estec

Keplerlaan 1, 2200 AG Noordwik. The Netherlands
+31-71-5656565

DOCUMENT

Earth Observation Guidelines for Interface Verification Requirements

Earth Observation Guidelines for Interface Verification Requirements v1.2.2.docx

Prepared by **Michele Zundo**
Reference **PE-TN-ESA-GS-319**
Issue **1.2.2**
Revision
Date of Issue **02-Sep-2013**
Status **Approved**
Document Type **Technical Note**
Distribution

European Space Agency
Agence spatiale européenne

APPROVAL

Title	Earth Observation Guidelines for Interface Verification Requirements
Issue 1.2.2	**Revision**
Author Michele Zundo. EOP-PEP	**Date** 02-Sep-2013
Approved by Pierre Viau, EOP-PE	**Date** 02-Sep-2013

CHANGE LOG

Reason for change	Issue	Revision	Date
First issue	1.0		17-Jun-2011
General cleaning (not distributed)	1.1		16-Sep-2011
Added Annex 1	1.2		01-Nov-2011
First issue new ESA doc template	1.2.1		15-Nov-2011
Editorial + RD update	1.2.2		02-Sep-2013

CHANGE RECORD

Issue 1.0	**Revision**		
Reason for change	**Date**	**Pages**	**Paragraph(s)**
First issue	17-Jun-2011	all	

Issue 1.1	**Revision**		
Reason for change	**Date**	**Pages**	**Paragraph(s)**
General cleaning (not distributed)	16-Sep-2011	all	

Issue 1.2	**Revision**		
Reason for change	**Date**	**Pages**	**Paragraph(s)**
Added Annex 1	01-Nov-2011	all	

Issue 1.2.1	**Revision**		
Reason for change	**Date**	**Pages**	**Paragraph(s)**
First issue new ESA doc template	14-Nov-2011	all	
Reworded requirement R-13	14-Nov-2011		Req R-13
Added Annex 2	14-Nov-2011	Annex 2	

Issue 1.2.2	**Revision**

Reason for change	Date	Pages	Paragraph(s)
Editorial in Change Record for 1.2.1	02-Sep-2013	2	
Updated version of RDs	02-Sep-2013	6	

Table of contents:

1 PURPOSE AND SCOPE

This TN contains a checklist for common requirements covering implementation, integrity and authentication features of any Ground System data interface, especially (but not only), using the Earth Observation File Format Standard, which affect and define the verification. It complements the ICD in such that it describes specific checks and provisions to ensure the robustness of the software system and a resilient implementation of mechanism exchanging data from both human and computer errors. It is assumed that file transfer is performed via standard FTP/SFTP/WebDAV/NFS protocol in case different transfer mechanisms are used the recommendations below should be tailored accordingly.

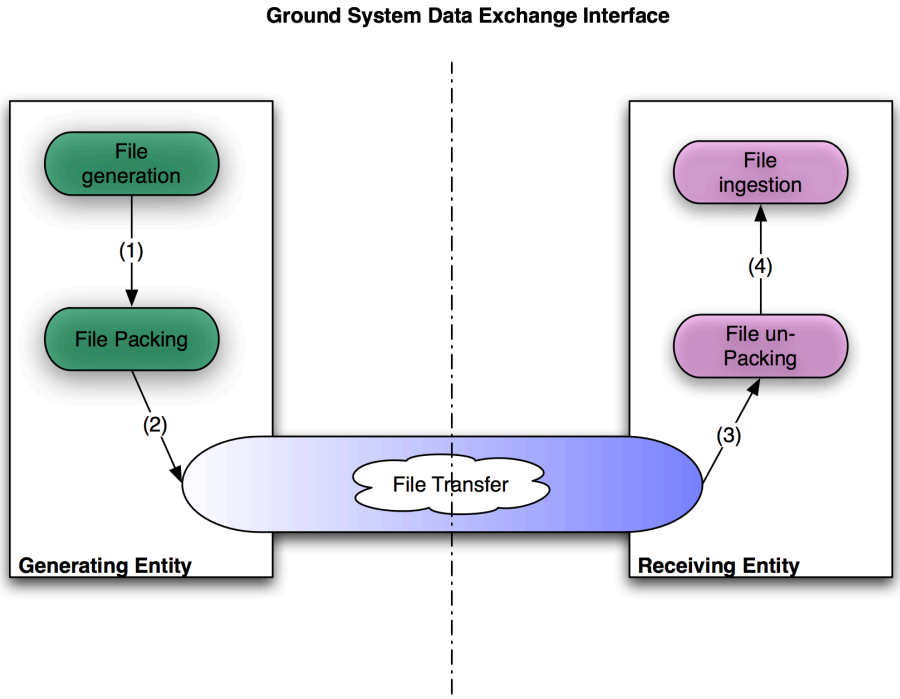

Fig 1. Typical File-based Data Interface in ESA EO Ground System

This TN indicates the verification and technical provision to be performed at both sides (originating and receiving) of the interfaces.

Requirements applicable only to file formatted as [FFSTD] are explicitly marked.

Requirement applicable to different part of interface refer to (1),(2), (3), or (4) of the Fig. 1 above.

I/F Requirement list shall be tailored depending on project needs and constraints. Annex 1 and 2 provides example/templates of common tailoring depending on type of interface and mission approach to confidentiality.

2 REFERENCE DOCUMENTS:

EO File Format Standard PE-TN-ESA-GS-000, version 2.0 final 03-May 2012 [FFSTD]
Handbook for EO XML and Binary Schemas, PE-TN-ESA-GS-121, version 1.6 [XMLSSTD]

3 GLOSSARY

Within the scope of this TN the following terms have the meaning described here below:

Authentication

Process to ensure that the received file has a certified originator (i.e. has been generated by a specific source). This process is implemented e.g. by a “signature” mechanism.

Integrity

Process to ensure that the file as generated is delivered intact to the recipient. (i.e not corrupted/affected during transport from originator to recipient) This process is implemented e.g. by “checksum” mechanism

Confidentiality

Process to ensure that even when physical file is available the information contained within cannot be accessed without authorisation. This process is implemented e.g. by mean of encryption mechanism.

Coherency check

Process ensuring that the semantically significant field of filename, headers and (optionally) of data field are consistent (e.g. validity period).

Format check

Process to ensure that XML headers are correctly formatted. This process is implemented e.g. by mean of a validating parser and schema.

Robustness
Feature of a receiving system which ensure its operation continue un-interrupted or gracefully degraded even in presence of erroneous/corrupted inputs.

4 REQUIREMENT CHECKLIST

4.1 Content, Integrity and Routing

R-01. The generating entity shall ensure, by software design, the coherency/identity between the content of the file and its filenaming especially when the latter has a semantic meaning (e.g. part of the name identifying validity, originator, version, etc) with the same information present inside the file.

R-02. [FFSTD] The generating entity shall ensure correctly format of all its generated XML files by:

a. Including schema according to [XMLSSTD] and in particular implement a strong version control on corresponding formats.

b. Ensure as much as possible that the allowed ranges/values within XML tags are specified via the XML schema.

c. Implementing a process using a validating parser that file is correctly formatted on both header and data block before packaging and transfer over interface to the receiving entity (i.e. at point (1))

d. raising an error in case discrepancies are detected

R-03. The generating entity shall ensure as much as possible the correct format of all its generated non-XML files (including TXT and binary data block if applicable) by:

a. define the method(s) and/or technique to allow verification (e.g. CRC, MD5, list of keyword)

b. implement corresponding automatic checks to ensure correctly format of all its generated files before packaging and transfer over interface to the receiving entity (i.e. at point (1))

c. raising an error in case discrepancies are detected

R-04. The generating entity shall ensure correct packaging has been performed by :

a. systematically monitoring the packaging process: e.g. for zip it shall ensure it completed without errors or re-invoking zip with -T flag on the generated file before tranfer (i.e. at point (2))

R-05. The generating entity shall ensure correct transfer of all files by:

a. systematically monitoring the output of the transfer process

b. raising an error in case problem is detected

R-06. The Receiving entity shall ensure correct reception of file by :

a. systematically monitoring the receiving process

b. verifying the completeness of the file

c. raising an error in case problem is detected

d. verify these error cases during integration and system tests

R-07. The ICD shall explicitely identify:

a. Retention Time (time after which the file is automatically deleted by the location used for the tranfer)

b. Clean-up policy (identifying who remove delete the files and when, e.g. Read and delete by receiving entity or read-only by receing entitity, etc)

R-08. The receiving entity shall :

a. implement the policies for file reception as per ICD (e.g. read-and-delete, retention time)

b. ensure that it is implemented in a robust way able to detect errors (e.g. preventing old files to be re-ingested in case clean up/deletion fails)

c. verify the robustness during integration and system tests

R-09. The receiving entity shall :

a. verify the correctness and completeness of the packaging by monitoring the extraction process (e.g. detecting unzip errors)

b. verify these error cases during integration and system tests

R-10. [FFSTD] The receiving entity shall sistematically verify the correct formatting of all the XML files by:

a. Implementing a process using a validating parser that file is correctly formatted on both header and data block (i.e. at point (4)) and the correct schema.

b. raising an error in case discrepancies are detected including values out of the expected range/values

c. verify these error cases during integration and system tests

R-11. The receiving entity shall verify as much as possible the correct format of all received non-XML files (including TXT and binary data block if applicable) by:

a. define the method(s) and/or technique to allow verification (e.g. CRC, MD5, list of keyword)

b. implement corresponding automatic checks to ensure correctly format of all received files (i.e. at point (4))

c. raising error in case discrepancies are detected

d. verify these error cases during integration and system tests

R-12. [FFSTD] The receiving entity shall implement an automatic mechanism to verify that the following information in the file are consistent/coherent/identical:

a. Information contained in Header

b. Information contained in Filename

c. Information contained in the data block (or body)

Note typical consistency checks to be performed are:

- *Identical Validity/sensing period in filename and header*
- *Identical version number in filename and header*
- *Identical Originating entity in filename and header*
- *Identical Destination satellite (or instance of it) in filename and header*
- *File class (TEST, OPER, etc) as per Mission specific tailoring in filename and header*
- *Data Block interval covered vs validity/sensing period (i.e. data in file falls within the declared time interval)*

R-13. [FFSTD] The Header constitutes the metadata identifying the file data therefore the routing of file within the originating and receiving system shall ensure that the header and data block are keept together as near as possible to the ingestion subsystem.

4.2 Authentication

R-14. The generating entity shall support authentication of the generated file at the receiving entity by computing (after packaging i.e. point (2)) the signature based on the packaged file and the private key. Both the file and the associated signature file shall be transmitted to the receiving entity.

Note: An example of implementation would be using a signature generated according to OpenPGP protocol defined in the RFC2440 (http://en.wikipedia.org/wiki/OpenPGP) and no encryption (e.g. with the GNU gpg software and key: DSA 1024 and no passphrase)

R-15. The receiving entity shall perform authentication of the received file at by using the file, its signature and the public key of the generating entity and reject any file failing it.

4.3 Confidentiality

R-16. The generating entity shall support encryption of the generated file at the receiving entity by computing (after packaging i.e. point (2)) the signature based on the packaged file and the private key and the encrypted file. Both the encrypted file and the associated signature file shall be transmitted to the receiving entity.

R-17. The receiving entity shall perform decryption of the received file at the by using the encrypted file, its signature and the public key of the generating entity and reject any file failing it.

5 ANNEX 1

This annex provides a guideline for defining criticality of different aspects of each I/F in case of Earth Explorer scientific missions. These guidelines can be used to tailor the list of requirements for a specific application and project. For other type of missions (e.g. operational) a similar guideline should be prepared by each Project and used to tailor the requirement list.

5.1 Criticality definitions

High if undetected anomaly could potentially result in:

- incorrect S/C commanding
- affect immediate S/C HKTM visibility at FOS
- endarge S/C safety
- any disruption S/C operation
- significantly disrupt E2E Mission output availability (product to users) especially for automatic ingestions
- disrupt E2E Mission output timeliness requirements (product to users)
- violation of Mission overall confidentiality rules/policy
- errors in planning/commanding interfaces with external entities (e.g. instrument provided/operated by other Agencies)

Medium if undetected anomaly would result in:

- violation of priority for privileged-users data access (e.g. calVal users, PI, etc)
- significant effort for recovery (e.g. resulting in rescheduling, re-processing, db cleanup, investigations, meetings, etc)
- incomplete/partial implementation of user data requests
- incomplete set of data for S/C monitoring at FOS

5.2 Typical I/F Criticalities for scientific missions (e.g. Earth Explorer)

Interface Type	Authentication	Integrity	Confidentiality	(Coherency, Format, etc) Robustness
Mission Planning Files (PDGS -> FOS)	High	High	Low	High
Mission Planning Files (FOS -> PDGS)	Low	Medium	Low	Medium
TC Files (User -> FOS)	High	High	Low	High
HKTM TM Files for operation (Station -> FOS)	Medium	High	Low	High
HKTM TM Files for long term monitoring (Station -> FOS)	Low	Medium	Low	Medium
HKTM TM Files for long term monitoring (Station/FOS -> PDGS)	Low	Medium	Low	Medium
Input to Mission Planning (user -> PDGS)	Medium	Medium	Low	Medium
OBSW Files (Provider-FOS)	High	High	Medium	High
Commanding Files from external entities/Agencies (Provider-FOS)	High	High	Low	High
Science TM Files (Station -> PDGS)	Low	High	Low	High
Science Downlink Planning Files (PDGS -> Station)	Medium	High	Low	High
Dynamic AUX Files: Meteo, Temperature, etc (Provider-PDGS)	Low	High	Low	High
Static AUX Files CCDB, instrument characterisation (Provider-PDGS)	Low	Medium	Low	High

6 ANNEX 2

This annex contains a template of the table to be tailored by the Project for each interface.

6.1 Tailoring Template (per each I/F)

I/F	***Interface ID***	
Requirement	**Applicable (YES/NO)**	**Comment**
Content, Integrity and Routing		
R-01		
R-02		
R-03		
R-04		
R-05		
R-06		
R-07		
R-08		
R-09		
R-10		
R-11		
R-12		
R-13		
Authentication		
R-14		
R-15		
Confidentiality		
R-16		
R-17		