system of the VGISC.

REQ-2.05 The following elements MUST also be reviewed at the Milestone M2:

- updated hardware configuration including hardware installation requirements
- software specifications
- preliminary User's Manual
- detailed Development Plan for all phases of the software development including the definition of the test tools
- Entity Relationship Diagrams

The main objective of the Milestone M3 Prototype is to verify that the software and system architecture meets the performance, interoperability, operational and functional requirements.

There may be the need to repeat intermediate Milestones, depending on the development approach adopted.

REQ-2.06 For each of the Milestones, a formal review and acceptance meeting MUST take place. The precise topics must be agreed during the specification phase.

It is understood that – depending on the specific phase – related contributions from different parties shall be subject to these reviews, which will be held in common by the parties involved. The final conclusion on the results of the project phase in question, i.e., the acceptance of reports and the authorisation to start the next phase, shall be drawn by the Steering Group.

In addition to the Milestones as mentioned above, the following meetings may take place on request of the vendor or Central Support Office:

- code reviews
- use case demonstration
- regular tests (iterative process for identifying further issues at an early stage)
- design meeting
- test readiness meeting
- prototype test meeting
- system test meeting
- user acceptance test meeting

REQ-2.07 The implementation of such additional events **MUST** be agreed with the vendor during the Kick-Off Meeting.

2.1.4 Project team staffing

REQ-2.08 The vendor **MUST** outline the project team staffing. The outline must contain the following items:

- curricula vitae and relevant experience of key staff and management personnel;
- personnel assigned to work on this project, along with their qualifications and relevant experience;
- names of project manager and main technical contact and number of work hours dedicated to the project for the duration of the project.

REQ-2.09 The vendor **MUST** clearly name all subcontractors and define their roles and working tasks.

REQ-2.10 The vendor **MUST** indicate precisely the extent of support possibly needed from Consortium staff.

2.1.5 Software development strategy

Software development

- REQ-2.11 The vendor **MUST** describe the method and approach to the software development and also provide examples of relevant projects.
- REQ-2.12 It is **DESIRABLE** that the vendor provides evidence of any current external certification of their proposed development practices (for example CMMI).
- REQ-2.13 The vendor **MUST** describe in detail the software development environment and process as well as the software delivery environments and related tools.
- REQ-2.14 It **MUST** be guaranteed that for all software tools ongoing support is provided.
- REQ-2.15 The software development **MUST** be performed according to the current proven professional practice.
- REQ-2.16 If the vendor chooses well proven frameworks for the development, each framework **MUST** be named.
- REQ-2.17 The vendor **MUST** assure that for each chosen framework ongoing support is guaranteed.
- REQ-2.18 The vendor **MUST** describe in detail the approach to Quality Assurance, including the approach to regular testing, in particular unit tests, performance test as well as the specific integration tests regarding the distributed operation of the software. For details please refer to the on Test and Verification Procedures.
- REQ-2.19 The vendor **MUST** describe in detail the approach to Software Documentation, including the detailed specification of interfaces, a unified glossary, system documentation as well as user documentation and administration documentation.
- REQ-2.20 The description **MUST** also include the documentation relating changes of interfaces and functionality of software modules. The vendor shall describe how changes of interfaces are handled on a technical level.
- REQ-2.21 The vendor **MUST** describe in detail the approach chosen to guarantee the required performance in terms of throughput and response times.
- REQ-2.22 The vendor **MUST** describe in detail the approach to Release Management and Updating / Upgrading of an operational VGISC, taking account of the different deployments of module versions (GISC, DCPC and NC). The different deployments will be detailed during the initial project phase.

Clarification: The requirement addresses the situation where a VGISC should be updated to version 1.2 while a DCPC still runs version 1.1. The new version 1.2 could e.g. change a relevant interface.

REQ-2.23 The vendor **MUST** describe the plans for dealing with local software changes at the Consortium members and merging these changes into the main development branch.

Clarification: The vendor should explain under what conditions the integration of new releases is covered by the maintenance fee, or how they plan to handle this. This requirement may be split into two requirements to distinguish the core software from localised versions.

REQ-2.24 It is **HIGHLY DESIRABLE** that the development is based on the software contributions provided by the Consortium members as described in the section on Software Contributions.

REQ-2.25 Wherever the vendor decides not to use SIMDAT, a detailed statement **MUST** be provided.

REQ-2.26 If the vendor finds bugs in the software contributions, he **MUST** inform and support the relevant parties.

Clarification: The requirement addresses the situation if the bidder found bugs e.g. in gcc or jdk. In these cases the vendor **MUST** report the bug to the software owner and provide the support necessary to solve the issue.

REQ-2.27 The vendor **MUST** comply with the different security and software development policies of each Consortium member.

Clarification: Table 1 provides the result of an initial assessment. Detailed information are provided if available. A number of security policies will apply at different levels, at this point the system should ensure that it is capable of accommodating different policies as defined and agreed by the Trust Relationships.

REQ-2.28 The vendor **MUST** use existing standards (described in appendix of ITT document).

REQ-2.29 The development **MUST** allow easy internationalisation.

Clarification: Internationalisation applies to user interfaces etc., but not to log statements. Log statements should be in English only.

REQ-2.30 The vendor **MUST** provide evidence as to why the chosen software architecture will guarantee a flexible, reliable, scalable, easily extendible and open architecture.

REQ-2.31 The system **MUST** be robust, as evidenced for example by its modular design. If e.g. the ad-hoc request function is not operating, the subscription and delivery function must still operate.

System architecture

REQ-2.32 The vendor **MUST** describe in detail the approach chosen for the overall system architecture and, in particular, performance, high availability, and disaster recovery.

REQ-2.33 The architecture **MUST** base on the existing operational environments of the Consortium members. In addition, the approach must contain a quantity structure for a growing data volume and number of requests.

Clarification: The software must be platform-independent and must run on all platforms listed in Table 1. The baseline platform used in the CSO is not yet determined.

Integration into the operation environments

REQ-2.34 The vendor **MUST** support installation of the software as directed by the VGISC Central Support Office.

Clarification: Details to the Central Support Office are after the launch 2009 available.

REQ-2.35 It is **HIGHLY DESIRABLE** that the implementation is infrastructure independent and fits seamlessly into the operational environments of the parties (see Table 1).

REQ-2.36 The vendor **MUST** provide guidance for localisation as part of the design document, taking the operational environments of the parties into account.

Clarification: Localisation here means support of different local system environments, not different local languages. The vendor should describe in detail e.g. which interfaces must be implemented to connect local data repositories.

Center / Part	DWD	Météo-France	UK MetOffice	ECMWF	EUMETSAT	met.no
Operational Environment						
Operation System	Linux Suse SLES 10	Redhat	HP Unix, RedHat	Linux Suse	SUN,AIX,Linux	Debian Linux
Database	Oracle 10g including XML-DB	PostgreSQL	Oracle, C-ISAM	PostgreSQL, MySQL	n/a	PostgreSQL, MySQL
Application Server	Oracle Application Server iAS 10.1.3	Jboss			n/a	
Cataloge Services	iOAI			n/a	n/a	
Grid Middleware	OGSA-DAI			n/a	n/a	
Storage (NAS, SAN, ...)	SAN, NAS				SNI	NAS
Authentication & Authorization	LDAP (eDirectory Novell)	LDAP		Active Identity	n/a	LDAP (iPlanet, OpenLDAP)
Tools						
System Management Tools (HP OpenView, ...)	BigBrother	HP OpenView	Tivoli, HP OpenView	Big Sister	SMS,GMC,Tivoli,Nagios	Nagios
Performance Management Tools				n/a	ORCA	
Audit Systems				n/a	SMART	
Batch - Systems	SMS			SMS	SMS.GEMS	SMS
Transaction Monitor						
Workflow Management System	SMS			SMS	SMS	SMS
Trouble Ticket Management System	AixBOMS	Remedy	Remedy	FootPrints	APT Tool	SW developed in-house + Bugzilla
Network						
Multicast		Retim2000		n/a		
Policies						
Security Policies	BSI guidelines http://www.bsi.de/literat/bsi_standard/index.htm ; SAGA http://kbst.bund.de/saga	IT Security	IT Security follows CESG guidelines.	ISO 17799	n/a	
Software Development Policies		Software Quality Assurance Plan		n/a	n/a	Producing Open Source Software (http://producingoss.com/), SCRUM (http://en.wikipedia.org/wiki/Scrum_%28development%29)
Concepts						
High Availability Concepts				24/7 support	Hot redundant OPE-VAL environments	Hot redundant environment for prioritized parts of operational suite

Table 1 Results of initial assessment

REQ-2.37 The development MUST provide interfaces to other software systems, e.g. trouble ticketing, performance management, and to collaboration infrastructure to enable a smooth communication between operational teams.

Table 1 provides the result of an initial assessment. Detailed information are provided if available (for DWD: Application server changed to both Oracle Application Servers – Oracle Application Server and Oracle WebLogic Server).

Clarification: During the dialogue the parties should define a minimum set of the software systems which MUST be supported for phase 1. It is intended that the vendor should produce a single set of generic interfaces which can then be used to interface to the variety of already existing systems.

2.1.6 Project management approach for the operational phase

Project team staffing

REQ-2.38 The vendor **MUST** outline the project team staffing.

Clarification: This refers to the project team in the operational phase, while REQ-2.08 refers to the team in the development phase.

REQ-2.39 The outline **MUST** contain the following items:

- curricula vitae and relevant experience of key staff and management personnel;
- personnel assigned to work on this project, along with their qualifications and relevant experience;
- names of project manager and main technical contact and number of work hours dedicated to the project for the duration of the project.

REQ-2.40 The structural model of the entire VGISC organisation, where the vendor's team **MUST** fit in, is described in detail in the document (see Appendix C, Ref. 5)

Clarification: Details to the Central Support Office are after the launch 2009 available. Responses times are part of the SLA.

2.2 Collaboration Infrastructure

The collaboration infrastructure is used for the communication between the software development company, the Central Support Office and the other members of the VGISC Consortium with respect to the distributed software development, bug tracking, version management and testing. The collaboration infrastructure will be operated by the Central Support Office and has to be used by the software development company.

The Central Support Office will set up the following environments:

- A wiki for communication and discussion streams
- Source code management (incl. version management)
- Asset management (incl. configuration management)
- Documentation facilities
- Bug and issue tracking system including the management of change requests
- Repository for test cases

REQ-2.41 The software company **MUST** use these CSO facilities and react in due time to issues raised in this way.

Clarification: We do not require the vendor to integrate the CSO in their system. The vendor should use his own infrastructure for the development. After the development the vendor creates a release for acceptance. This release has to be check-in the CSO source code repository by the vendor (which could be different to the vendor's one). The CSO will setup a bug and issue tracking system. The vendor has to use for accepting, closing, bugs (submitted by CSO) this system. The vendor is free to use an additional bug and issue tracking system at his own site for internal purposes.

In addition, the Central Support Office will operate a reference system as a dedicated computing environment with a typical software infrastructure used by the Consortium members. This reference system will be available to the software development company for tests and will be used for the Final Version of the User Acceptance Test as well as for the documentation of bugs and other issues.

Details on the software and hardware environments will be fixed during the dialog phase of this ITT and included in its final version.

2.3 List of Deliverables and Documentation

All documentation **MUST** be provided in English.

It is **DESIRABLE** that documentation also be provided in French and German.

All documents **MUST** at least contain the following elements:

- Title
- Version number
- Status with respect to confidentiality and completeness
- Authors
- Revision history
- Summary
- Purpose of document
- Glossary

The following documents **MUST** be included:

- Response to this Invitation To Tender
 - Each technical requirement, numbered in the document in the form REQ-n.mmm, should have a corresponding numbered statement of how it will be addressed or not.
 - All mandatory requirements, containing the capitalised word **MUST**, must be met completely.
 - Optional requirements, indicated by the capitalised words **DESIRABLE** or **HIGHLY DESIRABLE** should be indicated as being met, or not, or only met partially.
 - The pricing for the deliverables and any options
- Specification
 - Detailed description of the relevant operational environments of each member of the Consortium (as provided by the members)
- Design document
 - Implementation plan meeting the operational environments of the Consortium members.
- Documentation of all versions (prototype, new releases, final version)
 - Interface descriptions of all modules,
- All interfaces throughout the system must be fully documented, with example messages for all external interfaces
- Documentation relating to the Final Version for Acceptance Tests
 - User guide
 - Administration guide
 - Detailed description of the test cases used for the internal validation of the software including test results

- functional tests
- use case tests
- performance test
- failover and high availability tests
- Maintenance terms and conditions, including initial warranty period

Software to be delivered:

- Well documented complete source code of the system
- Used frameworks (compiled and source code version)
- Prototype (first verification of software and system architecture, gap analysis of use cases)
 - including test environments used during the software development
 - including initial configuration
- Final Version of the Software for Acceptance Tests
 - including test environments used during the software development
 - including initial configuration
- Test cases used for the validation of the software and interfaces.

Support:

- Maintenance terms and conditions
- Initial warranty period
- Installation support to the Central Support Office
- Training

3 Technical Requirements

3.1 Introduction to WIS Architectural Requirements

As presented in the WIS Compliance Specifications, the figure below presents the high-level functional architecture of WIS as a data flow model, diagrammed using IDEF0 (Integration Definition for Function Modelling). Figure 3.1 shows six major WIS functions to be implemented, labelled A1 through A6.

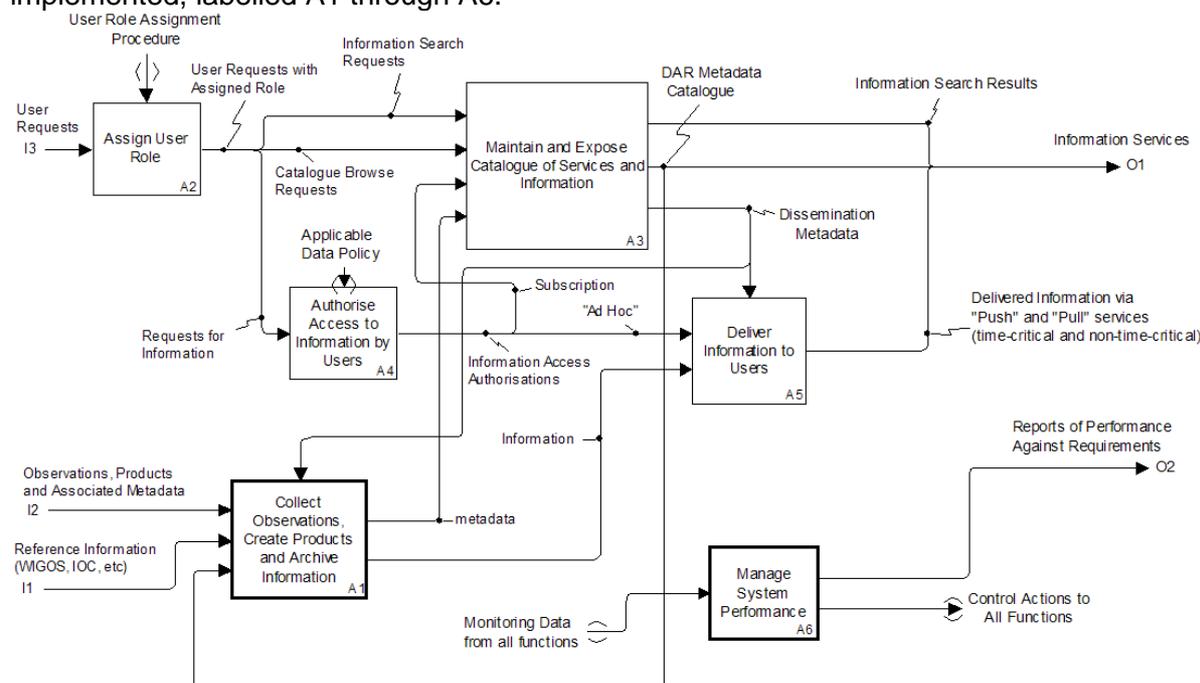


Figure 3.1 Major WIS Functions

To illustrate how the major functions of WIS interact in delivering services, it is useful to consider Use Cases typical of WIS Discovery, Access, and Retrieval users. In this scenario, the WIS user searches through a catalogue to find available WMO data and products relevant to his or her needs. The user searches by concepts such as subject keywords, geographic extent, and temporal range. The user then receives a relevance-ordered list of data and products including "data or product metadata" such as data origin, data type, generation date, availability, use constraints, etc. Once desired data or products have been identified, an authenticated user can request immediate retrieval or subscription for recurring delivery. The user's authorization for delivery of the data or product is checked then against his/her role. The WIS centre then facilitates delivery through any of a broad range of online and offline transmission options, and updates the "dissemination metadata" associated with the subscription.

Figure 3.2 traces the scenario of WIS Discovery, Access, and Retrieval through the high-level WIS data flow diagram. The data flow enters on the left as input I3 with a "User Request", in this case an "Information Search Request". Function A2 performs its "Assign User Role" function with this input, in accord with the applicable control, "User Role Assignment Procedure". The output of function A2, a "User Request with Assigned Role", is input to function A3, "Maintain and Expose Catalogue of Services and Information". Function A3 performs its function and delivers "Information Search Results" to the user as a type of output O1, "Information Services". Having identified a desired data or product using the "Information Search Results", the user then enters again on the left as input I3 with a "User

Request", which is now a specific "Request for Information". Function A4 performs its "Authorize Access to Information by Users" function with this input, in accord with the control, "Applicable Data Policy". The output of function A4 is an "Information Access Authorization". If the request is for recurring subscription, this output becomes input to function A3 for the purpose of updating "Dissemination Metadata". Together with "Ad Hoc" request inputs, the function A5, "Deliver Information to Users", performs the actions for its output, "Delivered Information", which is a type of output O1, "Information Services".

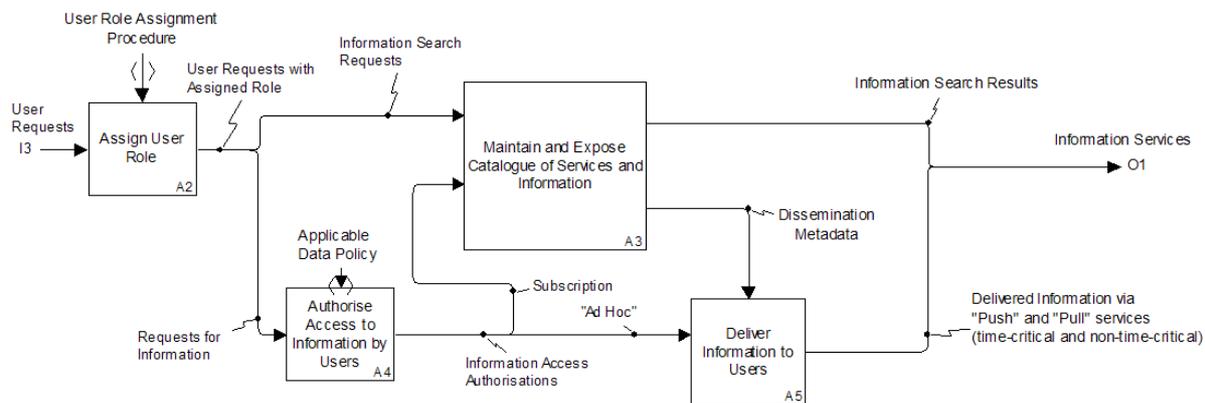


Figure 3.2 WIS Functions relevant to Discovery, Access, and Retrieval

3.1.1 General Architectural Requirement

Some technical requirements are very general and relate to the common aspects of the contexts in which the software will run. These are listed here, separately from the more specific functional requirements.

All technical requirements are assumed to be applicable to all the system components (i.e. individual VGISC nodes, the complete GISC, Internal DCPC, External DCPC and NC) unless specified otherwise..

- REQ-3.01 The system **MUST** comply with the WIS Compliance Specification [Ref 1].
- REQ-3.02 The vendor **MUST** supply software and interfaces to allow the Consortium members to run inter-operating VGISC nodes.
- REQ-3.03 The vendor **MUST** supply interfaces to allow the VGISC nodes to operate as a GISC according to the WMO Compliance Specification.
- REQ-3.04 The vendor **MUST** supply interfaces to allow the WMO specified GISC to inter-operate with an external DCPC.

Clarification: The DAR metadata catalogue is synchronized among VGISC nodes, hence interoperability is natural between the nodes. In such a way, the harvesting process as well as metadata standard are common to the nodes. The VGISC system shall be able to interoperate with external DCPCs both on exchanging metadata (for the catalogues) as well as receiving data for global dissemination.

- REQ-3.05 It is **DESIRABLE** that the vendor supplies software to allow the consortium members to run at least one External DCPC inter-operating with the WMO specified GISC.
- REQ-3.06 The vendor **MUST** supply software and interfaces to allow the Consortium members to run at least one internal DCPC inter-operating with the VGISC nodes.
- REQ-3.07 It is **HIGHLY DESIRABLE** that the VGISC node interfaces and the WMO specified GISC interfaces are compatible.
- REQ-3.08 It is **HIGHLY DESIRABLE** that the vendor supplies software and interfaces to allow the Consortium members to run WMO specified NCs inter-operating with the WMO specified GISC and DCPCs.
- REQ-3.09 The system **MUST** support at least TCP/IP as the transport mechanism.
- REQ-3.10 The System **MUST** be able to synchronise using the Network Time Protocol (NTP). (Scope: VGISC, GISC, Internal DCPC)
- REQ-3.11 The system and all its relevant components **MUST** be capable of running according to Universal Co-ordinated Time (UTC), independently of several local times across Europe
- REQ-3.12 The system **MUST** support IPv6 as well as IPv4.
- REQ-3.13 The system **MUST** support text encoded in the Unicode representation UTF-8.
- REQ-3.14 The vendor **MUST** provide evidence of the flexibility of its design and compliance with existing systems.

Clarification: The vendor **MUST** state how they will address the requirement for flexibility in the design and how they will provide the flexibility to interface to the variety of existing specified systems.

- REQ-3.15 The System **MUST** be able to interface with at least the following file services: FTP, SFTP, HTTP, HTTPS, SMTP, including the collection and dissemination of data, products and metadata.

REQ-3.16 The System **MUST** be robust, as evidenced for example by its modular design. E.g. If the ad-hoc request function is not operating, the subscription and delivery function must still operate.

REQ-3.17 Some products exist in multiple copies. There **MUST** be a mechanism to establish which copy is to be retrieved (e.g. for global exchange products, the 'data-pool' of the corresponding VGISC node is the primary data source. (Scope: VGISC, GISC)

Clarification: For example, if a product exists on several GISCs, the copy on the 'nearest' GISC should be supplied.

REQ-3.18 The System **MUST** take into account the variety of transport mechanisms or networks that may be used to collect and disseminate data, products and metadata. These networks may include:

- i. RMDCN
- ii. The public internet
- iii. VPN
- iv. Multicast disseminations

REQ-3.19 The system **MUST** use the transport mechanism or network solution appropriate to the priority of the data, product or metadata type.

Clarification: It is expected that the system will prioritise data and products using a small number of priorities, such as 1 (high) to 4 (low) as used in current MSS technology.

3.2 Function A1 - Collect Observations, Create Products and Archive Information

3.2.1 Introduction (WIS Architectural Requirements)

Function A1 has two major classes of input: Observations, Products, and Associated Metadata; and, Reference Information. This function has two major classes of output: information and metadata. Function A1 accepts control information from applicable policies and from Function A3, Maintain and Expose Catalogue of Services and Information.

Function A1 has three external interfaces that are subject to WIS Compliance Specifications, specifically:

- WIS-TechSpec-1, Uploading of Metadata for Data and Products
- WIS-TechSpec-2, Uploading of Data and Products
- WIS-TechSpec-3, Centralization of Globally Distributed Data

3.2.2 VGISC Requirements in Addition to WIS Compliance

In overview, function A1 consists of three tasks:

- Collecting information,
- Creating information,
- Storing information.

The first task is responsible for collecting information from WWW WIS nodes, in part by interfacing with the Message Switching Systems, and therefore building on the GTS vertebral column. This task is also responsible for collecting information from all WMO programmes supported by the WIS.

Information creation includes local production (NC or DCPC), unpacking of bulletins or files and packing of bulletins or files according to distribution requirements (DCPC), as well as the creation of information on information: metadata. The first, local production, is – a priori – outside the VGISC scope.

Information may be archived at all levels in the WIS topology, but GISCs have the responsibility to store essential products in a cache and forward them to other GISCs for global exchange. The metadata catalogue is also required to be shared among all GISC nodes.

3.2.3 Inputs and Outputs

The inputs and outputs to function A1: “Collect Observations, Create Products and Archive Information” are listed below as found on Figure 7, “WIS functions A1 through A6” (Ref. [1]). The A1 function is further decomposed in Appendix A processes A11 (national information), A12 (regional, programme-related and specialized information) and A13 (global information). Further decomposition of processes A12 and A13 (Ref. [1], Appendix A) are also relevant here in the VGISC framework.

3.2.3.1 Observations, Products and Associated Metadata (input)

REQ-3.20 The system **MUST** be able to upload and/or receive data and products to/from the appropriate WIS centres.

- REQ-3.21 The system MUST provide a configurable mechanism to allow for the upload and receipt of data and products from other WMO programmes (e.g. Global Atmospheric Watch).
- REQ-3.22 The system MUST be able to upload and/or receive Discovery Access and Retrieval metadata for multiple types of data or products including files, messages and reports to/from the appropriate WIS centres (batch mode).

Clarification: A common agreement at the moment is that the desired DAR metadata granularity is at the GTS bulletin level. The possibility to lower the granularity to the report level is an interesting option which should be investigated. Note that both options could be considered: either an individual DAR metadata for each collected report or a single DAR metadata at the bulletin level, combined with sub-setting service operating on the bulletin. The Vendor should advise on the possible consequence on the DAR metadata catalogue and on the complexity of the system.

- REQ-3.23 The system MUST provide a configurable mechanism to allow the upload and receipt of DAR metadata for data and products from other WMO programmes.
- REQ-3.24 It is DESIRABLE that the System is able to interface with the following file services: OpenDAP, OAI-PMH. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC)
- REQ-3.25 The system MUST provide a fully specified interface with existing Message Switching Systems (MSS) at the partner nodes to perform WMO-FTP and control the collection of Global Telecommunication System (GTS) products. (Scope: VGISC, Internal DCPC)
- REQ-3.26 The system MUST offer a strategy to maintain the collection and dissemination of the products defined as the global dataset, in the event of a failure of the MSS at one site or a failure of one of the collecting nodes. (Scope: VGISC)

Clarification: The requirement can be split into two parts. The first part, the backup of a failing MSS remains the responsibility of the partners and is generally implemented with a spare MSS. The second part in the requirement is the backup of the collection, or link between the MSS to the VGISC/DCPC.

The suggested solution that data providers have several possible entry points to the WIS is indeed a simple solution to consider for both parts of the requirement. In both cases, it would stress the need for a configurable scope of the collection at the VGISC / DCPC node: data / products not normally collected by the backup node would need to be ingested in a backup scenario.

Another solution in the case of a failing collection could involve the MSS: data or products would be rerouted to the backup node (or its MSS). The interface to the MSS could allow for such a request to be posted.

The need is seen for a comprehensive description of the interface to the MSS and the different and complex backup scenarios. It has been agreed that a specific working group will study the question.

- REQ-3.27 The system MUST be capable of automatically generating DAR metadata “on the fly” at the receipt of self documented data and products, if the data or product arrives with no associated DAR metadata record in the catalogue. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC)

Clarification: The context of the requirement – absence of associated DAR metadata in the catalogue – is important, and the on the fly creation of DAR metadata is not to be envisaged as a routine practice which would overwrite DAR metadata records already in the catalogue.

Also, the context is to be understood as absence of an associated product DAR metadata, and not of an associated instance metadata.

The determination of the critical nature of the incoming data / product could be included. Also it should be kept in mind that the data provider remains the best authority to describe the product. The data provider could therefore be (automatically?) notified of the missing DAR metadata, and could be prompted to consider and modify the draft “on the fly” metadata. The generated metadata will be marked as "generated automatically" to indicate possibility of incorrect information. After being manually verified / validated by the data provider, this mark will be removed.

REQ-3.28 It is DESIRABLE that the vendor demonstrates this capability for alphanumeric GTS bulletins. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC)

Clarification: The need for an up-to-date WMO # 9 Volume C1 and Volume A is understood to be necessary, but not fulfilled in practise. This will cause problems in automatic generation (currently a GTS metadata prototype exists (software candidate)), but the vendor is only responsible for data that is available. For the data provider it is possible to run the GTS Metadata Generator on a local (partial, up to date) copy of Volume C1. This would fill the gap in the DAR metadata population.

REQ-3.29 It is DESIRABLE that the vendor demonstrates this capability for BUFR, GRIB, NetCDF formats. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC)

Clarification: Only a part of these metadata are available in the formats listed. Consequently it is not always possible to create a complete metadata from the content alone. Some systems might use contextual information to fill the gaps.

3.2.3.2 Reference Information (WIGOS, IOC, etc) (input)

REQ-3.30 The system MUST provide tools for converting existing WMO metadata, vocabularies and catalogues (volume C1, manual on Codes, etc) to the WMO Core Profile 1.1 of ISO 19115:2003 and ISO Technical Corrigendum 1:2006. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC)

Clarification: The GTS Metadata Generator is expected to be used. The Generator uses WMO # 9 Volume C1 as well as many other elements of information extracted from other WMO references or constructed for the purpose. For bulletins not yet documented in Volume C1, see comment on REQ-3.28. For missing necessary information on documented bulletins, the Generator already implements alternate solutions (e.g. determination of bulletin category) and manages to create metadata records compliant with version 1.1 of the WMO Core Profile of ISO 19115.

The requirement first refers to the transitional conversion from WMO # 9 Volume C1 entries into WMO Core Profile metadata records. Conversion of existing WMO metadata really refers to the system capability to ingest and understand metadata records complying with previous versions of the profile. This flexibility is already required by the need to ingest – for instance – metadata from other WMO programmes, possibly complying with other profiles. This conversion of existing WMO metadata also calls for the capability of the system to output - on demand – WMO Core Profile compliant DAR metadata for any product in the catalogue.

Lastly, concerning other catalogues such as the WMO # 306 Manual on Codes, a rephrasing of the requirement is under consideration: the system should « offer tools to maintain

existing catalogues, create new catalogues and edit these catalogues in order to convert to WMO Core Profile metadata. »

By catalogues are meant true ISO catalogue representation of parts of WMO references. Items from the catalogues would be referred to in the metadata records as xlinks.

3.2.3.3 DAR Metadata Catalogue (input)

- REQ-3.31 The system **MUST** provide a web based interface to edit the metadata records treated as entries in the DAR metadata catalogue (add, change or delete of elements in a record as well as whole records). The facility **MUST** include support for validating metadata against its schemas, and verifying that the values of the metadata elements conform to value domain lists. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC)
- REQ-3.32 The System **MUST** be able to associate every collected data or product and every created data or product to a (DAR) metadata in the catalogue. This DAR metadata may be either already present in the catalogue, or uploaded or created by the System.
- REQ-3.33 The system **MUST** provide a strategy to handle collected data for which no metadata record can be found, so that the data is not automatically lost.
- REQ-3.34 Metadata records automatically created at the receipt of self documented products **MUST** go through a verification procedure before being inserted into the synchronized DAR catalogue. (Scope: VGISC, GISC, Internal DCPC, NC)

3.2.3.4 Dissemination Metadata (input)

- REQ-3.35 The System **MUST** provide a scheduling and triggering mechanism to support the creation of products and data bulletins / files that are either event-driven or scheduled by time. (Scope: VGISC, GISC, Internal DCPC, NC)

Clarification: The phrase “the creation of products and data bulletins / files” should be understood to mean “the preparation for dissemination of products and data bulletins / files”. This preparation involves use of the dissemination metadata, which has the particular details for each user subscription. The information thus created is not treated as persistent, and no DAR metadata record is necessary. Also, see clarification on REQ-3.35 about the desired granularity of the DAR metadata

- REQ-3.36 The System **MUST** be able to unpack files to extract information. The System **MUST** be able to pack the relevant information into files according to the distribution requirements expressed in the dissemination metadata. (Scope: VGISC, GISC, Internal DCPC, NC)

Clarification: WMO already provides a file naming convention for data and associated metadata records in WMO # 386 Manual on the GTS. The same reference also provides a file naming convention for incoming WMO-FTP files (note: WMO 00 and WMO 01). It should be noted also that such packed formats as WMO-FTP are expected only in a dedicated link: the link with the local MSS, and not in all incoming links.

As for REQ-3.35, dissemination metadata records are here as the context. For the user point of view, are packed together data / products corresponding to the user subscription requests.

REQ-3.37 It is DESIRABLE that the System is able to unpack bulletins to extract information. It is DESIRABLE for the System to be able to pack the relevant information into bulletins according to the distribution requirements expressed in the dissemination metadata. (Scope: VGISC, GISC, Internal DCPC)

Clarification: Whether unpacking reports and observations from bulletins and packing them as new pseudo-compilations is truly in the scope of the system is our interrogation. The general agreement is that this capability is maybe not required in our first approach of the system, but may come as an added functionality later on. The requirement is only DESIRABLE here. The vendor should however investigate the feasibility and consequences of such an option, and provide elements for the discussion. Simple solutions may exist, for instance the use of a component already developed by the vendor.

3.2.3.5 Metadata (output)

REQ-3.38 The DAR metadata associated with every collected or created data or product MUST typically document routinely available data / products and MUST be able to document on occasion individual instances of data or product.

REQ-3.39 The DAR metadata MUST be able to be accepted in multiple formats provided the mandatory elements (ISO 19115 Core profile) of information are present. (Scope: VGISC, GISC, Internal DCPC, External DCPC)

REQ-3.40 The DAR metadata MUST be homogeneous in content.

Clarification: Given that DAR metadata will be accepted in multiple formats, a mechanism is necessary to relate those elements, whose content is equivalent semantically. This will have the effect making the catalogue homogenous in content.

The records created by the GTS Metadata Generator may be considered as homogeneous in content as they use the same description of a bulletin feature, independently of the bulletin origin, e.g., the description of one of the WMO formats, and the associated keywords.

REQ-3.41 The system MUST pursue the consolidated view of the DAR metadata catalogue among GISC / VGISC nodes. Changes to the DAR metadata catalogue MUST be shared among GISC / VGISC nodes. (Scope: VGISC, GISC)

REQ-3.42 The system MUST ensure that changes to the DCPC DAR catalogue are propagated to the GISC / VGISC nodes. (Scope: VGISC, GISC, Internal DCPC, External DCPC)

3.2.3.6 Information (output)

REQ-3.43 The system MUST be able to specify and accommodate a variety of data policies. Data policies include global, DCPC specific, GISC specific or VGISC node specific policies. In particular the system MUST accommodate the

Congress Resolution 40 which defines the global “Essential” data policy and the respective rules of Resolution 25.

- REQ-3.44 All VGISC nodes must be able to share certain data and products, including but not limited to data and products labelled for global exchange (e.g. “Essential” data or products). As these will exist in multiple copies, the VGISC system **MUST** provide a mechanism for identifying the location of the original and any particular copy of the data or products. (Scope: VGISC, GISC)

Clarification: Identifying the original copy is necessary in the synchronization process among centres until all centres have a copy of the new file. The original copy is to be understood as the data / metadata provided at its entry point in the WIS: e.g. at the VGISC / DCPC where the data / metadata was collected from the provider.

- Identification is necessary, if the synchronization is interrupted,
- Identification is necessary as only the provider of the original copy may decide that the file should be discarded as obsolete.

- REQ-3.45 “Essential” data or product collected by a GISC **MUST** be cached for at least 24 hours and shared with adjacent GISC. The exchange strategy **MUST** avoid loops. (Scope: VGISC, GISC)

3.3 Function A2 and A4 – Authenticate and Authorize Users

3.3.1 Introduction (WIS Architectural Requirements)

Input to Function A2, Assign User Role, consists of User Requests and the output consists of User Requests with Assigned Role. Function A2 also accepts control information in the form of User Role Assignment Procedures.

Input to Function A4, Authorise Access to Information by Users, consists of Requests for Information and the output consists of Information Access Authorisations. Function A4 also accepts control information from Applicable Data Policies.

Functions A2 and A4 together have four external interfaces that are subject to WIS Compliance Specifications, specifically:

- WIS-TechSpec-4, Maintenance of User Identification and Role Information
- WIS-TechSpec-5, Consolidated View of Distributed Identification and Role Information
- WIS-TechSpec-6, Authentication of a User
- WIS-TechSpec-7, Authorization of a User Role

3.3.2 VGISC Requirements in Addition to WIS Compliance

The virtual organisation as well as the concept of internal DCPCs to the VGISC system as compared with the WIS concept as defined in (See Appendix C, Ref.[1] – Ref.[3]) creates additional security issues to be handled within the functions assigning user role and authorising access to information by the various roles defined.

Additionally to the A2 and A4 functions, security requirements related to the other WIS functions as well controlling and management actions over A2 and A4 functions are listed in this section. The diagram below (Figure 3.3) expresses how Authentication and Authorisation functions will provide input to the monitoring function and how this last one will, when necessary, interact with the management function to control retrospectively the original modules.(E.g. The Authentication function will send messages to the monitoring function. A user attempts to authenticate a number of times all of which fail. The corresponding monitoring function will register the failures and raise an alarm to the management function which will block the user account and therefore block the authentication function for this user).

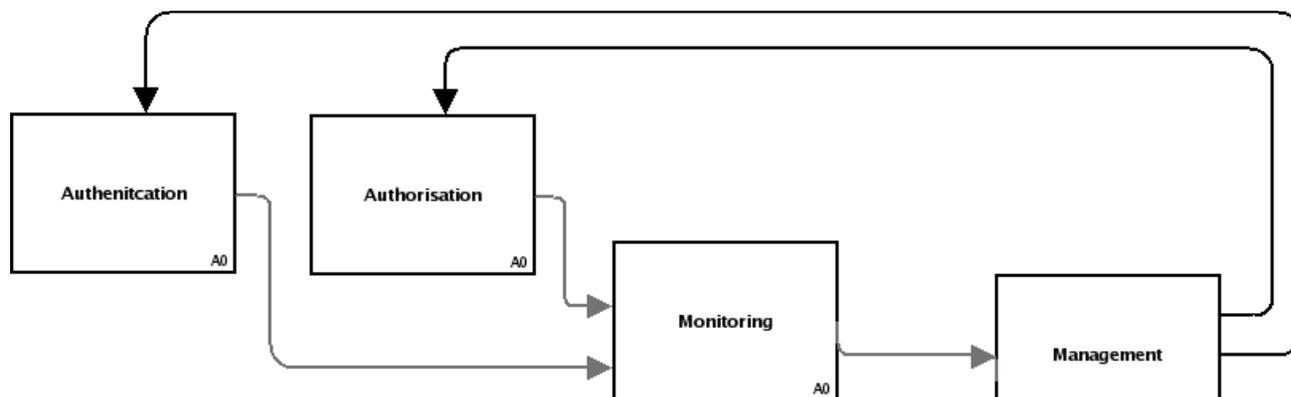


Figure 3.3: Schematic presentation of the relationship between the assign user role and authorise access functionality and the monitoring and management functions.

The VGISC system will deal with the following security functions:

- Authentication: Identifying who the user is
- Authorisation: Identifying what the user is allowed to do
- Trust: Definition of trust relationships among the interacting parties to cover the levels of trust in a distributed environment

The VGISC system must provide administrative functions for the management of user, role and trust relationships together with the monitoring and control of user activities with appropriate management functions.

Finally, the VGISC system must provide back-up scenarios in which one of the partners takes over the responsibilities of another partner in the case of a system failure. In this context, the authentication of users from a trusted remote site must be supported.

Security will be a cross-cutting activity affecting all the metadata, data and services that will require protected access.

3.3.3 Security Requirements

Background

The system must meet specific requirements in the areas listed below:

- Information security requirements
- Authentication
- Authorisation
- User/Role/VO Management
- Monitoring
- Performance requirements
- Security system requirements

3.3.4 Overall Requirements

REQ-3.46 The system **MUST** ensure availability, including the following:

- a. The system responds according to the relevant Service Level Agreements (when needed).
- b. Very high availability is required because some of the services delivered by the system are safety critical. (e.g. Emergency managers must be able to process hazard warning on an expedited basis....)

Clarification: SLA compliance can be defined when service specification is available and recommended measures by the vendor are proposed regarding the critical services. For the cases where back up scenarios are requested, synchronisation of user data (roles and credentials) should be done with acknowledgment of the user or via configuration for high-availability users (e.g. an administrator). Credentials are -private user data-, so default synchronisation would break confidentiality.

REQ-3.47 The system **MUST** maintain confidentiality, including the following:

- a. The systems **MUST** interact with Trusted Parties only.
- b. The system requires confidentiality in two senses, private information by individually identifiable users **MUST** be kept confidential and some information (including logging information) may be subject to release, constrained by national policies.

(Scope: VGISC, GISC, Internal DCPC, NC)

Clarification: Remote logging should maintain user confidentiality and therefore logging actions from a remote user should be addressed by a unique reference that can be resolved only at the authenticating centre. Most centres would apply Data Protection laws for user private data.

REQ-3.48 The system **MUST** provide mechanisms for setting up trust relationships among centres. (Scope: VGISC, GISC, Internal DCPC, NC)

Clarification: Within the Trust relationship remote data access/subscription from authenticated users must be allowed (provided they have right access):

Internal DCPC publish metadata (global and other) to the VGISC node.

- a. For the cases where metadata describing global data is requested, then the data will also be retrievable at the VGISC node (local access).
- b. For the cases where metadata describes “other data”, then the data will be extracted from its original location at the DCPC-int (remote access) and delivered to the user without having to login twice (SSO).

External DCPC -not part of the Trust Relationship- will also be able to publish metadata (global and other) to a VGISC node.

- a. For the cases where metadata describing global data is requested, then the data will also be retrievable at the VGISC node (local access).
- b. For the cases where metadata describes “other data”, then the user will be advertised the location of the data e.g. via url. User will need to go to the location advertised and login again via authenticating method of the external DCPC. No SSO will apply in this case and user will need to register with the external DCPC.

REQ-3.49 The System **MUST** provide mechanisms for notifying the members of the trust relationships regarding policy updates. (Scope: VGISC, GISC, Internal DCPC, NC)

Clarification: Members of the same trust relationship should have common understanding of the policies, and therefore updates in any of the shared policies should be notified to all the members of the relationship.

REQ-3.50 The System **MUST** provide mechanisms for publishing to the register of roles as agreed among the members of the trust relationships. (Scope: VGISC, GISC, Internal DCPC, NC)

Clarification: See comments from 3.49. Roles agreed by members of the trust relationship should be advertised equally to all members. This includes VGISC nodes, internal DCPC and NC.

REQ-3.51 The system **MUST** allow the partners to configure the levels of trust established in agreed common policies. (Scope: VGISC, GISC, Internal DCPC, NC)

Clarification: “Agreed policies” refer to the association policy, role and permission. These associations will be agreed between sites at the level that allows the operation of the VGISC system. Other associations might be allowed out of the scope of the VGISC. e.g. A bilateral trust agreement might be established with a centre outside the VGISC. A trust relationship implies a number of centres with some common understanding of the policies translated into certain roles with the appropriate access conditions.

REQ-3.52 The system **MUST** be able to establish, update and share among VGISC centres sets of rules derived from common policies at the level of metadata, data and services. These sets of rules pertain to types of users and their permissions to access, change or use metadata, data and services. (Scope: VGISC, GISC, Internal DCPC, NC)

Clarification: Where standard global data access practices already exists, sharing of a common policy would simplify the access outside the VGISC. These policies when related to WMO scope should be standardise in the appropriate WIS manual.

REQ-3.53 The VGISC **MUST** have a fully decentralised solution. That is, there must not be only one repository of users or policies. (Scope: VGISC, GISC, Internal DCPC, NC)

REQ-3.54 Data Access policies **MUST** be translated into roles applicable to the users of the system, e.g. the role of researcher might be defined to have update permission for raw data pertaining to climate model input, while the role of forecaster might be defined to have read only permission for validated products.

Clarification: Priority to hide whole metadata record will be given over hiding sub-tree of metadata within a record. Vendor should study if this solution is feasible.

REQ-3.55 Roles **MUST** also be applicable to intersystem exchanges, e.g. GISC to GISC exchanges might be subject to such data access policies. (Scope: VGISC, GISC, Internal DCPC, NC)

Clarification: Requirement contemplates using the same software for intersystem exchanges in the cases where the policies are recognised by the external entities.

Within the VGISC access to an external DCPC will recognise neither policies nor SSO (unless a dedicated agreement is set up). See clarification at 3.47

REQ-3.56 All metadata, data or services **MUST** be associated with one or more roles, either as part of a group or individually.

Clarification: Roles can be defined within the scope of a trusting domain and therefore a number of members of the trusting domain (as a group) would be able to recognise those roles in order to do associations to metadata, data or services.

The requirement does not apply to external sites outside the VGISC. Policies are known to the Trusting members only. External sites will not share the policies an therefore will not provide SSO solutions. See clarification REQ-3.48

REQ-3.57 The role information of an authenticated user **MUST** be available to the centre where the request for metadata, data or service is handled.

Clarification: Users at VGISC node might find some metadata describing data located at an internal DCPC, in this case the user authenticated at the VGISC node will need to be

authorised at the DCPC (who is ultimately responsible for the data). In this case the DCPC will need the role information associated to the user in order to grant or deny access to the data. This would not be the case if the VGISC user finds some data located at the external DCPC as the user would be redirected to the external DCPC and asked for full registration, to access the data.

- REQ-3.58 The System will be run in a production environment on computer systems operated by the partners, using both private networks and the public internet. The system therefore **MUST** accommodate a range of security constraints including the following:
- a. Deployments with encryption and/or on private networks including Virtual Private Networks.
 - b. Firewalls, proxies, “DMZs” and port constraints.

Clarification: Standard encryption protocols are referred to in this requirement, the software should be capable of running in any of the environments above mentioned, e.g. proxy configuration might be needed for programmatic access of service calls for those clients behind a firewall. Full specification of the running ports should be given when connecting services across institutions its firewalls and DMZs. Service configuration should allow easy redeployment in several environments e.g. Internet vs. RMDCN

- REQ-3.59 The System **MUST** allow for configuration of the security level between any two end points. (e.g. configuration of the encryption strength).

Clarification: There are institutions where policies enforce certain security access constraints e.g. Only connections made of high level encryption are allowed. As a distributed architecture service calls are point to point (server/client), and from the application perspective it should be possible to configure different key strengths to connect to different end-points. Of course with both ends supporting the same strength.

- REQ-3.60 The data and metadata transfer (only for security relevant components) between user and the System **MUST** be capable of being handled as encrypted dataflow.

Clarification: There will be metadata subject to security restrictions, and therefore the transfer of such metadata between the user and the System should be done through an encrypted transport protocol.

- REQ-3.61 The metadata transfer (only for security relevant components) between the VGISC system and another GISC **MUST** be capable of being handled as encrypted file. (Scope: VGISC, GISC)

Clarification: File encryption will be redundant when transport protocol is already encrypted, however we cannot guarantee that external interactions will provide encrypted transport channels. In that case, encryption should be done at the file level and therefore configurable behaviour would be make it optional.

3.3.5 Performance Requirements

- REQ-3.62 The System **MUST** ensure that the secure data transport protocols used have performances at least comparable with HTTPS or SSL-like protocols.

REQ-3.63 The VGISC system as a whole MUST be capable of supporting in the order of 2,000 concurrent authenticated users.

Clarification: It is envisaged that the eventual global WIS system may need to support 20,000 concurrent users. In any case the system should be scalable..

REQ-3.64 The system as a whole MUST be capable of supporting in the order of 10,000 concurrent anonymous users.

Clarification: : It is envisaged that the eventual global WIS system may need to support 100,000 concurrent anonymous users. In any case the system should be scalable.

The above figures are based on the expected numbers of centres eventually comprising the WIS, and the existing measured usage of the EUMETNET MeteoAlarm system (Ref. [8]).

REQ-3.65 The time per authentication process MUST not exceed 20 seconds and it is DESIRABLE that it is less than 10 seconds, and should be as short as possible. (Scope: VGISC, GISC, Internal DCPC, NC)

3.3.6 Assign User Role (Authentication)

REQ-3.66 The system MUST provide the mechanism to authenticate users in addition to handling requests from users authenticated at other centres.

- a. E.g. system administrator at a GISC needs to be authenticated using the local authentication mechanism of that GISC.
- b. E.g. a researcher coming to a GISC needs to be authenticated using the authentication mechanism of an NC or a DCPC.
(Scope: VGISC, GISC, Internal DCPC, NC)

Clarification: This topic should be for discussion with the vendors. Use cases will be provided to cover all scenarios.

REQ-3.67 The interfaces for authentication mechanism MUST include both a human interface, e.g. web form, and a machine service interface. (Scope: VGISC, GISC, Internal DCPC, NC)

REQ-3.68 The System MUST provide a single sign-on solution, i.e. users authenticate only once. (Scope: VGISC, GISC, Internal DCPC, NC)

Clarification: SSO is requested for the web interface and the command line (web services) clients within the VGISC

REQ-3.69 The System MUST provide well defined interfaces to support different authentication schemes, e.g. presentation of certificates, entering of a password, or acknowledgment of a policy statement as presented. (Scope: VGISC, GISC, Internal DCPC, NC)

TBD: This is subject of strong limitation of carrier method used by user.

Clarification: The user authentication mechanism list is not exhaustive, and not imposed. The best authentication scheme should be implemented for the best method allowing cases where low level authentication might be desired e.g. self registration and acknowledgement of policy statement for certain datasets. And other cases where strong authentication e.g.

PKI based certificates for remote command line administrators. Or user name and password for general public web access.

REQ-3.70 The authentication and authorisation functions **MUST** provide mechanisms for reacting to management controls including blocking of authentication for specific cases (“blacklist”). (Scope: VGISC, GISC, Internal DCPC, NC)

Clarification: Blacklist expected to be proposed according to breaches of the SLA when defined. e.g. Someone ingesting a big load of metadata records to saturate the system. The system itself should raise an alarm if occupying X% of bandwidth and identify the user for blacklisting.

3.3.7 Authorise Access to Information by Users

REQ-3.71 User **MUST** not be able to access particular metadata, data nor services unless they have the appropriate roles.

REQ-3.72 Authorisation **MUST** only be granted to authenticated users known to the local centre or authenticated users from trusted remote centres. (Scope: VGISC, GISC, Internal DCPC, NC)

Clarification: REQ-3.66 Refers to the AuthN function, this one refers to AuthZ.

3.3.8 User Roles

REQ-3.73 The System **MUST** support a variety of roles (see Appendix D for examples) to allow for the different access privileges for services, data, and metadata. (Scope: VGISC, GISC, Internal DCPC, NC)

3.3.9 Manage System Performance Security Requirements

REQ-3.74 The System **MUST** ensure that only correctly authorised administrators have access to the control functions for the system. (Scope: VGISC, GISC, Internal DCPC, NC)

Clarification: Ref REQ-3.46, REQ-3.54, REQ-3.57, REQ-3.73

3.4 Function A3 - Maintain and Expose Catalogue of Services and Information

3.4.1 Background

The VGISC system must accommodate all types of data and products, and of any granularity. In the GTS context, 'data' usually refers to observations, whereas 'product' usually refers to forecasts and warnings. However, there is no clear distinction between data and products, and this document often uses these names interchangeably, according to the context.

The WIS distinguishes between data/products and data/product instances. This distinction is similar to the differentiation between classes and objects in object-oriented programming. Instances are defined in Appendix A as individual occurrences of defined classes of data or products.

A product defines the abstract characteristics of a meteorological data set. The granularity of a product is user-dependant. For example, a product can specify a single GRIB file or all GRIB files of all model runs during the last 12 months. A product instance is an instantiation of the appropriate product. It is a real data set, e.g. a meteorological bulletin, a set of GRIB files or a subset of a climate time series.

The high level requirements concerned with metadata are:

- DCPCs and NCs ensure that metadata are created for the data and products.
- DCPCs and NCs ensure that those metadata are kept up to date.
- A GISC establishes and operates the following services for the data and products:
 - Discovery service
 - View service
 - Delivery service

Three logical metadata catalogues are required for WIS:

- Discovery, Access and Retrieval (DAR) catalogue
- Service catalogue
- Dissemination catalogue

All three catalogues must be implemented in a Global Information System Centre (GISC) of WIS, and therefore in a VGISC also. Implementing rules, recommendations and guidelines are given for the development of these catalogues and their contents, i.e. the metadata.

The three logical catalogues will allow authenticated and authorised users to find and retrieve data and products, which may be real time or historical. Some of the data and products that are handled by the VGISC nodes are designated for global exchange with other GISCs in near real time with a finite time of residence in the system. Other data/products can be historical. E.g. offered by DCPCs, including the DCPC functionality of Météo-France, UK Met Office and DWD. Of course, DCPCs may also offer real time data too.

There is no definitive list of available data/products. It is one of the intents of WIS, and this procurement, to enable the development of such a list.

"Essential data" is a subset of the "global data" as defined by polices established in WMO Resolutions 40 and 25.

There is no firm requirement as to whether the metadata of product instances should be stored in the DAR catalogue or not.

3.4.2 Purpose and Scope

The scope of this section is to detail the requirements relating to the services and information catalogue, such that the following goals are fulfilled and met.

- international and national meteorological centres, i.e. DCPCs and NCs, can be connected consistently to the VGISC
- the interactions between GISCs, e.g. the synchronisation of metadata, are standardised
- the interactions between a GISC and its respective DCPCs and NCs are standardised

The implementing rules are in conformance with European and international standards, regulations of WMO, current practices in stakeholder communities, and relevant European initiatives such as e-Government.

In particular, ISO 19115-conforming DAR metadata are only required for products and not for product instances.

A definition of the Maintain and Expose Catalogue of Services and Information function is provided at [1], WIS function A3.

3.4.3 Introduction (WIS Architectural Requirements)

Many of the functions required to generate, maintain and expose metadata are common to the GISC, DCPC and NC functions. According to [1] there are four inputs, three outputs and the control and monitoring data flow. These are summarised below. The detailed technical requirements follow, in a high level grouping for convenience.

Function A3 has four external interfaces that are subject to WIS Compliance Specifications, specifically:

- WIS-TechSpec-8, DAR Catalogue Search and Retrieval
- WIS-TechSpec-9, Consolidated View of Distributed DAR Metadata Catalogues
- WIS-TechSpec-13, Maintenance of Dissemination Metadata
- WIS-TechSpec-14, Consolidated View of Distributed Dissemination Metadata Catalogues

3.4.4 Inputs and Outputs

Metadata (input)

The VGISC system will exchange metadata with other GISCs. It will accept metadata from DCPCs and NCs

Catalogue Browse Requests (input)

The VGISC system will accept authenticated and authorised requests from NCs or via other GISCs. The catalogue can be browsed in a variety of ways

Information Search Requests (input)

The VGISC system will accept authenticated and authorised queries from NCs and other GISCs.

Subscription (input) from Information Access Authorisation

The VGISC system will support subscriptions services to authenticated and authorised users.

Information Search Results (output)

A query may return multiple results, which could be refined or selected to a single result.

Information Services (output)

A query result can be used to invoke either an ad hoc data request or a subscription service to the data or be used to expose more detailed metadata. The delivery options for the data would be indicated.

Dissemination Metadata (output)

The VGISC system needs to deliver data to other GISCs, DCPCs and NCs. The VGISC nodes may have differing dissemination needs.

Control and Monitoring (both input and output)

There are requirements for performance monitoring and control, and well as at the policy level.

3.4.5 Requirements

In some areas, whether the scope encompasses NCs, or not, is not yet completely clear. These are marked “NC tbd”.

3.4.5.1 General Requirements

REQ-3.75 It **MUST** be possible that a metadata record of the DAR catalogue describes a data set of any granularity. Especially, it **MUST** be possible to distinguish between products and product instances. (Scope: VGISC, GISC, Internal DCPC, External DCPC and NC)

REQ-3.76 In the case where products are available through multiple services, it **MUST** be possible to associate a separate service instance with each such product. E.g. over different delivery mechanisms, or with different SLAs. (Scope: VGISC, GISC, Internal DCPC, External DCPC and NC)

Clarification: For example, a product consisting of observations may be available from two different services, One may be offered by a VGISC node, the other by a DCPC. The system must allow for a selection between the two services.

REQ-3.77 Each metadata record of the DAR catalogue **MUST** be uniquely identified by a URI. (Scope: VGISC, GISC, Internal DCPC, External DCPC and NC)

- REQ-3.78 Each metadata record of the service catalogue MUST be uniquely identified by a URI. (Scope: VGISC, GISC, Internal DCPC, External DCPC and NC)
- REQ-3.79 The system MUST implement a discovery, access and retrieval (DAR) catalogue. (Scope: VGISC, GISC, Internal DCPC, External DCPC)
- REQ-3.80 The system MUST implement a dissemination catalogue. (Scope: VGISC, GISC, Internal DCPC)
- REQ-3.81 The system MUST implement a registry for role authorizations as defined by the VGISC policy. (Scope: VGISC, GISC, Internal DCPC, NC)

Metadata Standards Requirements

- REQ-3.82 It is HIGHLY DESIRABLE that the system meets the requirements of the INSPIRE directive. (Scope: VGISC, GISC, Internal DCPC, External DCPC and NC)
- REQ-3.83 The system MUST produce metadata that validate against XML schemas produced according to ISO 19139:2007. (Scope: VGISC, GISC, Internal DCPC, External DCPC and NC)
- REQ-3.84 The system MUST support, as searchable elements of the DAR catalogue, at a minimum, the mandatory and conditional elements in the WMO Core Profile 1.1. (Scope: VGISC, GISC, Internal DCPC, External DCPC)
- REQ-3.85 The system MUST support, as searchable elements of the service catalogue, at a minimum, the mandatory and conditional elements of ISO 19119. (Scope: VGISC, GISC, Internal DCPC, External DCPC)
- REQ-3.86 The system MUST support the WMO Core Profile of the ISO 19115:2003 standard, at least for Version 1.1. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)
- REQ-3.87 It is DESIRABLE that the System fully supports the extension mechanisms of ISO 19115:2003 in order to deal with metadata conforming to multiple profiles, e.g. the Marine Community Profile or the next version of the WMO Core Profile, or multiple versions of these profiles simultaneously. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)
- REQ-3.88 It is DESIRABLE that the system supports the optional elements in version 1.1 of the WMO Core Profile of ISO 19115:2003 and ISO Technical Corrigendum 1:2006. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)
- REQ-3.89 References to external code lists MUST be validated. (Scope: VGISC, GISC, Internal DCPC, External DCPC)
- REQ-3.90 When validating metadata, Xlinks and XIncludes MUST also be validated. (Scope: VGISC, GISC, Internal DCPC, External DCPC)

Clarification: XLinks are mostly used in metadata descriptions for the reference of entries in other catalogues. The validation of such XLinks is to test whether the referenced entry really exists. The VGISC system could use local copies of these catalogues for validation in order to avoid performance and reliability problems.

REQ-3.91 It is DESIRABLE that the system will support metadata according to the current ISO draft standard DIS 19115 Part 2 – Imagery and Grids and the eventual full standard when published. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

Metadata Management Requirements

REQ-3.92 The system MUST support the ability to restrict access and visibility of some elements of metadata records. E.g. politically sensitive, or still in draft. (Scope: VGISC, GISC, Internal DCPC, External DCPC and NC)

TDB QUESTION: Do the word access and visibility indicate the same thing or they mean something else - for example editing vs. viewing?

Clarification: Generally, metadata should be freely available and there should be no restrictions on the access to metadata records. If there were metadata information which should be hidden from a group of unauthorised users, then this information would not be put into the metadata collection.

Data/product metadata are part of the DAR catalogue and remain in the catalogue after the data/product instances are deleted from the Cache.

Metadata for data/product instances, if they exist, evolve with the content of the Cache and disappear from the catalogue when the instances are deleted.

Details and management of the product instance metadata will be further clarified during the dialogue phase.

REQ-3.93 It is DESIRABLE that the system includes support for the maintenance of controlled vocabularies. (Scope: VGISC, GISC, Internal DCPC, External DCPC and NC)

Clarification: Examples of these controlled vocabularies include: GEMET subject terms, WMO Volume A, WMO Volume C1, and local copies of station lists, lists of expected bulletins

REQ-3.94 The system MUST maintain the integrity of the metadata records, and provide import and export of the full records for both WMO Core Profile 1.1 and ISO 19119. (Scope: VGISC, GISC, Internal DCPC, External DCPC)

REQ-3.95 The system MUST implement a service catalogue. (Scope: VGISC, GISC, Internal DCPC, External DCPC)

Clarification: Data or a product can be associated with a service. The service will accept requests in order to generate an instance of the product. For example, there could be a product that describes the daily mean air temperature values of all German stations. A service may exist, which will query the subset of values for a given set of stations during a given period of time.

A common example for the service catalogue is for a sophisticated user to discover the existence of services using the search interface specified for the DAR catalogue.

Another example that distinguishes services of interest involves ‘sub-setting’ of a product (e.g. one report from a bulletin, a sub grid or individual point from a grid, portion of a picture, individual element from larger multi-element record or file).

- REQ-3.96 It is DESIRABLE that the system supports services metadata in a well known standard, such as ebRIM, UDDI or ISO 19119:2006. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)
- REQ-3.97 The system MUST support the synchronisation of other configurable sets of metadata amongst the component nodes of the VGISC. (Scope: VGISC, GISC, Internal DCPC, NC)
- REQ-3.98 The system MUST support the synchronisation of configurable sets of metadata with other GISCs. (Scope: VGISC, GISC, Internal DCPC, NC tbd)

Searching Requirements

- REQ-3.99 The System MUST support searching on keywords (full text), subject terms, spatial bounding boxes, date / time ranges. (Scope: VGISC, GISC, Internal DCPC, External DCPC and NC)
- REQ-3.100 It is DESIRABLE that the system supports searching on any of the elements within the ISO 19115:2003 and ISO 19119:2006. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)
- REQ-3.101 Spatial bounding boxes may extend across poles and the “date line”. Searching on spatial bounding boxes MUST support at minimum lat / long. coordinates specified in Spatial Reference Systems EPSG:4326. (Scope: VGISC, GISC, Internal DCPC, External DCPC and NC)
- REQ-3.102 The system MUST support searches performed according to ISO 23950 using SRU profile version 1.2 (over both HTTP GET and POST, but it is not required to support SRU through WSDL/SOAP) (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)
- REQ-3.103 It is DESIRABLE that the system supports the refinement of searches, such as using named result sets. (Scope: VGISC, GISC, Internal DCPC, External DCPC and NC)

Clarification: E.g. An initial search returns a large number of results. The user decides to continue by searching again, but only within the initial search results.

- REQ-3.104 It is DESIRABLE to have support for thesaurus extensions, i.e. designation of extra search terms drawn from a hierarchical vocabulary wherein terms are related as “broader than”, “narrower than” and “use for” (preferred term among equivalent terms). This should be implemented using the scan operation of ISO 23950 with the Zthes profile. (Scope: VGISC, GISC, Internal DCPC, External DCPC and NC)

Clarification: Thesaurus extensions, or expansions, allows a term or phrase in a user search to be replaced with a set of custom terms before the actual search is performed. This feature improves search quality by handling unique, obscure, or industry-specific terminology.

- REQ-3.105 It is DESIRABLE that searches can be stored for re-use at a later time. (Scope: VGISC, GISC, Internal DCPC, External DCPC and NC)

Clarification: Storing the parameters is a common technique to allow a searcher to get results on a recurring repeat basis.

REQ-3.106 It is DESIRABLE that the system supports searches according to other query languages and schemes, such as OGC/CSW. (Scope: VGISC, GIS, Internal DCPC, External DCPC and NC)

Clarification: Google, SQL, UDDI, etc

REQ-3.107 It is HIGHLY DESIRABLE that the results of search queries either data or metadata) can be presented in a range of presentation formats, such as Web Map Services, XHTML or PDF. (Scope: VGISC, GIS, Internal DCPC, External DCPC and NC)

Clarification: This desirable requirement addresses the need of users to get their information in a range of appropriate formats.

REQ-3.108 It is DESIRABLE that tools are provided for tuning the response to search queries such as configuring the ranking algorithm applied when generating results. (Scope: VGISC, GIS, Internal DCPC, External DCPC and NC)

Clarification: For example, search results may be ordered synoptically rather than by proximity, or results corresponding to keywords 'rain' or 'precipitation' are not ranked.

3.5 Function A5 - Deliver Information to Users

3.5.1 Introduction (WIS Architectural Requirements)

Input to Function A5, Deliver Information to Users, consists of Information and Information Access Authorisations. Output from Function A5 consists of Delivered Information via "Push" and "Pull" Services (time-critical and non-time-critical). Function A5 also accepts control information in the form of Dissemination Metadata.

Function A5 has three external interfaces that are subject to WIS Compliance Specifications, specifically:

- WIS-TechSpec-10, Downloading Files via Dedicated Networks
- WIS-TechSpec-11, Downloading Files via Non-dedicated Networks
- WIS-TechSpec-12, Downloading Files via Other Methods

Function A5 also has control and performance monitoring interfaces.

3.5.2 VGISC Requirements in Addition to WIS Compliance

A definition of the Deliver Information to Users function is provided in the WIS Compliance Specifications (WIS function A5). The VGISC system must deliver the data, products, and metadata intended for global distribution to authorized end-users and to other GISCs. In addition to the GISC and VGISC roles, the software has also to cover the data-delivery requested by the DCPC-components operated by partners.

The routine delivery service and the ad hoc request service must be fully integrated into the VGISC failover requirement, and this must be supported by the DAR and dissemination metadata design. In the event of a VGISC node failure, each other VGISC node shall have the capability of taking over the routine delivery service, although this should be manually initiated.

The VGISC system must provide a web-based interface for authorized users to manage and schedule the routine delivery service, and access to the management functions must be configurable. The VGISC system must also provide for ad hoc requests through a web-based interface for authorized users.

3.5.3 Requirements

3.5.3.1 General Requirements

REQ-3.109 Product Prioritization: The system **MUST** provide the capability for both manual and automatic product prioritization based upon the service level agreement of the receiver and the priority assigned by the sender, as well as the content of the metadata. (Scope: GISC, VGISC, Internal DCPC)

Clarification: In general, the system must automatically schedule the delivery of subscribed products within the constraints given by the full set of service level agreements. In addition, the system must allow for manual override of automatically scheduled deliveries at the discretion of the sender or receiver. For example, prioritization on the basis of timeliness products can be formulated as part of the product metadata, prioritization between users (based on Service Level Agreements between VGISC and user, managed by the sales department of the sender) and prioritization between different subscriptions of a user, self-configured by the user.

If priorities described as part of product metadata (e.g.: relation between warnings and climates), these priorities should be included into the hierarchy (should be discussed as part of the dialogue).

REQ-3.110 The VGISC system **MUST** support the fact that multiple data channels are configured between nodes, to enable separation of data based on data type and priority. (Scope: GISC, VGISC, Internal DCPC)

REQ-3.111 Subscription services **MUST** support products offered by internal DCPCs. (Scope: GISC, VGISC, Internal DCPC)

Clarification: These products can be hosted in the cache pool of the VGISC node or offered via a service by an internal DCPC. End-user subscriptions are not committed to other GISC, but other GISC can be handled like a user (see REQ-3.122)

REQ-3.112 It is **DESIRABLE** that notifications of changes to products and services are available for subscription. (Scope: GISC, VGISC, Internal DCPC, External DCPC)

Clarification: Focuses of the requirement are modifications of the content of products (e.g. changes of expended stations of a bulletin – modifications of Vol. C1) or production instructions (services) of a product, not the provision of new instances of a product.

REQ-3.113 The VGISC system **MUST** be able to process requests for data or products and allow the checking of the status of that request. (Scope: GISC, VGISC, Internal DCPC, External DCPC)

REQ-3.114 The System **MUST** provide a mechanism to override the usual delivery method, such as for very large products or datasets. (Scope: GISC, VGISC, Internal DCPC)

REQ-3.115 The System **MUST** be able to deliver data or products either synchronously or asynchronously, since retrieving some very large datasets or off-line data (e.g. data stored on tapes) can take several hours. (Scope: GISC, VGISC, Internal DCPC)

3.5.3.2 Information Access Authorisation (input)

REQ-3.116 End users **MUST** only be able to initiate their own subscription. End users **MUST** be able to manage their own subscription details. (Scope: GISC, VGISC, Internal DCPC, External DCPC)

REQ-3.117 Delivery operators **MUST** be able to monitor all subscriptions. (Scope: GISC, VGISC, Internal DCPC)

REQ-3.118 Delivery administrators **MUST** be able to manage all subscriptions. (Scope: GISC, VGISC, Internal DCPC)

3.5.3.3 Dissemination Metadata (input)

REQ-3.119 The full current set of unrestricted DAR metadata **MUST** be treated by the System as a product, so that authorized users could subscribe to it and receive all metadata records that are public. (Scope: GISC, VGISC)

Clarification: It is enough to restrict the access (public / not public) at the level of file containing the full current set of unrestricted DAR metadata.

REQ-3.120 All or part of the DAR metadata **MUST** be available for delivery to authorized users. (Scope: GISC, VGISC, Internal DCPC, External DCPC)

Clarification: (New formulation) Complete or parts of the DAR metadata sets **MUST** be available for delivery to authorized users (Scope: GISC, VGISC, Internal DCPC, External DCPC)

REQ-3.121 The dissemination metadata structure **MUST** allow the user to specify destination properties (e.g. primary and alternate delivery addresses and mechanisms (URLs) and transmission priority levels) as a function of the primary or failover VGISC node. (Scope: GISC, VGISC)

3.5.3.4 Information Search Results (output)

REQ-3.122 The System **MUST** be able to send data to a user based on an event, such as: arrival of product (as soon as data arrives), time deadline (at a time specified by the user). A user may be either an end-user or a more general destination: a VGISC node, or a dissemination service, etc. (Scope: GISC, VGISC, Internal DCPC, External DCPC)

Clarification: (new formulation): The system **MUST** be able to send data to a user based on an event, such as: arrival of products (as soon as data arrives), time deadline (at a time specified by the user). A user may be either an end-user or a more general destination: a VGISC node or an other GISC (VGISC, GISC, IntDCPC, ExtDCPC).

The time deadline specifies only the start time of the subscription activity (details of the activities during the subscription process are depending on the type of the product and/or the configuration of the subscription by the user.

REQ-3.123 The “ad hoc” request service **MUST** support the same transport mechanism as the routine delivery service and pull services, such as download and view (depending on the requested product). (Scope: GISC, VGISC, Internal DCPC)

REQ-3.124 It is **DESIRABLE** that the routine delivery service has a clear interface to add additional file transfer methods. (Scope: GISC, VGISC, Internal DCPC, External DCPC)

REQ-3.125 The System **MUST** ensure that all VGISC nodes will not transmit data back to the transmitting node. (Scope: GISC, VGISC)

REQ-3.126 The same product **MUST** not be delivered more than once to the same user by different nodes. (Scope: VGISC, Internal DCPC)

3.6 Function A6 - Manage System Performance

3.6.1 Introduction (WIS Architectural Requirements)

Inputs to Function A6, Manage System Performance, consist of Monitoring Data from all Functions. Function A6 has two major classes of output: Reports of Performance against Requirements, and Control Actions to All Functions.

Function A6 has one, generic external interface subject to WIS Compliance Specifications, specifically:

- WIS-TechSpec-15, Reporting of Quality of Service.

Function A6 also has an array of control and performance monitoring interfaces. These are detailed below in subsections 3.6.6 and following.

3.6.2 VGISC Requirements in Addition to WIS Compliance

The VGISC system is a number of diversely located nodes, which will be responsible for delivering data, products, and metadata intended for global distribution to authorized end-users and to other GISCs, in conformance with the WIS Compliance Specifications ([1]).

In addition to the VGISC role, the software also has to cover the data-delivery requested by the DCPC components operated by partners. The data and products can be delivered using both a routine delivery service and an ad hoc request service.

The effective and efficient provision of these services will rely heavily on the management and monitoring functions described in this section. System performance management is based on three main functions:

- Monitoring - logging of all events, transactions and actions.
- Reporting - the production of reports, based on the monitored events and actions.
- Controlling - manual and automated actions performed as a result of an event.

3.6.3 General Requirements

The external DCPC will run the software on its own and will be not connected to the respective services of the VGISC Virtual Organisation.

REQ-3.127 The system **MUST** give evidence of the capability to address the complexities of monitoring and managing the diversely located nodes of the VGISC. This includes the ability to consume existing SNMP messages. (Scope: VGISC, GISC tbd, NC tbd)

Clarification: The system must be able to receive SNMP messages from the other nodes. The use of SNMPv3 is acceptable.

REQ-3.128 **Local Monitoring:** Customizable tools, techniques, and/or procedures **MUST** be provided which will aid in the capacity and performance monitoring, reporting and execution of routine checks on the System. (Scope: GISC tbd, VGISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.129 **Remote Monitoring:** Customizable tools, techniques, and/or procedures **MUST** be provided to allow for the monitoring of any VGISC node remotely by

operators/technicians located at any other VGISC node. (Scope: GISC tbd, VGISC, NC tbd)

REQ-3.130 An interface **MUST** be provided to integrate these custom monitoring tools with other commercial monitoring packages that are used at the VGISC Partner sites: Tivoli, HP OpenView, Big Brother. (Scope: GISC tbd, VGISC, NC tbd)

Clarification: There are a variety interface mechanisms, ranging from SNMP(V.3) as the lowest common denominator to interface with the variety of monitoring tools for the partner sites.

REQ-3.131 **Remote Access:** Capability **MUST** be provided to enable System technical support staff to access the VGISC System remotely – such as from the home office, subject to security controls. (Scope: VGISC, GISC, Internal DCPC, External DCPC)

REQ-3.132 The System **MUST** collate all exported logs and events from all nodes. (Scope: VGISC, Internal DCPC)

REQ-3.133 The System **MUST** ensure that no logs or events are lost during the collation of logs or events. (Scope: GISC tbd, VGISC, Internal DCPC, NC tbd)

REQ-3.134 The System **MUST** allow authorised administrators to configure the level of event elements that are recorded in the logs.

Clarification: The system should support different levels of log information, such as debug, info, warning, critical. It must be possible to configure which levels of log information are recorded in the logs, and for which functions. For example, debug level events for the ingestion function may only be recorded when investigating a problem.

REQ-3.135 The user interface **MUST** allow authorised administrators to configure what elements are displayed.

REQ-3.136 The System **MUST** be configurable in terms of the colour coding of events and the audible alarms.

REQ-3.137 The software **MUST** provide a function to export the event and transaction information. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

Clarification: It must be possible for the system to export logs relating to system events and data/metadata transfers, which this requirement covers. REQ-3.146 relates to the ability to schedule the export of the log information, as well as being able to export the logs on an ad-hoc basis.

REQ-3.138 The System **MUST** provide a log-file ingestion/analysis module.

Clarification: Users should, through a specific software module, be able to examine, sort and filter log file entries to aid problem investigation, which may include picking sub-fields to display (e.g. filter by error type, time and node).

REQ-3.139 The System **MUST** be documented as to its operating environment and technology dependencies.

REQ-3.140 The System **MUST** provide a user interface to enable authorised administrators and operators to carry out their respective control actions.

Clarification: REQ-3.131 requests an interface which can be used by operators when remote from the office. This interface may be a simple command line interface, rather than a GUI. REQ-3.183 relates to the need for the control/management function to be able to send control commands to the other functions of the system.

REQ-3.141 The System MUST allow for different levels of severity of event, such as Information, Warning, Critical.

REQ-3.142 The System MUST provide the ability to search and filter event and transaction logs.

REQ-3.143 The System MUST report the status of each node within the VGISC. (Scope: VGISC, Internal DCPC)

Clarification: The requirement is for the operator to see the status of their 'own' VGISC elements (which includes their Internal DCPC), as well as have an overview of VGISC as a whole. In the case of external DCPC and NC, the VGISC node monitors the status of its interfaces to them.

REQ-3.144 The System MUST provide a configurable, consolidated view of all logs and events between all nodes of the VGISC. (Scope: VGISC, Internal DCPC)

REQ-3.145 The System MUST provide access to all message, system, application and operator logs, by authorised administrators and operators, for analysis and display.

REQ-3.146 The System MUST ensure that message log files covering a configurable period are made available for down-loading on a scheduled basis. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC)

Clarification: The system should allow the format of the log files and the method of the retrieval to be configurable.

REQ-3.147 The System MUST ensure that all message, system, application and operator logs are retained for a configurable number of days. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC)

REQ-3.148 The system MUST maintain the integrity of the data, including the following:

- a. The system does not lose data or allow data to be corrupted
- b. The system does not lose metadata or allow metadata to be corrupted.

(Scope: VGISC, GISC, Internal DCPC, External DCPC)

Clarification: The system must maintain the integrity of the data and metadata by ensuring that the data and metadata are transmitted intact and without corruption.

3.6.4 Performance Requirements

All numbers are a proposal, not fixed values and subject to hardware/network limitations. Proposals are also needed for the DCPC services

REQ-3.149 **Targeted Uptime:** The VGISC service MUST be available 99.9% of the time measured on a 30 day basis. The maximum service downtime, in any one occurrence, MUST not exceed 30 minutes. Each node of the system individually MUST be available 98% of the time measured on a 30 day basis.

The maximum individual node downtime, in any one occurrence, MUST not exceed 120 minutes. (Scope: VGISC, GISC)

REQ-3.150 **System Transit Time:** The high priority data and products MUST traverse the VGISC infrastructure in 10 seconds or less during peak traffic periods. All other data and products (non-priority) MUST traverse the infrastructure in 60 seconds or less during peak traffic volume periods. This requirement is based on the current WMO requirements: Real-time, time critical (timeliness 2 minutes), Real-time, operational critical (timeliness 10 minutes), Real-time, operational (timeliness 30 minutes) (Scope: VGISC, GISC, NC tbd)

Clarification: Typically, high priority data are smaller than lower priority data. The average size of high priority data would be less than 1Mbytes, and the average size of lower priority data may be 10Mbytes. Traverse refers to making the data available on all nodes of the VGISC, i.e. the process of synchronising new data across all nodes of the VGISC.

REQ-3.151 **System Transit Time:** The dissemination and DAR product metadata, including all changes to it, MUST be made available to all VGISC nodes within a configurable time period, to be no more than 15 minutes (Scope: VGISC, GISC)

Clarification: Only changes to DAR metadata should be disseminated to all other VGISC nodes in less than 15 minutes. It is likely that no more 10% of the DAR metadata may change on a daily basis, in the order of 500 DAR metadata changes per 15 minutes at peak.

REQ-3.152 **System Throughput:** The System MUST provide the capability to process 50 data or metadata transactions per second or 3000 data or metadata transactions in 60 seconds (not sustained) during a peak time. The average for a normal (non-peak) period will be in the range of 12 data or metadata transactions per second or 720 data or metadata transactions within a 60 second period. (Scope: VGISC, GISC)

Clarification: System throughput refers to the input processing of data and metadata such that it is ready to be made available to all nodes within the VGISC. Current MSS technology easily handles 20 input transactions and 200 output transactions per second. A metadata transaction is the addition, deletion or modification of a unique item of metadata. This does not include other metadata actions such as validation.

This requirement should be split into two separate requirements, one for data and another for metadata throughput:

3.152a - "**System Throughput:** The system MUST provide the capability to ingest and replicate 50 products per second at a peak time, and 12 products per second at a non-peak time."

3.152b - "**System Throughput:** The system MUST provide the capability to process 1 to 2 DAR metadata transactions per second at a peak time, and 2 DAR metadata transaction per 10 seconds at a non-peak time."

REQ-3.153 **Product Size:** Each VGISC system node MUST include the capability to collect, store and disseminate products with sizes between 10 bytes and 1 Gbytes in size. The average size for data or metadata will fall between the range of 600 bytes and 1 Mbyte in size. The total "received" bytes per day will average about 10 to 100 Gbytes, whereas the average transmitted bytes will

average in the 25 to 1,500 Gbytes range per day depending on the specific node. (Scope: VGISC, GISC, Internal DCPC tbd)

Clarification: Product refers to all data that each VGISC node will hold in its data pool. It is likely that no more 10% of the DAR metadata may change on a daily basis.

REQ-3.154 **Spike Handling:** Each VGISC system node as well as the VGISC system itself MUST smoothly process a data or metadata or other load spike – in other words it shall accept a large (two times normal peak load) influx of data without the system experiencing significant slowdowns. The VGISC System MUST do this without experiencing any: loss of data recognition, loss of data transmit time, loss of duplicate elimination function, loss of any database capability, or loss of any data distribution capability. (Scope: VGISC)

Clarification: The peak throughput figure is 50 data and 1 to 2 DAR metadata transactions per second. The system must be capable of handling a spike of twice this, i.e. 100 data or 5 DAR metadata transactions per second.

REQ-3.155 **Non-Disruptive Backups:** Non-disruptive backup procedures MUST be implemented on all nodes of the system. Non-disruptive database backup procedures MUST also be implemented on the system databases – i.e. - the VGISC databases MUST not be shut down during backups. (Scope: VGISC, Internal DCPC tbd)

Clarification: Backup here refers to the archiving of data and metadata, such as offline tape backup.

REQ-3.156 **Communication Lines and Queues:** The VGISC System MUST provide the capability through adapters/protocol software to interface to and/or receive input or distribute output via at least 100 physical connections and upward of 1200 or more logical communication queues (data channels). The maximum size of a queue MUST be configurable. (Scope: VGISC, GISC)

Clarification: Each VGISC node may have connections to the local MSS, possibly remote MSS (as a backup for other nodes), internal DCPCs and external DCPCs. As these connections may use a variety of transfer protocols, the node must be capable of interfacing with a number of physical connections. Each connection may be split into a number of logical channels, supporting different data types. Physical connections refer to the physical lines into the system.

This requirement should be refined to read: “The VGISC system MUST provide the capability through adaptors/protocol software to interface to and /or receive input or distribute output via at least 1200 logical communication queues (data channels), running over a small number of physical connections. The maximum size of a queue MUST be configurable.”

REQ-3.157 **System Throughput:** The VGISC system MUST have sufficient capability to exceed current throughput by at least 100% growth over the next 2-3 years which would translate to 100 data or metadata interactions per second. (Scope: VGISC, GISC)

REQ-3.158 **System Volume:** The System MUST have the capability to handle an increase in data or metadata incoming volume, from the current daily volume of 1 million plus files or products to expected rates of 5 million per day; daily

transmitted data or metadata volume from the current 10 million transmissions to 50 million data or metadata transmissions per day. (Scope: VGISC, GISC)

Clarification: Throughput is 50 input transactions per second, at peak. This could equate to as many as 500 output transactions per second, at peak. If this rate is constant through the day, this could mean as many as 40 to 50 million output transactions per day. These values are given as a guide to the level of traffic that the system may be required to support.

REQ-3.159 The vendor MUST provide evidence that the system has been designed to allow continuous operation 24x7. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.160 The vendor MUST provide evidence that the system can be updated without disrupting normal operations. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

Clarification: The VGISC system must be capable of providing continuous service even when an individual node is being updated. The service provided by the node being updated would need to be supported or backed up by the other nodes in the system.

3.6.5 Failover Requirements

REQ-3.161 Each VGISC node MUST provide coordination and mutual failover with other VGISC nodes. (Scope: VGISC, GISC)

Clarification: Each VGISC node must be capable of taking over some of the work of another node, in the event of a node failure. This requirement is duplicated in REQ-3.167 and REQ-3.168.

REQ-3.162 All metadata and globally distributed data MUST be synchronised between all VGISC nodes. (Ref. [1]). (Scope: VGISC)

REQ-3.163 Each VGISC node MUST, as a minimum, maintain a cache of configurable length (at least 24 hours of globally distributed data). (Ref. [1]).

REQ-3.164 VGISC Node failovers MUST be handled in such a way to prevent data or metadata from becoming stranded or lost on the failing node. (Scope: VGISC, Internal DCPC)

REQ-3.165 The System MUST be capable of automatically restarting following restoration of power after failure, without loss of event and transaction information. (Scope: VGISC, GISC)

Clarification: Transaction information refers to the metadata relating to ongoing transactions at the time of the power failure. The initiator of the transaction will be responsible for restarting the transmission, but there must be no loss of event or transaction information during the outage.

REQ-3.166 In the event of a VGISC node failure, each VGISC node MUST have the capability to take over some of the functions of another VGISC node, although this must be manually initiated. (Scope: VGISC)

REQ-3.167 The VGISC the system MUST allow for the failover of the dissemination functions to the other VGISC nodes. (Scope: VGISC)

Clarification: The failover may be handled automatically, or may be triggered by an operator action or request.

REQ-3.168 In the event of a VGISC node failure, planned maintenance or downtime, the VGISC system **MUST** be able to manage the migration of data and metadata flows and DAR functionality to other nodes within the VGISC. (Ref. [5]) (Scope: VGISC)

Clarification: This requirement has many implications for the virtual organisation, including our internal and external communications. Further clarification will be given in the next version of the requirements.

REQ-3.169 In the case that any impact or disruption to other partner sites could occur when any single part of a VGISC system fails, such as the catalogue node, the data repository or the VGISC data replication function, all operations **MUST** cease on this system. (Ref. [5]) (Scope: VGISC)

REQ-3.170 The VGISC system **MUST** allow the re-creation of the catalogues at a node from another node. (Scope: VGISC)

REQ-3.171 The VGISC backup and recovery process **MUST** be able to be controlled by the automatic operation process or by operators. (Ref. [5]) (Scope: VGISC)

Clarification: The backup must include system and software configuration information which would allow the restoration of the service in the event of any failure (which may include database table templates etc). For example, where a node fails, the database should first be restored from tape, and then synchronised with the other nodes. As stated in other requirements, data should not be lost. Further clarification may be given in the next version of the requirements.

REQ-3.172 The authentication and authorisation functions **MUST** be encompassed within the backup arrangement of the centre where they operate. This includes downloading and uploading of user credentials and role information among other data and information. (VGISC, GISC, DCPC internal)

REQ-3.173 It is **DESIRABLE** that the system provides support for internal DCPCs to implement backup and recovery of essential services. (Ref. [1]). (VGISC, DCPC internal)

Clarification: Further clarification may be given in the next version of the requirements.

3.6.6 Input and outputs

Figure 7, “WIS Functions A1 through A6” ([1]) defines the inputs to the Manage System Performance function as “Monitoring Data from All Functions”, and defines the outputs as the “Reports of Performance Against Requirements” and “Control Functions to All Functions”.

3.6.6.1 Monitoring Requirements from All Functions

REQ-3.174 The monitoring function **MUST** log all events and actions from all other VGISC functions.

Clarification: The system should log details of all data transactions and metadata modifications, all operator actions, and all user interactions with the system.

REQ-3.175 The VGISC system MUST be able to trace a product from its arrival in the VGISC to its dissemination. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.176 The System MUST maintain a log of all transactions. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

Clarification: A transaction refers to the input or output of any data or product, and the creation, modification and deletion of any piece of metadata.

REQ-3.177 Each log MUST as a minimum include details of data identifier, data size, date/time of transaction. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.178 The System MUST provide a monitoring capability that can be logged and, started and stopped at specific times. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

Clarification: The monitoring function must display the current status of the local and remote VGISC systems. For example, the monitoring should include data-pool status (utilisation), inter-node connection status, a graphical “traffic light” system for all components of the VGISC, allowing at-a-glance monitoring, and further in-depth information available by interacting with the display. The items to be monitored would be those important to delivering and maintaining the “VGISC service” (e.g. those where the performance do not meet requirements). The vendors are invited to propose those items which should be monitored.

REQ-3.179 The System MUST provide an alert function for processing the late important collected information. (Scope: VGISC, GISC, Internal DCPC, NC tbd)

REQ-3.180 The System MUST provide an alert function for processing the saturation of the data cache. (Scope: VGISC, GISC, Internal DCPC, NC tbd)

Clarification: It is likely that the data pool, i.e. the area where data is cached locally on each node, will be of finite size, so the application must be capable of providing alarms when the data pool reaches 80%, 90% and 100% of its defined capacity.

3.6.6.2 Reports of Performance against Requirements

REQ-3.181 The System MUST be able to produce reports based on the received logs and events. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.182 The System MUST be able to configure the contents and format of the reports generated. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.183 The System MUST be able to provide reports on request from an authorised user or automatically, either according to a defined schedule or a defined event or transaction. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

Clarification: An example of a transaction or event triggering a report would be the arrival of a message of high importance, or when the size of the data pool exceeds 80% capacity. The interface will be a GUI managed by an operator.

3.6.6.3 Control Functions to all Functions

REQ-3.184 The System MUST be able to generate control functions/actions for output to all other functions, and to operators and authorised users. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

Clarification: Data and metadata transactions are an example of control functions. Other control functions may include the stopping and starting of the inter-node data links, stopping and starting the logging functions, etc. An example of a control function may be a request to stop or start the ingestion of data from an NC, DCPC, MSS.

REQ-3.185 The System MUST be able to associate logs and events with corresponding actions. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.186 The number of failures required to trigger an alarm and the number of times an alarm is raised MUST be configurable. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.187 The VGISC system MUST enable authorised users to control the flow of data and metadata between VGISC nodes. (Scope: VGISC, NC tbd)

Clarification: The control function must include the ability to stop and start the data and metadata flows between VGISC nodes, and offer the ability to re-route data through other nodes, in addition to other functions to be developed.

3.6.7 Requirements from Function A1 - Collect Observations, Create Products and Archive Information

3.6.7.1 Monitoring Interface

REQ-3.188 The monitoring/supervision of the System MUST provide an alert function for the late arrival of important collected information. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.189 The monitoring/supervision of the System MUST provide a monitoring function for checking the different queues associated to the collect, create and archive functions. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.190 The monitoring/supervision of the System MUST provide an alert function for preventing the saturation of the data cache. (Scope: VGISC, GISC, NC tbd)

Clarification: This requirement is very similar to REQ-3.180. It is likely that the data pool, i.e. the area where data is cached locally on each node, will be of finite size, so the application must be capable of providing alarms when the data pool reaches 80%, 90% and 100% of its defined capacity. Managing the saturation could involve the removal of the oldest and lowest priority data from the pool, or the closure of the input data channels.

REQ-3.191 The monitoring/supervision of the System MUST provide an alert function for managing corrupt collected metadata. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.192 The monitoring/supervision of the System MUST provide an alert function for managing corrupt collected data. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.193 The System MUST allow for different levels of severity of event on receiving information, such as Information, Warning, Critical. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.194 The monitoring/supervision of the System MUST provide an alert function for the arrival of Critical information (e.g. Warning), to be handled in different ways according to the information severity. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

Clarification: The system must provide different levels of event, and it must be possible to configure the system to handle the different levels of event in different ways.

REQ-3.195 The monitoring/supervision of the System MUST provide a display function for the collected data or products. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

Clarification: The system should provide a function to display the log information, and allow an operator to view a product, as selected by the operator.

REQ-3.196 The monitoring/supervision of the System MUST provide a correction/amendment function for the data or products. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

Clarification: It is possible that some data, on arrival into the system, will not be correctly formatted. For data which can be manually corrected, such as text data formats, the system should provide a user interface where these data can be displayed and corrected by an operator.

3.6.7.2 Reporting Interface

REQ-3.197 The System MUST provide a log-file for the ingestion module. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.198 The System MUST provide a specific log-file for the GTS ingestion module. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.199 The System MUST provide a log-file for the MSS feeding module. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.200 The System MUST provide a log-file for the replication module. (Scope: VGISC, NC tbd)

REQ-3.201 The System MUST log information concerning the pack and unpack processes. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.202 The System MUST log information concerning file transfers operated via a number of protocols including at least: FTP, SFTP, FTP WMO, HTTP, HTTPS, SMTP. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.203 The System MUST provide a log-file for the DAR metadata creation modules including:

- a. on the fly creation,
- b. creation based on reference information,
- c. downloading of metadata from a provider,

- d. manual metadata creation via a Web interface.
(Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

3.6.7.3 Controlling Interface

REQ-3.204 The System MUST provide a user interface to enable authorised administrators and users to carry out the following actions: DAR metadata creation, checking and validation of new DAR metadata. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.205 The VGISC system MUST offer an interface to control that the collection of GTS products is maintained in the event of a failure of the MSS at one site or a failure of one of the collecting nodes. (Scope: VGISC, NC tbd)

Clarification: This requirement relates to ensuring that local data collected by a local MSS is still forwarded into the VGISC in the event of a failure of the local MSS. The VGISC will consist of three GISC nodes, which will each be responsible for the collection of data and products from their area of responsibility and forwarding this data to the VGISC. This data collection would normally be performed by the local MSS. In the event of the local MSS failing, a process is required which will enable the local data for that node to be collected, possibly by other MSS, and forwarded into the VGISC.

REQ-3.206 The System MUST provide an interface to control that a (DAR) metadata in the catalogue is associated to every collected data or product and to every created data or product. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

Clarification: The system must ensure that appropriate DAR metadata records exist for every collected or created data or product. Where metadata does not exist and cannot be generated, the system should archive the information and the originator of the product is notified.

REQ-3.207 The System MUST provide a control interface to validate metadata records against their schemas (records either automatically created at the receipt of self documented products or received or built in different ways). (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.208 The System MUST provide an interface to manage the creation of products and data bulletins / files that are either event-driven or scheduled by time. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.209 The System MUST provide an interface to force the routing of products and data bulletins / files. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

Clarification: The system must allow the manual transmission of datasets to users on an ad-hoc basis, independently of any subscriptions.

3.6.8 Requirements from Functions A2 - Assign User Role and A4 - Authorise Access to Information by Users

3.6.8.1 Monitoring Interface

There are various functionalities required to handle authorised users and their access to information and services within the VGISC system. The functions performing authentication

and authorisation should report to the monitoring function which in return provides the required information to the management function. During this process the privacy of person related information should be respected at the VGISC level. Personal user information should only be resolved at the local level within the VGISC.

REQ-3.210 The System MUST respect confidentiality of user identifiable information. Accordingly the monitoring function MUST deal with user references to be resolved only at the authenticating centre.
(Scope: VGISC, GISC, Internal DCPC, External DCPC, NC)

Clarification: External DCPC should not be in the scope of this requirement, because external DCPC do their own business with their users, and VGISC will never have to monitor external DCPC users. For the cases where back up scenarios are requested, synchronisation of user data (roles and credentials) should be done with acknowledgment of the user or via configuration for high-availability users (e.g. an administrator). Credentials are -private user data-, so default synchronisation would break confidentiality.

Distinction between users:

- a. General Purpose Users: e.g. Researches, asking for archive data.
- b. Expert /High availability Users: An administrator, users subscribed to real time data.

3.6.8.2 Reporting Interface

REQ-3.211 The authentication and authorisation functions MUST provide both routine and exception condition reporting to the System monitoring function.

- a. Routine reporting e.g. number of current authenticated users, data download profiles, etc ...
- b. Exception reporting e.g. number of authentication attempts that failed, number of sessions that ended abnormally.

(Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

Clarification: External DCPC should not be in the scope of this requirement, because external DCPC do their own business with their users, and VGISC will never have to monitor external DCPC users.

3.6.9 Requirements from Function A5 - Deliver Information to Users

3.6.9.1 Monitoring Interface

REQ-3.212 The System MUST provide logging for the following events.

- a. a subscription request is submitted by a user
- b. a subscription request is approved by an administrator
- c. an ad-hoc request arrives
- d. user pull result
- e. a subscribed product is delivered (every time it happens)

(Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

3.6.9.2 Reporting Interface

REQ-3.213 The System MUST produce reports based on a variety of delivery mechanisms:

- a. The number of users required/made an ad-hoc request per product.
- b. The number of users subscribe to a product in an interval of time.

- c. The number of users who are subscribed at this moment per product.
- d. The % of successful ad-hoc requests served.
- e. The % of subscribed products sent successfully.
- f. Timeliness.

(Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

Clarification: A product is a single piece of data, such as a WMO bulletin, which can be identified and delivered to a user. For some data or products there will be an agreed deadline for it's availability. In this case, the timeliness measurement would relate to the product being available in the data pool by a certain time.

3.6.9.3 Controlling Interface

REQ-3.214 An end user **MUST** be able to request for a subscription. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.215 An end user **MUST** be able to manage/update their subscription details. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

Clarification: This requirement is a duplication of requirement REQ-3.116.

REQ-3.216 An end user **MUST** be able to follow the status of his ad-hoc requests. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.217 The administrator of the VGISC system **MUST** be able to validate/grant a subscription. (Scope: VGISC, GISC, Internal DCPC, NC tbd)

REQ-3.218 The administrator of the VGISC system **MUST** be able to manage the subscription details of all users. (Scope: VGISC, GISC, Internal DCPC, NC tbd)

REQ-3.219 The administrator of the VGISC system **MUST** be able to follow the status of all users' ad-hoc requests. (Scope: VGISC, GISC, Internal DCPC, NC tbd)

REQ-3.220 The administrator of the VGISC system **MUST** be able to follow the status of all users' subscriptions (delivery). (Scope: VGISC, GISC, Internal DCPC, NC tbd)

3.7 Function A7 – Web Interface

3.7.1 Definition

The system will have to interface to a variety of existing Web interfaces at the partners' sites. These existing interfaces support a variety of functions, including monitoring, management and dissemination. Some will be used by internal users and some by authenticated external users.

Clarification:

For external users, a range of solutions is possible, such as the German users of the VGISC system using the German node and similarly for France and UK. Or, one VGISC node could take turns at being the definitive node for all users, with re-direction. For example, by declaring one URL. However, one of the fundamental principles of WIS is that users can choose where to connect to the system given that addresses are known.

3.7.2 Introduction

3.7.2.1 Background

Any of the 6 basic high level functions identified in [1] could potentially require a Web based interface. Some of the 15 high interfaces specified in [1] naturally lend themselves to Web based interface, whereas others would more appropriately support programmatic interfaces.

3.7.2.2 General

REQ-3.221 The System **MUST** support a variety of web based interfaces customised to each of the partners' sites.

REQ-3.222 The System **MUST** support a variety of web based functions, including, but not restricted to:

- a. Discovery, Access and Retrieval
- b. System Monitoring
- c. System Management
- d. Dissemination
- e. System Administration

REQ-3.223 The System **MUST** support a variety of users, including at least:

- a. Authenticated and authorised internal users
- b. Authenticated and authorised external users

Clarification: Anonymous or 'guest' users are included in the definition of authenticated and authorised external users.

REQ-3.224 The vendor **MUST** state which functions or interfaces are common across all partners sites and which are tailored to be specific to each site, if a partner has requested a tailoring for his special requirements.

REQ-3.225 The vendor **MUST** provide evidence of how the VGISC web based interfaces meets the requirements for Flexibility, Configurability, Modularity, Scalability.

REQ-3.226 The vendor **MUST** provide evidence of how the VGISC web based interfaces meets the requirements for security, including separation at design level between public and private functions.

REQ-3.227 The vendor **MUST** provide evidence of how they will address the requirement for multi-language support (e.g. file based messages for localisation of fixed text messages text).

3.7.2.3 Technology

REQ-3.228 The vendor **MUST** state which browsers are supported by the System.

REQ-3.229 It is **DESIRABLE** that the System supports at least:

- a. Microsoft Internet Explorer Version 6 or later
- b. Firefox Version 2.0 or later

REQ-3.230 The vendor **MUST** state which technologies by version, are used by the Web based interfaces, e.g. CSS Version 2.0, XHTML Version 1.0, XSLT Version 1.0, RSS Version 1.0, PHP Version 5.0

REQ-3.231 The supported browsers **MUST** operate with the highest levels of security

REQ-3.232 The vendor **MUST** state where and why the system uses any technologies that can be potentially inappropriately exploited, such as persistent cookies , JavaScript, ActiveX and applets.

REQ-3.233 It is **HIGHLY DESIRABLE** that persistent cookies are not used.

REQ-3.234 It is **HIGHLY DESIRABLE** that Web interfaces do not use downloaded applets.

REQ-3.235 The vendor **MUST** state the level of W3C accessibility to which the system has been implemented and state how they will demonstrate this.

3.7.2.4 Functions

REQ-3.236 It is **DESIRABLE** that the following functionality is supported, but not limited to:

- a. 'Multi selection' of items from a list
- b. Command line interface as well as web-based for some administration functions
- c. Blocking of persistent cookies

Clarification: Regarding a: At this point we are not able to see where it would be useful, but during design of UI we can take the requirement on account.req-reply}

Regarding c: Some members of the Consortium implement a security policy that does not allow cookies to persistent beyond the current session.

REQ-3.237 The System **MUST** provide end-users the ability to browse and discover entries in the catalogue of available data and products through a web-based interface. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.238 The System **MUST** provide end-users with a web interface to allow them to monitor the status of their subscription or ad hoc request. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

Clarification: Both are intended.

REQ-3.239 The System **MUST** provide an operator interface for alerts for late important information, or saturation of cache. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.240 The System **MUST** provide a web-based interface for authorized administrators to manage and schedule the routine delivery service. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC tbd)

REQ-3.241 The scope of the user's access to the management functions **MUST** be configurable. (Scope: VGISC, GISC, Internal DCPC, External DCPC, NC)

4 Use Cases

4.1 Introduction

In addition to the GIS functionality as described in the respective WMO documents, the distributed nature of the VGISC implementation requires certain additional functionality, which is summarized in the following sections.

The treatment of "Use Cases" in this document follows the guidance and template published by Karl. E. Wiegers (with permission granted to use, modify, and distribute the template). Use Cases were introduced within an object-oriented development methodology but have been extended into a general technique for requirements analysis and user interface design. Each Use Case should describe how a user would interact with the system to accomplish a particular task. Use Cases, by definition, must be described in terms of the user's work terminology, not the jargon of software designers. The objective of documenting Use Cases is to get at fundamental system functions as the user would interact with the system. Because a Use Case description is not concerned with implementation constraints or technology details, such documentation makes it easier for the system user and the system designer to agree on essential system requirements.

The following table provides a key to the elements of the Use Case template as used herein. With some of the Use Case descriptions there is also a graphical representation of the Use Case in the style of Unified Modelling Language (UML).

Use Case Goal - Brief description of the reason for and outcome of this Use Case, or a high-level description of the sequence of actions and the outcome of executing the Use Case.
Actors - An actor is a person or other entity, external to the system being specified, who interacts with the system (includes the actor that will be initiating this Use Case and any other actors who will participate in completing the Use Case). Different actors often correspond to different user classes, or roles, identified from the customer community that will use the product.
Trigger - Event that initiates the Use Case (an external business event, a system event, or the first step in the normal flow.
Pre-conditions - Activities that must take place, or any conditions that must be true, before the Use Case can be started.
Post-conditions - The state of the system at the conclusion of the Use Case execution.
Normal Flow - Detailed description of the user actions and system responses that will take place during execution of the Use Case under normal, expected conditions. This dialog sequence will ultimately lead to accomplishing the goal stated in the Use Case name and description.
Alternative Flows - Other, legitimate usage scenarios that can take place within this Use Case.
Exceptions - Anticipated error conditions that could occur during execution of the Use Case, and how the system is to respond to those conditions, or the Use Case execution fails for some reason.
Includes - Other Use Cases that are included ("called") by this Use Case (common functionality appearing in multiple Use Cases can be described in a separate Use Case included by the ones that need that common functionality).
Notes and Issues - Additional comments about this Use Case and any remaining open issues that must be resolved. (It is useful to Identify who will resolve each such issue and by what date.)

Table 4.1. Key to Elements in the Use Case Template

Each Use Case should be associated with one or more Test Cases that will be used to verify that a delivered system actually functions as the designers intended. However, there should

be additional Test Cases, especially to verify system functions that may not be apparent to users, such as system internal control functions. The following sections list all Use Cases, details of which can be found in Appendix E.

4.2 GISC Use Cases

GISC 1, Provide Metadata for Data or Product
 GISC 2, Upload Data or Product to GISC
 GISC 3, Control Metadata Association to Data or Product
 GISC 4, Manage Cache of Data across GISCs
 GISC 5, Maintain Identification and Role Information for WIS Users
 GISC 6, Discover Data or Products
 GISC 7, Ad Hoc Request for Data or Product ("Pull")
 GISC 8, Subscribe to Data or Product ("Push")
 GISC 9, Download Data or Product from GISC
 GISC 10, Provide Dissemination Metadata
 GISC 11, Report Quality of Service across GISCs
 GISC 12, GTS metadata generation from WMO Volume C1 reference

4.3 VGISC Use Cases

The Use Cases below come in addition to the WMO GISC Use Cases and attempt to take the virtualisation of the VGISC into account. Some of those Use Cases are discussed in general in the SIMDAT D18.1.1 deliverables and can be classified into the following topics:

- Access Data and Metadata
- Provide Data and Metadata
- Manage VO
- Manage VGISC Infrastructure (DCI)
- Monitor and Control the VGISC

As explained in the introduction, an extension is done to take the ingestion of the GTS essential data into account.

VGISC 1, Provide Metadata for Data or Product
 VGISC 2, Upload Data or Product to VGISC
 VGISC 3, Control Metadata Association to Data or Product
 VGISC 4, Manage Cache of Data across VGISC
 VGISC 5, Maintain Identification and Role Information for VGISC Users
 VGISC 6, Discover Data or Products
 VGISC 7, Ad Hoc Request for Data or Product ("Pull")
 VGISC 8, Subscribe to Data or Product ("Push")
 VGISC 9, Download Data or Product from the VGISC
 VGISC 10, Provide Dissemination Metadata
 VGISC 11, Report Quality of Service inside the VGISC
 VGISC 12, GTS metadata generation from WMO Volume C1 reference
 VGISC 13, GTS MSS feeding in the VGISC
 VGISC 14, Data Replication in the VGISC
 VGISC 15, GTS Ingestion in the VGISC
 VGISC 16, Backup inside the VGISC
 VGISC 17, Management of the information classes (between WMO and the Central Support Office)

4.4 DCPC Use Cases

4.4.1 Internal DCPC

1. Metadata for data or products and Upload of files
 - Internal DCPC 1, Provide Metadata for Data or Product
 - Internal DCPC 2, Make Data or Product Available to DCPC
 - Internal DCPC 3, Control Metadata Association to Data or Product
2. User Management
 - Internal DCPC 4, User Registration
 - Internal DCPC 5, User Authentication
 - Internal DCPC 6, User Authorisation
3. DAR Catalogue
 - Internal DCPC 7, Discover Data or Products
4. Dissemination Metadata and Download of files
 - Internal DCPC 8, Ad Hoc Request for Data or Product ("Pull")
 - Internal DCPC 9, Subscribe to Data or Product ("Push")
 - Internal DCPC 10, Download Data or Product from DCPC
 - Internal DCPC 11, Provide Dissemination Metadata
5. Quality of Service
 - Internal DCPC 12, Report Quality of Service across VGISC Centres
 - Internal DCPC 13, Monitoring the DCPC
 - Internal DCPC 14, Backup
 - Internal DCPC 15, Recovery
 - Internal DCPC 16, Install Software Updates

4.4.2 External DCPC

1. Metadata for data or products and Upload of files
 - External DCPC 1, Provide Metadata for Data or Product
 - External DCPC 2, Make Data or Product Available to DCPC
 - External DCPC 3, Control Metadata Association to Data or Product
2. User Management
 - External DCPC 4, User Registration
 - External DCPC 5, User Authentication
 - External DCPC 6, User Authorisation
3. DAR Catalogue
 - External DCPC 7, Discover Data or Products
4. Dissemination Metadata and Download of files
 - External DCPC 8, Ad Hoc Request for Data or Product ("Pull") hosted by the DCPC
 - External DCPC 9, Subscribe to Data or Product ("Push") hosted by the DCPC
 - External DCPC 10, Download Data or Product from DCPC
 - External DCPC 11, Provide Dissemination Metadata
5. Quality of Service
 - External DCPC 12, Report Quality of Service across WIS Centres
 - External DCPC 13, Monitoring the DCPC
 - External DCPC 14, Backup
 - External DCPC 15, Recovery
 - External DCPC 16, Install Software Updates

5 Software Contributions

5.1 Introduction

A software contribution is a software distribution that will be presented to vendors for consideration in different aspects:

As a set of reusable software modules that implement some of the requirements of the ITT specification.

and/or

As software offered for evaluation to reuse designs, ideas and experience gained on any of the areas specified on the ITT.

The following list covers software contributions presented by the partners:

- EFTS_Agents (EUMETSAT)
- FIMEX (METNO)
- GEMS/SMART (EUMETSAT)
- METAMOD (METNO)
- SIMDAT (ECMWF)
- GTS Modules contributed to SIMDAT: Metadata Creation (Meteo France)
- GTS Modules contributed to SIMDAT: ingestion / retrieve / feeding (Meteo France)
- WebWerdis (DWD)

A summary table at the end of the section is presented with the areas that each of the software package covers in some aspect as presented in the definition of software contribution.

5.2 EFTS_Agents

5.2.1 Description

The Extended File Transfer Software (EFTS) Agents is a collection of processes that do local or remote file transfer, copying, and manipulation. It can be used to:

- Transfer files to or from a remote server using various transfer protocols (SFTP, FTP, email).
- Pre-process files before physically copying or (hard or symbolically) linking them into one or more other directories.
- Check remote connections regularly

The EFTS_Agents can run as daemon processes with a configurable cycle time, or as 'single-shot' processes.

Typical uses of the software are the following:

- As a central collector of files from several directories to one directory from where the files are further processed.
- As a distributor of files from one directory to other directories from where the files are further processed.
- As a service on a Windows NT/2000/XP PC copying files and pushing them to another server via a file transfer protocol.

- As an automatic distributor and archiver (or replicator) for incoming files.
- As a server connection checker.
- As a file poll agent that gathers files regularly from remote servers.
- As a file push agent that transfers files regularly to remote servers.
- As a generator of request files for files that are processed by the EFTS_Agents Application.

The EFTS_Agents software is written in Java and can therefore be used on multiple platforms without the need of having to recompile the software.

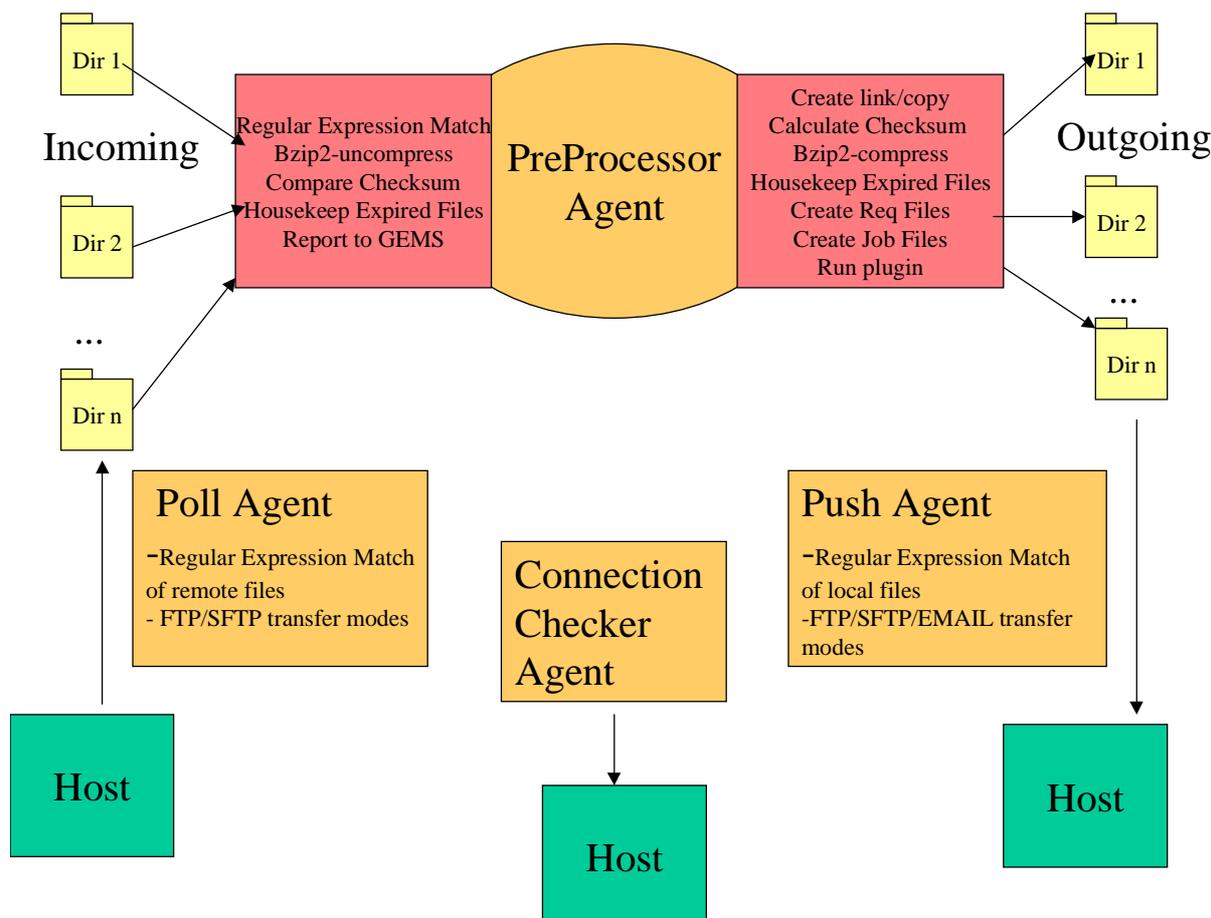


Figure 5.1 EFTS_Agents overview

5.2.2 Status of the software

The EFTS_Agents were developed at EUMETSAT and have been running for more than 4 years at EUMETSAT operational environment.

Currently the version 2.50 is available at the EUMETSAT website, [Useful Programs & Tools](#).

The software is maintained at EUMETSAT.

5.2.3 Potential Use within VGISC

EFTS_Agents could be use for any file transfer necessary within the VGISC (upload of data/metadata, download of data/metadata, exchange of information between nodes, ...)

5.2.4 Current license status

General Public License

5.2.5 Contact Details

Lothar Wolf

European Organisation for the Exploitation of Meteorological Satellites

Am Kavalleriesand, 31

D-64295, Darmstadt

Email: Lothar.Wolf@eumetsat.int

Phone: +49 (0) 6151 807405

5.3 FIMEX

5.3.1 Description

File Interpolation, Manipulation and EXtraction (FIMEX) is an attempt to solve common problems discovered when exchanging gridded data, e.g. the receiver

- wants another data-format
- wants a different map projection
- wants a smaller area or shorter time period than covered by the original data file (data reduction)
- wants a different vertical coordinate (e.g. can't use model levels, need pressure levels)

The software is being developed at the Norwegian Meteorological Institute (METNO) to support International Polar Scientists (IPY) with access to Numerical Weather Prediction (NWP) data for modelling and field work purposes. It is intended to be used in two ways:

- As part of the web portal solution METAMOD 2 (see Chapter 5.5) where it should offer functionality for the user to determine the file format, map projection and data reduction wanted before receiving the data.
- As part of an automatic distribution mechanism to a group of user interested in a subset (parameters, area, time, etc) of full data set.

It is implemented using C/C++, using PROJ.4 and the Common Data Model.

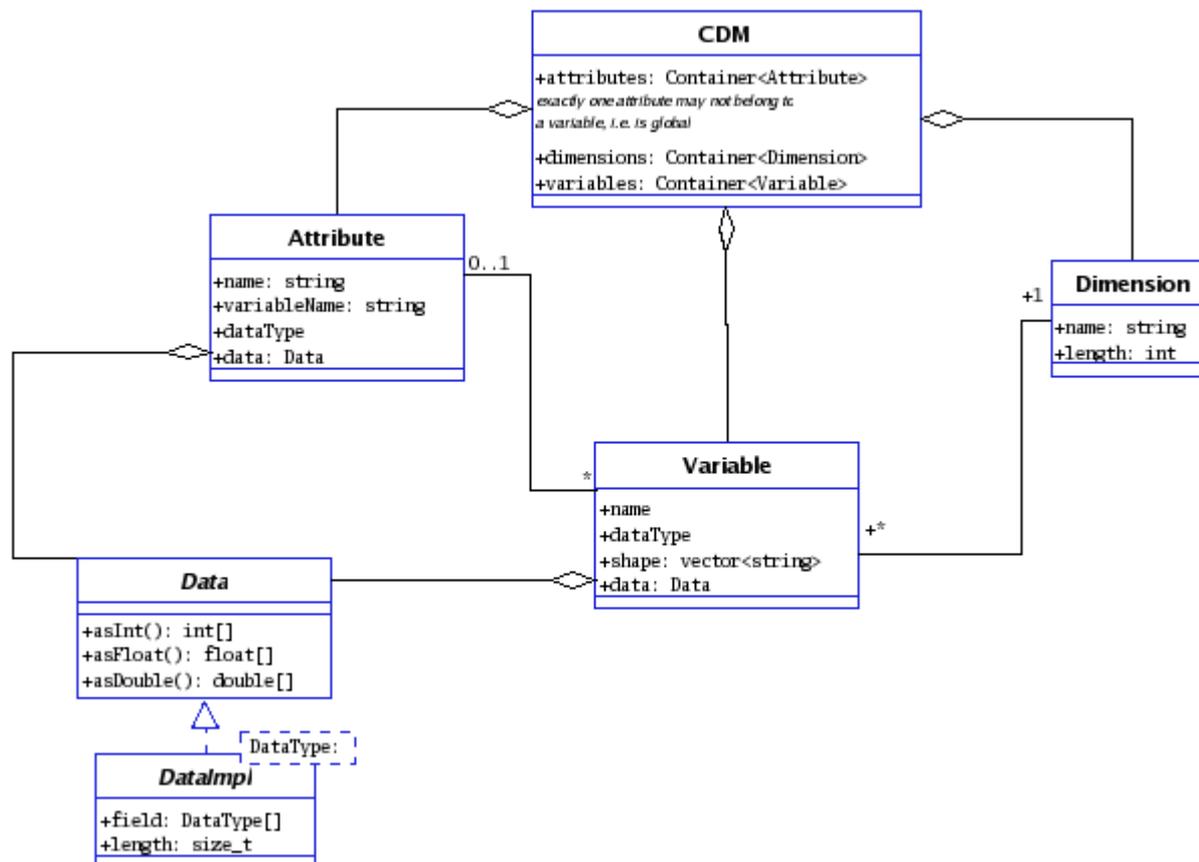


Figure 5.2 FIMEX data model

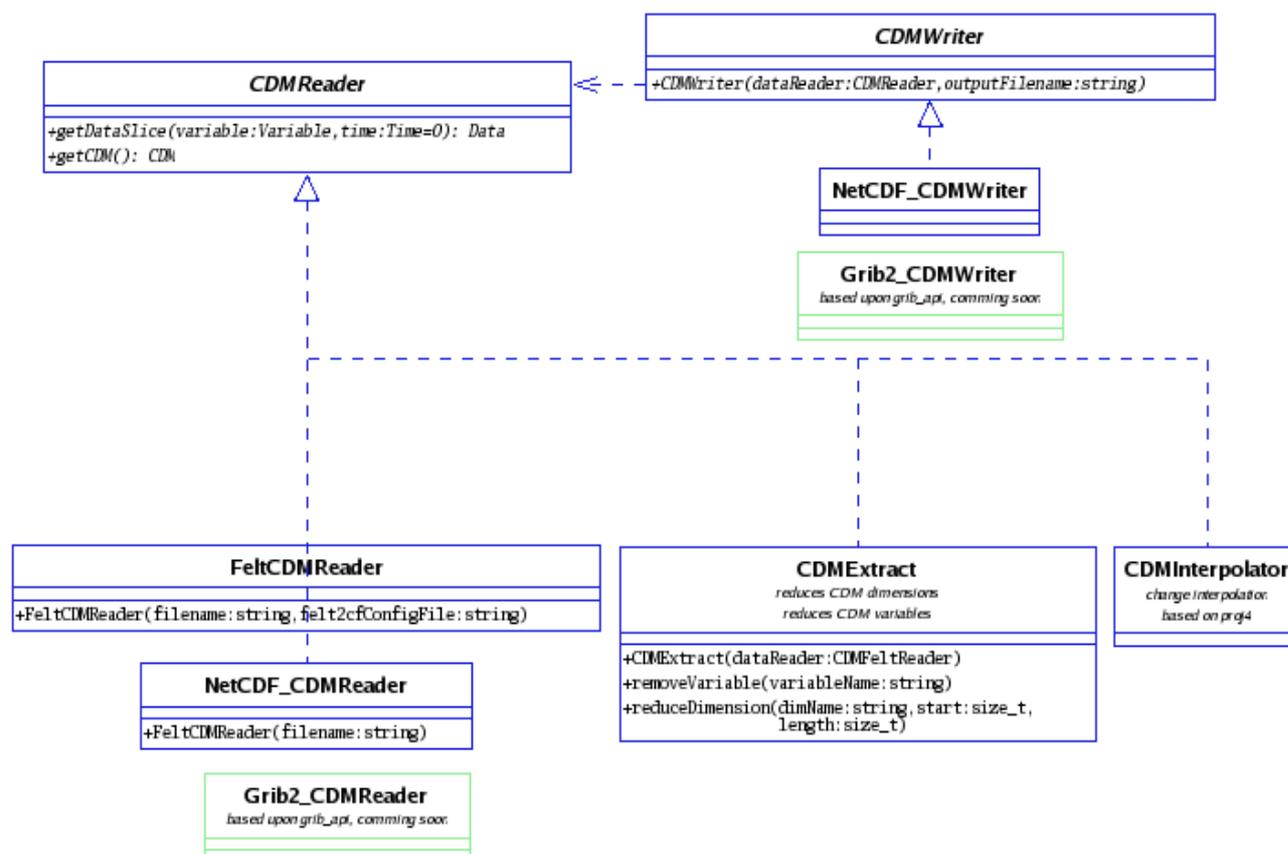


Figure 5.3 FIMEX I/O chain

5.3.2 Status of the software

The software is still under development, first operational use is expected in May 2008 for International Polar Year purposes when it will be used for data reduction when providing Numerical Weather Prediction data (e.g. ECMWF and METNO HIRLAM) for modelling and field work purposes. Currently it supports flat files (METNO specific binary format for NWP output), NetCDF and GRIB support is under development.

5.3.3 Potential Use within VGISC

FIMEX is intended to be used within a portal solution or an automatic push mechanism based upon templates defining the file format, map projection, geographical area, time period, parameters etc the user wants to receive.

5.3.4 Current license status

LGPL 2.0 or higher. A wiki and Subversion repository is underway.

5.3.5 Contact Details

Øystein Godøy
 Norwegian Meteorological Institute
 P.O.BOX 43 Blindern
 NO-0313 OSLO
 Norway
 Email: o.godoy@met.no

5.4 GEMS/SMART

5.4.1 Description

Generic Event Monitoring Software (GEMS) and Scheduling, Monitoring, Analysis and Reporting Tool (SMART) are two software packages, developed at EUMETSAT, that used together provide a complete system, application and data flow monitoring and reporting system.

GEMS has been designed and implemented by the EUMETSAT OPS Maintenance and Engineering Department to provide event monitoring functionality to a number of heterogeneous, multi-platform, multi-site facilities. It has been designed to be platform independent and to be easily integrated into new and legacy applications.

Thanks to a simple three tier architecture (client - server - client) and powerful redundancy concepts, it allows reliable, easy and consistent event monitoring from a small [remote, platform independent] set of consoles of a number of facilities reducing equipment, space and maintenance costs.

The implementation of GEMS is based on 100% pure Java software and has been tested on a number of platforms (SUN Solaris, Windows NT, HP-UX, Linux). It provides a simple API from both Java and C languages and a command line interface for raising events.

A number of standard agents have been implemented and are or will be part of GEMS, among them are: file system usage monitoring, monitoring of log files (translating entries in them into events), checking of host reachability via FTP, process statistics monitoring, etc.

An Internet browser interface for real-time monitoring and historical browsing is also provided. The latter allows investigation of anomalies and comparison of sequence of events at different times.

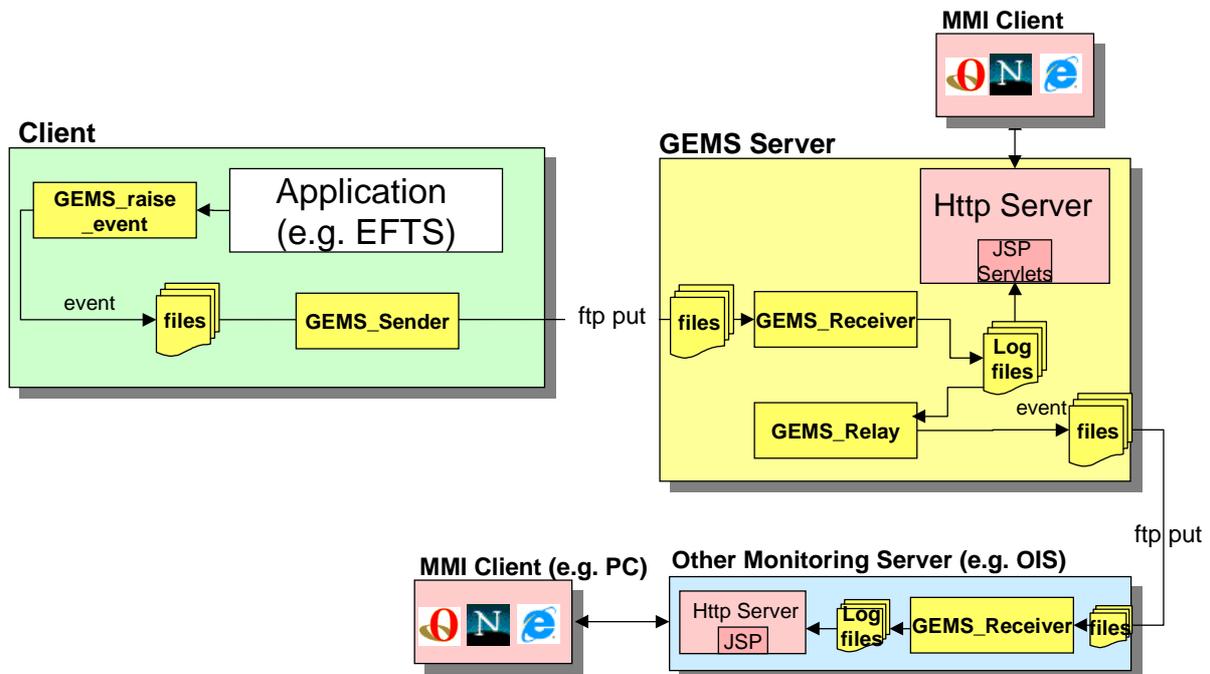


Figure 5.4 Architecture of GEMS

The Generic Event Monitoring Software (GEMS) consists of several Java daemons which run on clients as well as on the GEMS server.

SMART is designed to provide end to end monitoring of operational services and reporting functionality.

The key features of SMART are:

- Scheduling the planned activities and expected events.
- Monitoring the completeness, timeliness and quality of the activities.
- Analysis and Reporting of the service availability and performance, supplying summary reports.

Inside an operational service, data are processed by a set of facilities. At each processing stage the relevant facility generates status messages (events), with the support of GEMS.

Typical events are: File sent/received, Product processing messages and System and reachability alarms. GEMS filters these messages in ASCII log files per facility and makes them available to SMART, as we can see at the following figure.

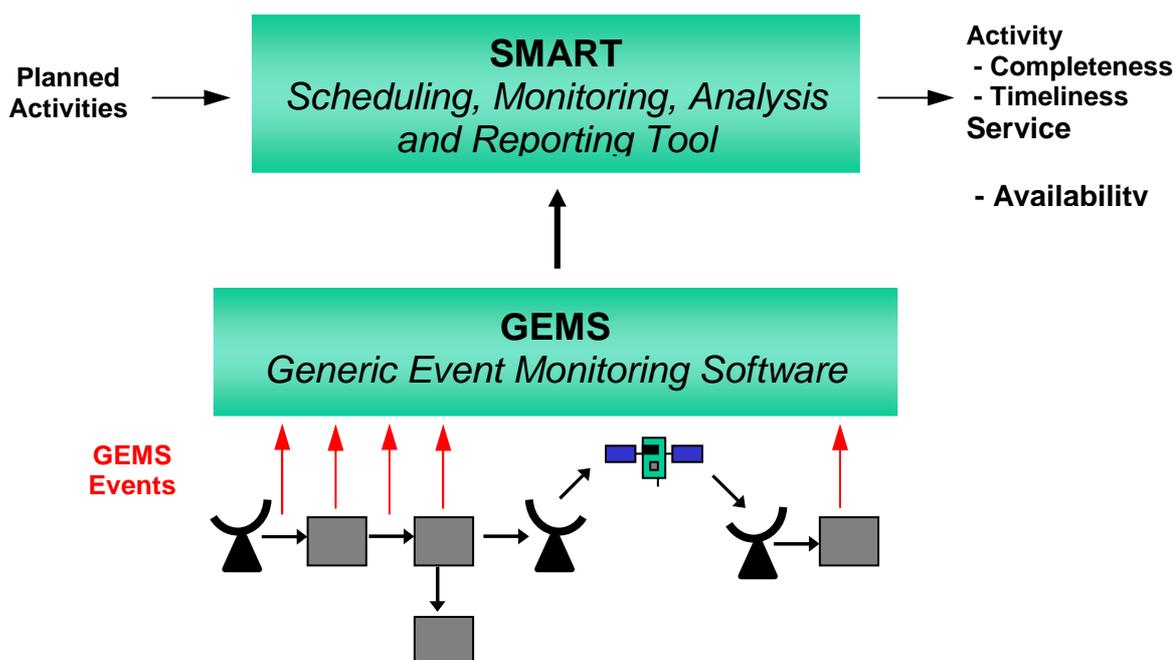


Figure 5.5 Context overview of SMART

SMART collects these events and compares them with the pre-configured expectations for that service, providing near real time information about the processing chain for each operational service. In addition, when a certain condition is detected in an operational service, SMART alerts about the situation.

All this information is stored for later access.

Finally, SMART allows the generation of reports to obtain summary information over long periods and to allow investigation of anomalies.

SMART source code is 100% pure Java and the information and configuration items are stored in XML files, which confer to the software a high degree of configurability.

5.4.2 Status of the software

Both software packages are currently used for monitoring and reporting on EUMETSAT operational services.

GEMS has been running in operational since 2002 and SMART since 2004.

Also, both software packages are maintained at EUMETSAT.

5.4.3 Potential Use within VGISC

GEMS could be used to monitor the System at the local nodes, or to extract the relevant information of the VGISC system logs at the local nodes in form of GEMS events, these GEMS events will, then, be exchanged/relayed to the rest of the nodes, so that at every node a **global monitoring view** of the VGISC system is possible.

Over GEMS, SMART could run in order to perform an end-to-end monitoring of the data received/exchanged/sent (follow data flow) and reporting on this (QoS reports).

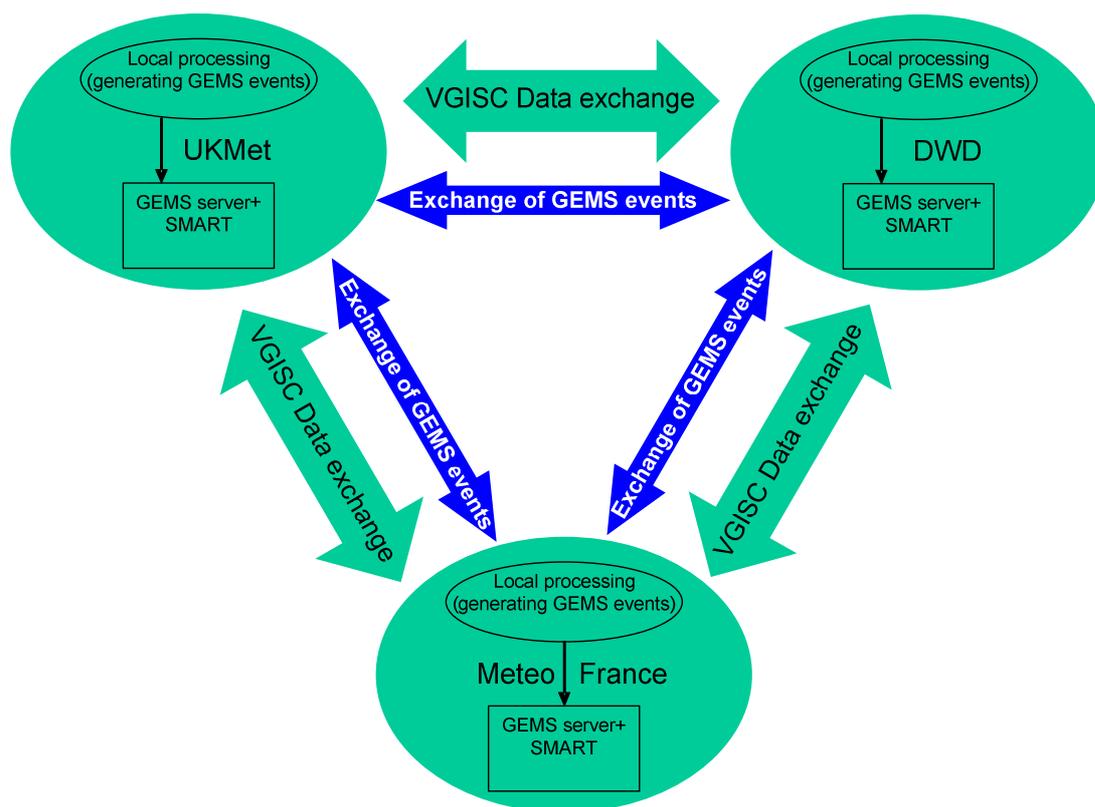


Figure 5.6 Schematic illustration of the potential use of SMART within the VGISC

5.4.4 Current license status

General Public License

5.4.5 Contact Details

Lothar Wolf

European Organisation for the Exploitation of Meteorological Satellites

Am Kavalleriesand, 31

D-64295, Darmstadt

Email: Lothar.Wolf@eumetsat.int

Phone: +49 (0) 6151 807405

5.5 METAMOD 2.x

5.5.1 Description

During 2001/2002, the Norwegian Meteorological Institute (METNO) implemented a web based tool (MetaMod) for searching data archived under the NoSerC project (<http://noserc.met.no/>). This tool was adapted for DAMOCLES database search in 2006/2007. The web interface and the overall functionality of the tool were very much improved during the DAMOCLES development, and just a small part of the original code base has remained unchanged. Other projects at METNO have also contributed to the development process. The software is now named METAMOD2, to distinguish it from the original MetaMod tool that is still occasionally maintained.

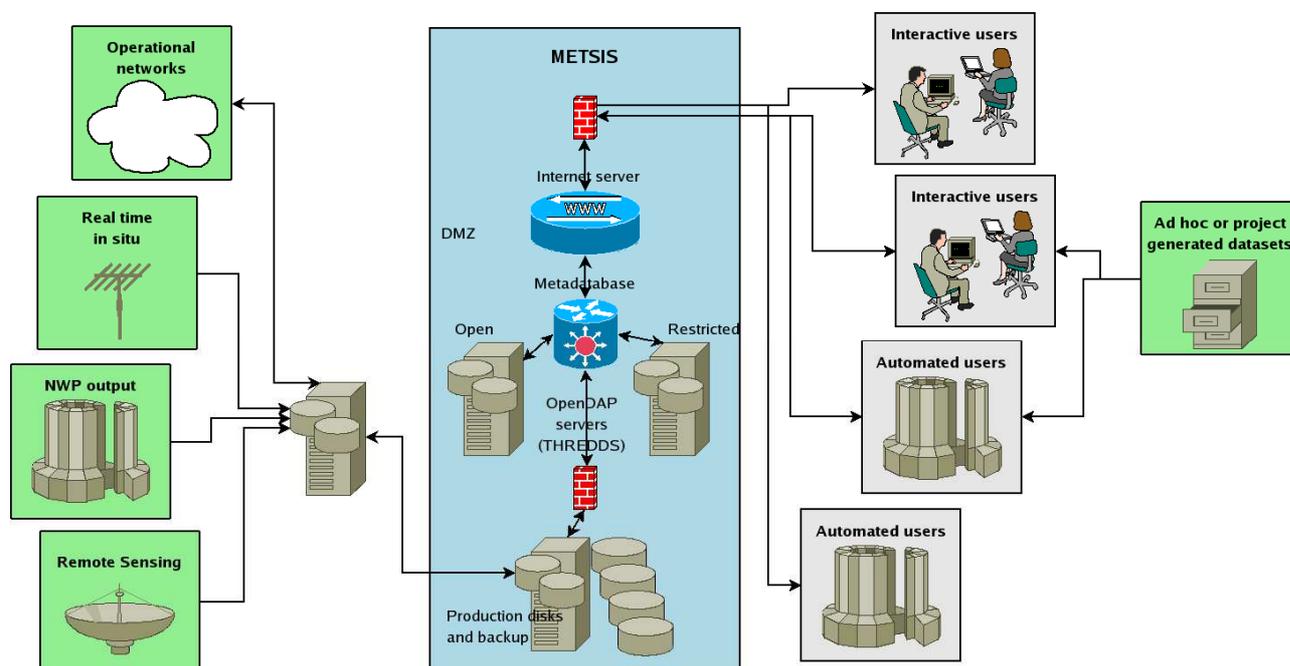


Figure 5.7 METAMOD 2.x is a portal solution providing Discovery, Access and Retrieve functionality for scientific projects along with tools for metadata handling etc.

The purpose of the METAMOD2 software is twofold:

- To manage a data repository containing scientific data sets.
- To keep a database containing metadata that describes the data sets in the data repository, as well as other data sets found in external data repositories (not managed by METAMOD2 software).

As additional projects were seen to benefit from using METAMOD2 software, a need for making the software independent of a single project emerged. This was obtained by organizing the software in different modules, and by separating all project specific aspects into a configuration file. METAMOD2 now comprise the following modules:

METAMODBASE Database and corresponding administrative tools.

METAMODSEARCH Web based search facility.

METAMODUPLOAD Web based upload facility for data files.

METAMODQUEST Web based questionnaire for registering metadata.

The configuration file describes an actual implementation of a web application based on METAMOD2 software. First of all, the file lists which of the four modules that are used in the application. Any combination of the four modules is allowed. If the METAMODBASE module is not a part of an application, the configuration file must reference another METAMOD2 application that uses the METAMODBASE module. In this way, several applications may share the same database.

The software is implemented on a Linux system with Apache web server. PHP is used to implement dynamic web content, and Perl is used to implement tasks not directly involving web content generation. The database is based on PostgreSQL. Metadata elements use controlled vocabularies from GCMD and CF1.0 as well as WMO keywords. Tools for extraction of metadata from NetCDF/CF files are part of METAMODUPLOAD. Access to the actual datasets is provided through HTTP, FTP, OpenDAP. Use of THREDDS Data Server (OpenDAP and OGC WCS) is being examined currently as well as metadata exchange using OAI-PMH.

5.5.2 Status of the software

The software is being used for several International Polar Year projects (e.g. http://damocles.met.no/data_management/, <http://ipycoord.met.no/>, <http://dokipy.met.no/>).

5.5.3 Potential Use within VGISC

METAMOD 2 provides a sample portal solution that can be used to discover, access and retrieve products, as well as mechanisms for interactive upload/download of data sets/products.

5.5.4 Current license status

GPL 2.0 or higher. A wiki and Subversion repository is underway.

5.5.5 Contact Details

Øystein Godøy
Norwegian Meteorological Institute
P.O.BOX 43 Blindern
NO-0313 OSLO
Norway
Email: o.godoy@met.no

5.6 SIMDAT

5.6.1 Description

SIMDAT is a four year project funded by the European Commission, under the Information Society Technologies Programme (IST). The main objective of the project is to raise awareness of the advantages of data grids in important industrial sectors. It focuses on four application areas: automotive, aerospace, pharmaceutical industries and meteorology.

The SIMDAT project is managed by the Fraunhofer Institute for Algorithms and Scientific Computing (SCAI). It started on 1 September 2005 and will end on 31 October 2008.

DWD, Météo France, EUMETSAT and ECMWF join the SIMDAT project to work on the meteorological activity. Software developments and lead of the meteorological activity were assigned to ECMWF. The meteorological partners took SIMDAT as an opportunity to fund the developments of an European VGISC

The project soon gained some popularity amongst some other meteorological institutes worldwide distributed, and additional collaborators decided to join the prototype to follow closely the initiatives and progress done towards the implementation of a VGISC.

The software developed by the meteorological activity of SIMAT is called Virtual Meteorological Centre (VMC), in order to distinguish it from the other SIMDAT developments (e.g. automotive, aerospace ...). In the scope of this document the term "SIMDAT" refers to the outcomes of the meteorological activity of the EU project and it will be used interchangeably with the term "VMC".

The VMC software comprises of a series of components for building a distributed infrastructure that allows metadata publishing and synchronisation, integration of existing legacy data access systems and provides a front-end portal for discovering, accessing and delivering real-time and archived datasets in a secure and controlled environment.

The SIMDAT architecture has been modularised into three components:

Data Repository: Is the interface to data legacy systems. It represents a layer of abstraction between a particular data system and the rest of the SIMDAT infrastructure. This component also facilitates the publishing of metadata to the rest of the infrastructure.

Catalogue Node: Is the backbone of the SIMDAT infrastructure that provides a virtualisation layer between the different centres. Communication with the rest of the components is implemented through an XML-based message protocol. The catalogue node offers a variety of services such as metadata synchronisation cataloguing and indexing, peer-to-peer routing service, data request handling (subscriptions and ad-hoc requests) and authentication and authorisation services.

Portal: Is a web based user interface providing a front-end to some of the services implemented at the catalogue node such as discovery of datasets, login, dataset request (pull) and subscription, dataset shopping cart and download.

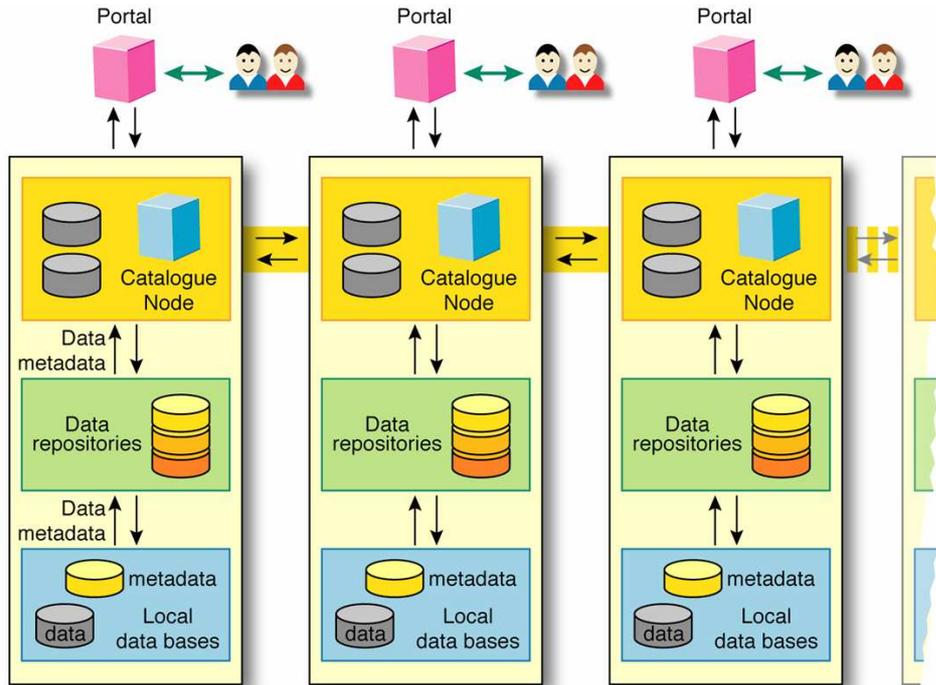


Figure 5.8 SIMDAT Architecture: Modular components

5.6.2 Status of the software

The VMC software will finish all developments by October 2008, end of the SIMDAT project. The software has been developed in several phases, with three major software releases during the lifetime of the SIMDAT project.

The VMC prototype provides connectivity among 11 meteorological centres distributed world-wide since 2007. The prototype is running continuously on a 24/7 basis.

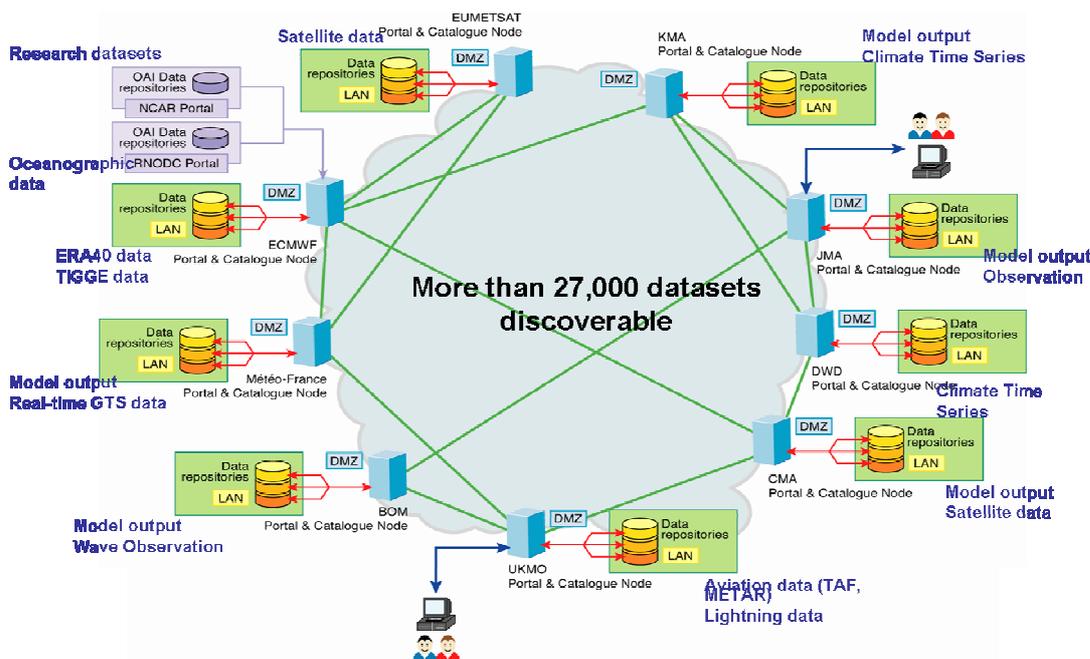


Figure 5.9 VMC prototype: Participating centres

The SIMDAT software has proven to be an effective way to demonstrate the complexity that a distributed infrastructure poses in every sense, from organisational to technical challenges. The software development philosophy has always been oriented towards a seamless integration with existing environments focusing on the transparency of distributed aspects.

5.6.3 Potential Use within VGISC

The SIMDAT software has implemented many of the requirements stated for the formulation of a VGISC.

The following features have characterised SIMDAT for its uniqueness and therefore reusability of the ideas, design or implementation is highly recommended.

- It is a fully decentralised system. All sites connected to the infrastructure are true peers and have equal rights. As a result, there is no single point of failure, and the system will continue to function when a site is down.
- The sites do not have to be fully interconnected. In order to join the infrastructure, a site needs only to connect to at least one other peer. This facilitates the addition of new partners and ensures that the infrastructure is scalable and can accommodate a large number of sites.
- Each site synchronises its catalogue with its peers. As a result, each site holds a copy of the catalogue of all data available throughout the system, providing very fast search and browsing facilities to the end user.
- The system provides a very simple way of interfacing with existing data repositories, such as relational databases or archive systems, without any impact on the local infrastructure or disruption of operational activities. This has been demonstrated by the ease with which new collaborators are joining the infrastructure and publishing their data.
- Through its virtual organisation, the system provides secure methods for the management of users and data policies in a distributed fashion, allowing a finely tuned access control, ranging from globally accessible data to data available by bilateral agreements.
- The system provides a transparent access to remote data. Once a user has discovered a dataset of interest using the web portal, it can be downloaded from the same portal, without having to contact the site which holds the data. Although totally distributed, this is a true *“one-stop-shop”* from each access point.
- The system supports asynchronous data retrieval. This is often necessary for data that is held offline, such as data from the MARS archive.

5.6.4 Current license status

The SIMDAT software is distributed and licensed for use under the terms of the Apache License, Version 2.0.

5.6.5 Contact Details

Baudouin Raoult
E C M W F
Shinfield Park
Reading
RG2 9AX
UNITED KINGDOM
Email:baudouin.raoult@ecmwf.int

5.7 GTS Modules contributed to SIMDAT: Metadata Creation

5.7.1 Description

Météo France is tasked in January 2006 to develop a SIMDAT acquisition module for Global Telecommunication System (GTS) products. The modules presented here are part of the third project based on specifications expressed in July 2007. The scope of the acquisition is limited to essential GTS bulletins declared to the WMO # 9 Volume C1 Reference Catalogue. The creation of a metadata record for every such bulletin is a preliminary requirement in order to discover the bulletin and retrieve its instances via the SIMDAT portal. The metadata generation is static - or rather regular – to reflect the content of the WMO catalogue, rather than dynamic, at the arrival of bulletin instances.

The identified template - metadata records given as illustrations for version 1.1 of the WMO Core Profile of the ISO 19115 standard – defines the metadata structure and determines the need for information. The study of the main information source: volume C1, as well as the study of other WMO references further refines this need. Considered references include WMO # 9 Volume A catalogue of observing stations, WMO # 386 Manual on the GTS, WMO # 306 Manual on Codes, etc.

The generation procedure adopts 3 general principles:

- provide as much or more information in the metadata record as in the catalogue declarations,
- enrich this information either by decrypting encoded fields or by connecting elements of information,
- improve the general homogeneity of the information.

Several elements contribute to implementing this philosophy. Notable is a set of loose interpretation rules derived from patterns observed in free-format text fields in volume C1. Also contributing are “(business model) information classes” constructed to meet the need for supplementary information: usable representations of WMO references, as well as all necessary association tables or decoding grids. As more than one centre may run the module, a “white-list” is introduced to deal the publishing responsibilities and avoid redundancies. The white-list and the information classes are intended to be centrally available in order to ensure homogeneity of the published records.

The system is developed in java 1.6.0.2 and runs as an independent module at the data repository level in the SIMDAT topology. WMO Volume C1, the “white-list” and “information classes” are downloaded from their respective sources at the start of the procedure. Created metadata records are deposited in a directory harvested by the SIMDAT Node. The impact of the module on the SIMDAT code is limited to a set of new translation tables to guide the Node into the metadata elements.

5.7.2 Status of the software

The software is under development – as of April 2007. Although metadata records intended for SIMDAT are already generated, the module’s potential use in the VGISC or more generally WIS context now prompts for more demanding metadata standards - in particular, compliance with the ISO 19115 norm and INSPIRE directive. In addition, the status depends on the validation of the general procedure, rules and business model classes by the appropriate WMO authorities.

5.7.3 Potential Use within VGISC

Global exchange of GTS essential bulletins is mandated among GISC nodes in the future WIS. Data publishers (National Centres, NC) have the responsibility to provide documentation for their products in the form of compliant metadata records. The module could serve this purpose at the NC level, or the responsibility could be delegated to the appropriate DCPCs, therefore becoming one functionality of the VGISC system.

5.7.4 Current license status

The license status is pending: it awaits completion of the developments and validation.

5.7.5 Contact Details

Jean-Pierre Aubagnac
Météo – France – DSI / DEV
42 avenue Coriolis,
31057 Toulouse
FRANCE
Email: jean-pierre.aubagnac@meteo.fr

5.8 GTS modules contributed to SIMDAT: ingestion / retrieve / feeding

5.8.1 Description

Météo France is tasked in January 2006 to develop a SIMDAT acquisition module for Global Telecommunication System (GTS) products. The modules presented here are part of the third project based on specifications expressed in July 2007. The metadata generation module is described independently. The project includes three additional functionalities:

- a GTS Ingester daemon,
- a SIMDAT GTS service for the retrieval,
- a MSS feeding daemon.

Replication of essential GTS products among peer nodes is not developed in SIMDAT and out of the scope of the Météo-France development. Simple interfaces to this future functionality were however imagined for the GTS modules.

GTS bulletin instances are collected into files according to the WMO FTP Protocol – Manual on the GTS - Attachment II.15. The files appear in one or several output channels of the local Message Switching Service (MSS). The GTS ingester daemon unpacks files upon arrival and filters bulletin instances by their header. The index of locally published metadata, produced during the metadata generation, determines the scope of the ingestion. Only instances with bulletin metadata listed in the index are stored in the data repository cache. The same instances are also packed with their credentials (unique bulletin identifier, ingestion and publication data repository/ies) into simple format files deposited in an “outgoing for replication” directory. The cache is regularly purged. Merging the local index with indexes produced in other centres results in extending the scope of the ingestion: a functionality which could contribute to a back-up strategy.

The SIMDAT GTS service extends the SIMDAT complex data repository data source and data retrieve services. The services are solicited by messages from the Node to check for the availability of new data and to retrieve specified products.

The MSS feeding daemon awaits the arrival of simple format files in an “incoming from replication” directory. Bulletin instances are unpacked from deposited files. Only instances absent from the local GTS cache are inserted in the cache. The same bulletin instances are also sorted by WMO code form, number and time according to WMO instructions, packed into WMO FTP Protocol files and proposed to the local MSS.

The GTS daemons are developed in java 1.6.0.2 and run in the background at the data repository level. The GTS data cache is implemented as a PostgreSQL relational database.

5.8.2 Status of the software

The software is under development – as of April 2007. The GTS retrieve service is under development, the GTS daemons are in the testing phase.

5.8.3 Potential Use within VGISC

The VGISC system must provide a fully specified interface with the existing MSS at the partner nodes to collect GTS products, and must also provide a strategy to maintain this collection of GTS products in the event of a failure of the MSS at one site. The modules are an approach to this interface for product collection and retrieval. The configurable index of ingested products could contribute to the back-up strategy.

5.8.4 Current license status

The license is pending and awaits completion.

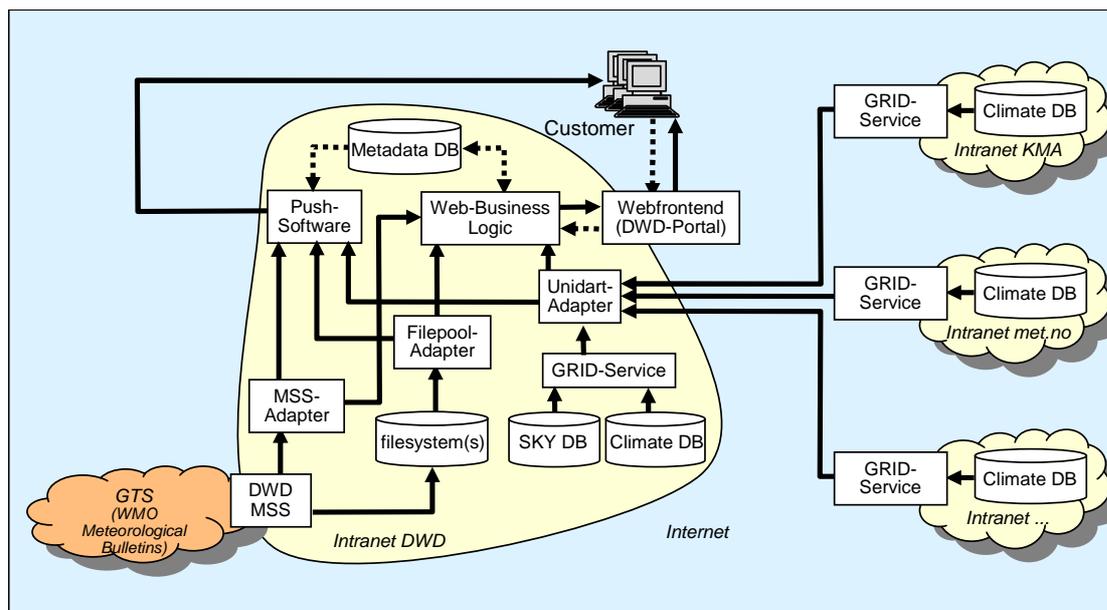
5.8.5 Contact Details

Jean-Pierre Aubagnac
Météo – France – DSI / DEV
42 avenue Coriolis,
31057 Toulouse
FRANCE
Email: jean-pierre.aubagnac@meteo.fr

5.9 WEBWERDIS

5.9.1 Description

Web Weather Request and Distribution System, WebWerdis, is a web-based self service distribution tool, developed by DWD. Universities / research facilities in Germany and the member of the UNITART project (<http://www.eumetnet.eu.org/>) use this tool for there own data supply (ad-hoc requests or subscription service).



WebWerdis is developed as scalability, modularity and SOA orientated system. The system consists of following components.

Webfrontend:

- different web-based user interface
- common web business components

Adapter (Filepool-, Unidart-, MSS-):

- Universal request/response interfaces between the distribution tool and the different data-sources as well as production tools/data-providers (local or remote);
- Interface to the push software and to the pull components of the webfrontend.

Metadata database:

- Container of product and product instance catalogues as well as the catalogues of customised information, like carts destinations and subscriptions;
- Container of the control information of the subscription tool, adapters and the webfrontend.

Subscription software:

Time or event triggered distribution of customised subscriptions (based on open-source software: AFD: <http://www.dwd.de/AFD> and quartz: <http://www.opensynphony.com/quartz>).

5.9.2 Status of the software

WebWerdis (subscription component)	in use since January 2007
AFD (Automatic File Distributor)	primary file distribution tool of the DWD, operationally since 1997

5.9.3 Potential Use within VGISC

The subscription component (including: WebWerdis subscription metadata model, WebWerdis adapters, scheduler and AFD) could be used within VGISC.

5.9.4 Current license status

WebWerdis (subscription component): open for evaluation during the VGISC ITT
 AFD (Automatic File Distributor): open-source (GPL – General Public License)

5.9.5 Contact Details

Subcomponent	Custodian
WebWerdis	Siegfried Fechner; DWD; Germany; D-63067 Offenbach, Kaiserlei 42; phone: +49 (69) 8062-2865; email:siegfried.fechner@dwd.de
WebWerdis data model, subscription metadata	Siegfried Fechner; DWD; Germany; D-63067 Offenbach, Kaiserlei 42; phone: +49 (69) 8062-2865; email:siegfried.fechner@dwd.de
Adapter	Alexander Maul; DWD; Germany; D-63067 Offenbach, Kaiserlei 42; phone: +49 (69) 8062-2571; email:alexander.maul@dwd.de
Scheduler	Rudolf Tröller; DWD; Germany; D-63067 Offenbach, Kaiserlei 42; phone: +49 (69) 8062-2570; email:rudolf.troeller@dwd.de
AFD (Automatic File Distributor)	Holger Kiehl; DWD; Germany; D-63067 Offenbach, Kaiserlei 42; phone: +49 (69) 8062-2562; email:holger.kiehl@dwd.de

5.10 Summary table: Potential Use of Software contributions within VGISC

	Functions	EFTS Agents	FIXMEX	GEMS/SMART	METAMOD	SIMDAT	GTS metadata generation	GTS ingestion retrieve feeding	Web Werdis
	WIS functions								
1	Uploading of Metadata for Data and Products	√			√	√	√		
2	Uploading of Data and Products	√			√			√	
3	Centralization of Globally Distributed Data								
4	Maintenance of User Identification and Role Information					√			
5	Consolidated View of Distributed Identification and Role Information					Implemented Trust Domains			
6	Authentication of a User					√			
7	Authorization of a User Role					√			
8	DAR Catalogue Search and Retrieval				√	√	√	√	√
9	Consolidated View of Distributed DAR Metadata Catalogues					√			√
10	Downloading Files via Dedicated Networks	√				√		√	√
11	Downloading Files via Non-dedicated Networks	√			√	√			√
12	Downloading Files via Other Methods	√				√			√
13	Maintenance of Dissemination Metadata					√			√
14	Consolidated View of Distributed Dissemination Metadata Catalogues					√			
15	Reporting of Quality of Service			√					
	Additional functions for VGISC								
16	Collect Observations, Create Products, and Archive Information						√	√	
17	Assign user role, Authorise access to information by users					√			
18	Maintain and Expose Catalogue of Services and Information					√	√		
19	Deliver Information to Users	√				√		√	√
20	Manage System Performance			√					
21	Web Interface (was Internet Portals (external, internal))		√		√	√			√

6 Test and Verification Procedures

6.1 Introduction

This section defines the high level requirements and objectives of the test and verification activities for the VGISC software, but NOT to provide the detailed test plans and the test cases.

6.2 Mission Statement

The major objective of VGISC software testing is to verify the system functions are implemented as specified, and the performance, reliability and security features of the software meet requirements.

Design Review, Prototype Review, System Test and User Acceptance Test are the necessary validation and verification phases in the development and delivery of the VGISC software.

- The Design Review and the Prototype Review are to determine the consistency of design with requirements, and the adequacy of design.
- The System Test is to validate the functions, performance, user interface and security of the VGISC software meet all specifications in the development environment before it delivered to the Users.
- The User Acceptance Test is to confirm the VGISC software is ready for operational use. It includes three phases which will focus on different features of the VGISC software. Phase I is the test at the Central Support Office (CSO) and should focus on the business functions and technical features. Phases II is the test at each partner site, and should focus on the external interface, security and backup/restore features. Phase III is the test at all partner sites in parallel, and should be focus on the failover and reliability features.

6.3 Test Conditions

The CSO and all the partner sites have to be fully involved in phased delivery and testing of the software system, and provide the resources and facilities for each test phase as required.

6.3.1 Test Bed

The Phase I of the User Acceptance Test will be done on the test bed at the CSO. The necessary test environment, including computer hardware, operating system, and network conditions shall be provided by the CSO.

Moreover, the test bed at the CSO should be kept available for supporting the necessary testing of each release version until the VGISC project closes.

6.3.2 Client Platform

The Phase II and III for the User Acceptance Test will be done on the client platforms at each partner site. The client platform, including computer hardware, operating system, and network conditions, shall be prepared by the partner sites before the test. The interfaces between the local systems and the VGISC system should be developed by each partner site and ready for testing before the UAT Phase II.

6.3.3 Test Data

The test data, including meteorological products, metadata (product metadata and DAR metadata), as well as some corrupt data and metadata, shall be provided by the CSO for the System Test and UAT Phase I, and by the partner sites for the UAT Phase II and III.

6.3.4 Personnel

The responsibility for reviewing the design and the prototype is with the partners, and the responsible persons have to be appointed.

The CSO must have enough personnel to execute the responsibilities of reviewing the test plans and test results for the System Test and all the User Acceptance Tests, performing the testing of the UAT Phase I, and providing necessary technical support to the partner sites in the UAT Phase II and III.

The local test team at each partner site must be setup for performing the testing of the UAT Phase II and III.

6.4 Test Requirements

The major functional and non-functional features for the VGISC software must be tested.

The detailed test plans and test cases for each test phase will be developed by the CSO in conjunction with the partners and possibly the vendor, according to the defined templates and requirements.

The test results and analysis should be reported by the vendor company at the end of each test phase.

6.4.1 Features To Be Tested

The features listed in the table below must be tested. All the sub-requirements expanded in each feature must be targeted by the corresponding test cases.

(The following table needs to be updated according to the VGISC technical requirements)

A. Functional area	
A1. Interoperable Interfaces	WIS-TechSpec-1 Uploading of Metadata for Data and Products
	A1-2 Uploading of Data and Products
	A1-3 Centralization of Globally Distributed Data
	A1-4 Maintenance of User Identification and Role Information
	A1-5 Consolidated View of Distributed Identification and Role Information
	A1-6 Authentication of an User
	A1-7 Authorization of an User Role
	A1-8 DAR Catalogue Search and Retrieval
	A1-9 Consolidated View of Distributed DAR Metadata Catalogues
	A1-10 Downloading Files via Dedicated Networks
	A1-11 Downloading Files via Non-dedicated Networks
	A1-12 Downloading Files via Other Methods
	A1-13 Maintenance of Dissemination Metadata
	A1-14 Consolidated View of Distributed Dissemination Metadata Catalogues
	A1-15 Reporting of Quality of Service
A2. Internal functions	A2-1 Collect Observations, Create Products, and Archive Information
	A2-2 Assign user role, Authorize access to information by users
	A2-3 Maintain and Expose Catalogue of Services and Information
	A2-4 Deliver Information to Users
	A2-5 Manage System Performance
	A2-6 Web Interface (was Internet Portals (external, internal))
A3. External Interfaces	A3-1 Interfaces with the local systems at each partner site Notes: the behavior of the local systems are out of the VGISC scope
B. Non-functional area	
B1. Performance	The required performance refers to the section Performance Requirements in the chapter Manage System Performance.
B2. Security	The required security refers to the section Security Requirements in the chapter Authenticate and Authorize Users.

6.4.2 Test Plans

The detailed test plan for the System Test and each UAT phase will be developed by the CSO and the applicable partner(s) before each test. The following items are necessary in developing the test plan for each test phase.

- Knowledge of the application architecture, business functions supported by the system.
- All software features and combinations of software features to be tested. The test design specifications associated with each feature and each combination of features must be identified and documented.
- All features and specific combinations of features that will not be tested along with the reasons.
- The following focus areas should be included for each test phase:
 - a) Test Data Initialization

- b) Process Flows
- c) Interface File(s)
- The sequence of test runs, tool requirements, expected results, and test verification method must be identified.
- Both the necessary and desired properties of the testing environment, including the computer hardware, communication links and network, operating system, support software and testing tools, as well as the testing environment security requirements needed to complete testing activities, must be identified and documented.
- All key personnel associated with the application must be identified and documented.
- All sign-off procedures must be documented.
- The risks and assumptions associated with testing tasks must be identified. The table below provides examples. A similar table should be filled out and kept up based on the actual scenarios that develop before and during each portion or phase of VGISC testing.

Risk #	Risk or Issue	Probability	Impact	Mitigation Actions
1	The SIT applications cannot be tested within the dictated timeframe.	High	Med	Prioritize the testing; extend the timeframe
2	The defects are not resolved within the dictated timeframe	Med	Med-Low	Detail every known potential problem; evaluate work arounds
3	Key personnel are not available during test timeframe	Med	High-Med	Ensure others are trained as backups; ensure key personnel execute most difficult testing prior to departing.
4	Access to the facility due to the holiday timeframe is limited	Med	Med	
5	All the SIT Applications are not tested	High	Med	Prioritize testing and make concerted effort to complete on time.

6.4.3 Test Cases

Each test listed in the detailed test plans should have a test case. The test cases will be developed by the CSO and applicable partner(s) before each UAT test phase. The template and requirements for developing a test case are given as follows. There should be at least one test case for each of the use cases given in this ITT.

Test Case Name			
<i>Assign an unique name for this test case</i>			
Test Case ID	<i>Assign an unique identifier for this test case</i>	Created By	
Component	<i>Identify the software component to be exercised by this test case</i>	Creation Date	
		Modified By	Marta Gutierrez
		Modified Date	
Requirements Covered			
<i>Describe the functional or non-functional requirements covered by this test case</i>			
<i>Identify references to the relevant item documentation (requirements specification, design specification)</i>			
Purpose of test			
<i>Describe the purpose for running this test case</i>			
Precondition			
<i>Identify the necessary environment and input required to run this test case</i>			
Test Steps			
<i>(Describe the method and procedure to run this test case, and the expected results for each step)</i>			
Description			
Expected Results			
1			

<p>2</p> <p>...</p>
<p>Results <i>(Report the results for running this test case)</i></p>
<p>Date Run Tester Results</p> <p>1 <i>Date for running this test case</i> <i>Name of the test player</i> <i>Actual results of running this test case</i></p>

6.4.4 Test Reporting

At the end of each test phase, a Test Report should be presented to certify that all test cases necessary to test objectives were successfully completed and giving the total number of outstanding problems and the severity assigned to each. The following status should be contained in the report.

- Number of test cases planned
- Number of test cases successfully completed
- Number of test cases that could not be executed (with reasons, why)
- Test results showing
 - Functions working
 - Functions not working
- Conclusions
- Issues outstanding, if any
- Recommendations
- Action plan

6.5 Design Review

The Design Review is to ensure that the software design meets the functional requirements. The CSO and the responsible persons nominated by the partner sites are responsible for making the review of the design specification and the detailed design developed by the vender company.

6.6 Prototype Review

The prototype version of the VGISC software is required to contain all major functions. The Prototype Review is to ensure the system functional and technical solution for the VGISC software meets the requirements. The CSO and the responsible persons nominated are responsible for reviewing the prototype delivered by the vender company.

6.7 System Test

The System Test is an integrated factory test to validate the functions, performance, user interface and security of the VGISC software in the development environment before it is delivered to the User Acceptance Test.

6.7.1 Test Strategies

The following test strategies are mandatory for the System Test.

- 1) IT Verification
 - **Automated Testing:** Verify codes by using testing tools.
 - *play test case*
 - *testing the main functions, checking the technical logs, checking the software keep on running in the good way without checking the results of the functions*
- 2) Functional Validation
 - a) **Business Function Testing:** Verify that the business functions operate according to the detailed requirements, the external and internal design specifications. The functional features included in the section 4.1 must be tested. All the sub-requirements expanded in each feature must be targeted by the corresponding test cases.
 - b) **User Interface Testing:** Verify that the user interface meets the functional requirements, is easy to use and friendly. The interface features included in section 4.1 must be tested. All the sub-requirements expanded in each feature must be targeted by the corresponding test cases.
- 3) Performance Validation
 - a) **Performance Testing:** Verify that the application meets the expected level of performance in a production-like environment. The performance features included in section 4.1 must be tested. All the sub-requirements expanded in each feature must be targeted by the corresponding test cases.
- 4) Security Validation
 - a) **Security Testing:** Verify that the application provides an adequate level of protection for confidential information and data belonging to other systems. The integrity of the software's security controls, the audit ability of the software's security mechanism and the security of distributed data should be tested. The security features included in section 4.1 must be tested. All the sub-requirements expanded in each feature must be targeted by the corresponding test cases.

6.7.2 Entrance and Exit Criteria

Entrance Criteria	Exit Criteria
<ul style="list-style-type: none"> Detailed Test Plan documented Test cases documented Test process defined Test criteria defined Unit testing and Integration testing completed Unit test report and Integration test report reviewed by the CSO 	<ul style="list-style-type: none"> Outstanding defects within quality target. Test assets catalogued and stored Test report reviewed by the VGISC Project Office.

6.7.3 Estimated Test Duration

The detailed test duration for the System Test could be planned by the vender company. But, the test actives must be done, and the test report must be reviewed by the VGISC Project Office before the VGSIC software is delivered to the User Acceptance.

6.8 Test at the CSO (UAT Phase I)

The test at the CSO is the first phase for the User Acceptance Test to verify that the software meets the specified requirements, including functional and non-functional requirements, and is ready for operational use. The testing will be done on the test bed at the CSO.

6.8.1 Test Strategies

The following test strategies are requested for the UAT Phase I.

- 1) IT verification
 - **Automated Testing** □ Verify codes by using testing tools.
 - *play test case*
 - *testing the main functions, checking the technical logs, checking the software keep on running in the good way without checking the results of the functions*
- 2) Functional validation
 - **System Integration Testing:** Verify that each application executes properly within the integrated VGISC software. It is not verified that all applications can execute simultaneously. Until all the SIT applications are fully tested, it is not prudent to proceed to the interoperability testing. The term “fully tested” incorporates the following activities within the testing group as provided in the table below.

	Tester	Test Cases	Test Files	Installed and Test run	Test Scripts	Results Approved	Cycle 1 Test Date
Application 1	Jane Doe	100	100	100	100	100	10/28/2008
Application 2	John Q. Public	100	100	50	0	100	
Application 3	Alex Whoever	100	100	100	50	100	
.....							

- Interoperability Testing:** This testing will verify all applications can run together in the integrated VGISC software in a harmonious manner. The test activities should start with those applications which are tested at that time with the rest added in a controlled fashion, until all applications are being exercised simultaneously, using canned data feeds as deemed appropriate by the test team and test cases. The order of module insertion should be determined. The tests shall accommodate multiple instances of each module as appropriate, and include error conditions testing. After that, a “fully loaded” operability test, which exercises the software with all applications running simultaneously with live data, should be conducted for at least 24 hours. The example test component tables are as follows.

Functional Flows

FLAWS	NAME
VGISC Functional Flow 1	
VGISC Functional Flow 2	
VGISC Functional Flow 3	
VGISC Log Functions	
VGISC Ad Hoc Request/Reply	
VGISC Error handler	

Database Table

TABLES	NAME
switching_dir	Needs to be refreshed from production
process	Needs to be refreshed from production
metadata	Needs to be refreshed from production
error_table	Needs to be refreshed from production
bulletin	Needs to be truncated prior to test start
report	Needs to be truncated prior to test start

Applications

Build-Only / Application	Name

Special Cases

Special Cases / Applications	NAME

VGISC Infrastructure

Components	NAME
Database	
Middleware	
Front-End Processor	
Application	
Operating Systems (Linux, Windows)	
Monitoring	

3) Performance validation

- **Load/Stress Testing:** Exercise the software using live data for a period of at least 24 hours. Utilizing an Input Generator, increase the data flow rate into the software incrementally up to 5 times the normally expected flows. The test evaluates the ability of the software to operate at peak performance for an extended period of time. It tests the effect of simultaneous multiple accesses to an application by loading up the inputs and monitoring the effect on that application. This test will test the VGISC software using data volumes and transaction rates in excess of those expected in order to demonstrate the software will accommodate growth. It will also identify weaknesses that could cause failure during peak loading. Only real-life scenarios should be considered and will include error conditions commonly seen by users on the legacy system.

6.8.2 Entrance and Exit Criteria

Entrance Criteria	Exit Criteria
<ul style="list-style-type: none"> • Detailed Test Plan documented • Test cases documented • Test process defined • Test criteria defined • System testing completed • System test report reviewed by the CSO 	<ul style="list-style-type: none"> • Outstanding defects within quality target. • Test assets catalogued and stored • The test at the CSO signed off by the VGISC Project Office and the vender company.

6.8.3 Estimated Test Duration

The estimated test time for the UAT Phase I is 5 days.

6.9 Test at each partner site (UAT Phase II)

The test at each partner site is the second phase for the User Acceptance Test to verify the external interface, security and backup/restore features for the VGISC software. It will be implemented on each partner site separately.

6.9.1 Test Strategies

The following test strategies are requested for the Reliability Acceptance Test.

- 1) **Localization Testing:** Exercise the software using live data feeds at each partner site to verify the interfaces between the VGISC software and the local systems. Only real-life scenarios should be considered and will include error conditions commonly seen by users on the legacy system.
- 2) **Security Testing:** Verify that the application provides an adequate level of protection for confidential information and data belonging to other systems. The integrity of the software's security controls, the audit ability of the software's security mechanism and the security of distributed data should be tested.
- 3) **Backup/Restore Testing:** Verify the backup procedures and restore processes for products and metadata meet the defined requirements at each partner site internally.

6.9.2 Entrance and Exit Criteria

Entrance Criteria	Exit Criteria
<ul style="list-style-type: none"> • Detailed Test Plan documented • Test cases documented • Test process defined 	<ul style="list-style-type: none"> • Outstanding defects within quality target. • Test assets catalogued and stored • UAT Phase II signed off by the VGISC

<ul style="list-style-type: none"> • Test criteria defined • UAT Phase I completed 	Project Office and the vender company.
--	--

6.9.3 Estimated Test Duration

The estimated test time for the UAT Phase II is 5 days.

6.10 Test at all partner sites in parallel (UAT Phase III)

The third phase for the User Acceptance Test is to verify the interoperability and reliability for the VGISC software. It will be implemented on all partner sites, and include a 30 day continuous operating test carried out on all partners at the same time.

6.10.1 Test Strategies

- 1) **Failover Testing:** Simulate failure of hardware, software, and power to evaluate impact on and restoration capability of the VGISC software. It evaluates the ability to recover from errors after simulated hardware, software, network (routers, servers, hubs, cable) failures in order to measure the effectiveness of the contingency processes and capabilities. Only real-life scenarios should be considered and will include error conditions commonly seen by users on the legacy system.
- 2) **Reliability Testing:** Exercise the software using live data feeds from each partner site at the same time. The test evaluates the performance and ability of the software to run at each partner site by operating non-stop for 30 days of testing (pending decision by management). It is to verify that the software has the capability to function properly under lifelike conditions required by business owners to meet response times, transaction rates, and resource use typically encountered during “normal” operational scenarios. It is suggested the partner sites have real users participate in this testing in order to provide a more realistic test scenario. Only real-life scenarios should be considered and will include error conditions commonly seen by users on the legacy system.

6.10.2 Entrance and Exit Criteria

Entrance Criteria	Exit Criteria
<ul style="list-style-type: none"> • Detailed Test Plan documented • Test cases documented • Test process defined • Test criteria defined • UAT Phase II completed 	<ul style="list-style-type: none"> • Outstanding defects within quality target. • Test assets catalogued and stored • UAT Phase III signed off by the VGISC Project Office and the vender company.

6.10.3 Estimated Test Duration

The estimated test time for the UAT Phase III is 30 days.

6.11 Testing for release version

A new release for the VGISC software should be tested on the test bed to validate that reported defects are fixed and that any updated and/or expanded features work correctly before it is delivered to the partner sites. The vender company should provide the corresponding test cases together with the new release. The CSO is responsible for performing the testing activities on the test bed.

As for the release version with minor changes, e.g. from the version 3.2 to 3.3, the test cases can focus only on the changes. But for the major release changes, e.g. from the version 3.7 to 4.0, the test cases should also cover the compatibility and interoperability with the previous version in addition to any changes.

7 Maintenance and Training

7.1 Definition

It is now best practice to refer to system and software maintenance as part of a set of larger scale processes called Release Management.

Any mandatory requirements will depend solely on the decision on how the supplier develops and delivers the solution.

Assume that Quality Assurance will be managed mainly by the supplier otherwise detailing the requirements and constraints is too complex.

Release Management expected deliverables when taking delivery of release components:

- Release Note
- Installer packages/components
- Testing evidence
- Installation and Back-out Guide to include validation checking tasks
- Support Guide(s)
- User Guide(s)

These would all need to be Quality Assured by the relevant Consortium members through Release Management conformity checking processes.

7.2 General Requirements

Unless stated otherwise, it is assumed these requirements apply to optional components as well as core.

- REQ-7.01 All documentation **MUST** be provided in English.
- REQ-7.02 It is **DESIRABLE** that documentation also be provided in French and German.
- REQ-7.03 The vendor **MUST** specify their Release Management processes.
- REQ-7.04 The vendor **MUST** conform to local change management processes.
- REQ-7.05 The vendor **MUST** specify the expected local testing environment (if special localisation actions are contracted by a partner).
- REQ-7.06 It is **DESIRABLE** that the vendor supply maintenance and change schedules at least one year in advance.
- REQ-7.07 The vendor **MUST** specify their Configuration Processes and Release policies (e.g. packaged binary release or source code release require on-site builds).
- REQ-7.08 The vendor **MUST** specify their support policies for:
- a. Support levels, with response times,
 - b. Reporting procedures,
 - c. Escalation procedures.

8 Standards

This section contains references to the appropriate versions of documents for all official standards referenced throughout the VGISC ITT document.

- [OGC CSW] OpenGIS Catalogue Services Specification, version 2.0.2, ISO Metadata Application Profile, is available at http://portal.opengeospatial.org/files/?artifact_id=21460
- [ISO 15000] ISO 15000-3:2004 Part 3: Registry information model specification (ebRIM) is available at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39974
- [ISO 23950] SRU (Search/Retrieval via URL) profile of ISO 23950 is available at <http://www.loc.gov/standards/sru/>
- [ISO 19115] ISO 19115:2003/Cor 1:2006 ISO 19115 Geographic information -- Metadata is available at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44361
- [ISO 19115-2] ISO/DIS 19115-2 Geographic information -- Metadata -- Part 2: Extensions for imagery and gridded data is available at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39229
- [ISO 19119] ISO 19119:2005/Amd 1:2008 ISO 19119 Geographic information -- Services is available at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44268
- [ISO 19139] ISO/TS 19139:2007 ISO 19139 Geographic information -- Metadata -- XML is available at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=32557

Appendix A - Glossary of Terms

Access	Access to services, functionality or data within WIS.
Actions	Controlling actions performed automatically or by authorised operators or users.
Ad hoc request	A request that does not require the system oversight expected for a subscription or other managed request
Ad-hoc delivery	Delivery of a specific set of data or products, on a one-off basis.
Asynchronous delivery	Delivery that does not block local processing from continuing.
Authentication	A process for verification of the identity of a user
Authorisation	A process for controlling user activities within a system to only actions defined as appropriate based on the user's role
Broadcast	A type of telecommunications wherein clients only receive on a one-way connection and sessions are initiated by the host server.
Catastrophic Failure	A situation triggered by an event with the consequence that the WIS system is not able to perform the services it should.
Certificate	Digital identity certificate or public key certificate used to identify users and institutions. Within WIS it is used to enable Trust Relationships.
Client-server	A type of telecommunications wherein a server is always listening for a client to initiate a session and the clients do some processing while servers do most of the processing.
Code List	A controlled and extendable vocabulary.
Communications-centric	Focused primarily on managing communications aspects of a system.
Continuity of Operations	When experiencing a Catastrophic Failure the WIS system should be restored and able to continue its normal service level within a specified time window.
Credentials	Information that is used to determine what a user should be able to do within the system.
Data-centric	Focused primarily on managing the data aspects of a system.
Discovery, Access and Retrieval metadata	Catalogue records describing available data and products and how these may be retrieved.
Dissemination metadata	Records describing the schedule and the means by which data and products are to be delivered to subscribers.
Essential	Data / Products intended for global exchange, as defined by Annex 1 to Resolution 40 (CG-XII) or Resolution 25 (CG-XIII) (Ref. 4).
Events	Something happening at a specific time and that can enable an action.
File transfer	A telecommunications procedure wherein a file is sent directly to its destination in one session.
Instance	The individual occurrence of a defined class of items, such as data, metadata, product or service
Interacting parties	E.g. WIS centres communicating or WIS User and WIS Centres communicating.
Interoperability	The ability to perform a task that spans discrete system components implemented with information and communications technology.
Interoperable interface	A connection between system components that is designed to enable operation with components developed separately.
Intersystem	Internal to the WIS system.
Level of trust	An agreement with a defined scope to cover two or more parties.

Logically centralized but physically distributed catalogue	Each GISC has a physical instance of a DAR Metadata Catalogue of WIS. Multiple methods can be envisioned for the implementation of a logically centralised view of this catalogue.
Machine Service Interface	Interfaces that enables computers to communicate without human intervention.
Metadata	Records containing various characteristics associated with a data or product or service.
Network-centric orientation	Interfaces are seen as active points of contact on networks, where structured messages are communicated between distinct system components.
Node	A component of the VGISC, rather than a GISC.
Non-synchronous metadata	That part of the catalogue that does not have to be synchronized with other catalogues
Pack	Insert information into a bulletin or file according to respective metadata.
Peer-to-peer	A type of telecommunications wherein both ends must listen and either can initiate a session, and processing responsibilities can be fully distributed.
Product instance	The individual occurrence of a defined class of products
Publish-subscribe	A telecommunications procedure wherein a publishing host delivers information directly or provides a cue used by subscribers to fetch the information.
Pull	The receiver initiates the transmission, and the transmitter provides data to the receiver only as it is read.
Push	The transmitter initiates the transmission, and continuously notifies the receiver whenever new data is available.
Real-time	Provision of information quickly enough to enable reaction during a given process.
Registry	A controlled catalogue with restricted access and limited exposure
Request-response	A telecommunications procedure wherein a session may have multiple dialogues consisting of requests answered by responses.
Role	The Role of a WIS User determines the services/functionality that specific User is able to access.
Routine delivery	Delivery of a specific set of data or products, on a regular basis.
Service level	The common understanding between a provider and a user concerning measurable attributes of the service provided, such as availability, performance, etc.
Service Oriented Architecture	A discipline for building software systems, derived from distributed computing and modular programming techniques, and focused on defining the interfaces between communicating software components that provide distinct functions.
Single Sign On	Users are authenticated only once and can after that gain access to the services of the distributed system.
Spatial bounding box	A geographically specified rectangle containing the location of an item of interest.
Store-and-forward	A telecommunications procedure wherein a file is sent to an intermediate destination and then forwarded to the final destination.
Synchronized metadata	Records of parts of a catalogue that have been synchronized, whether synchronous or not.
Synchronous delivery	Delivery that blocks local processing until the transfer is complete.
Synchronous metadata	That part of a catalogue that must be synchronized with other catalogues, whether actually synchronized or not.
Terminal-host	A type of telecommunications wherein a terminal is always

	connected to the host computer and the host computer performs almost all of the processing.
Transactions	Communication between WIS Centres or a WIS Centre and a User in order to perform a certain action.
Trust Relationship	Specification of how and who the WIS creates trust. A trust relationship is a necessary requirement for Single Sign On to work.
Trusted Remote Centre	WIS centre that has a Trust Relationship with another WIS centre.
Unpack	Extract information from a bulletin or file.
Use Case	Description of how a goal is achieved through interactions between external actors and particular parts of the system being designed.
User	A user of the WIS system. This can e.g. be an administrator of the system or a scientist looking for data.
User Credentials	The privileges of a user, i.e. information that is used to determine what a user should be able to do within the system.
User Identifiable Information	Information that can be related to a specific person.
WIS Centre	WMO Information Centre, i.e. one of National Centre (NC), Data Collection or Production Centre (DCPC), Global Information System centres (GISC). (See Appendix C, Ref.1 – Ref.3 for details).
X-Include	XML include, defines the ability for XML files to include all or part of an external file.
X-Link	XML linking language, an XML mark-up language used for creating hyperlinks in XML documents.
Zthes	An abstract model for representing and searching thesauri, or other types of vocabulary.

Appendix B - Abbreviations

BUFR	Binary Universal Form for the Representation of meteorological data
Cg	World Meteorological Congress
CBS	Commission for Basic Systems
CSO	Central Support Office
CSW	Web Catalogue Service
DAR	Discovery, Access and Retrieval
DCPC	Data Collection or Production Centre
DMZ	Network “demilitarized zones”
ebRIM	e-business Registry Information Model
ECMWF	European Centre for Medium Range Weather Forecasts
EUMETSAT	European Organisation for the Exploitation of Meteorological Satellites
FTP	File Transfer Protocol
FTP WMO	File Transfer Protocol, using WMO format file contents
GDPFS	Global Data Processing and Forecast System
GEO	Group on Earth Observation
GEOS	Global Earth Observations System of Systems
GISC	Global Information System Centre
GOS	Global Observing Systems
GRIB	Gridded Binary
GTS	Global Telecommunication System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
ICAO	International Civil Aviation Organisation
ICG-WIS	Inter-Commission Coordination Group on WMO Information System
IGDDS	Integrated Global Data Distribution System
IMTN	Improved Main Telecommunication Network
IPv4	Internet Protocol version 4 (using 32-bit addresses)
IPv6	Internet Protocol version 6 (using 128-bit addresses)
ISO	International Organization for Standardization
ISS	Information Systems and Services (Division of World Weather Watch)
ITT	Invitation To Tender
MSS	Message Switching System
MTN	Main Telecommunication Network
NC	National Centre
NetCDF	Network Common Data Form
NMC	National Meteorological Centre
NMHS	National Meteorological and Hydrological Service
OAI-PMH	Open Archives Initiative Protocol for Metadata Harvesting
OGC	Open Geospatial Consortium
OpeNDAP	Open-source Project for a Network Data Access Protocol
PDF	Portable Document Format
PDP	Policy Decision Point
PEP	Policy Enforcement Point
QoS	Quality of Service
RMDCN	Regional Meteorological Data Communication Network
RM-ODP	Reference Model for Open Distributed Processing (ISO/IEC 10746)
RTH	Regional Telecommunication Hub
SDI	Spatial Data Infrastructure
SFTP	Secure File Transfer Protocol

SIT	System Integration Testing
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol / Internet Protocol
UAT	User Acceptance Test
UC	Use Case
UDDI	Universal Description, Discovery and Integration
URI	Uniform Resource Identifier
URN	Uniform Resource Name
VGISC	Virtual Global Information System Centre
VO	Virtual Organisation
VPN	Virtual Private Network
WIGOS	WMO Integrated Global Observation Systems
WIS	WMO Information System
WMC	World Meteorological Centre
WMO	World Meteorological Organization
WWW	World Weather Watch (Department of World Weather Watch)
XHTML	Extensible Hypertext Mark-up Language
XML	Extendable Mark-up Language

Appendix C - References

- Ref.1: WMO Information System Compliance Specifications of GIS, DCPC, and NC;
Version 1.0, 14 Dec 2007
- Ref.2: WMO Information System (WIS) User Requirements; Draft, Version 0.3, 14 Dec 2007
- Ref.3: Project and Implementation Plan: WMO Information System; Draft, Version 0.6, 17 Dec 2007
- Ref.4: Cg-XII, Geneva, 30 May-21 June 1995
- Ref.5: Organisation Concept of an Operational VGISC; Version 1.0, 20 Nov 2007
- Ref.6: National Weather Service: MS3 Test Strategy and Master Test Plan, Version 1.6
- Ref.7: ITT Drafting Group: Technical requirements
- Ref.8. Meteoalarm usage statistics
<http://www.euroforecaster.org/latenews/meteoalarm.pdf> ,
http://www.alexandria.com/data/details/traffic_details/meteoalarm.eu

Appendix D – Special Clarifications

D.1. General

1. VGISC/GISC/DCPC/NC/ role clarification

Concerning national users a range of solutions is possible, such as the German users of the VGISC system using a German node and similarly for France and UK. Or, one VGISC node could take turns at being the definitive node for all users, with re-direction. Or there is one URL as suggested. However, one of the fundamental principles of WIS is that users can choose where to connect to the system given addresses are known.

Details must be clarified during the dialogue phase.

2. Management of trusted users

User databases will not be central. User management will be performed at the individual sites. The trust relationship should determine what are the security levels between the members that agree to the relationship.

3. Correlation between actors and rules

The actors of the use cases don't necessarily need to be the same as the user roles. User roles were identified and provided as examples of the variety of "policies implementations (or roles)" that the system will be dealing with. An actor of the use cases defined in APPENDIX E might hold one or more of the user roles defined in APPENDIX D.

4. Clarification on data/metadata/products

Data/products managed by the VGISC-cache are not historical (real-time with well-known time of residence). Other data/product (e.g. offered by DCPCs, including DCPC functionality of MF, UK Met Office and DWD VGISC nodes) can be historical.

The important point is that the VGISC system must accommodate all types of data and data of any granularity.

In the GTS context, to be more specific, data usually refers to observations, whereas product refers to forecasts and warnings. Instances are defined in Appendix A as individual occurrences of defined classes of data or products.

see Ref 2 "WMO Information System (WIS) User Requirements; Draft Version 0.3, 14 Dec 2007", priority of the communities (Ref 2, chapter 3) could be discussed during the dialogue. There is no definitive list of available data. It is the intent of WIS, and this procurement, to enable the development of such a list.

"Essential data" is a subset of the "global data". Definitions of 'Essential' will change and will be different for different communities.

The data/metadata rates are mentioned in REQ 3.152.

5. Description of VGISC cache

Specification of a VGISC-cache:

- container of data/products with well-known time of residence,
- typical examples of data/products are meteorological bulletins being transmitted for global exchange between GISC-nodes,
- ad-hoc requests and pushed distributions of those data/products are served from the VGISC-cache,
- VGISC-cache/VGISC-data pool will be filled automatically with routine data/products,
- aged data/products are automatically deleted after the time of residence,

- content of the caches are synchronized/replicated among VGISC nodes.

Product metadata are part of the product catalogue and remain in the catalogue after the product instances are deleted from the Cache.

Metadata for product instances, if they exist, evolve with the content of the Cache and disappear from the catalogue when the instances are deleted. Details and management of the product instance metadata will be further clarified during the dialogue phase.

See also R.-G. Hoffman: TD01 - VGISC Presentation - Industry Day.pdf "WMO Information System and VGISC";

D.2. Metadata issues

1. The WIS concept distinguishes between products and product instances. This distinction is similar to the differentiation between classes and objects in object-oriented programming. A product defines the abstract characteristics of a meteorological data set. The granularity of a product is user-dependant. For example, a product can specify a single GRIB file or all GRIB files of all model runs during the last 12 months. A product instance is an instantiation of the according product. It is a real data set, e.g. a meteorological bulletin, a set of GRIB files or a subset of a climate time series.
2. ISO-compliant metadata descriptions are only required for products and not for product instances.
3. Whether metadata of product instances will be stored in the DAR catalogue is a decision of system design.
4. XLinks are mostly used in metadata descriptions for the reference of entries in catalogues. The validation of such XLinks means that it should be tested whether the referenced entry really exists. The VGISC system can use local copies of these catalogues for validation in order to avoid performance and reliability problems.
5. Metadata should be freely available. There should be no restrictions on the access to metadata descriptions because this could make the handling of metadata very complicated. If there is metadata information which should be hidden from a group of unauthorised users, then this information should not be put into the metadata description.
6. A product can be associated with a service. The service will accept requests in order to generate an instance of the product. For example, there could be a product that describes the daily mean air temperature values of all German stations. A service may now exist, which will be able to query the subset of values for a given set of stations during a given period of time.
7. Services, which are related to a product, are described with ISO-19119.

D.3. Security Aspects within VGISC

1. Within the VGISC: A VGISC node, an Internal DCPC and Internal NC must be able to establish a Trust Relationship.
2. User Confidentiality must be kept, so centres would be responsible for their own users and therefore user private data is kept distributed. This will include credentials also.

3. For the cases where back up scenarios are requested, synchronisation of user data (roles and credentials) should be done with acknowledgment of the user or via configuration for high-availability users (e.g. an administrator). Credentials are - private user data- , so default synchronisation would break confidentiality.

Distinction between users:

- b. General Purpose Users: e.g. Researches, asking for archive data.
 - c. Expert /High availability Users: An administrator, users subscribed to real time data.
4. Within the Trust relationship it is foreseen that the same understanding of roles would benefit scalability issues within the VGISC. Having to map organisational roles across n organisations would not scale in a large deployment.
 5. Within the Trust relationship remote data access/subscription must be allowed: e.g. Internal DCPC publish metadata (global and other) to the VGISC node.
 - a. For the cases where metadata describing global data is requested, then the data will also be retrievable at the VGISC node (local access).
 - b. For the cases where metadata describes “other data”, then the data will be extracted from its original location at the DCPC-int (remote access) and delivered to the user without having to login twice (SSO).
 6. External DCPC -not part of the Trust Relationship- will also be able to publish metadata (global and other) to a VGISC node.
 - a. For the cases where metadata describing global data is requested, then the data will also be retrievable at the VGISC node (local access).
 - b. For the cases where metadata describes “other data”, then the user will be advertised the location of the data e.g. via url. User will need to go to the location advertised and login again via authenticating method of the external DCPC. No SSO will apply in this case and user will need to register with the external DCPC.

D.4. Security Aspects outside VGISC

Access to other GISCs from the VGISC will imply a bilateral agreement where the conditions of access will be prescribed. Global data, metadata is synchronised across GISCS and therefore available to the respective GISCS users. Where other data of interest not available a given GISC-A is discovered at a different GISC-B, then dedicated agreements would be necessary as to how GISC-B makes available the data to GISC-A.

As of today there is no technical solution for Inter-GISC communication, so if a solution is reached for the communication between the VGISC centres, then possibility of scaling up the same solution to Inter-GISC communication would be of great benefit.

D.5. Performance numbers

New numbers will be expressed in the next iteration of the ITT to reflect on a give node:

Authenticated users
Number of hits per second

Appendix E - User Roles

This appendix lists the examples of the required roles, as identified within each technical function. The roles required by VGISC may include, but are not restricted to, the following roles:

E.1 Collect Observations, Create Products and Archive Information

Providers of data:

- VGISC node data provider (includes DCPC and MSS at NCs)
- WIS (external to VGISC) data provider
- MSS (external to VGISC) data provider
- WMO program data provider
- External data provider

Providers of metadata:

- WIS centre DAR metadata provider
- VGISC node DAR metadata provider
- WMO program DAR metadata provider
- External DAR metadata provider
- Authorised dissemination metadata providers
- Authorised service metadata providers.

Builders of DAR metadata

- GTS Reference Information provider (e.g. WMO Volume C1)
- WMO Reference Information provider
- External Reference Information provider

Administration roles:

- Administrator (superuser, function specific)
- Remote Administrators

E.2 Manage System Performance

Administration roles:

- VGISC local system administrator
- VGISC local 24x7 operations team
- VGISC remote system administrator
- VGISC remote 24x7 operations team

E.3 Maintain and Expose Catalogue of Services and Information

- Anonymous (read only access to non restricted metadata)
- VGISC metadata editor (create or modify metadata on behalf of the owner of the data or products and create or modify dissemination/delivery metadata)
- VGISC metadata quality assurance (quality assurance of created or modified metadata)
- VGISC metadata administrator (managing of all metadata activities of the VGISC system)

E.4 Deliver Information to Users

- VGISC delivery operator (monitoring of all subscription activities of a VGISC-node)

- VGISC delivery administrator (managing of all subscription delivery activities of a VGISC-node)

E.5 Web Interface

Data providers:

- VGISC node (including DCPC, MSS),
- WIS,
- MSS,
- WMO Programme,
- External.

Metadata Providers:

- WIS DAR,
- VGISC node DAR,
- WMO Programme DAR,
- External DAR,
- Authorised dissemination,
- Authorised Service.

Reference information:

- GTS
- WMO
- External

User roles:

- Various Sys admin,
- remote admin

Appendix F - Detailed Description of Use Cases

F.1 GISC Use Cases

Use Case GISC 1, Provide Metadata for Data or Product

Use Case Goal	Metadata for any data or product file to be available from the GISC is created or updated in the DAR Metadata Catalogue of the GISC
Actors	Metadata Originator (NC or DCPC) Metadata Catalogue Publisher (GISC)
Pre-Conditions	(1) The Metadata Originator is authorized to update the DAR Metadata Catalogue for the associated file(s) (2) The Metadata Originator has the necessary information and the ability to update the DAR Metadata Catalogue for the associated file(s) (3) The Metadata Catalogue Publisher supports facilities for authorized Metadata Originators to update the metadata for the associated file(s)
Post-Conditions	The DAR Metadata Catalogue has changes made by the Metadata Originator
Normal Flow	The authorized Metadata Originator uses a facility supported by the Metadata Catalogue Publisher to update the DAR Metadata Catalogue for the associated file. Typically, two kinds of maintenance facilities are supported. One is a file upload facility for "batch" updating (add, replace, or delete metadata records treated as separate files). The other is an online form for changing metadata records treated as entries in the DAR Metadata Catalogue (add, change, or delete of elements in a record as well as whole records). The Metadata Catalogue Publisher maintains the updated DAR Metadata Catalogue as a searchable resource offered to all authorized searchers (see Use Case B.6). The Metadata Catalogue Publisher also shares the metadata as a part of the logically centralized but physically distributed catalogue across WIS centres.
Notes and Issues	This set of actions is a simple extrapolation from existing GTS practice, adding the particular standard format for WIS metadata.
Last Updated	22 Feb 2008
Last Updated By	Eliot Christian

Use Case GIS C 2, Upload Data or Product to GIS C

Use Case Goal	Data or product is sent as a file to a GIS C
Actors	Data Sender (NC or DCPC) Data Receiver (GIS C)
Pre-Conditions	(1) Appropriate metadata to be associated with the file is already available in the DAR Metadata Catalogue of the GIS C (2) The Data Sender is authorized to send the file to the Data Receiver (3) The Data Receiver supports a method for uploading the file, which the Data Sender is able to use
Post-Conditions	The data or product uploaded by the Data Sender is received and stored by the Data Receiver.
Normal Flow	The Data Sender uses his authorized access to send the file using an appropriate transmission method supported by the Data Receiver. Typically, the transmission is accomplished using GTS or a file transfer method available over the Internet. A file naming convention or other agreed mechanism is used to make an association between the file and its metadata.
Notes and Issues	This set of actions builds on existing GTS practice, supplemented with other file transfer mechanisms such as the Internet.
Last Updated	22 Feb 2008
Last Updated By	Eliot Christian

Use Case GIS C 3, Control Metadata Association to Data or Product

Use Case Goal	Confirm that metadata for a data or product file at the GIS C already exists in the DAR Metadata Catalogue before the data or product is available
Actors	Data Sender (NC or DCPC) Data Receiver (GIS C)
Pre-Conditions	(1) Data or product has been sent as a file from a Data Sender (2) DAR Metadata Catalogue is current with all updates
Post-Conditions	An error is communicated when there is not confirmation that a given file is associated appropriately with metadata in the DAR Metadata Catalogue
Normal Flow	On receipt of a file containing a data or product, the Data Receiver checks the current DAR Metadata Catalogue to confirm that the file has an associated metadata record. If such a record is not found within two minutes after receipt of the file, an error message is sent to the Data Sender.
Notes and Issues	This control action addresses the condition wherein data arrives before its associated metadata. Rather than rejecting the file immediately, a grace period of two minutes is allowed before the data file is regarded as erroneous.
Last Updated	22 Feb 2008
Last Updated By	Eliot Christian

Use Case GISC 4, Manage Cache of Data across GISCs

Use Case Goal	GISCs manage a logically centralized collection containing at least a 24 hour cache of data and products agreed by WMO for routine global exchange
Actors	Data Administrators at each of the GISCs
Pre-Conditions	(1) At each GISC, the cache of data and products received from NCs and DCPCs in its area of responsibility is current (2) Transmission and control mechanisms across GISCs are available (3) All Data Administrators are authenticated and authorized as needed
Post-Conditions	The cache of data and products is accessible as a logically centralized collection that includes current data and products at each GISC
Normal Flow	A Data Administrator monitors the transmission methods and control mechanisms that enable a logically centralised view of the physically distributed cache of data and products. Depending on the methods in place, a Data Administrator takes various corrective actions whenever the cache is not available as required.
Notes and Issues	At this point in WIS system design, it has not been decided how the GISCs will accomplish centralization of the cache.
Last Updated	22 Feb 2008
Last Updated By	Eliot Christian

Use Case GISC 5, Maintain Identification and Role Information for WIS Users

Use Case Goal	Internal and external users of WIS are able to be identified as needed for their authentication, and their role information is maintained as needed for their authorizations to perform specific functions
Actors	Users of WIS (internal and external) Administrators of authentication and authorization at GISCs
Pre-Conditions	(1) Administrators have agreed authentication policies delineating the credentials required to establish identity of a WIS user (2) Administrators have agreed authorization policies delineating which roles are authorized to perform each WIS action (3) Administrators have mechanisms to create and maintain identification information needed for authentication of users of WIS (4) Administrators have mechanisms to create and maintain role information needed for authorization of authenticated users of WIS
Post-Conditions	WIS Centres collectively have the ability to authenticate each user of WIS and authorize him to perform all of the functions appropriate to his role, and only those functions appropriate to his role
Normal Flow	Identification and role information about candidate or current users of WIS are to be recorded through facilities controlled by WIS Centres. Typically, two kinds of facilities should be supported. One is a file upload facility for "batch" updating (add, replace, or delete the identification and role records as separate files). The other is an online form for changing identification and role records (add, change, or delete elements in a record as well as whole records). Administrators of authentication and authorization at WIS Centres share the updated identification and role information as a resource available as needed across WIS Centres.
Notes and Issues	At this point in WIS system design, mechanisms have not been decided for handling identification and role information as needed across WIS centres.
Last Updated	22 Feb 2008
Last Updated By	Eliot Christian

Use Case GISC 6, Discover Data or Products

Use Case Goal	A user of WIS finds available WMO data or products that he wants to receive.
Actors	Data Searcher
Pre-Conditions	(1) The DAR Metadata Catalogue is accessible for browsing or searching (2) The GISC infrastructure provides a unified catalogue view to the user (i.e., the catalogue is logically centralized although physically distributed)
Post-Conditions	The Data Searcher has information needed to select relevant data or products.
Normal Flow	The Data Searcher discovers available WMO data and products by browsing the DAR Metadata Catalogue or by searching the DAR Metadata Catalogue using discovery concepts such as subject keywords, geographic extent, and temporal range. As a result of his browsing or searching, the Data Searcher gets a relevance-ordered list of data and products including "data or product metadata" such as data origin, data type, generation date, availability, and use constraints, among other characteristics.
Notes and Issues	At this point in WIS system design, multiple methods can be envisioned for logically centralizing the physically distributed DAR Metadata Catalogue.
Last Updated	22 Feb 2008
Last Updated By	Eliot Christian

Use Case GISC 7, Ad Hoc Request for Data or Product ("Pull")

Use Case Goal	A user of WIS requests WMO data or product on an ad hoc basis
Actors	User of WIS GISC
Pre-Conditions	(1) The desired data or product has been identified by the user of WIS (2) The user of WIS has been authenticated and authorized to retrieve the desired data or product from the GISC (3) Delivery is achievable through one of the supported mechanisms for the transmission of the desired data or product, and within the published service level commitment of the GISC
Post-Conditions	Data or product is readied for delivery to the user of WIS according to the service level commitment of the GISC
Normal Flow	Once the user has identified the desired data or product, he requests delivery on a one-time basis. The GISC authenticates the user and checks authorization for delivery of the product according to the user's role. The GISC then sets up delivery through any of a broad range of online and offline options.
Last Updated	22 Feb 2008
Last Updated By	Eliot Christian

Use Case GISC 8, Subscribe to Data or Product ("Push")

Use Case Goal	A user of WIS can subscribe to receive data or products on a recurring basis
Actors	User of WIS GISC
Pre-Conditions	(1) The desired data or product has been identified by the user of WIS (2) The user of WIS has been authenticated and authorized to retrieve the desired data or product from the GISC (3) Delivery is achievable through one of the supported mechanisms for the transmission of the desired data or product, and within the published service level commitment of the GISC
Post-Conditions	Data or product is readied for delivery to the user of WIS according to the service level commitment of the GISC
Normal Flow	Once the user has identified the desired data or product, he requests to subscribe to receive the data or products on a recurring basis. The GISC authenticates the user, checks authorization for delivery of the product according to the user's role. The GISC then sets up delivery through any of a broad range of online and offline options. As necessary, the GISC updates the Dissemination Metadata associated with the subscription.
Last Updated	22 Feb 2008
Last Updated By	Eliot Christian

Use Case GISC 9, Download Data or Product from GISC

Use Case Goal	A user of WIS receives from a GISC, on an ad hoc or subscription basis, data or products transmitted as files
Actors	User of WIS GISC
Pre-Conditions	(1) Data or product is ready for delivery to the authenticated and authorized user, as requested through one of the supported transmission mechanisms and according to the service level commitment of the GISC (2) For subscription delivery, the GISC has access to subscription information in the Dissemination Metadata Catalogue
Post-Conditions	Selected data or products are received by the user of WIS
Normal Flow	The GISC sends files containing the requested data or products, using an appropriate transmission method as indicated in the associated subscription information accessible through the Dissemination Metadata Catalogue. Typically, the transmission is accomplished using GTS or a file transfer method available over the Internet, such as HTTP, OpeNDAP, FTP, SFTP, GFTP, email, etc). In any case, transmission must be efficient and reliable (checksum and error recovery mechanisms are required at minimum).
Last Updated	22 Feb 2008
Last Updated By	Eliot Christian

Use Case GIS 10, Provide Dissemination Metadata

Use Case Goal	Metadata concerning delivery specifics of subscription(s) to data and products from a GIS are created or updated in the Dissemination Metadata Catalogue
Actors	Subscription Registrar (NC or DCPC) Dissemination Catalogue Publisher (GIS)
Pre-Conditions	(1) The Subscription Registrar is authorized to update the Dissemination Metadata Catalogue for the given subscription(s) (2) The Subscription Registrar has the necessary information and the ability to update the Dissemination Metadata Catalogue for the given subscription(s) (3) The Dissemination Catalogue Publisher supports facilities for authorized Subscription Registrars to update the metadata for the given subscription(s)
Post-Conditions	The Dissemination Metadata Catalogue has changes made by the Subscription Registrar
Normal Flow	The authorized Subscription Registrar uses a facility supported by the Dissemination Metadata Catalogue Publisher to update the Dissemination Metadata Catalogue for the given subscription(s). Typically, two kinds of maintenance facilities are supported. One is a file upload facility for "batch" updating (add, replace, or delete metadata records treated as separate files). The other is an online form for changing metadata records treated as entries in the Dissemination Metadata Catalogue (add, change, or delete of elements in a record as well as whole records). The Dissemination Metadata Catalogue Publisher maintains the updated Dissemination Metadata Catalogue as a reference resource accessible as part of a logically centralized but physically distributed catalogue across GISs.
Notes and Issues	At this point in WIS system design, it is has yet to be defined how each Dissemination Metadata Catalogue Publisher will communicate changes to each physically distributed part of the logically centralized Dissemination Metadata Catalogue.
Last Updated	22 Feb 2008
Last Updated By	Eliot Christian

Use Case GISC 11, Report Quality of Service across GISCs

Use Case Goal	Managers of GISCs receive performance reports of operations against agreed quality of service indicators
Actors	GISC Managers
Pre-Conditions	(1) Measurable quality of service indicators are agreed (2) Schedule of reporting and specifics of reporting formats are agreed
Post-Conditions	GISC managers have performance information needed to manage WIS operations across the range of GISC services
Normal Flow	On a schedule as mutually agreed, all GISC managers send performance reports of operations against agreed quality of service indicators.
Notes and Issues	It can be anticipated that WIS will eventually have agreements that address quality of service requirements. These should include data and network security as well as performance and reliability. Such agreements might be formalized into WIS standards, and perhaps Technical Specifications. Or, a looser set of conventions may simply document the variety of service level expectations reported across communities of WIS end-users. Although not yet addressed in WIS system design, performance reports can be generated efficiently by having each GISC upload its reports to a single analysis site within a fixed time window.
Last Updated	22 Feb 2008
Last Updated By	Eliot Christian

Use Case GISC 12, GTS metadata generation from WMO Volume C1 reference

<p>Use Case Goal</p>	<p>A GISC system uses the WMO # 9 Volume C1 operational catalogue to build DAR metadata records for essential GTS data or products:</p> <ul style="list-style-type: none"> • Asynchronously before ingesting the GTS data flow, • To reflect the current state of the catalogue, • Using a set of shared resources termed “Information Classes” built and maintained to meet the need for information, • Using a mechanism to deal the metadata publishing responsibilities among actors without gaps nor overlaps. <p>The metadata records are made available for the update of the DAR metadata catalogue.</p>
<p>Actors</p>	<p>WMO Data Source provider, Supplementary Information Provider (“Information Classes”, controlled vocabulary, distribution of the publishing responsibilities), Metadata Generator (GISC)</p>
<p>Pre-Conditions</p>	<p>A shared set of resources (termed “Information Classes”) are constructed and maintained to provide the information needed to populate the metadata elements in the GTS metadata records.</p> <p>Their purpose is to expand the information contained in Volume C1 declarations. Typically by decoding cryptic fields (e.g. TTAAii designator, ICAO or WMO station indexes, etc) and by connecting separate elements of information.</p> <p>They are of many types: representations of available WMO references (e.g. WMO # 9 Volume A, sections of the WMO # 306 Manual on Codes or of the WMO # 386 Manual on the GTS, etc), information collected from sparse WMO sources or information created for the purpose (e.g. meeting the need to sort and classify data or products).</p> <p>A variety of processes are involved in their construction, ranging from dynamic generation to manual collection.</p>
<p>Post-Conditions</p>	<p>DAR GTS metadata records are made available for the update of the DAR Metadata Catalogue.</p>
<p>Normal Flow</p>	<p>The Metadata Generator regularly re-generates metadata records for GTS bulletins under its responsibility to reflect changes to the Volume C1 catalogue, changes to the maintained Information Classes or to the distribution of publishing responsibilities.</p> <p>The procedure first obtains the up-to-date input elements from the WMO Data Source Provider (current Volume C1) and from the Supplementary Information Provider (all additional elements). All elements serve to initialise in memory the association tables or style sheets needed by the procedure.</p> <p>A GTS DAR metadata record is created for an entry in Volume C1 only:</p> <ul style="list-style-type: none"> • If the bulletin is determined as essential, • If the bulletin falls under the publishing responsibility of the Metadata Generator. <p>Distributing the responsibility among Metadata Generators may be achieved by designing a set of simple filters :</p> <ul style="list-style-type: none"> • Each filter determines the scope of the generation for each actor, • The list of filters is comprehensive and avoids redundancies: each given essential bulletin declared in Volume C1 exactly matches one of the filter: its

	<p>metadata record is published by exactly one actor.</p> <ul style="list-style-type: none"> • Regular expressions on the bulletin abbreviated header line AHL are a simple yet effective implementation of these filters. • In particular, regular expressions only imposing conditions on the collecting / compiling CCCC centre included in the bulletin AHL header are an easy solution to define a national or inter-national area of responsibility.
Notes and Issues	<p>(1) Changes in the distribution of the Metadata Generation responsibility will introduce overlaps or gaps in the generated populations until all actors have re-generated the metadata under their responsibility.</p> <p>Synchronisation of these generations could therefore be envisaged.</p> <p>(2) The creation of metadata records for data or products is the responsibility of the data or product producer (NC or DCPC), but could be delegated in the case of GTS products to the GIS (or VGISC node).</p> <p>(3) A central repository for supplementary information elements – e.g. at the Central Support Office – will facilitate the maintenance of these resources, and ensure homogeneity in content of the metadata records generated at distinct Centres.</p>
Last Updated	15 July 2008
Last Updated By	Duncan Jeffery

F.2 VGISC Use Cases

Use Case VGISC 1, Provide DAR Metadata for Data or Product

SIMDAT Use Case Reference	D18.1.1 UC2.2
SIMDAT VGISC View Reference	3.2.2.1 VGISC metadata feed
Use Case GISC Reference	Use Case GISC 1
Use Case Goal	<p>A provider of data or products (like a DCPC) can send or update DAR metadata records to indicate the availability of new datasets or reflect changes to hosted datasets. In both cases, the VGISC catalogue is locally updated and the update is forwarded to the other VGISC nodes in order to maintain the unique catalogue view.</p> <p>The DAR metadata record can be obtained in four ways:</p> <ul style="list-style-type: none"> • uploaded / received from the data or product provider, • built from reference information (see Use Case VGISC 12), • manually created by the data or product provider using a Web interface, • built on the fly (no currently identified Use Case). <p>The VGISC system includes a mechanism to update the catalogue.</p> <p>A synchronization mechanism is needed to update the catalogue of the other VGISC nodes.</p>
Actors	<p>DAR Metadata Originator (NC or DCPC) DAR Metadata Catalogue Provider/Publisher (VGISC)</p>
Pre-Conditions	<p>(1) The DAR Metadata Originator is authenticated and authorised to provide metadata record(s) for the update of the DAR metadata catalogue.</p> <p>(2) The DAR Metadata Originator has the necessary information to build the new metadata records and the ability to provide those records to the DAR metadata catalogue Provider/Publisher.</p> <p>(3) The Metadata Catalogue Provider/Publisher supports a mechanism to upload or receive DAR metadata records from authorized Metadata Originators.</p> <p>(4) The Metadata Catalogue Provider/Publisher provides additional mechanisms for the creation of DAR metadata records: from references, on the fly at the receipt of data or product, via a manual web based interface.</p> <p>(5) The VGISC provides a synchronization mechanism to offer a unique consolidated view of catalogue to the user.</p>
Post-Conditions	<p>The DAR Metadata Catalogue reflects the changes initiated by the Metadata Originator.</p>
Normal Flow	<p>Authenticated and authorised actors (external, internal DCPCs or NCs) regularly provide new DAR metadata records or update existing records to reflect changes to their datasets. The system updates the metadata catalogue accordingly.</p> <p>The VGISC may also possibly play the role of DAR Metadata Originator (e.g.; GTS metadata generated from WMO references).</p> <p>The authorized Metadata Originator uses a mechanism offered by the Metadata Catalogue Provider/Publisher to update the DAR Metadata Catalogue. Are supported in particular:</p> <ul style="list-style-type: none"> • A file upload facility for „batch“ updating (adds, replace, or delete metadata

	<p>records treated as separate files).</p> <ul style="list-style-type: none"> An online form for changing metadata records treated as entries in the DAR Metadata Catalogue (add, change, or delete of elements in a record as well as whole records).
Notes and Issues	<p>The GISC and VGISC issues are very close.</p> <p>The creation of DAR metadata records for data or products is the responsibility of the data or product producer (NC or DCPC), but could be delegated to the VGISC (or GISC) node. This can be envisaged in particular for the creation of GTS metadata records.</p>
Last Updated	11 July 2008
Last Updated By	Jacques Roumilhac & Jean-Pierre Aubagnac

Use Case VGISC 2, Upload Data or Product to VGISC

SIMDAT Use Case Reference	D18.1.1 UC2.1
Use Case GISC Reference	Use Case GISC 2
SIMDAT VGISC View Reference	3.2.2.1 VGISC real-time data feed
Use Case Goal	<p>The VGISC node receives real-time data or product from the NC and DCPC under its area of responsibility and from other GISC or VGISC nodes via:</p> <ul style="list-style-type: none"> the ingestion of GTS bulletins or files (from the local MSS), the replication of essential data or products (from other GISC or VGISC nodes), possibly a file transfer method available over the internet from remote NC or DCPC. <p>The VGISC verifies the identity and privileges of the actor before updating its databases. Essential data is stored for at least 24 hours.</p>
Actors	<p>Data Sender (MSS at local NC or DCPC, others GISC or VGISC nodes, other NC and DCPC)</p> <p>Data Receiver (VGISC)</p>
Pre-Conditions	<p>(1) A DAR metadata record associated to the data or product is already available in the VGISC DAR Metadata Catalogue.</p> <p>(2) The Data Sender is authorized to send data or products to the Data Receiver.</p> <p>(3) The Data Receiver supports a mechanism for uploading data or product files. The Data Sender is authorized to use it.</p> <p>(4) The main traffic links are in place and operational: GTS link with the local MSS, replication and file transfer</p>
Post-Conditions	<p>The data or product uploaded by the Data Sender is received and stored by the Data Receiver. New datasets are accessible through the VGISC.</p>
Normal Flow	<p>Data and product are made available to the VGISC node according to one of the following methods:</p> <ul style="list-style-type: none"> via the GTS link (Ingestion Use Case VGISC 15, Mandatory), via the replication mechanism between GISC or VGISC nodes (Replication Use Case VGISC 14, Mandatory), via a supported file transfer method available over the Internet or dedicated links (Optional). <p>A mechanism exists (e.g. file naming convention) to associate the data or product files with their metadata.</p>
Notes and Issues	<p>Received data or products are temporarily stored (24 hour minimum depth) at the VGISC node in a dedicated database termed Cache or Data Pool.</p> <p>VGISC nodes may exchange products other than essential with other nodes, according to bilateral or multilateral agreements.</p>
Last Updated	11 July 2008
Last Updated By	Jacques Roumilhac & Jean-Pierre Aubagnac

Use Case VGISC 3, Control Metadata Association to Data or Product

Use Case GISC Reference	Use Case GISC 3
Use Case Goal	<p>Confirm that metadata for a data or product file proposed to a VGISC node already exists in the DAR Metadata Catalogue before the data or product is accepted.</p> <p>The VGISC node verifies the association before replication.</p>
Actors	<p>Data Sender (MSS at local NC or DCPC, others nodes, others NC and DCPC)</p> <p>Data Receiver (VGISC)</p>
Pre-Conditions	<p>(1) The main traffic links are in place and operational: GTS link with the local MSS (GTS Ingestion Use Case VGISC 15), replication mechanism between GISC or VGISC Nodes (Replication Use Case VGISC 14), standard file transfer methods over the internet or dedicated links.</p> <p>(2) A data or product has been made available to the VGISC Node by a Data Sender.</p> <p>(3) The catalogue of DAR metadata is up-to-date.</p>
Post-Conditions	<p>(1) Data or product files with a matching DAR metadata record in the catalogue are accepted (for insertion in the local Data Pool).</p> <p>(2) Global exchange data or products are proposed to the replication mechanism.</p> <p>(3) Files without associated DAR metadata record are handled so as not to lose the contained data or product and a monitoring alert is triggered.</p>
Normal Flow	<p>A file naming convention or another agreed mechanism is used to make the association between the data or product file and its DAR metadata. The association may be straight forward or product specific, and therefore require a preliminary identification of the data or product type.</p> <p>On receipt of a file containing a data or product, the VGISC node checks if an associated metadata record exists in the current DAR Metadata.</p> <p>If such is the case, the data / product is inserted in the Data Pool. Data or products intended for global exchange are proposed for replication.</p> <p>If the association is impossible, the data or the product is handled according to a predefined strategy and not automatically lost, and a monitoring alert is fired. A 2 minute grace period is offered to allow for the late transmission of the associated metadata records. This tolerance is for instance interesting in the case of data and metadata transmitted as file pairs as allowed by the WMO FTP protocol.</p>
Notes and Issues	<p>The failure of the consultation of the DAR metadata catalogue must not prevent the processing of data or product, a possible issue in the case of time-critical or operation critical products. The implementation of the product to DAR metadata association must therefore avoid a complete dependence on the DAR Catalogue consultation functionality.</p>
Last Updated	11 July 2008
Last Updated By	Jacques Roumillhac & Jean-Pierre Aubagnac

Use Case VGISC 4, Manage Cache of Data across VGISC nodes

Use Case GISC Reference	Use Case GISC 4
Use Case Goal	<p>The VGISC nodes store a synchronous collection (or Cache or Pool) of data or products.</p> <p>The Cache contains at least the essential data and product available in the last 24 hours. Essential data and products are agreed by WMO for routine global exchange.</p>
Actors	VGISC nodes, VGISC administrators
Pre-Conditions	<p>(1) The system accommodates a global data policy.</p> <p>(2) All the parameters of the replication mechanism are set and configurable by the authorised administrator, including:</p> <ul style="list-style-type: none"> • the list of essential data or product to be replicated, possibly built and maintained up-to-date by extracting information from the DAR metadata records as they are made available or modified, • the list of all the different points of storage (data repositories) for replicated data or products. <p>(3) A mechanism is available to distinguish the original copy of each data or product exchanged globally among GISC or VGISC nodes from other copies.</p> <p>(4) Transmission and control mechanisms across VGISC nodes are available.</p> <p>The data transfer must be efficient and reliable (checksum and error recovery mechanism are available). Several transport mechanisms are possible (HTTP, OpenDap, FTP, SFTP, GFTP etc).</p>
Post-Conditions	<p>A global view of the synchronization of the different Caches is provided to the VGISC administrator.</p> <p>A monitoring alert is triggered if the replication process is interrupted.</p>
Normal Flow	<p>The GTS link is the main source of data or products bound for replication among GISC or VGISC Nodes. The scope of the GTS ingestion (Use Case VGISC 15) includes or is limited to GTS data or products labelled as essential by WMO.</p> <p>Data or products coming from others sources can also be replicated.</p> <p>The replication mechanism (Use Case VGISC 14) is in continuous operation: newly proposed data or products are taken into account, all the while continuing the replication process for data or products not yet synchronous among Caches. An interface is available to the authorized administrator to configure and monitor the process.</p>
Notes and Issues	<p>The replication mechanism must avoid infinite loops.</p> <p>The source data repository for a data or product may differ from the repository documented in the associated DAR metadata in the event of a backup of the data collection function.</p> <p>Local requests for replicated data or products may either be processed locally (local copy retrieved from the local Data Pool), or at the source data repository: where it was inserted into the VGISC system.</p>
Last Updated	16 July 2008
Last Updated By	Jacques Roumilhac & Jean-Pierre Aubagnac

Use Case VGISC 5, Maintain Identification and Role Information for VGISC Users

SIMDAT Use Case Reference	D18.1.1 UC6 D18.1.1 UC3.3
Use Case GISC Reference	Use Case GISC 5
Use Case Goal	<p>VGISC Users need to be identified by the system in order to have access to services, data and metadata, including:</p> <ul style="list-style-type: none"> • retrieval or subscription to data or products, • provision of data / metadata to the VGISC system, • management of the Virtual Organization, • management of the different functionalities of the VGISC system, • monitoring & control of the different functionalities of the VGISC system. <p>Identification is a three-step process decomposed as: registration, authentication and authorization.</p> <p>Authorized administrators (registration officer) can register and un-register users, as well as update their profile. The profile of a user includes the elements needed for the user authentication, as well as the definition or scope of the user authorizations. The authorization of a user to perform some of the system functionalities is set according to one of the predefined models or roles published in the register of roles. A given role yields access to an ensemble of datasets according to one or several data policies.</p>
Actors	All kinds of users, and in particular administrators of authentication and authorization at VGISC nodes.
Pre-Conditions	<p>(1) Agreed authentication policies list the credentials required to establish the identity of a VGISC user.</p> <p>(2) Agreed authorization policies determine the VGISC actions authorized for every published user role including:</p> <ul style="list-style-type: none"> ○ (end-)user roles, ○ administrator roles, ○ provider (of data and metadata) roles. <p>(3) The system offers mechanisms to configure the identification information needed to authenticate a VGISC user.</p> <p>(4) The system offers mechanisms to create and update the role information needed to authorize an authenticated VGISC user.</p> <p>(5) The user and role information is shared and synchronized amongst the different nodes (design provided by the bidder)</p>
Post-Conditions	VGISC nodes collectively have the capability to authenticate each user of VGISC and authorize him/her to perform all of the functions appropriate to his role, but only the functions appropriate to his role.
Normal Flow	<p>The VGISC node belongs to the VGISC domain of trust and all roles are known to all nodes.</p> <p>The identification process follows:</p> <ul style="list-style-type: none"> • authentication at the registering node based on credentials / certificates, • authorization at the registering node according to the published roles,

	<ul style="list-style-type: none"> • authorisation valid at all nodes in the trust domain. <p>An authorized administrator has access to an interface to propose modifications to the definitions of the user roles.</p> <p>A (local) authorized administrator has access to an interface to register / un-register users under his / her responsibility, as well as to update their profile.</p> <p>The two responsibilities are dissociated.</p>
Notes and Issues	The bidder will propose a design to solve all open questions
Last Updated	11 July 2008
Last Updated By	Jacques Roumilhac & Jean-Pierre Aubagnac

Use Case VGISC 6, Discover Data or Products

SIMDAT Use Case Reference	D18.1.1 UC1.1
Requirement Package Reference	Maintain and Expose Catalogue of Services and Information
Use Case GISC Reference	Use Case GISC 6
Use Case Goal	<p>A user needs to be able to connect to the system to discover the available datasets.</p> <p>Discovery is either done by browsing the catalogue or by submitting a single search or iterative searches.</p> <p>In all cases, the system returns a list of relevant datasets documented with information such as the data origin, location, type, creation date, availability, data policy, etc...</p>
Actors	All kinds of users, including anonymous users
Pre-Conditions	<p>(1) The catalogue is accessible to all and the discovery can be done by all.</p> <p>(2) The VGISC infrastructure provides a unified view of the catalogue to the user. Each node has a copy of the catalogue and a mechanism exists to synchronize the copies between nodes.</p>
Post-Conditions	The data receiver has obtained the necessary information to select the datasets relevant to his / her search.
Normal Flow	<p>The user discovers available WMO data and products by</p> <ul style="list-style-type: none"> • browsing the DAR Metadata Catalogue, • searching the DAR Metadata Catalogue using discovery concepts such as subject keywords, geographic extent, and temporal range. <p>As a result, the user obtains a relevance-ordered list of data and products including "data or product metadata" such as data origin, data type, generation date, availability, and use constraints, among other characteristics.</p>
Notes and Issues	
Last Updated	11 July 2008
Last Updated By	Jacques Roumilhac & Jean-Pierre Aubagnac

Use Case VGISC 7, Ad Hoc Request for Data or Product ("Pull")

SIMDAT Use Case Reference	D18.1.1 UC1.2 D18.1.1 UC1.4
Use Case GISC Reference	Use Case GISC 7
Use Case Goal	<p>A user can retrieve datasets by formulating a request. The request can either be direct or determined by successive refinements of the data or product search. The VGISC catalogue offers a global view of the data that the VGISC can serve.</p> <p>The requested data or product has one of the two following types:</p> <ul style="list-style-type: none"> • Data distributed among the VGISC nodes: the VGISC acts as the Data Provider for this type and sends the local copy of the data or product to the Data Receiver. • Data hosted by a DCPC only: the DCPC acts as a Data provider and sends the data or product to the Data receiver. <p>In both cases, mechanisms are available to efficiently transport the data from the VGISC to the users and between VGISC nodes if necessary.</p> <p>Quality of service mechanisms like request cost estimation and queuing mechanisms are used to always provide the same level of service for all the users.</p>
Actors	All kinds of users
Pre-Conditions	<p>(1) The catalogue is accessible to all and the discovery can be done by all</p> <p>(2) The catalogue provides a global view of the data available from the VGISC. All VGISC nodes have a copy of the catalogue and a mechanism exists to synchronize the copies between nodes.</p> <p>(3) The desired data or product has been identified by the user</p> <p>(4) The user must be authenticated and authorized in order to retrieve non public data.</p>
Post-Conditions	The Data or product is made ready for delivery to the Data Receiver. The Data Receiver is informed of the status of the request.
Normal Flow	<p>Once the user has identified the desired data or product, he / she may request delivery on a one-time basis. The user has been authenticated within the VGISC Node or at a trusted centre. The VGISC checks if the user is authorized for retrieval of the product according to the user's role.</p> <p>The requested data is located by the system. It may either be available locally or at a trusted centre. It may be readily available or may need to be extracted from one of the meteorological database. The data is made available to one of the VGISC nodes and ready for delivery to the Data Receiver through a broad range of online and offline options..</p> <p>The data transfer must be efficient and reliable (checksum and error recovery mechanism are available). The user can select a transport method among several possible mechanisms (HTTP, OpenDap, FTP, SFTP, GFTP, email, etc).</p>
Notes and Issues	Large volume data or offline data may require asynchronous download.
Last Updated	27 June 2008
Last Updated By	Jacques Roumilhac & Jean-Pierre Aubagnac

Use Case VGISC 8, Subscribe to Data or Product ("Push")

SIMDAT Use Case Reference	D18.1.1 UC1.3 D18.1.1 UC1.4
Use Case GISC Reference	Use Case GISC 8
Use Case Goal	<p>A user can subscribe to datasets to receive them on a recurring basis. Different subscription policies are defined such as:</p> <ul style="list-style-type: none"> • deliver products as they become available, • deliver only when a determined number of products is available, etc... <p>The user can apply to any predefined subscription and dissemination policies and manage its subscription details. Different data transports are available for selection (FTP, SFTP, HTTP, GFTP, etc)</p>
Actors	All kinds of users
Pre-Conditions	<p>(1) The user must be authenticated and authorized to subscribe to non public data and manage its subscription information,</p> <p>(2) The desired data or product has been identified by the user of the VGISC,</p> <p>(3) The system provides mechanisms to define & manage subscription policies,</p> <p>(4) The system provides mechanisms to efficiently transport data between the VGISC nodes.</p>
Post-Conditions	<p>The subscription request is sent to the Subscription Registrar for (validation and) registration of the associated Dissemination Metadata record in the Dissemination Metadata Catalogue.</p> <p>The user receives an acknowledgement of the current status of his / her subscription(s).</p>
Normal Flow	<p>Once the desired data or product is identified, the user may request to subscribe to receive the data or products on a recurring basis. The VGISC node authenticates the user and checks authorization for delivery of the product according to the user's role. A Subscription Registrar is involved in (possibly automatically) registering the subscription and updating the associated Dissemination Metadata and Dissemination Metadata Catalogue.</p>
Notes and Issues	
Last Updated	11 July 2008
Last Updated By	Jacques Roumilhac & Jean-Pierre Aubagnac

Use Case VGISC 9, Download Data or Product from the VGISC

SIMDAT Use Case Reference	D18.1.1 UC1.4
Use Case GISC Reference	Use Case GISC 9
Use Case Goal	<p>A user of the system receives data or products from a VGISC Node or DCPC on an “ad hoc” or recurring basis. Data may either be readily available or extracted from one of the meteorological database. It is readied for delivery and either pushed to (subscription) or pulled by the Data Receiver (direct retrieve).</p> <p>The data transfer must be efficient and reliable (checksum and error recovery mechanism are available). Several transport mechanisms are available (HTTP, OpenDap, FTP, SFTP, GFTP, email, etc).</p>
Actors	<p>Data Source: VGISC node or DCPC,</p> <p>Data Receiver: All kinds of users</p>
Pre-Conditions	<p>(1) The user must be authenticated to retrieve data,</p> <p>(2) The VGISC provides mechanisms to efficiently transport data to the user,</p> <p>(3) In the subscription mode, the receiving system is known by the VO,</p> <p>(4) The VGISC provides mechanisms to efficiently transport data between VGISC nodes if necessary.</p>
Post-Conditions	The user has obtained the desired data or product.
Normal Flow	<p>The Data Source sends files containing the requested data or products using :</p> <ul style="list-style-type: none"> • the transmission method indicated in the associated Dissemination Metadata, • the transmission method selected for the one-time delivery (pull). <p>Typically, the transmission is accomplished using GTS or a file transfer method available over the Internet, such as HTTP, OpenDap, FTP, SFTP, GFTP, email, etc). In any case, transmission must be efficient and reliable (checksum and error recovery mechanisms are required at minimum).</p>
Notes and Issues	
Last Updated	16 July 2008
Last Updated By	Jacques Roumilhac & Jean-Pierre Aubagnac

Use Case VGISC 10, Provide Dissemination Metadata

SIMDAT Use Case Reference	
Use Case GISC Reference	Use Case GISC 10
Use Case Goal	Dissemination metadata records containing the details of current subscriptions are created or updated in the Dissemination Metadata Catalogue.
Actors	Subscription Registrars: VGISC nodes, DCPC or NC, Dissemination Catalogue Publisher (VGISC nodes)
Pre-Conditions	(1) The system provides mechanisms for updating the Dissemination Catalogue, either by the upload of one or several metadata files, or via an online form for the edition of a particular metadata record. (2) The Dissemination Catalogue Publisher has a mechanism to provide a consolidated view of the Dissemination Metadata Catalogue among VGISC nodes. (3) The Subscription Registrar is properly authenticated and authorized to modify the Dissemination Metadata Catalogue, (4) A number of subscription requests await registration / validation by the Subscription Registrar
Post-Conditions	The Dissemination Catalogue has changed
Normal Flow	The authorized administrator (Subscription Registrar) uses a facility offered by the system to register / validate subscriptions and create new Dissemination Metadata records or update existing records in the Dissemination Catalogue. This typically can be done by uploading a number of metadata files or by using a form to create a new record or modify an existing record. Several agreed policies (e.g. depending on the data or product type, requesting user role, etc) will allow a fully automated process or one awaiting manual validation. Changes to the Dissemination Metadata Catalogue are made available (or visible) to other VGISC nodes.
Notes and Issues	
Last Updated	16 July 2008
Last Updated By	Jacques Roumilhac & Jean-Pierre Aubagnac

Use Case VGISC 11, Report Quality of Service inside the VGISC - Monitoring

SIMDAT Use Case Reference	A part of D18.1.1 UC 5.1 - 5.2 - 5.3 - 5.4
Use Case GISC Reference	Use Case GISC 11
Use Case Goal	<p>The Managers of VGISC receive performance reports of operations against agreed quality of service indicators.</p> <p>The operators or administrators need to be able to monitor and control</p> <ul style="list-style-type: none"> • the data acquisition and raise alarms if the expected data are not received on time, • how the data flows between the VGISC nodes and raise alarms in case of problems. <p>They also are granted to restart the failing data transfers.</p>
Actors	Administrators, Operators
Pre-Conditions	Tools available
Post-Conditions	Control of the virtual organization
Normal Flow	It can be anticipated that VGISC will eventually have agreements that address quality of service requirements. These should include data and network security as well as performance and reliability. Such agreements might be formalized. Or, a looser set of conventions may simply document the variety of service level expectation.
Notes and Issues	The bidder will propose a design for solving all the questions
Last Updated	14 May 2008
Last Updated By	Jacques Roumilhac

Use Case VGISC 12, GTS metadata generation from WMO Volume C1 reference

SIMDAT Use Case Reference	No reference
Use Case GISC Reference	Use Case GISC 12
SIMDAT VGISC View Reference	No reference
Use Case Goal	<p>A VGISC node uses the WMO # 9 Volume C1 operational catalogue to build DAR metadata records for essential GTS data or products:</p> <ul style="list-style-type: none"> Asynchronously before ingesting the GTS data flow (Use Case VGISC 15), To reflect the current state of the catalogue, Using a set of shared resources termed “Information Classes” built and maintained to meet the need for information (Use Case VGISC 17), Using a mechanism to deal the metadata publishing responsibilities among actors without gaps nor overlaps. <p>The metadata records are made available for the update of the DAR metadata catalogue.</p>
Actors	<p>WMO Data Source provider,</p> <p>Supplementary Information Provider (“Information Classes”, controlled vocabulary, distribution of the publishing responsibilities),</p> <p>Metadata Generator (VGISC nodes)</p>
Pre-Conditions	<p>A shared set of resources (termed “Information Classes”) are constructed and maintained to provide the information needed to populate the metadata elements in the GTS metadata records.</p> <p>Their purpose is to expand the information contained in Volume C1 declarations. Typically by decoding cryptic fields (e.g. TTAAii designator, ICAO or WMO station indexes, etc) and by connecting separate elements of information.</p> <p>They are of many types: representations of available WMO references (e.g. WMO # 9 Volume A, sections of the WMO # 306 Manual on Codes or of the WMO # 386 Manual on the GTS, etc), information collected from sparse WMO sources or information created for the purpose (e.g. meeting the need to sort and classify data or products).</p> <p>A variety of processes are involved in their construction, ranging from dynamic generation to manual collection.</p>
Post-Conditions	DAR GTS metadata records are made available for the update of the DAR Metadata Catalogue.
Normal Flow	<p>The Metadata Generator regularly re-generates metadata records for GTS bulletins under its responsibility to reflect changes to the Volume C1 catalogue, changes to the maintained Information Classes or to the distribution of publishing responsibilities.</p> <p>The procedure first obtains the up-to-date input elements from the WMO Data Source Provider (current Volume C1) and from the Supplementary Information Provider (all additional elements). All elements serve to initialise in memory the association tables or style sheets needed by the procedure.</p> <p>A GTS DAR metadata record is created for an entry in Volume C1 only:</p> <ul style="list-style-type: none"> If the bulletin is determined as essential, If the bulletin falls under the publishing responsibility of the Metadata

	<p>Generator.</p> <p>Distributing the responsibility among Metadata Generators may be achieved by designing a set of simple filters :</p> <ul style="list-style-type: none"> • Each filter determines the scope of the generation for each actor, • The list of filters is comprehensive and avoids redundancies: each given essential bulletin declared in Volume C1 exactly matches one of the filter: its metadata record is published by exactly one actor. • Regular expressions on the bulletin abbreviated header line AHL are a simple yet effective implementation of these filters. • In particular, regular expressions only imposing conditions on the collecting / compiling CCCC centre included in the bulletin AHL header are an easy solution to define a national or inter-national area of responsibility.
Notes and Issues	<p>(1) Changes in the distribution of the Metadata Generation responsibility will introduce overlaps or gaps in the generated populations until all actors have re-generated the metadata under their responsibility.</p> <p>Synchronisation of these generations could therefore be envisaged.</p> <p>(2) The creation of metadata records for data or products is the responsibility of the data or product producer (NC or DCPC), but could be delegated in the case of GTS products to the VGISC (or GISC) node.</p> <p>(3) A central repository for supplementary information elements – e.g. at the Central Support Office – will facilitate the maintenance of these resources, and ensure homogeneity in content of the metadata records generated at distinct Centres.</p>
Last Updated	16 July 2008
Last Updated By	Jean-Pierre Aubagnac & Jacques Roumilhac

Use Case VGISC 13, GTS MSS feeding in the VGISC

Use Case GISC Reference	Use Case GISC 9
Use Case Goal	<p>The VGISC node receives essential data or product from other GISC or VGISC nodes from the replication process (Use Case VGISC 14) according to the inter-nodes protocols.</p> <p>Replicated essential data or product collected at a remote MSS (Use Case VGISC 15) are forwarded to the local MSS. This reverse link to the MSS will become necessary as the GTS links between MSS are progressively cut.</p>
Actors	Data Receiver (local NC or DCPC equipped with an MSS) Data Sender (VGISC node)
Pre-Conditions	<p>(1) The system accommodates a global data policy.</p> <p>(2) Metadata records associated with the data or products received from the replication are already available in the DAR Metadata Catalogue (mainly built from WMO Volume C1 according to Use Case VGISC 12)</p> <p>(3) The local MSS supports a method for uploading data or product files according to the WMO FTP protocol.</p> <p>(4) The data or products received from replication are documented with the necessary reference information, including:</p> <ul style="list-style-type: none"> • a reference to the associated DAR metadata record, • a reference to the repository (centre) where the associated DAR metadata was published, • a reference to the source repository (centre) for the data.
Post-Conditions	“Unknown” data or products – that is, absent from the local VGISC Cache - are inserted in the Cache and forwarded to the local MSS according to the appropriate protocol.
Normal Flow	<p>The VGISC MSS feeding functionality polls the dedicated link for new data files proposed by the replication mechanism.</p> <ul style="list-style-type: none"> • The data or products and associated reference information are extracted from the received files, • Data or products already present in the local Cache are not considered, • Data or products absent from the local Cache are both inserted in the Cache and proposed to the local MSS.
Notes and Issues	
Last Updated	16 July 2008
Last Updated By	Jacques Roumilhac & Jean-Pierre Aubagnac

Use Case VGISC 14, Data Replication in the VGISC

Use Case GISC Reference	Use Case GISC 2
Use Case Goal	The replication process disseminates real-time data or product between VGISC or GISC nodes according to inter-node protocols. Only essential data or products are replicated.
Actors	Data Sender and Receiver (VGISC node)
Pre-Conditions	(1) The system accommodates a global data policy. (2) All the parameters of the replication mechanism are set and configurable by the authorised administrator, including: <ul style="list-style-type: none"> • the list of essential data or product to be replicated, possibly built and maintained up-to-date by extracting information from the DAR metadata records as they are made available or modified, • the list of all the different points of storage (data repositories) for replicated data or products. (3) A mechanism is available to distinguish the original copy of each data or product exchanged among VGISC nodes from other copies. (4) Transmission and control mechanisms across VGISC nodes are available for data or products and relevant reference information, including source repository (centre), metadata publishing repository, reference to the associated metadata record, etc.
Post-Conditions	The replicated data or product is available to the Receiver VGISC node for possible inclusion in the local Cache and forwarding to the local MSS (Use Case VGISC 13). A mechanism exists to track the original copy as well as all other copies of the data or product.
Normal Flow	(1) The VGISC replication process polls the dedicated link for incoming data or product files: new data or products are extracted from the files along with their tracking information, (2) Data or products not recognized as essential are discarded, (3) Data or products absent from the local cache are inserted in the Cache and possibly forwarded to the local MSS (see Use Case VGISC 13) (4) Depending on the replication strategy, data or products whose source data repository matches the local data repository may be considered as fully replicated and discarded. (5) Remaining essential data or products are packed with their reference information and proposed again for replication, as they may not have completed the whole replication process among VGISC nodes.
Notes and Issues	A mechanism is required to avoid infinite loops. A mechanism is also required to assess the completeness of the replication process for each replicated data or product.
Last Updated	16 July 2008
Last Updated By	Jacques Roumilhac & Jean-Pierre Aubagnac

Use Case VGISC 15, GTS Ingestion in the VGISC

SIMDAT Use Case Reference	Part of D18.1.1 UC2.1
Use Case GISC Reference	Part of Use Case GISC 2
Use Case Goal	The VGISC node receives essential GTS real-time data for its area of responsibility from the ingestion of the GTS data flow. Ingestion occurs at the local MSS level according to the WMO FTP protocol. The data is stored for at least 24 hours in the local cache.
Actors	Data Sender (MSS at local NC or DCPC) Data Receiver (VGISC node)
Pre-Conditions	(1) Metadata records associated with the ingested data and products are available in the DAR Metadata Catalogue (mainly built from the Volume C1 reference, Use Case VGISC 12), (2) A mechanism exists to identify essential GTS bulletins, (3) A mechanism exists to identify bulletins under the (ingesting) responsibility of the Data Receiver, (4) The Data Sender is authorized to send files to the Data Receiver, (5) The Data Receiver supports a method for uploading files according to the WMO FTP protocol.
Post-Conditions	Ingested essential GTS data or product are stored for 24 hours in the VGISC Cache.
Normal Flow	The VGISC GTS ingestion functionality polls the dedicated MSS link for incoming files: <ul style="list-style-type: none"> • the GTS bulletins are extracted from the File wrapper • bulletins identified as either not essential and / or out of the Data Receiver ingesting responsibility are discarded. • retained bulletins are stored for 24 hours in the local Cache and proposed for replication.
Notes and Issues	A simple implementation is to have matching metadata publishing responsibilities and bulletin ingestion responsibilities. Both responsibilities may however differ. One example is a back-up strategy for the GTS collection function which may (temporarily) require that sets of GTS bulletins are ingested in data repositories different from their default source repository.
Last Updated	16 July 2008
Last Updated By	Jacques Roumilhac & Jean-Pierre Aubagnac

Use Case VGISC 16, Backup inside the VGISC

SIMDAT Use Case Reference	No reference
Use Case GISC Reference	No reference
Use Case Goal	Administrators of the VGISC nodes are able to backup VGISC relevant information (only the ones necessary to keep/fulfil the interface to VGISC services working).
Actors	VGISC Node Administrator
Pre-Conditions	(1) Administrator is Authenticated and Authorized to perform administrative tasks in the VGISC Node. (2) Data and metadata are available for backup.
Post-Conditions	Data and metadata backup complete.
Normal Flow	The Administrator sets up a backup process (what, when, ..). The VGISC node runs an automated process that backs up the data to media on a routine basis as necessary and inform the Administrator.
Notes and Issues	Every WIS Centre will have its own backup process. The information/data to backup should include at least the data or products available at the VGISC node, their corresponding metadata and user information.
Last Updated	17 June 2008
Last Updated By	Duncan Jeffery

Use Case VGISC 17, Management of the information classes (between WMO and the Central Support Office)

SIMDAT Use Case Reference	No reference
Use Case GISC Reference	No reference
Use Case Goal	Authorized administrators are able to update the set of “Information Classes” or supplementary information resources required for the construction of GTS (and other) DAR metadata records from reference catalogues.
Actors	WMO Data Source provider, Supplementary Information Provider Administrators (“Information Classes”, controlled vocabulary, distribution of the publishing responsibilities)
Pre-Conditions	(1) A shared set of resources (termed “Information Classes”) are constructed and maintained. They are made available from the Supplementary Information Provider. They aim at providing all necessary information for the creation of DAR metadata records from reference catalogues (e.g. according to Use Case VGISC 12). (2) The Supplementary Information Provider offers a mechanism for the update of the “Information Classes”. This includes primarily a file upload facility. (3) Authorized administrators have access to the Supplementary Information Provider updating facilities.
Post-Conditions	The shared resources hosted by the Supplementary Information Provider are updated. Changes to these resources will be reflected by the following generations of metadata records.
Normal Flow	Authenticated Administrators at the Supplementary Information Provider may modify the set of resources made available for the automatic generation of DAR metadata records from reference catalogues. Several such roles may exist, and the authorization may depend on the “Information Class” which needs updating. The process may be at the initiative of the Administrator, or solicited by the WMO Data Source Provider, for instance to reflect changes to one of the relevant WMO references (e.g. WMO # 306 Manual on Codes). A file upload facility is the primary updating method available. Simple online editors may also be envisaged. A variety of processes are involved in the construction of the “Information Classes”, ranging from dynamic generation to manual collection. As a consequence, the most probable situation is that of an “expert” local re-creation of one or several “Information Classes” by the authorized Administrator, followed by one or several file uploads.
Notes and Issues	(1) Changes to the “Information Classes” will result in inconsistencies in the metadata population, at least until all automatic metadata are re-generated. (2) It is the case in particular for the mechanism distributing the responsibility of the GTS metadata generation among actors. Here, redundant metadata records with differing sources will co-exist in the transition phase, while the DAR metadata records do not all take the change into account. An automatic re-generation of the population may be desirable in this situation.
Last Updated	16 July 2008
Last Updated By	Jean-Pierre Aubagnac

F.3 Internal DCPC Use Cases

F3.1 Metadata for data or products and upload of files

Use Case Internal DCPC 1 Provide Metadata for Data or Product

Use Case Goal	Metadata for any data or product file to be available from the DCPC is created or updated in the DAR Metadata Catalogue of the DCPC
Actors	Metadata Originator
Pre-Conditions	<ol style="list-style-type: none"> 1. The Metadata Originator is authorized to update the DAR Metadata Catalogue for the associated file(s) 2. The Metadata Originator has the necessary information and the ability to update the DAR Metadata Catalogue for the associated file(s) 3. The Metadata Catalogue Publisher supports mechanisms for authorized Metadata Originators to update the metadata for the associated file(s) 4. The DAR metadata is able to handle both open and restricted (sensitive) metadata records.
Post-Conditions	The DAR Metadata Catalogue has changes made by the Metadata Originator
Normal Flow	<p>The authorized Metadata Originator uses a mechanism supported by the Metadata Catalogue Publisher to update the DAR Metadata Catalogue for the associated file.</p> <p>Typically, two kinds of maintenance facilities are supported. One is a file upload facility for "batch" updating (add, replace, or delete metadata records treated as separate files). The other is an online form for changing metadata records treated as entries in the DAR Metadata Catalogue (add, change, or delete of elements in a record as well as whole records).</p> <p>The Metadata Catalogue Publisher maintains the updated DAR Metadata Catalogue as a searchable resource offered to all authorized searchers.</p> <p>The Metadata Catalogue Publisher also shares the metadata across WIS centres.</p>
Notes and Issues	As "Metadata Originator" can act NCs or other DCPCs (that upload a file to the DPCP or share its metadata), as well as users/systems internal to the DCPC (that create/publish new DCPC data or products).
Last Updated	15 June 2008
Last Updated By	Øystein Godøy

Use Case Internal DCPC 2 Make Data or Product available to DCPC

Use Case Goal	Data or product is available as a file at the DCPC
Actors	Data Sender
Pre-Conditions	<ol style="list-style-type: none"> 1. The Data Sender is authorized to send the file to the Data Receiver 2. The Data Receiver supports a method for uploading the file, which the Data Sender is able to use
Post-Conditions	The data or product uploaded by the Data Sender is received and stored by the Data Receiver.
Normal Flow	<ol style="list-style-type: none"> 1. The Data Sender uses his authorized access to send the file using an appropriate transmission method supported by the DCPC. Typically, the transmission is accomplished via GTS, Internet or dedicated links using standard file transfer methods. A file naming convention or other agreed mechanism is used to make an association between the file and its metadata. 2. The DCPC checks if the file has an associated metadata record in its DAR Metadata Catalogue following the actions described in Use Case Internal DCPC 3 Control Metadata Association to Data or Product. 3. The DCPC stores the file in a proper storage location. 4. The metadata is updated with a URI of where the associated file is stored.
Notes and Issues	As "Data Sender" can act NCs or other DCPCs that make available a file to the DPCP; as well as users/systems, internal to the DCPC, that create new DCPC data or products.
Last Updated	15 June 2008
Last Updated By	Øystein Godøy

Use Case Internal DCPC 3 Control Metadata Association to Data or Product

Use Case Goal	Confirm that metadata for a data or product file at the DCPC already exists in the DAR Metadata Catalogue before the data or product is available
Actors	Data Sender
Pre-Conditions	<ol style="list-style-type: none"> 1. Data or product has been made available as a file from a Data Sender 2. DAR Metadata Catalogue is current with all updates
Post-Conditions	An error is communicated when there is no confirmation that a given file is associated appropriately with metadata in the DAR Metadata Catalogue
Normal Flow	On receipt of a file containing a data or product, the Data Receiver checks the current DAR Metadata Catalogue to confirm that the file has an associated metadata record. If such a record is not found within a specified period after receipt of the file, an error message is sent to the Data Sender.
Notes and Issues	<ol style="list-style-type: none"> 1. As "Data Sender" can act NCs or other DCPCs that upload a file to the DPCP; as well as users/systems, internal to the DCPC, that create new DCPC data or products. 2. This control action addresses the condition wherein data arrives before its associated metadata. Rather than rejecting the file immediately, a grace period is allowed before the data file is regarded as erroneous.
Last Updated	15 June 2008
Last Updated By	Øystein Godøy

F3.2 User management

Use Case Internal DCPC 4 User registration

Use Case Goal	Users of the VGISC system will be able to be identified at the DCPC via their credentials.
Actors	User of the VGISC system
Pre-Conditions	<ol style="list-style-type: none"> 1. Administrators have agreed policies delineating which roles are authorized to perform each action within the VGISC system 2. Administrators have mechanisms to create and maintain identification information needed for authentication of users of the VGISC system, 3. Administrators have mechanisms to create and maintain role information needed for authorization of authenticated users of the VGISC system. 4. The DCPC support mechanisms for user registration.
Post-Conditions	The User of the VGISC system is registered at the DCPC, is uniquely identifiable within the VGISC system and has assigned a set of roles.
Normal Flow	<ol style="list-style-type: none"> 1. The user applies for an account for accessing certain data or products, and using a mechanism supported by the DCPC provides all needed details (username, password, contact information, ...). 2. The DCPC stores the information and notifies the Administrator. 3. The Administrator validates the information against the data policy applicable to the data or products the user wants to register to. 4. The Administrator assigns roles to the user and activates the account. 5. The DCPC stores the user credentials and notifies the user about the successful registration.
Notes and Issues	<ol style="list-style-type: none"> 1. This is a basic registration process without compromising any implementation. 2. In some circumstances it may be beneficial to insert user information from an existing user database into the VGISC system (e.g. at one of the partner sites). In those cases an interface where existing user information may be translated into VGISC system roles etc must be available.
Last Updated	15 June 2008
Last Updated By	Øystein Godøy

Use Case Internal DCPC 5 User Authentication

Use Case Goal	Users are able to demonstrate their identity to the DCPC in order to perform all the operations that require authentication.
Actors	User of the VGISC system
Pre-Conditions	<ol style="list-style-type: none"> 1. Administrators have mechanisms to create and maintain identification information needed for authentication of users of the VGISC system. 2. User has registered at the DCPC (UC External DCPC 4) 3. User has made a request for a data or product that requires authentication or has decided to login. 4. The DCPC support services for authentication.
Post-Conditions	The User of the VGISC system is authenticated at the DCPC and is able to perform all the operations that require authentication.
Normal Flow	<ol style="list-style-type: none"> 1. The user credential is introduced using a service supported by the DCPC (username, password / credentials,...). 2. The DCPC checks the credentials against the registered information. 3. The DCPC accepts or rejects the User.
Notes and Issues	Different authentication schemes might have to be supported according to existing legacy practices or Trusting agreements.
Last Updated	15 June 2008
Last Updated By	Øystein Godøy

Use Case Internal DCPC 6 User Authorisation

Use Case Goal	Users of the VGISC system have access to restricted data or products and functionalities of the DCPC.
Actors	User of VGISC system
Pre-Conditions	<ol style="list-style-type: none"> 1. Administrators have agreed authorization policies delineating which roles are authorized to perform each VGISC system action 2. Administrators have mechanisms to create and maintain role information needed for authorization of authenticated users of the VGISC system 3. The User of the VGISC system is authenticated. 4. The User has made a request for a restricted data or product, or wants to use a restricted functionality. 5. The DCPC supports agreed authorisation policies. 6. The DCPC supports mechanisms to trust users authenticated in other VGISC centres.
Post-Conditions	The User of VGISC system is authorised to access to the restricted data or products or to use a restricted functionality.
Normal Flow	<ol style="list-style-type: none"> 1. An authenticated user request originated from the DCPC itself or a trusted VGISC centre is received at the DCPC. 2. The DCPC verifies that requests originated at a remote site are formulated from VGISC centres of the trusting agreement. 3. The DCPC will read user roles. If these were at a remote trusted site, there should be mechanisms to attach the user roles to the request. (or to query for them remotely) 4. The DCPC will be able to grant or deny access to the data, product or service requested according to the roles provided to the user. (By matching the user role with that of the data, product or service requested)
Notes and Issues	The VGISC system might need to support several authorisation schemes of several levels e.g. acknowledgement by the user of a given policy versus strong fine grained authorisation attributes defined at different groups.
Last Updated	17 June 2008
Last Updated By	Marta Gutierrez

F3.3 DAR catalogue

Use Case Internal DCPC 7 Discover Data or Products

Use Case Goal	A user of the VGISC system finds available data or products that he wants to receive.
Actors	Data Searcher
Pre-Conditions	<ol style="list-style-type: none"> 1. The DAR Metadata Catalogue is accessible for browsing or searching 2. Restricted metadata are not exposed to data searchers
Post-Conditions	The Data Searcher has information needed to select relevant data or products.
Normal Flow	The Data Searcher discovers available data and products by browsing the DAR Metadata Catalogue or by searching the DAR Metadata Catalogue using discovery concepts such as subject keywords, geographic extent, and temporal range. As a result of his browsing or searching, the Data Searcher gets a relevance-ordered list of data and products including "data or product metadata" such as data origin, data type, generation date, availability, and use constraints, among other characteristics.
Notes and Issues	
Last Updated	15 June 2008
Last Updated By	Øystein Godøy

F3.4 Dissemination metadata and download of files

Use Case Internal DCPC 8 Ad Hoc Request for Data or Product ("Pull")

Use Case Goal	A user of the VGISC system requests data or product on an ad hoc basis
Actors	User of the VGISC system
Pre-Conditions	<ol style="list-style-type: none"> 1. The desired data or product has been identified by the User 2. The desired data is located either locally or at a trusted VGISC centre.
Post-Conditions	<ol style="list-style-type: none"> 1. Data or product is readied for delivery to the User according to the service level commitment of the DCPC 2. The User is informed on the status of the request.
Normal Flow	<p>Once the user has identified the desired data or product, he requests delivery on a one-time basis. The User has been authenticated within the DCPC or at a Trusted node of the VGISC system to retrieve the desired data. The DCPC checks the user is authorized for delivery of the product according to the user's role. The DCPC then sets up delivery through any of a broad range of online and offline options.</p> <ol style="list-style-type: none"> 1. The User requests the product. 2. The DCPC locates the requested data either locally or in a trusted remote VGISC centre. 3. Either the local or the trusted remote VGISC centre acknowledges the user authentication and authorisation. 4. The requested data is prepared for download. 5. The local or trusted remote VGISC centre returns the information on where to download data to the VGISC user.
Notes and Issues	<ol style="list-style-type: none"> 1. For some datasets and user groups this might be bandwidth demanding. In such cases the DCPC should set up a local cache retrieving the requested data from the other VGISC centre and serving them to VGISC users. The DCPC should be prepared to serve specific user groups by preparing the required bandwidth. 2. Some datasets may require asynchronous download due to large data volume or offline storage.
Last Updated	17 June 2008
Last Updated By	Marta Gutierrez

Use Case Internal DCPC 9 Subscribe to Data or Product ("Push")

Use Case Goal	A user of the VGISC system can subscribe to receive data or products on a recurring basis
Actors	User of the VGISC system
Pre-Conditions	<ol style="list-style-type: none"> 1. The desired data or product has been identified locally or at a remote trusted centre by the User 2. The User has been authenticated and authorized to retrieve the desired data or product. 3. The DCPC provides mechanisms for defining and managing subscription information which the User is able to use.
Post-Conditions	<ol style="list-style-type: none"> 1. Data or product is readied for delivery to the User according to the service level commitment of the DCPC 2. The dissemination catalogue has changed. 3. The User is informed on the status of the request.
Normal Flow	<ol style="list-style-type: none"> 1. The User has identified the desired data or product, either locally or within a remote trusted VGISC centre and requests to subscribe to receive the data or products through a chosen transport mechanism on a recurring basis. 2. The DCPC authenticates the user and checks authorization for delivery of the product according to the user's role. 3. The Dissemination Metadata associated with the subscription is updated.
Notes and Issues	For some datasets and user groups this might be bandwidth demanding. In such cases the DCPC should set up a local cache. The DCPC should be prepared to serve specific user groups by preparing the required bandwidth.
Last Updated	15 June 2008
Last Updated By	Øystein Godøy

Use Case Internal DCPC 10 Download Data or Product from DCPC

Use Case Goal	A user of the VGISC system receives from a DCPC, on an ad hoc or subscription basis, data or products transmitted as files
Actors	User of the VGISC system
Pre-Conditions	<ol style="list-style-type: none"> 1. Data or product is ready for delivery to the authenticated and authorized user, as requested through one of the supported transmission mechanisms and according to the service level commitment of the DCPC 2. For subscription delivery, the DCPC has access to subscription information in the Dissemination Metadata Catalogue
Post-Conditions	Selected data or products are received by the User
Normal Flow	<ol style="list-style-type: none"> 1. The transmission of the files containing the requested data or products is initiated between the User and the VGISC system. 2. The files can either be pulled by the user (ad hoc request) or be pushed to the user (subscription). 3. An appropriate transmission method is used as indicated in the associated subscription information accessible through the Dissemination Metadata Catalogue. Typically, the transmission is accomplished via GTS, Internet, dedicated links or multicast systems using standard file transfer methods.
Notes and Issues	Some datasets represents challenges concerning data volume or data access (e.g. offline tape storage). Those datasets should be served through some asynchronous service.
Last Updated	15 June 2008
Last Updated By	Øystein Godøy

Use Case Internal DCPC 11 Provide Dissemination Metadata

Use Case Goal	Metadata concerning delivery specifics of subscription(s) to data and products from a DCPC are created or updated in the Dissemination Metadata Catalogue
Actors	<ol style="list-style-type: none"> 1. Subscription Registrar 2. Dissemination Catalogue Publisher
Pre-Conditions	<ol style="list-style-type: none"> 1. The Subscription Registrar is authorized to update the Dissemination Metadata Catalogue for the given subscription(s) 2. The Subscription Registrar has the necessary information and the ability to update the Dissemination Metadata Catalogue for the given subscription(s) 3. The Dissemination Catalogue Publisher supports facilities for authorized Subscription Registrars to update the metadata for the given subscription(s)
Post-Conditions	The Dissemination Metadata Catalogue has changes made by the Subscription Registrar
Normal Flow	The authorized Subscription Registrar uses a mechanism supported by the Dissemination Metadata Catalogue Publisher to update the Dissemination Metadata Catalogue for the given subscription(s).
Notes and Issues	<ol style="list-style-type: none"> 1. As "Subscription Registrar" can act NCs or other DCPCs that share their Dissemination Metadata; as well as users/systems that subscribes to DCPC data or products (as in Use Case Internal DCPC 9 Subscribe to Data or Product ("Push")). 2. At this point in the VGISC system design, it has yet to be defined how each Dissemination Metadata Catalogue Publisher will communicate changes within the system.
Last Updated	15 June 2008
Last Updated By	Øystein Godøy

F3.5 Quality of service

Use Case Internal DCPC 12 Report Quality of Service across VGISC Centres

Use Case Goal	Managers of DCPCs receive performance reports of operations against agreed quality of service indicators
Actors	DCPC Managers
Pre-Conditions	<ol style="list-style-type: none"> 1. Measurable quality of service indicators are agreed 2. Schedule of reporting and specifics of reporting formats are agreed
Post-Conditions	DCPC managers have performance information needed to manage WIS operations across the range of DCPC services
Normal Flow	On a schedule as mutually agreed, all DCPC managers send performance reports of operations against agreed quality of service indicators.
Notes and Issues	<ol style="list-style-type: none"> 1. It can be anticipated that VGISC will have agreements that address quality of service requirements. These should include data and network security as well as performance and reliability. Such agreements might be formalized into WIS standards, and perhaps Technical Specifications. Or, a looser set of conventions may simply document the variety of service level expectations reported across communities of WIS end-users. 2. Although not yet addressed in VGISC system design, performance reports can be generated efficiently by having each VGISC Centre upload its reports to a single analysis site within a fixed time window.
Last Updated	15 June 2008
Last Updated By	Øystein Godøy

Use Case Internal DCPC 13 Monitoring the DCPC

Use Case Goal	Administrators of the DCPC are able to manage and monitor the DCPC and create reports.
Actors	DCPC Administrator
Pre-Conditions	Administrator is Authenticated and Authorized to monitor the DCPC
Post-Conditions	Monitoring reports have been created.
Normal Flow	<ol style="list-style-type: none"> 1. The Administrator chooses what to monitor with a view to detect and notify interested parties of failures. 2. The DCPC collects statistics about the parties being monitored. 3. The Administrator asks for a report on the statistics. 4. The DCPC returns the report requested to the Administrator.
Notes and Issues	Every VGISC Centre will have its own way to monitor the system. It is not decided yet if a global monitoring view will be available for the whole of VGISC
Last Updated	19 Mar 2008
Last Updated By	Beatriz Martinez Garcia

Use Case Internal DCPC 14 Backup

Use Case Goal	Administrators of the DCPC are able to backup relevant information.
Actors	DCPC Administrator
Pre-Conditions	<ol style="list-style-type: none"> 1. Administrator is Authenticated and Authorized to perform administrative tasks in the DCPC. 2. Data or metadata is available for backup.
Post-Conditions	Data backup complete.
Normal Flow	<ol style="list-style-type: none"> 1. The Administrator sets up a backup process (what, when...). 2. The DCPC runs an automated process that backs up the data to media on a routine basis as necessary and inform the Administrator.
Notes and Issues	<ol style="list-style-type: none"> 1. Every VGISC Centre will have its own backup process. 2. The information/data to backup should include at least the data or products available at the DCPC, their corresponding metadata and user information.
Last Updated	17 June 2008
Last Updated By	Marta Gutierrez

Use Case Internal DCPC 15 Recovery

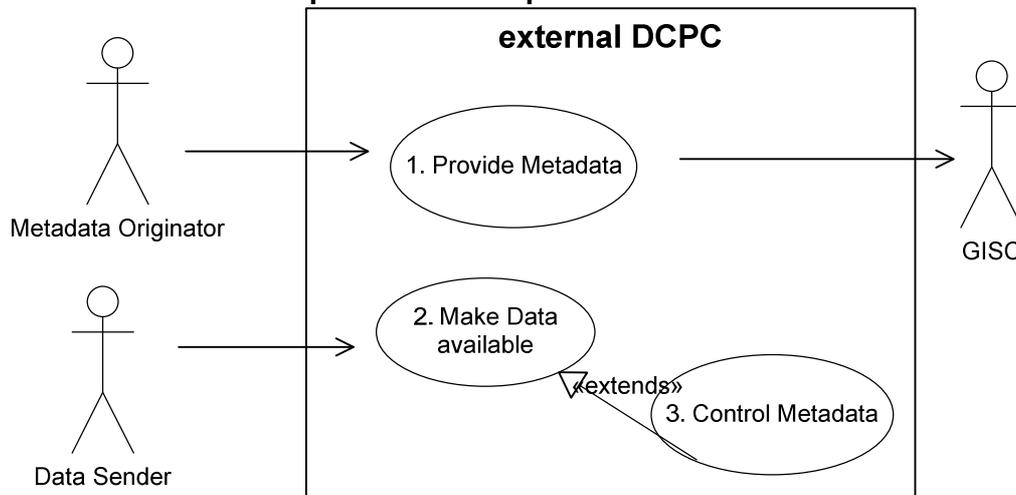
Use Case Goal	Administrators of the DCPC are able to recover relevant information.
Actors	DCPC Administrator
Pre-Conditions	<ol style="list-style-type: none"> 1. Administrator is Authenticated and Authorized to perform administrative tasks in the DCPC. 2. A media containing a previous version of the relevant data is available (see Use Case Internal DCPC 14 Backup).
Post-Conditions	Data restoration complete.
Normal Flow	<ol style="list-style-type: none"> 1. The Administrator locates the last available version for the data on media and makes it accessible. 2. The DCPC runs a process that reads the data from the media and restores the data, informing the Administrator when finished.
Notes and Issues	Every VGISC Centre will have its own recovery process. A general VGISC interface is required.
Last Updated	15 June 2008
Last Updated By	Øystein Godøy

Use Case Internal DCPC 16 Install Software updates

Use Case Goal	Administrators of the DCPC are able to update the software installed at the DCPC without decrease QoS level.
Actors	DCPC Administrator
Pre-Conditions	<ol style="list-style-type: none"> 1. The Administrator is Authenticated and Authorized to perform administrative tasks in the DCPC. 2. An update to the existing software is available.
Post-Conditions	Updated software has been installed.
Normal Flow	<ol style="list-style-type: none"> 1. The Administrator informs other VGISC centre administrators and DCPC users about the coming update. 2. The Administrator stops the processes running with the existing software. 3. The Administrator installs the updated version of the software and restarts the software application processes. 4. The Administrator informs other VGISC centre administrators and DCPC users about the successful installation.
Notes and Issues	<ol style="list-style-type: none"> 1. The installation process must contain a verification step testing that the upgraded version is working as expected. 2. If the installation/upgrade fails the previously operational version must be recovered for operational use.
Last Updated	15 June 2008
Last Updated By	Øystein Godøy

F.4 External DCPC Use Cases

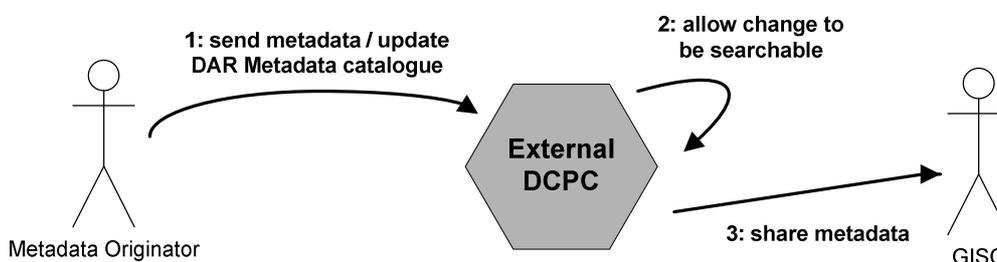
F.4.1 Metadata for data or products and Upload of files



Use Case External DCPC 1, Provide Metadata for Data or Product

Use Case Goal	Metadata for any data or product file to be either available from the DCPC or from other WIS Centres is created or updated in the DAR Metadata Catalogue of the DCPC and shared with the corresponding GIS.
Actors	Metadata Originator GIS
Pre-Conditions	(1) The Metadata Originator is authorized to update the DAR Metadata Catalogue for the associated file(s) (2) The Metadata Originator has the necessary information and the ability to update the DAR Metadata Catalogue for the associated file(s) (3) The Metadata Catalogue Publisher (DCPC) supports mechanisms for authorized Metadata Originators to update the metadata for the associated file(s) (4) The DAR Metadata Catalogue is able to handle both open and restricted metadata records.
Post-Conditions	The DAR Metadata Catalogue has changes made by the Metadata Originator
Normal Flow	1) The authorized Metadata Originator uses a mechanism supported by the DCPC to update the DAR Metadata Catalogue for the associated file. Typically, two kinds of maintenance mechanisms are supported. <ul style="list-style-type: none"> • One is a file upload mechanism for "batch" updating (add, replace, or delete metadata records treated as separate files). • The other is an online form for changing metadata records treated as entries in the DAR Metadata Catalogue (add, change, or delete of elements in a record as well as whole records). 2) The DCPC maintains the updated DAR Metadata Catalogue as a searchable resource offered to all authorized searchers. 3) The DCPC also shares the metadata with its corresponding GIS.
Notes and Issues	As "Metadata Originator" can act NCs or other DCPCs (that upload a file to the DCPC or share its metadata), as well as users/systems internal to the DCPC (that create/publish new DCPC data or products).
Last Updated	16 June 2008
Last Updated By	Beatriz Martinez Garcia

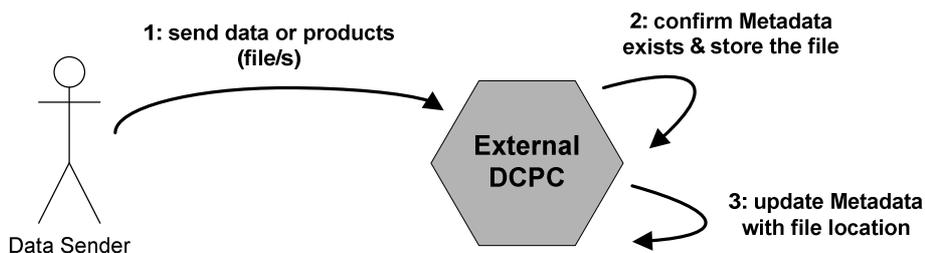
Typical scenario:



Use Case External DCPC 2, Make Data or Product available to DCPC

Use Case Goal	Data or product is available as a file at the DCPC.
Actors	Data Sender
Pre-Conditions	(1) The Data Sender is authorized to send the file to the DCPC (2) The DCPC supports a method for uploading the file, which the Data Sender is able to use
Post-Conditions	The data or product uploaded by the Data Sender is received and stored by the DCPC.
Normal Flow	<ol style="list-style-type: none"> 1. The Data Sender uses his authorized access to send the file using an appropriate transmission method supported by the DCPC. Typically, the transmission is accomplished via GTS, Internet or dedicated links using standard file transfer methods. A file naming convention or other agreed mechanism is used to make an association between the file and its metadata. 2. The DCPC checks if the file has an associated metadata record in its DAR Metadata Catalogue following the actions described in "Use Case external DCPC 3". 3. The DCPC stores the file in a proper storage location. 4. The metadata is updated with the file location where the associated file is stored.
Notes and Issues	As "Data Sender" can act NCs or other DCPCs that made a file available to the DPCP; as well as users/systems, internal to the DCPC, that create new DCPC data or products.
Last Updated	16 June 2008
Last Updated By	Beatriz Martinez Garcia

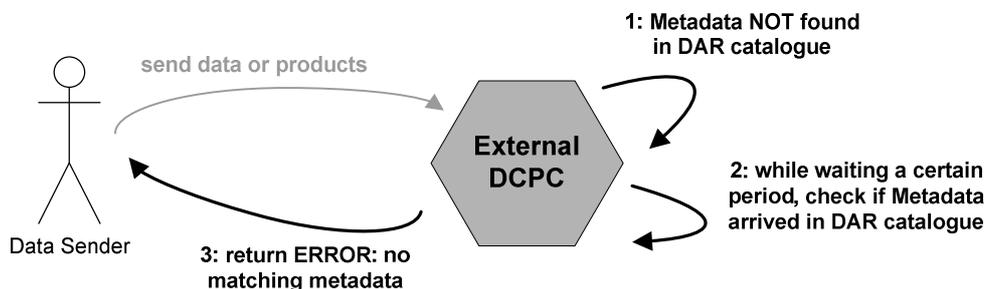
Typical scenario:



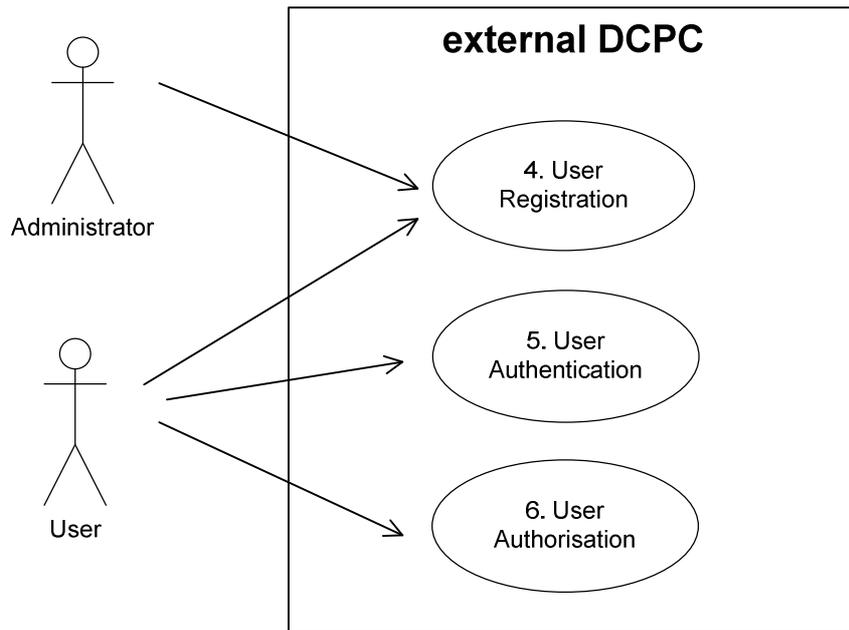
Use Case External DCPC 3, Control Metadata Association to Data or Product

Use Case Goal	Confirm that metadata for a data or product file at the DCPC already exists in the DAR Metadata Catalogue before the data or product is available
Actors	Data Sender
Pre-Conditions	(1) Data or product has been made available as a file by a Data Sender. (2) DAR Metadata Catalogue is current with all updates
Post-Conditions	An error is communicated when there is not confirmation that a given file is associated appropriately with metadata in the DAR Metadata Catalogue
Normal Flow	On receipt of a file containing a data or product, the DCPC checks the current DAR Metadata Catalogue to confirm that the file has an associated metadata record. If such a record is not found within a specified period after receipt of the file, an error message is sent to the Data Sender.
Notes and Issues	1. As "Data Sender" can act NCs or other DCPCs that upload a file to the DPCP; as well as users/systems, internal to the DCPC, that create new DCPC data or products. 2. This control action addresses the condition wherein data arrives before its associated metadata. Rather than rejecting the file immediately, a grace period is allowed before the data file is regarded as erroneous.
Last Updated	16 June 2008
Last Updated By	Beatriz Martinez Garcia

Typical scenario (starts in "Use Case external DCPC 2"):



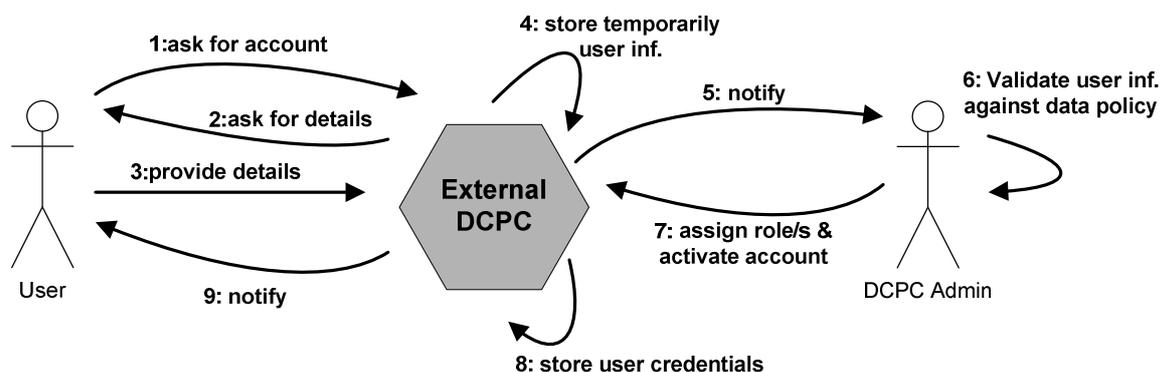
F.4.2 User Management



Use Case External DCPC 4, User Registration

Use Case Goal	Users will be able to be identified at the DCPC via their credentials.
Actors	User Administrator of user management at the DCPC
Pre-Conditions	(1) Administrators have mechanisms to create and maintain identification information needed for authentication of users. (2) Administrators have mechanisms to create and maintain role information needed for authorization of authenticated users. (3) The DCPC support mechanisms for user registration.
Post-Conditions	(1) The User is registered at the DCPC, is uniquely identifiable within the DCPC and has assigned a set of roles.
Normal Flow	1. The user applies for an account for accessing certain data or products, and using a mechanism supported by the DCPC provides all needed details (username, password, contact information,...). 2. The DCPC stores the information and notifies the Administrator. 3. The Administrator validates the information against the data policy applicable to the data or products the user wants to register to. 4. The Administrator assigns roles to the user and activates the account. 5. The DCPC stores the user credentials and notifies the user about the successful registration.
Notes and Issues	This is a basic registration process without compromising any implementation.
Last Updated	16 June 2008
Last Updated By	Beatriz Martinez Garcia

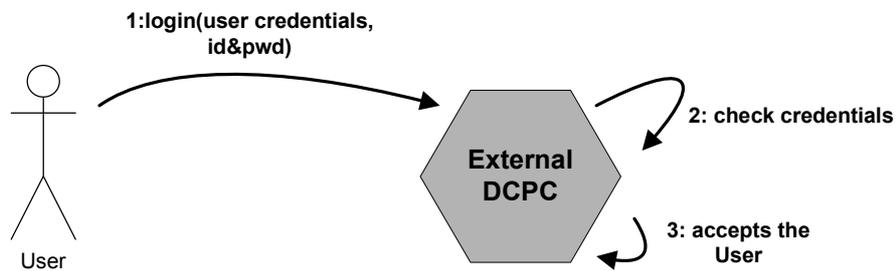
Typical scenario:



Use Case External DCPC 5, User Authentication

Use Case Goal	Users are able to demonstrate their identity to the DCPC in order to perform all the operations that require authentication.
Actors	User
Pre-Conditions	(1) Administrators have mechanisms to create and maintain identification information needed for authentication of users. (2) User has registered at the DCPC ("Use Case external DCPC 4") (3) User has made a request for a data or product that requires authentication or has decided to login. (4) The DCPC support mechanisms for authentication.
Post-Conditions	The User is authenticated at the DCPC and is able to perform all the operations that require authentication.
Normal Flow	1. The user introduces his credentials using a mechanism supported by the DCPC (username, password / credentials,...). 2. The DCPC checks the credentials against the registered information. 3. The DCPC accepts the User.
Notes and Issues	
Last Updated	16 June 2008
Last Updated By	Beatriz Martinez Garcia

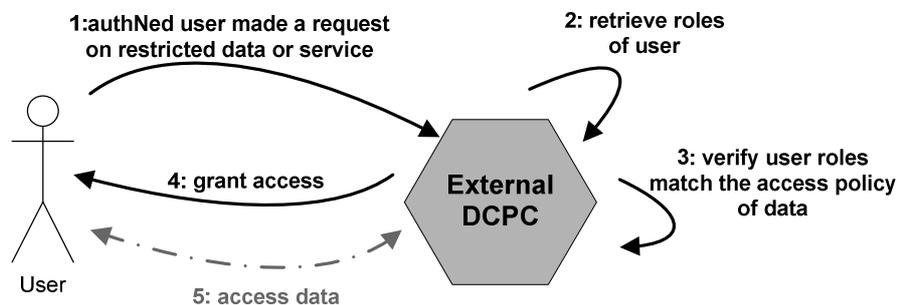
Typical scenario:



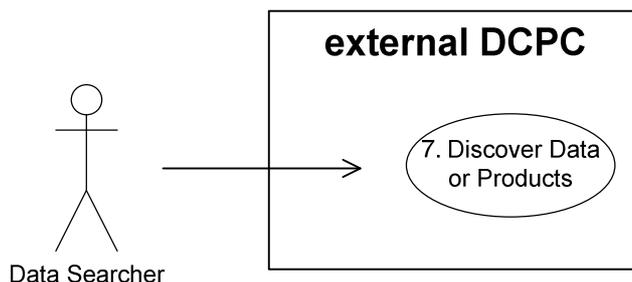
Use Case External DCPC 6, User Authorisation

Use Case Goal	Users have access to restricted data or products and functionalities of the DCPC.
Actors	User
Pre-Conditions	(1) Administrators have mechanisms to create and maintain role information needed for authorization of authenticated Users. (2) User is authenticated. (3) The DCPC support mechanisms for enforcing local authorisation policies.
Post-Conditions	The User is authorised to access to the restricted data or products or to use a restricted functionality.
Normal Flow	1. An authenticated User has made a request for a restricted data or product, or wants to use a restricted functionality. 2. The DCPC retrieves the roles of the User. 3. The DCPC verifies that the roles of the User match the data access policy of the data or product being accessed or of the functionality being used. 4. The DCPC grants the User.
Notes and Issues	
Last Updated	17 June 2008
Last Updated By	Beatriz Martinez Garcia

Typical scenario:



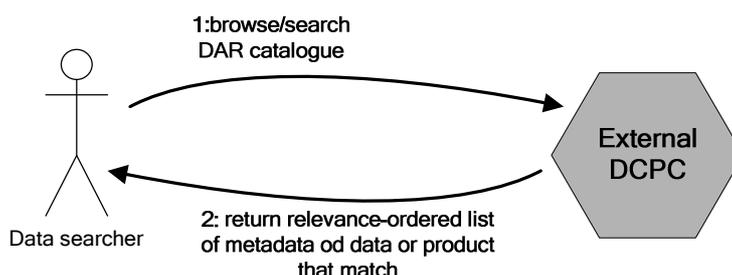
F.4.3 DAR Catalogue



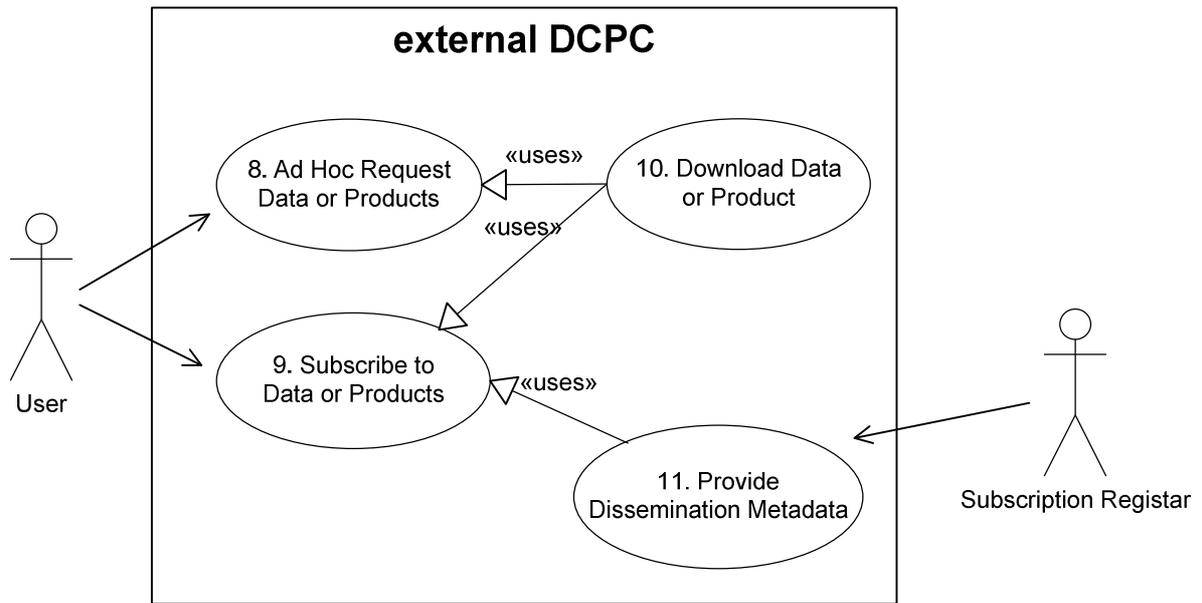
Use Case External DCPC 7, Discover Data or Products

Use Case Goal	A User finds available data or products that he wants to receive.
Actors	Data Searcher
Pre-Conditions	(1) The DAR Metadata Catalogue is accessible for browsing or searching. (2) Restricted metadata are not exposed to unauthorized Data searches.
Post-Conditions	The Data Searcher has information needed to select relevant data or products.
Normal Flow	<ol style="list-style-type: none"> 1. The Data Searcher discovers available data and products by browsing the DAR Metadata Catalogue or by searching the DAR Metadata Catalogue, using discovery concepts such as subject keywords, geographic extent, and temporal range. 2. As a result of his browsing or searching, the Data Searcher gets a relevance-ordered list of data and products including "data or product metadata" such as data origin, data type, generation date, availability, and use constraints, among other characteristics.
Notes and Issues	
Last Updated	16 June 2008
Last Updated By	Beatriz Martinez Garcia

Typical scenario:



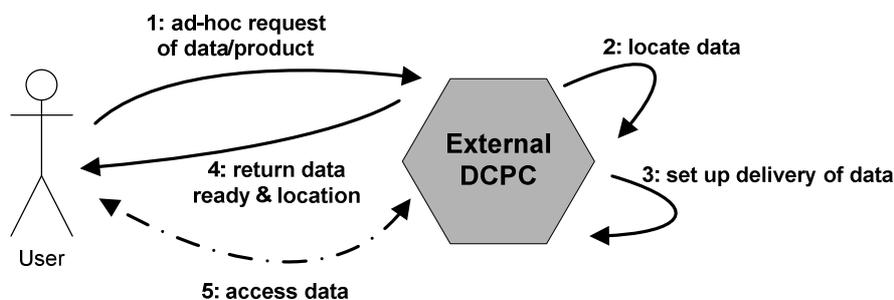
F.4.4 Dissemination Metadata and Download of files



Use Case External DCPC 8, Ad Hoc Request for Data or Product ("Pull") hosted by the DCPC

Use Case Goal	A User requests data or product on an ad hoc basis hosted by the DCPC.
Actors	User
Pre-Conditions	(1) The desired data or product has been identified by the User. (2) The desired data or product is located locally. (3) The User has been authenticated and authorized to retrieve the desired data or product from the DCPC. (4) Delivery is achievable through one of the supported mechanisms for the transmission of the desired data or product, and within the published service level commitment of the DCPC.
Post-Conditions	Data or product is readied for being accessed by the User according to the service level commitment of the DCPC.
Normal Flow	1. The user requests delivery of the desired data or product on a one-time basis. 2. The DCPC then sets up delivery through any of a broad range of online and offline options. 3. The DCPC notifies the user about the readiness and location of the data or product for downloading.
Notes and Issues	Some datasets may require asynchronous download due to large data volume or offline storage.
Last Updated	16 June 2008
Last Updated By	Beatriz Martinez Garcia

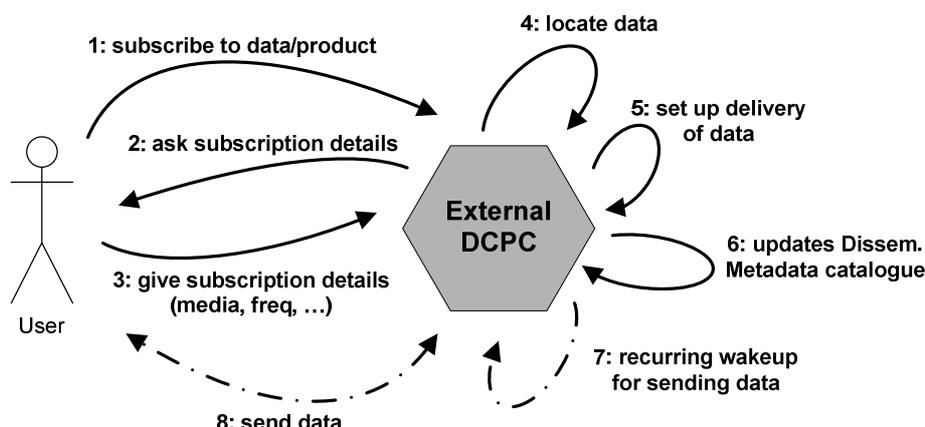
Typical scenario (including "Use Case external DCPC 10"):



Use Case External DCPC 9, Subscribe to Data or Product ("Push") hosted by the DCPC

Use Case Goal	A User can subscribe to receive data or products hosted by the DCPC on a recurring basis.
Actors	User.
Pre-Conditions	(1) The desired data or product has been identified locally by the User. (2) The User has been authenticated and authorized to subscribe to the desired data or product from the DCPC (3) The DCPC provides mechanisms for defining and managing subscription information, which the User is able to use. (4) Delivery is achievable through one of the supported mechanisms for the transmission of the desired data or product, and within the published service level commitment of the DCPC.
Post-Conditions	(1) Data or product is readied for delivery to the User according to the service level commitment of the DCPC. (2) The Dissemination Metadata catalogue has changed. (3) The User is informed about the status of the request.
Normal Flow	1. The user requests to subscribe to receive the desired data or products on a recurring basis. The user can choose between different subscription policies and manage its subscription details. 2. The DCPC then sets up delivery through any of a broad range of online and offline options. 3. As necessary, the DCPC updates the Dissemination Metadata associated with the subscription as described in "Use Case external DCPC 11". 4. The DCPC informs the user that the subscription is successful.
Last Updated	16 June 2008
Last Updated By	Beatriz Martinez Garcia

Typical scenario (including "Use Case external DCPC 10"):



Use Case External DCPC 10, Download Data or Product from DCPC

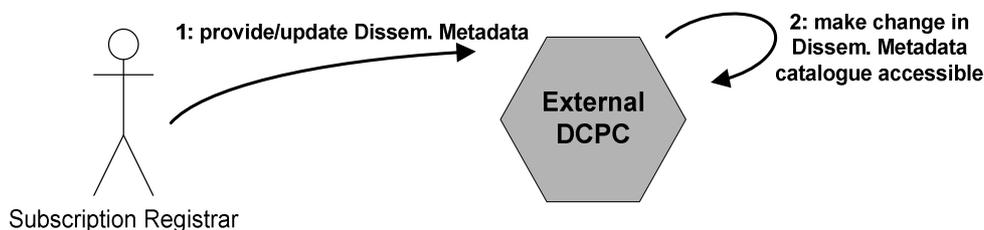
Use Case Goal	A User receives from a DCPC, on an ad hoc or subscription basis, data or products transmitted as files
Actors	User
Pre-Conditions	(1) Data or product is ready for delivery to the authenticated and authorized user, as requested through one of the supported transmission mechanisms and according to the service level commitment of the DCPC (2) For subscription delivery, the DCPC has access to subscription information in the Dissemination Metadata Catalogue
Post-Conditions	Selected data or products are received by the User.
Normal Flow	1. The transmission of the files containing the requested data or products is initiated between the User and the DCPC. 2. The files can either be pulled by the user (ad hoc request) or be pushed to the user (subscription). An appropriate transmission method is used as indicated in the associated subscription information accessible through the Dissemination Metadata Catalogue. Typically, the transmission is accomplished via GTS, Internet, dedicated links or multicast systems using standard file transfer methods.
Notes and Issues	Some datasets represents challenges concerning data volume or data access (e.g. offline tape storage). Those datasets should be served through some asynchronous service.
Last Updated	16 June 2008
Last Updated By	Beatriz Martinez Garcia

The typical scenario is included in "Use Case external DCPC 8" and "Use Case external DCPC 9".

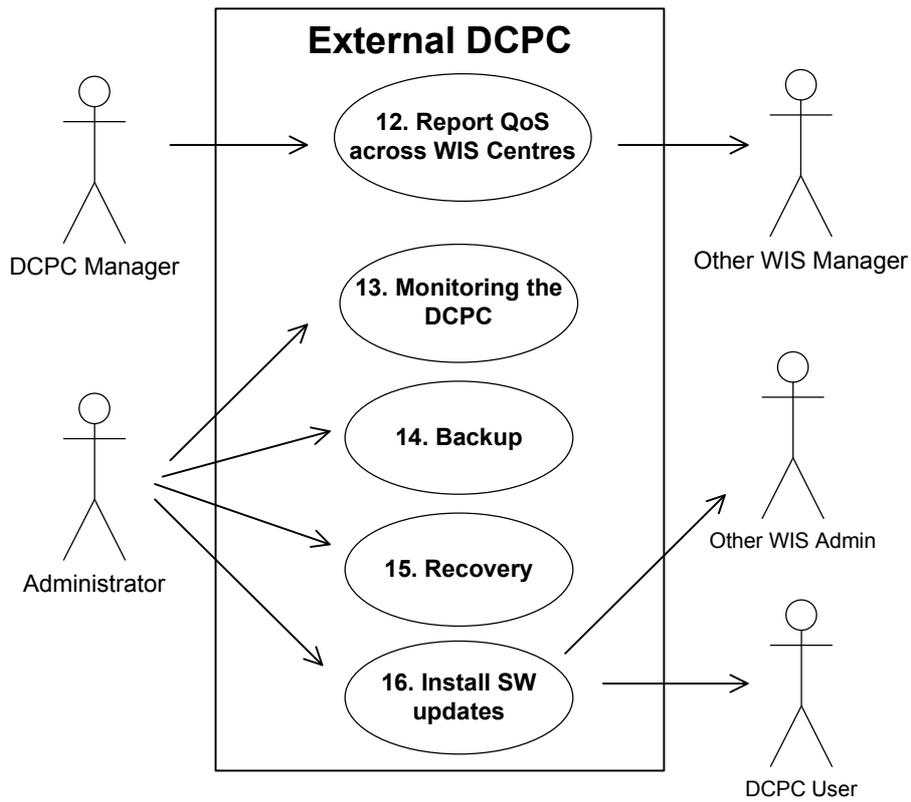
Use Case External DCPC 11, Provide Dissemination Metadata

Use Case Goal	Metadata concerning delivery specifics of subscription(s) to data and products from a DCPC are created or updated in the Dissemination Metadata Catalogue
Actors	Subscription Registrar
Pre-Conditions	(1) The Subscription Registrar is authorized to update the Dissemination Metadata Catalogue for the given subscription(s) (2) The Subscription Registrar has the necessary information and the ability to update the Dissemination Metadata Catalogue for the given subscription(s) (3) The Dissemination Catalogue Publisher (DCPC) supports mechanisms for authorized Subscription Registrars to update the metadata for the given subscription(s)
Post-Conditions	The Dissemination Metadata Catalogue has changes made by the Subscription Registrar
Normal Flow	1. The authorized Subscription Registrar uses a mechanism supported by the DCPC to update the Dissemination Metadata Catalogue for the given subscription(s). 2. The DCPC maintains the updated Dissemination Metadata Catalogue.
Notes and Issues	As "Subscription Registrar" can act NCs or other DCPCs that share their Dissemination Metadata; as well as users/systems that subscribes to DCPC data or products (as in "Use Case external DCPC 9").
Last Updated	16 June 2008
Last Updated By	Beatriz Martinez Garcia

Typical scenario:



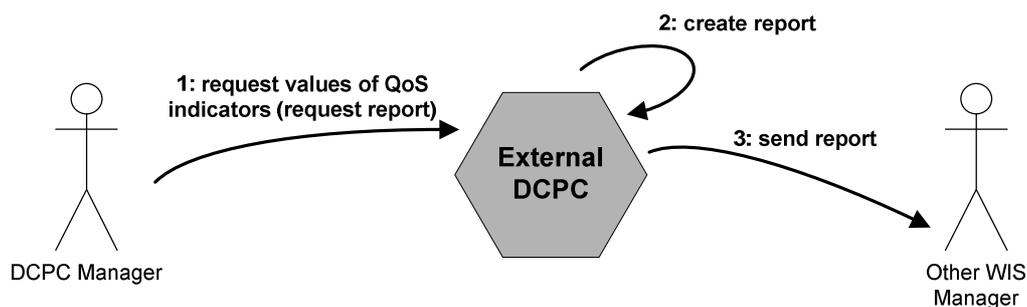
F.4.5 Quality of Service



Use Case External DCPC 12, Report Quality of Service across WIS Centres

Use Case Goal	Managers of DCPCs receive performance reports of operations against agreed quality of service indicators
Actors	DCPC Managers Other WIS Managers
Pre-Conditions	(1) Measurable quality of service indicators are agreed (2) Schedule of reporting and specifics of reporting formats are agreed
Post-Conditions	DCPC managers have performance information needed to manage WIS operations across the range of DCPC services
Normal Flow	On a schedule as mutually agreed, all DCPC managers send performance reports of operations against agreed quality of service indicators.
Notes and Issues	<ol style="list-style-type: none"> 1. It can be anticipated that WIS will eventually have agreements that address quality of service requirements. These should include data and network security as well as performance and reliability. Such agreements might be formalized into WIS standards, and perhaps Technical Specifications. Or, a looser set of conventions may simply document the variety of service level expectations reported across communities of WIS end-users. 2. Although not yet addressed in WIS system design, performance reports can be generated efficiently by having each WIS Centre upload its reports to a single analysis site within a fixed time window. 3. For an external DCPC the services related to SLA will those that deal with the data or products intended for global exchange within WIS (ex: QoS about data or products sent to the corresponding GIS, number of users subscribe to a data or product that is also available in another WIS Centre, etc...)
Last Updated	16 June 2008
Last Updated By	Beatriz Martinez Garcia

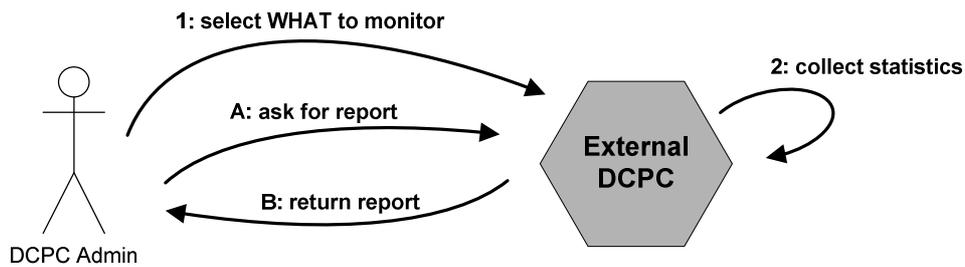
Typical scenario:



Use Case External DCPC 13, Monitoring the DCPC

Use Case Goal	Administrators of the DCPC are able to manage and monitor the DCPC and create reports.
Actors	DCPC Administrator
Pre-Conditions	Administrator is Authenticated and Authorized to monitor the DCPC
Post-Conditions	Monitoring reports have been created.
Normal Flow	<ol style="list-style-type: none"> 1. The Administrator chooses what to monitor with a view to detect and notify interested parties of failures. 2. The DCPC collects statistics about the parties being monitored. 3. The Administrator asks for a report on the statistics. 4. The DCPC returns the report requested to the Administrator.
Notes and Issues	Every WIS Centre will have its own way to monitor the system. It is not decided yet if a global monitoring view will be available for the whole WIS.
Last Updated	19 Mar 2008
Last Updated By	Beatriz Martinez Garcia

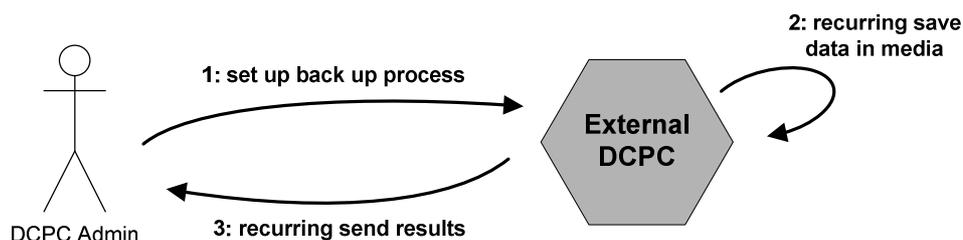
Typical scenario:



Use Case External DCPC 14, Backup

Use Case Goal	Administrators of the DCPC are able to backup WIS relevant information (only the ones necessary to keep/fulfill the interface to WIS services working).
Actors	DCPC Administrator
Pre-Conditions	(1) Administrator is Authenticated and Authorized to perform administrative tasks in the DCPC. (2) Data or metadata is available for backup.
Post-Conditions	Data backup complete.
Normal Flow	1. The Administrator sets up a backup process (what, when, ..). 2. The DCPC runs an automated process that backs up the data to media on a routine basis as necessary and inform the Administrator.
Notes and Issues	1. Every WIS Centre will have its own backup process. 2. The information/data to backup should include at least the data or products available at the DCPC, their corresponding metadata and user information.
Last Updated	01 April 2008
Last Updated By	Beatriz Martinez Garcia

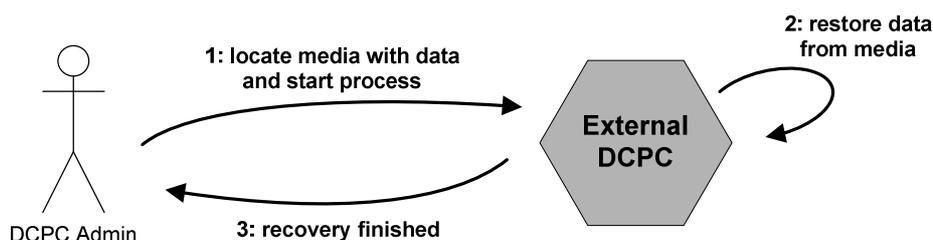
Typical scenario:



Use Case External DCPC 15, Recovery

Use Case Goal	Administrators of the DCPC are able to recover WIS relevant information.
Actors	DCPC Administrator
Pre-Conditions	(1) Administrator is Authenticated and Authorized to perform administrative tasks in the DCPC. (2) Media containing a previous version of the data or metadata is available (see "Use Case external DCPC 14").
Post-Conditions	Data restoration complete.
Normal Flow	1. The Administrator locates the last available version for the data on media and makes it accessible. 2. The DCPC runs a process that reads the data from the media and restores the data, informing the Administrator when finished.
Notes and Issues	Every WIS Centre will have its own recovery process.
Last Updated	20 Mar 2008
Last Updated By	Beatriz Martinez Garcia

Typical scenario:



Use Case External DCPC 16, Install Software updates

Use Case Goal	Administrators of the DCPC are able to update the software installed at the DCPC without decrease QoS level.
Actors	DCPC Administrator Other WIS Administrator DCPC User.
Pre-Conditions	(1) Administrator is Authenticated and Authorized to perform administrative tasks in the DCPC. (2) An update to the existing software is available.
Post-Conditions	Updated software has been installed.
Normal Flow	<ol style="list-style-type: none"> 1. The Administrator informs other WIS centre administrators and DCPC users about the coming update. 2. The Administrator stops the processes running with the existing software. 3. The Administrator installs the updated version of the software and restarts the software application processes. 4. The Administrator informs other WIS centre administrators and DCPC users about the successful installation.
Notes and Issues	<ol style="list-style-type: none"> 1. The installation process must contain a verification step testing that the upgraded version is working as expected. 2. If the installation/upgrade fails the previously operational version must be recovered for operational use
Last Updated	16 June 2008
Last Updated By	Beatriz Martinez Garcia

Typical scenario:

