Technical Environment and Standard Operating Procedures of the Publications Office

1 Purpose of the Document

This document provides an overview of the technical environment of the Publications Office as well as some general rules linked to the technical organisation of the Publications Office and applicable to all applications hosted at the Publications Office.

2 Disclaimer

The information contained in this document reflects the situation in force at the Publications Office at the time of writing and is subject to change.

The Publications Office can not be held liable for the consequences of any reliance on the information provided or for any inaccuracies in such information and it does not commit the Publications Office regarding the future evolution of its data processing and network environment.

The content of this document may vary in relation to any particular project. In particular, the environment to take into consideration for a specific project/purchase order – especially the exact software versions – will be determined at the very beginning of the project. This also includes the rules to apply by both parties in order to modify this environment.

The Publications Office strongly advises the contractor to ask for clarification should there be any doubt about the contents of this document. If requested by the contractor, a meeting can take place at the very beginning of the project to answer questions and provide examples of the expected documents.

3 Technical Environment of the Publications Office

3.1 Introduction

The Publications Office makes a distinction between systems used for office automation and administrative information systems on the one hand and systems used for production on the other hand. The quality of service and the constraints of availability are tighter for the production systems, since external partners with contractual agreements are already in place. Another important difference between these two types of information systems is linked to their architecture. The production information systems are usually spread over several servers and include complex production chains with processing on all nodes, whereas administrative and office automation systems are simpler and frequently use a one-to-many relationship between a server and its clients.

However, the same basic infrastructure is made available for both types of information systems, as described hereafter.

3.2 Application Architecture

The hardware and software architecture to use within a project is generally proposed by the contractor and should be compatible with industry best practices and the technical environment described in this document. The architecture must take the total cost of ownership into account and ensure the sustainability of the infrastructure and the technical environment described in this document. This architecture has to be validated by the Publications Office before implementation.

For the design of this architecture, the contractor has to take the following aspects into consideration:

The Publications Office has deployed a DRP (Disaster Recovery Plan) which makes use of two different geographical sites and is based on the following principles:

- The DRP conforms to the Contingency Plan of the Publications Office
- The data replication between the two sites is synchronous
- Both sites are hosting "active" applications

UNIX is the recommended environment for production systems while office automation systems are normally hosted on Windows servers.

The Publications Office fosters professional methods of managing systems and therefore implements monitoring and measuring tools for systems and produces statistics on the use of computing resources and on the quality of service provided.

The Publications Office promotes the implementation of a three-tier architecture, using thin clients, application servers and mainly Oracle databases for reasons of performance, scalability and flexibility.

3.3 Data Exchange

In general, application processes exchange data either by email, web services, or by Managed File Transfer (MFT) using dedicated tools.

The possibilities for file exchange mechanisms take into account whether the exchange takes part with external partners or concerns only internal exchanges of data.

Data exchanges that involve a network that is external to the European Commission must be secured (by using a secure and encrypted file transfer protocol, for example SFTP).

Managed File Transfer is the exchange of data (files) between applications – possibly running on distinct servers; the tools in use allow the triggering of processes based on the arrival of a file in a predefined directory (pre- and post-processing). The tools use FTP or SFTP as underlying protocol for file exchanges with external parties, internally a proprietary protocol is used. Due to the asynchronous character of file exchanges, the order of files exchanged is not guaranteed; if sequencing is an issue, it must be managed at application level.

The Publications Office strongly advises the contractor to ask for practical implementation guidelines before starting any development that could require integration or interaction with the MFT tools.

Files that have to be transferred between disparate systems should follow the **POSIX.1-2008 portable filename character set**; incompatibilities between different platforms and operating systems are to be avoided, e.g. avoid using reserved keywords of operating systems, the space character and the ampersand in files transferred between systems.

Direct dependencies between servers (e.g. NFS mounts, database links, etc.) are generally prohibited.

3.4 Security Provisions

A separate document describing the OP Minimum Security Requirements is attached to each Call for Tender for information processing system and/or services issued by the Publications Office. Any application, system or service that is introduced at the Publications Office has to comply with these requirements.

3.5 Other Provisions

The Publications Office promotes the virtualisation of services and the use of abstraction layers in order to increase flexibility. This implies in particular that:

- web-based applications must allow the deployment and the correct operation behind any http reverse proxy chain.
- applications must allow virtual hosting i.e. the binding of the application to only some of the IP addresses/hostnames of a multi-homed server
- applications must allow easy integration in the DRP of the Publications Office
- applications must be compatible with an MS Windows 2003/2008 terminal server architecture
- if the application depends on network services like DNS or LDAP, the server name or the IP address should not be hard-coded but should remain configurable

Before being put into production, all of the Publications Office's core business applications, which are often interdependent, are tested for incompatibilities on dedicated machines.

Authentication mechanisms must use the available centralised directory server infrastructure (ECAS server of the Commission, Active Directory server of the Publications Office,…)

Data archiving and purging mechanisms have to be foreseen and implemented so that data volume growth does not degrade application performance nor backup/restore

operations. Data management should in general be separated from modifications to be done of the application binary code or configuration files.

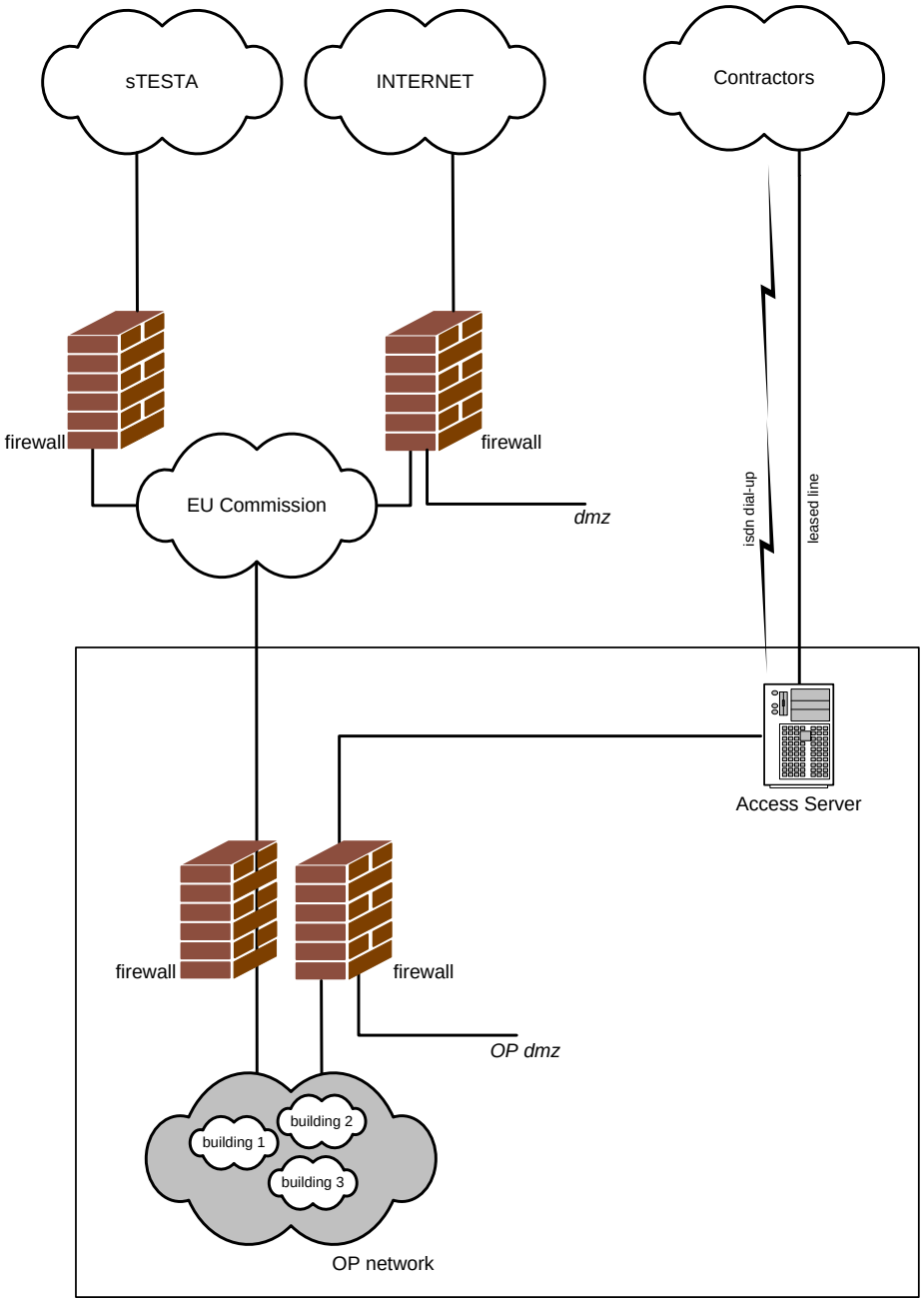
On the hardware side, the technical data processing infrastructure is currently made of several components that can be grouped into the following categories:

- Network and telecommunications
- Storage, backup and archiving systems
- Workstations and peripherals
- UNIX servers
- Windows servers

Details on these categories can be found in the relevant sections later in this document.

4 Network and Telecommunications

The Publications Office's staff is spread over several buildings. The Wide Area Network use leased lines, either over dark fiber high speed connections or connections to PSTN. The Publications Office's buildings use a common cabling system for the telephone as well as for the TCP/IP network for data. This structured cabling system uses copper connections category 5 (or higher) to desktop computers and high-end servers with a throughput of up to 10 Gbps and optical fiber connections for the backbone. Both networks deal with about 1 000 telephones and more than 1 500 Ethernet devices, and will continue to grow with potential new sites.



Leased lines are used for connections with the contractors working for the Publications Office and requires a signed security convention.

The most common application for the Publications Office remote access service is file transfer (FTP). Files are transferred via a FTP gateway installed in the Office DMZ.

The TCP/IP network is also interconnected with the network of the European Commission that is connected to the Internet and to the sTESTA network (Trans-European Services for Telematics between Administrations). The sTESTA network allows the Publications Office to establish private connections with most of the national Administrations of the EU Member States and most of the EU Institutions. FTPStore is a service offered by DIGIT/Commission for sending and receiving files over the public Internet or via the sTESTA network. FTPStore is not offering any notification or monitoring of file movements.

All accesses that make use of the network of the European Commission (e.g. Internet accesses) have to comply with the general security rules of the Commission. This also implies that all mentioned networks are interconnected through stateful inspection firewalls. In particular, outbound direct internet access is NOT allowed. Applications that require internet access have to be "proxy aware".

Fax services are carried out by redundant Windows servers and are part of the automatic production chains in the daily publishing process. The Publications Office has reached a high level of integration of telephone and IP-messaging services.

5 Storage, Backup and Archiving Systems

5.1 Storage

The Publications Office application data is centralised on SAN and NAS storage arrays for production and test systems.

For disaster recovery purposes data is online replicated in two data centres. On SOLARIS Cluster platforms the method for replicating the data is host mirroring. For Windows, Linux and VMWare platforms storage mirroring (synchronous) is implemented. The Storage Area Network is available in both data centres and all servers are configured in two separate fabrics. The inter-building links use DWDM communication channels.

About 250Terabytes of online storage capacity is available to end-users and applications. This amount is steadily growing due to the increased usage of electronic documents in the Publications Office; the increase rate is about 30% per year.

It's the aim to implement and realise a hierarchical storage management policy and infrastructure matching the Publications Office's business data requirements.

5.2 Backup: General Principles

The backup and restore service is built upon EMC NetWorker family software with EMC Data Domain disk libraries using the DDBoost protocol on a 10GB Ethernet network infrastructure. The architecture is designed to be redundant between both data centres, using cloning technologies. To enhance backup/restore performance, source based client deduplication is implemented on all server platforms. The current backup policy and procedures are described in the next section.

5.3 Backup: Current Policy and Procedures

5.3.1 Categories of Backup Jobs

The following backup jobs are distinguished:

- Full backup: backup of all data.
- Level backup (differential backup): backup of all data changes since the last lower level backup (full backup corresponds to level 0). Only one level is currently defined. Thus, level backups are always performed with respect to a full backup.
- Incremental backup: backup of data changed since the last backup, independently of its type.
- Synthetic Full backup: construct full backup from previous incremental backups

5.3.2 Backup Policy

- The jobs are scheduled between 8 p.m. and 5 a.m. The effective backup might start only after the scheduled pre-processing jobs (e.g. database snapshot) have been finished.
- Full backup jobs are generally run once per week and are distributed between all days of the week.
- Level jobs (i.e. differential jobs) are run 4 times per week between Monday and Friday every day the full backup job is NOT run.
- Incremental jobs are run once a day, except the day of full backup.
- The browse policy (direct access to file and directory information of the backed up file systems) and the retention policy are generally set to 60 days for production data sets. The retention period for all test/development data sets is 30 days.
- Backups on Data Domain devices stay online for the duration of the retention period; after the retention period expires, the Data Domain disk space used is freed
- Deduplication of data is used on the client server
- Compression is used on the Data Domain disk library
- Backed up/Cloned tapes are removed regularly by the computer centre operators and placed in the safe.
- Backup/cloning sessions are bi-directional; they are either initiated from the main data centre to the Disaster Recovery Data Centre or from the DR DC to the main DC.

5.3.3 Backup of Oracle Databases

One or a combination of the following techniques is used:

- **Logical database backup:** Oracle export dump files are generated while the database is in restricted access mode. These files are written on the file system of the corresponding servers. The database is then stopped and backups of the server file systems are made within the global backup framework.
- **Physical cold backup:** The database is stopped and backups of the server file systems are made within the global backup framework.
- **Physical hot backup:** An open database backup is done
- **RMAN** (Oracle recovery manager): All standard features of RMAN are used.
- **"Freeze"/Snapshot techniques:** In order to limit the unavailability of the database during the physical cold backup, the database is stopped only during the time needed to make a "freeze" or a snapshot of the file systems hosting the database. The "freeze" or the snapshot is then available for backup or restore purposes.
    - A **snapshot** consists in attaching an additional mirror volume for the desired directories and to make a synchronisation between the additional mirror and the mirrored volume.
    - A **"Freeze"** consists in keeping the state of a file system at the given “Freeze” time by means of a second file system with exactly the same directory structure. Prior to any modification of the "frozen" file system, the unmodified data is copied to the second file system. By combining both file systems, the “Frozen” state is always available.

5.3.4 Backup Implementation

It is the responsibility of the Publications Office to define the objectives to reach in terms of availability/unavailability of the application.

Based on these requirements, the contractor must define the backup procedures to implement in order to fulfil the requirements. Ideally, the contractor must base these backup procedures on techniques the Publications Office's staff is familiar with (see contents of this appendix).

If the wishes of the Publications Office in terms of availability cannot be satisfied with techniques the Publications Office's staff is familiar with, the contractor must provide a full description of the procedures and techniques to use so that the implementation by the Publications Office's staff could happen smoothly.

5.4 Archiving: General Principles

Within the objective to reduce costs and to create a tiered data protection regime, data which is not modified often is archived out of the primary storage arrays.

Archiving policies are in place. The archiving system is moving the target data towards dedicated archiving storage arrays. For disaster recovery purpose the archived data is replicated between both Data Centres.

In the future, the Publications Office will expand its archiving strategy for in-house developed application datasets.

5.5 Archiving: Current Policy and Procedures

5.5.1 Categories of Archive Jobs

The following archive jobs are distinguished:

Legal-internal structured/unstructured contents

- On demand: archiving data in specific pools with retention periods of 5,10,15 years and beyond
- Scheduled: e-mail /file service monthly policies
- Incremental: user administrators can post data into dedicated archiving directories having different retention periods

Unstructured contents

- Global Cloud enabled archive available for multiple applications accessible internally, externally or hybrid.

5.5.2 Archive Policy legal structured contents

- All archived data stays online and cannot be modified, neither deleted during the defined retention period
- Once the retention period expires , it's the user administrator responsibility to delete the data
- All archived data is tiered out of the primary storage towards specific archive storage arrays
- For disaster recovery the archived data is replicated between two sites
- After archiving, only data file relationships are backed up within the normal backup policy

5.5.3 Archive Policy for cloud enabled archive

- Regardless of the physical location it simply call up an http(http/s) address
- Access methods include REST (Representational State Transfer) /SOAP (Simple Object Access Protocol) Web services (external) as well as CAS and traditional file system access methods CIFS/NFS/IFS (internal).
- Can share storage resources across securely isolated applications and users with self-service access options
- Multiple replicas of the content are accessible across different geographies
- Content tearing policies automatically migrate, retain or delete data

5.5.4 Archive Implementation

It is the responsibility of the Publications Office to define the objectives to reach in terms of availability/unavailability of the archived data.

Based on these requirements, the contractor must define the archive procedures to implement in order to fulfil the requirements. Ideally, the contractor must base these archive procedures on techniques the Publications Office's staff is familiar with (see contents of this appendix).

If the wishes of the Publications Office in terms of availability cannot be satisfied with techniques the Publications Office's staffs is familiar with, the contractor must provide a full description of the procedures and techniques to use so that the implementation by the Publications Office's staff could happen smoothly.

Following products are used:

Product name	**Service**	**Hardware**
SourceOne	email	EMC Centera
CTA (cloud tearing appliance)	file sharing (CIFS/NFS/mixed)	EMC Centera
Atmos	long-term archiving - cloud enabled archive	EMC Atmos
Atmos -VE	Proof of Concept and development	shared storage
on demand	Data Centre	CD/DVD RIMAGE robot library

6 Workstations and Peripherals

In terms of software, the standard configuration for the workstations is the following:

Type	Product/Version
Operating system	MS Windows Seven 64b
Office automation suite	MS Office 2010 SP2
Web browser	MS Internet Explorer 8 & 9 (with 128 bits encryption) Firefox 24.6
XML tools	XMLSpy (development) XMetal (Authoring) MS XML 4.0 & 6.0
Reporting tools	Business Objects 6.5
Mail client	MS Outlook 2010 SP2
Connection middlewares	Oracle NET 10G
Anti-virus	McAfee VirusScan 8.8 + Antispyware
Application Locker	Win 7 Applocker: Software Restriction & Policies feature; Soft should be installed and operate from C:\Program Files or if not possible it should contain a digital signature.
BitLocker	Hard Drive encryption on Laptop.
Application Virtualization	Microsoft Application Virtualization (App-V) Client 5.0 SP1 + ThinApp
Miscellanous	Adobe Flash player 14 Shokwave 12 Java V 1.6 & 1.7 MS Dot NET 4 PowerBuilder client 2.0

Some other local production tools (Visio, Microsoft Project...) could also be found on the workstations as well as more specialised tools which are used for publishing (Adobe Photoshop, Adobe Acrobat Pro 8/ Pro 9 and Reader 10, Adobe CS5/5.5, QuarkXPress ...).

For security reasons, the Publications Office must sometimes apply hotfixes to ALL workstations.

In terms of hardware, the workstations are ranging from Pentium E6300 Dual Core 2.8 GHz to Pentium G3420 Dual Core 3.2 GHz/ with 4 to 8 GB of memory. Various types of peripheral equipment are also installed, such as local scanners, CD burners, etc.

A small number of workstations are UNIX-based or Macintosh-based (for DTP). In terms of hardware, the 12 MAC are ranging from 7 MAC PRO, 4 iMAC and 1 MacBook Pro.

Type	Product/Version
Operating system	MAC OS Snow Leopard; MAC OS Lion; Mac OS Mavericks
Office automation suite	MS Office 2011
Web browser	Safari, Firefox
Mail client	MS Outlook 2011
Anti-virus	McAfee VirusScan 9 + Antispyware
Remote control	RDC for MAC Client
Backup Product	Legato networker; Carbon Copy Cloner, Time Machine
Network	All Mac are connected to the Windows AD and Domain + There is a Mac Server for files and application sharing (Portfolio)
Miscellanous	Adobe Creative Suite CS5.5/6; Indesign CS5.5 + K4Plug-in/6; Incopy CS5.5/6, ACROBAT Pro10

All workstations are clients of the LANDesk Workstation Manager server V9, which allows remote control and software/hardware inventory.

Local data on the workstations is not backed up (no personal local drive) and users are therefore encouraged to use only shared resources for storing professional valuable/persistent information.

7 UNIX/LINUX Servers

The two Publications Office's datacentres host more than 50 Oracle servers/domains such as Oracle Enterprise servers (M5000, T4, T5220/T5240) and Sun Sunfire servers (V210, V890, SF25000). These servers host more than 140 virtual servers (Oracle container/zone).

In addition to the Solaris servers, some HP x86-64 servers run Red-Hat Enterprise Linux 6.4. Some of these host KVM-based virtual machines.

Solaris **SPARC 64 bit** is the production baseline Operating System; Red-Hat Enterprise Linux is mainly used for the monitoring and the indexing layer (IDOL).

The trend is to move smoothly the Solaris/SPARC baseline to RedHat/x86.

The main products used are described below and the usage of ReadHat/x86 is subject to discussion and approval by the Publications Office.

Type	**Product/Version installed**	**Product/Version recommended for new projects**
Operating system	Solaris 10 in zone/container	Solaris 11 in zone/container
DBMS	Oracle from 10g to 11g R 2 ADABAS 5.1	Oracle 12c Character set: AL32UTF8
Text retrieval	Oracle Intermedia/Context	Oracle Intermedia/Context
Web servers	Apache 2.x	Apache 2.x
Application servers	Apache Tomcat 5-6 JBoss 5 Oracle WebLogic 10	Apache Tomcat 7 JBoss 7 Oracle WebLogic 12c[1]
ERP	Oracle Financials 11i	Oracle Financials 11i
Programming languages	Java 1.5.x/1.6.x Natural 6.2	Java 7 (1.7.0_80)
Scripting languages	Perl 5.6 sh/ksh	Perl 5.10 sh/ksh
Workflow/Document management systems	EMC[2] Documentum Content Svr 6.6, 6.7 (incl. CRS/DTS module)	EMC[2] Documentum Content Svr 7
Reporting tools	Business Objects WebI 2.7	Business Objects XI 3.1
Enterprise architecture and business modelling tool	ARIS platform: Business & IT Architect (IDS-Scheer) v7.1SR 8 or higher	ARIS platform: Business & IT Architect (IDS-Scheer) v7.1SR 8 or higher
Search and index tools	HP Autonomy IDOL 7.5	HP Autonomy IDOL 7.6
Web Semantic OWL/RDF	Oracle Semantic Technology 11.2.0.3	Oracle Semantic Technology 11.2.0.3
Web analytics tools	Webtrends Analytics v8.7d Marketing Warehouse v4.0 (Windows 2008 version)	Webtrends Analytics 9.2 Visitor Data Mart 9.2
XML related tools	XSV (XSML Schema) RXP (DTD)	XSV/XERCES (XML Schema) RXP (DTD)

[1] The use of WebLogic must be justified and must be validated by the Office

	SAXON (XSLT)	SAXON/XALAN (XSLT)
Middleware	Managed File Transfer tools	Managed File Transfer tools
Monitoring, measurement and production management tools	Nagios/Centreon Oracle Enterprise Manager – Grid control EMC ControlCenter Sextant MPI 9.5	Centreon Oracle Enterprise Manager – Grid control EMC ControlCenter Sextant MPI 10
Backup	Networker 8.0.2.5	Networker 8.1 SP1
Build tools	Apache Maven 1 & 2, Apache Ant™ 1.6/1.7/1.8	Apache Maven 2, Apache Ant™ 1.8
Source code management	Apache™ Subversion® (SVN) 1.6.2	Apache™ Subversion® 1.6.2
Workflow management	Atlassian JIRA 4.4	Atlassian JIRA 4.4

More than 120 Oracle instances (production + test) are currently installed for about 60 different applications.

All servers are connected to the storage via the SAN. Oracle cluster is used across the two datacentres.

7.1 Standard File System Organisation on UNIX Systems (Directory Structure)

In order to ease the co-existence of applications on the same server and to ease the potential move of an application to another server, applications are generally installed under **/applications/*application_name*/** where ***application_name*** refers to the name of the application.

This level is then subdivided into:

- /applications/*application_name*/users which is itself subdivided into:
  - **/applications/*application_name*/users/system**: directory simulating the root directory for the application. Specific products used by the application are installed here (e.g. the web server is installed under /applications/*application_name*/users/system/apache/, the application server is installed under /applications/*application_name*/users/system/tomcat/).
  - **/applications/*application_name*/users/oracle**: Oracle application, oracle environment, and oracle admin directory.
  - one or more directories **/applications/*application_name*/users/*user_name***: home directories of the users *user_name* used by the application. These directories are linked to **/home/*user_name***. Generally, there is only one directory **/applications/*application_name*/users/*user_name*** and ***user_name*** is identical to ***application_name***.
- **/applications/*application_name*/xchange**: root of interfaces (in case of exchange of data with remote applications). The following specific structure is used:
  - /applications/application_name/xchange/import/remote_application_x/(sublevel if necessary) for incoming data and
  - /applications/application_name/xchange/export/remote_application_x/(sublevel if necessary) for outgoing data

where ***application_name*** refers to the name of the application and ***remote_application_x*** refers to the name of the remote application.

e.g. /applications/eub/xchange/eudor/in is used for the data flow exchange from eudor to eub.

/applications/eub/xchange/gescom/gcb/out is used for the data flow exchange from eub to the gcb part of gescom.

- **/applications/*application_name*/oradata**: Oracle datafiles.
- **/applications/*application_name*/oraexp**: Oracle exports
- **/applications/*application_name*/oralog**: Oracle online archive logs.

Deviations from this description are possible but the Publications Office must first validate the deviations.

```
/applications
 |
 -- /application_name
     |
     -- /users
     |   |
     |   -- /system    (installed by Publications Office)
     |   |   |
     |   |   -- /init.d                              Start/stop scripts
     |   |   |
     |   |   -- /product_1                           (e.g. Tomcat, Apache, ...)
     |   |   |
     |   |   -- /...
     |   |   |
     |   |   -- /product_n
     |   |
     |   -- /oracle                                  Oracle binaries
     |   |
     |   -- /user_name_1                             (link to /home/user_name_1)
     |   |
     |   -- /...
     |   |
     |   -- /user_name_n                             (link to /home/user_name_n)
     |
     -- /oradata                                     Oracle data files
     |
     -- /oraexp        (if required)                 Oracle export
     |
     -- /oralog                                      Oracle logs
     |
     -- /data_1        (e.g. Documentum file store)  application data
     |
     -- /data_...      (if required)                 application data
     |
     -- /data_n        (if required)                 application data
     |
     -- /xchange
         |
         -- /import/remote_application_1
         -- /export/remote_application_1
         -- ... other interfaces ...

(The names of the different file systems are marked in bold)
```

8 Windows Servers

The Publications Office computing centre hosts about 200 MS Windows servers in a Windows 2003 R2 Active Directory domain. Some servers are virtual machines running on VMware/vSphere. All new physical servers are 2 or 4 CPU servers. Some are installed in cluster mode (for critical data and processing).

Besides standard functions like user authentication, roaming profiles, home directories, shared drives (public/group) and print services that are spread over several servers in order to improve reliability and performance, the Windows servers also host services like email (Exchange 2007), fax gateways, Share Point 2007, standalone applications and other small information systems (in-house developments, automated tasks using Microsoft Office products, small SQL server DB, IIS servers with Coldfusion, etc.).

Type	**Product/Version installed**	**Product/Version recommended for all new developments**
Operating system	MS Windows 2008 Server standard edition/enterprise edition	MS Windows 2008 /2012Server standard edition/enterprise edition
OS virtual servers	VMware vSphere 5.X	VMware vSphere 5.x
DBMS	MS SQL Server 2005/2008	MS SQL Server 2005/2008/2012
Intranet / Collaborative	SharePoint 2007	SharePoint 2007/ 2013
Web servers	IIS 7.5	IIS 7.5
Application servers	ColdFusion MX 8/9/10	ColdFusion X 8/9/10
Programming languages	Visual Basic .Net	Visual Basic .Net
Mail servers	MS Exchange 2010	MS Exchange 2010/2013
Reporting tools	SCOM2012 / PROMODAG	SCOM2012 / PROMODAG
Backup	Networker 7.5 SP1	Networker 8.0.2.3
Archiving System	Source One / FMA	Source One / FMA

For business critical reasons, Windows clusters host the Exchange server with about 1400 mailboxes, the shared drives and the disk spaces accessible to all end-users. All production data is stored on the SAN.

Regarding security on the server side, anti-virus checking is performed on the Microsoft Exchange mailboxes and regularly on file systems.

9 Standard Operating Procedures

This section provides information on the operational procedures and standards of A4 Infra/Ex (the Exploitation section of the Infrastructures unit of the Publications Office).

9.1 Management of Bug Reports and Change Requests

Contractors and suppliers must propose procedures that specify how to manage bug reports and change requests. These procedures must allow the unambiguous identification of every bug report and change request. The Publications Office hosts an instance of the Jira issue tracking product that is accessible from the internet and may be used for this purpose.

9.2 Software Deliveries

The Publications Office receives software deliveries (application releases, updates and patches) from contractors to be installed in its computer environment. Subversion was selected as the tool to ensure that software deliveries are received in a correct and structured way. Apache™ Subversion® (SVN) is a version control system that manages revisions of files and directories and keeps a history of changes.

A separate document (Software Delivery Integration and Source Code Management, part of the tender specifications) describes the role of Subversion (SVN) in software delivery and installation in more detail, and particularly how it integrates other procedures in force at the Publications Office.

The Publications Office reserves the right to measure the quality of software deliveries it receives from contractors and suppliers, based on agreed-upon criteria, and reject any software delivery that does not fulfil these quality criteria. These criteria should be defined and validated in the project kick-off meeting by the different parties.

The Publications Office monitors the compliance of software deliveries with contractual obligations that arise as part of this contract; non-compliance with contractual obligations concerning the delivery of software may lead to rejection of the delivery. The compliance with standards and procedures will be measured and recorded and feedback will be given to the contractor, who is obliged to take these remarks into account for subsequent deliveries.

The Publications Office reserves the right to request information from contractors and suppliers concerning the development and delivery process. To this end, the contractor may be required to fill in a set of templates that will enable the Publications Office to gain insight into how the contractor complies with industry standard best practices concerning software development processes.

The Publications Office will measure metrics of the source code delivered in a process based on automated tools and on request deviating results must be justified or corrected by the contractor.

A software delivery can concern either a full installation or a partial installation that needs to be installed over an existing installation, for example as part of a patch or a hotfix. It should be clearly indicated whether a delivery concerns a full or a partial installation to be able to estimate the effort required. The installation instructions must be customised and targeted to the particular installation.

Application software delivered to the Publications Office by the contractor shall comply with the following rules:

- The contractor must define a detailed and **unambiguous numbering scheme** and use it for each software delivery.
- The delivery should contain **the source code of the application and the executable binary code** that can be deployed and installed by following the installation instructions.
  - Please note that if the contractor makes the source code available in a way that the Publications Office is able to compile the application binary files from it, the resulting binaries will be used for the installation instead and the contractor does not need to deliver the executable binary code.
- Each delivery that contains the source code of the application shall include a **build procedure** detailing how to build the executable code from the source code. The build procedure should contain a default target so that the build process can be automated.
- The first delivery of an application should be as complete as possible and include all required components; subsequent deliveries should only contain the updated components required for the current installation request.
- The delivery has to be uploaded to the **revision control system** of the Publications Office, which is currently based on Subversion.
- Each delivery shall include **installation instructions** (in electronic, editable format); the minimum contents of the installation instructions are further detailed in section *9.5 Installation Instructions*.
- Each delivery shall include a **release note** (in electronic format) containing the following information:
  - project/application name
  - unambiguous identification[1] of the version of the delivered software
  - for partial deliveries, the version of the application that is a prerequisite for the installation of the delivered package
  - for full deliveries, whether or not the installation has to take place on a clean environment
  - details on the changes or enhancements that are implemented with the delivered release
  - approximate uncompressed size of the delivery
  - a reference to the installation instructions (as defined in *9.5 Installation Instructions*)
  - information about test results and the test procedure
- Each delivery shall include a **TEST folder** containing all the necessary information to be able to verify that acceptance testing has been performed by the contractor before the software was delivered. This folder will contain:
  - test procedures and test cases executed
  - test data used
  - test results and/or execution report

9.3 Technical Tests

Before an application is put into production, the Publications Office will conduct specific technical tests to assess whether the application adheres to the operational requirements of being run and operated in its data centre.

[1] In accordance with the procedure defined in the approved quality plan

Depending on the results of these technical tests, the Publications Office reserves the right to reject a software delivery.

The contractor must foresee in the planning of the project a dedicated period of time for the execution of technical tests.

The technical tests will be performed by the Publications Office's staff in close collaboration with the contractor and based on the test procedures and test cases prepared by the contractor.

The contractor will prepare a report of the execution of the technical tests. The contractor will deliver this report to the Publications Office, together with the test data used. The test procedures and test cases will first be validated by the Publications Office.

The test procedures/test cases must allow validating at least the following elements:

- application start and stop procedure
- application backup and restore procedure (including consistency checks after restore)
- disk space usage
- location of the log files
- periodic operational tasks (data reorganisation, purging, archiving, indexing...)
- correct working of the interfaces
- virtualisation capability (suitability of the application to be moved from one server to another) in the context of disaster recovery (DRP) and high availability (HA)

The effectiveness of the procedures but also their efficiency will be tested. Their impact on the overall performance of the system will be evaluated too.

The test procedures/test cases must refer to procedures described in the System Operation Manual in order to validate this manual. The minimal contents of the **System Operation Manual** are described in section 9.6 System Operation Manual, the contractor is free to add any other information deemed useful.

For the execution of the technical tests the Publications Office uses monitoring and measurement tools listed in section 7 UNIX/LINUX Servers and section 8 Windows Servers.

The technical tests will be conducted with a significant amount of data in order to evaluate the impact of data volume on effectiveness, performance and efficiency of the application.

Special attention will be placed on the CPU, I/O and memory intensive and time consuming tasks like:

- data archiving
- data purging
- data reorganisation
- data consistency check
- data synchronisation
- data indexing
- statistics

9.4 Installations

For each application, two different environments are set up at the Publications Office, a test environment and a production environment. No software installation in the

production environment will be allowed without prior validation in the test environment.

The Publications Office strongly advises the contractor to set up at their premises a development environment similar (e.g. same OS version, same RDBMS version…) to the target production environment. It remains the responsibility of the contractor to make sure that the delivered software will run correctly in the technical environment of the Publications Office.

The installation of hardware, the operating system and other low-level software remains the responsibility of the Publications Office. The installation of application software is done by a dedicated team of integrators. If the complexity of an installation requires special expertise, the support or assistance of a technical expert of the contractor may be formally requested by the Publications Office; this support may be provided off-site (remotely by email or telephone) or on-site, depending on the specific situation.

Apart from the test and the production environments, the Publications Office may decide to set up an additional environment in order for contractors/suppliers to demonstrate that the software delivered can be installed and run correctly within the technical environment of the Publications Office while conforming to the requirements as described in the technical and functional specifications. In this case, the contractor will perform all installation and configuration tasks, with the assistance of technical staff of the Publications Office. The contractor will be granted the necessary access rights so that all necessary installation and configuration tasks can be performed. The granted access rights will be limited to those allowed by the security standards of the Publications Office. If the Publications Office requests the contractor to perform this demonstration, no associated costs will be reimbursed.

In order to ensure smooth installation and to evaluate the need for assistance or support by the contractor, the installation instructions should be delivered to the Publications Office 5 days before the official software delivery date, i.e. 5 days before the start of the official installation period.

The Publications Office uses a tool (Atlassian JIRA) to manage installation requests. Atlassian JIRA is a web-based application that can be accessed from the internet, which makes it possible for the contractor to monitor the progress of an installation request.

9.5 Installation Instructions

This section details the minimum contents of the installation instructions. The Publications Office will provide a template to help with creating the installation instructions on request.

9.5.1 General Conditions and Limitations

The installation document is a compulsory requirement for each delivery and has to provide step-by-step instructions to be executed, organised in a sequential and logical manner.

The installation instructions should contain all information necessary to perform the implementation tasks of the installation by an experienced system integrator without knowledge of the application.

Variables and parameters of the application that have dependencies with other software applications or the operating system should be made configurable. Variables

and parameters that need to be changed or adapted for a specific environment have to be clearly marked and if their values are unknown, sufficient information has to be provided that makes it possible to identify the required value.

The installation instructions have to clearly indicate who will be responsible for the execution of a particular task; complex actions should be broken down into smaller tasks; as far as possible, where different actors are involved in the execution of tasks, these tasks should be grouped together by actor to minimise a back-and-forth between different teams and to make the installation process more seamless.

9.5.2 Specific Conditions and Limitations

- the internal standards and procedures of the Publications Office pertaining to the installation and operation of software applications must be respected
- use of root user is prohibited; installations are to be done using a user identification that is specifically created to install and run the application; where root access is required during installation, this must be explicitly stated
- use of sysdba is prohibited where database access is required
- kernel and system parameters should not be changed
- hard-coded IP addresses have to be avoided

9.5.3 Pre-requisites

The installation instructions describe in detail the hardware configuration (agreed at the beginning of the project) and the software configuration that has to be in place before the installation is started.

- Minimum hardware requirements (CPU, memory, disk space, network throughput, etc) in compliance with the standards of the Publications Office.
- Software requirements (version, patches, specific configuration parameters, required modules, etc) for software required to install the software delivery, for example the operating system, tools, and other pre-requisite software. For some software, for example Oracle, some supplementary modules might be required. In case of specific patches or service packs required, the exact version of the concerned application or component that has to be in place before the application can be installed should be specified.

9.5.4 Application Interface/Data Flow

The installation instructions should give an end-to-end description of each data flow.

For each flow, the following elements should be described:

- origin (source server name and directory)
- destination (target server name and directory)
- protocol to be used (including user identification and password required if applicable)
- estimate of volume of data exchanged
- how data transfers are scheduled or triggered
- description of pre- or post-processing commands to be executed
- error handling (including users and email distribution lists to inform)

9.5.5 Application Installation

This section concerns the information that needs to be provided for the installation of the application software. In case the application architecture follows the client/server model, the installation instructions for client and server have to be kept separate.

- **Preparation**
  - Description of the tree structure of the installed files
  - List of all compressed and uncompressed files included in the delivery
  - List of file systems to create with sizing
  - Description of the logical and physical layout of the Oracle Database (if any), taking into account the following rules:
    - each database schema must contain at least two table spaces, one for the data and one for the index (e.g. if there are 2 oracle schemas, 4 table spaces are created: 2 table spaces for the data and 2 for the indices)
    - extra table spaces can be foreseen to address special needs (e.g. in case of partitioning)
    - for each table space, the initial size of the corresponding data file must be specified
  - List of specific users, groups, and roles to be created and, for the database, the privileges to grant (the DBA role is not allowed). Generally, for web-based applications, the user accessing database objects through the web interface is not the owner of these objects in order to avoid accidental deletion of objects. This implies that the required privileges should be granted to the user accessing the database objects.
  - Environment variables to define; variables will be used in order to avoid hard-coded values in the application source code or scripts; variable names should be meaningful.
- **Installation Procedure**
  - The installation procedure should be organised in clearly identified steps. Each step should have a sequence number, an application level description and technical comments.
  - The installation procedure should be based on scripts to launch commands rather than on sequences of commands to type to avoid typing or cut-and-paste mistakes.
  - The installation procedure should produce an installation log file.
  - The installation procedure should be able to cope with the standard configuration of the host system.
  - The installation instructions must offer the opportunity to arbitrarily and independently choose the installation, execution and data directories.
  - The installation instructions should contain the location of the configuration files and a list and description of useful parameters.
  - The configuration parameters should be grouped in a minimum of configuration files; global configuration files should be used to avoid multiple definitions of the same parameters or variables. A section of the installation instructions should list all configuration parameters, their description, and the specific values used for the installation in the environment of the Publications Office. If technically possible, application parameters should be set in configuration files that are outside of application files (ear, war, jar, …).

- For easier installation, administration and trouble-shooting, the log files produced by the application should be contained in as few folders as possible; log4j or a similar logging framework should be used.
- The log files produced by the application and underlying systems must be properly managed; in particular, log files should be rotated daily and a mechanism should be foreseen to limit the number of log files.
- Oracle scripts should appropriately use the "commit" statement, together with the "whenever sqlerror exit rollback" and "whenever oserror exit rollback" statements in order to ensure application data consistency in case of errors.
- Ideally, all scripts needed to build the elements of the database (i.e. creation of the table spaces, tables, indices, triggers, users and roles including the privileges to grant access and to load data) should be delivered. An alternative is to deliver a script to create the table spaces and the users and the export (dump) of the data.

- **Post-installation**

The installation instructions should contain a check list that details:

- the list of all files modified during the installation
- the list of periodic jobs to schedule
- a procedure to check the correct installation/working of the application: basic checks to be performed by the person in charge of the installation should allow to check if the application is behaving correctly without requiring a full functional validation.

- **System Uninstall**

A detailed procedure how to uninstall the application should be provided that follows the same general remarks as the ones for the installation instructions.

9.6 System Operation Manual

This section describes the minimum contents of the system operation manual.

9.6.1 Hardware and Software Architecture

This section should contain:

- schemas that depict the hardware and software architecture
- a list of installed software including:
  - name of the product/tool
  - version
  - installation parameters (e.g. installation path, users, groups, environment variables...)
- a description of all file systems used by the application with their content and specific access rights (including any temporary space used)
- a description of the specific users, groups, and roles used by the application
- details of the network configuration including:
  - interfaces used
  - IP addresses
  - virtual hosting
  - IP and port bindings
  - specific routing
  - name servers
  - LDAP servers used

- local name resolution

9.6.2 Configuration

- **Application Start-up and Shutdown**

  The sequence of steps to start and stop the application and any dependencies will be described. It must be possible to automate the start/stop procedure; the contractor is requested to deliver start/stop scripts for the application that can be integrated in the operating system service management framework.

- **Configuration Files**

  This section should specify:

  - the location of the configuration files on the hard disk
  - a list of useful parameters and their description
  - how to modify these parameters

- **Log Files**

  This section should specify:

  - a description of the contents of the log files
  - the location of the log files on the hard disk
  - how to set different log levels
  - clean-up and archiving (regular purge and rotation)

9.6.3 User Management

- **User Management**

  This section should describe:

  - how to create and delete users
  - how to manage access rights and privileges
  - information on the authentication mechanisms used by the application

9.6.4 Backup and Restore

- **Backup Procedure**

  A detailed backup procedure that includes at least the following elements must be provided:

  - list of file systems/directories to backup (including pattern of file names to backup)
  - scheduling/triggering schema
  - pre- and post-processing commands to execute
  - specific techniques to use (e.g. snapshot, hot backups...)

- **Restore Procedure**

  A detailed restore procedure covering the most common disaster situations should be provided. Special attention should be put on the following aspects:

  - sequencing of the restore operations in order to minimise the downtime
  - consistency checks to execute
  - repair/resync procedures to execute
  - system operation checks after restore

- **Copy Procedure**

A detailed procedure on how to copy an existing installation from one environment to another must be delivered. This procedure should allow creating a copy of for example the production environment to a test environment. This procedure must clearly indicate the parameters to modify in order to have a fully operational system in the test environment after completion of the copy procedure. The procedure must require as few manual interventions as possible.

9.6.5 Monitoring

- **Monitoring**

The contractor must deliver instructions on how to check the availability and the response time of the application; it should be easy to integrate these checks in an automated monitoring system (for example, a set of URLs to check); currently, the monitoring system at the Publications Office is based on Centreon. The instructions and checks to be performed should cover all major components of the application, including components that the application depends on (like database server, middleware and other computer software that provides services to the software application beyond those available from the operating system).

This section should contain:

- a list of file systems to monitor with thresholds and critical values
- a list of processes to monitor with thresholds and critical values
- the description of monitoring and alert mechanisms included in the application
- a list of resources (e.g. URLs in the case of a web application) that can be monitored in an automated and unattended manner by a system and network monitoring application

9.6.6 Application Management

The system operation manual should contain at least the following section with the suggested minimum contents.

- **Administration Interfaces**

A detailed description of all available application administration interfaces will be provided. This section will at least include:

- how to access the administration interface
- a description of the functionality and features
- instructions for use

- **Periodic Tasks**

The tasks that have to be executed on a regular basis should be described in this section. It should be possible to automate these tasks as much as possible, for example by providing a script. For each task, the following information will at least be provided:

- description of the task
- procedure to execute
- how to schedule or trigger the task

Special attention should be put on the description of resource intensive and time consuming tasks like:

- data archiving
- data purging

- data reorganisation
- data consistency check
- data synchronisation
- data indexing
- statistics

- **Database Management Tasks**

  All specific database-related tasks that are not already described above should be described here.

- **Best Practices and FAQs**

  A description of best practices for dealing with common issues, troubleshooting procedures, hints and tricks, and a list of frequently asked questions should be included here.

9.7 Access to the Environment of the Publications Office

No direct access (telnet, ftp...) to the Publications Office's environment (production or test) will be granted to the contractor.

Specific interfaces (e.g. Web/CGI) have to be developed for the administration of the application (e.g. periodic follow-up) and/or the production follow-up, if required. Especially the access to interfaces (data exchange directories) must be controlled by the application in order to validate the contents of the data exchanged and to allow the "replay" of data transfers.