European Parliament IT Environment

Author: DG ITEC

Version: 18

Date: April 2017

Table of Contents

1 General Introduction

1.1 Purpose

The main objective is to present the **European Parliament's IT environment**.

1.2 Glossary

Abbreviation	Description
DG ITEC	Directorate General for Innovation and Technological Support
DES	Directorate for Development and Support
ESIO	Directorate for Infrastructure and Equipment
OPERATIONS	ICT Operations and Hosting Unit
EP	European Parliament
Europarl	European Parliament's website www.europarl.europa.eu
BPM	Business analysis and Project Management Department
STANDARDS	Standards and ICT Security Unit
LSA	Local System Administrator
LSU	Local Support Unit
RHEL	RedHat Enterprise Linux

2 Context

2.1 Main Parliament sites

Parliament has three main sites:

- **Strasbourg**, where ordinary part-sessions are held (one week a month on average);
- **Brussels**, which mainly hosts parliamentary committee meetings and the political groups; the additional part-sessions are held there; MEPs' offices, political group secretariats and some Parliament Secretariat departments are located there;
- **Luxembourg**, where the other Parliament Secretariat departments are located.

In those three cities, Parliament occupies a number of buildings containing offices and meeting rooms; it also has information offices in all EU Member States.

Mobility is a major feature of Parliament's working environment and comes into play at various levels:

- between the main sites - Brussels, Luxembourg and Strasbourg - depending on the Parliament activity concerned;
- within each site, all of which are made up of a number of buildings;
- between premises, within EU Member States, which may or may not be owned by Parliament;
- more globally for specific user categories (nomadic workers or teleworkers).

2.2 IT organisational setup

The information and communications technologies used within Parliament are provided by the Directorate-General for Innovation and Technological Support (ITEC), through its two directorates - Directorate for Development and Support (DES) and – Directorate for Infrastructure and Equipment (ESIO).

DES and ESIO operate in the context of partial IT decentralisation, combining what they contribute centrally with what IT teams contribute locally, within directorates-general (DGs) and political group secretariats, to the running of Parliament's information and communications systems.

IT management at departmental level (DGs and political groups) is handled by Local Support Units (LSU). Each LSU is administered by a Local System Administrator (LSA) team.

DG ITEC/DES and DG ITEC/ESIO 's central-level responsibilities are:

- to devise and grow infrastructure and architecture facilities (servers, work stations, networks, telecoms, security, etc.);
- to lay down methodological and technical rules and standards and verify compliance with them;
- to look for, test and implement new hardware and software solutions;
- to develop and maintain central applications intended for all in-house and external users (Intranet and Internet respectively) and central applications intended for a number of organisational units (DGs, political groups, directorates, units, services, etc.);
- to provide LSA teams and end users with general second-level hardware and software support.
- to provide first level hardware and software support to end users in specific parts of the EP end users populations (e.g. MEPs, certain DGs, special services).

LSA teams' responsibilities are:

- to manage departmental equipment (departmental servers, work stations, peripherals, etc.);
- to develop and maintain departmental applications intended for users within the same organisational unit;
- to provide end users with first-level hardware and software support (if not provided by DES).

3 IT Environment

3.1 Network infrastructure

Parliament currently has a routed TCP/IP network infrastructure.

3.1.1 Local Area Networks (LAN)

The following LAN technologies are used at present:

- Switching Ethernet
- VLAN
- Fast Ethernet / Gigabit Ethernet / 10 Gigabit Ethernet

3.1.2 Wide Area Networks (WAN)

Parliament's main sites - Brussels, Luxembourg and Strasbourg - are interlinked via a WAN designated EPINET HD with roughly 1 Gbit to 10 Gbit (on specific links) TCP/IP throughput.

Parliament has various resources for external communications:

- Internet;
- Network interlinking the European Institutions and the Member States.

3.1.3 Building wiring

IT wiring in all Parliament buildings is based on the following rules:

- horizontal cabling: multipurpose wiring, four twisted pairs, Category 5, 6, 6A or 7;
- vertical cabling: multi-mode optical fibre / monomode optical fibre / twisted pairs.

At the Brussels, Luxembourg and Strasbourg sites, copper wiring and optical fibres (single-mode and multi-mode) are the main media used for interconnecting buildings.

3.1.4 Network administration

Administration of Parliament's network is handled via redundant stations at each site.

3.2 Telephony

European Parliament's Ericsson PABX, in use since 1996, has been taken out of service early 2017. Since that moment, all of European Parliament's telephony is based on the Cisco telephony over IP solution. The main elements of the new Cisco-based telephony system are the following: Cisco IP phones, mostly videoconference-enabled, for all nominative users. Analogue phones, connected to redundant telephony gateways, serve as emergency phones in the corridors. Cisco UCCX supports over 10 call centres internal to European Parliament. Cisco UNITY supports European Parliament's voice messaging system. JDM Software's Peterconnects system is the main tool of European Parliament's switchboard. A Rightfax fax-server, integrated with Microsoft Outlook for receipt and transmission of faxes, replaced the individual fax-machines.

3.3 Servers

3.3.1 Servers for centralised IT management in Parliament

ESIO's computer centre houses Windows, UNIX and LINUX servers for centralised IT management in Parliament. The servers provide the following services:

- **Windows servers**:
  - File servers, terminal server, system supervision;
  - Logon validation services (Active Directory), DNS, DHCP, folder replication, data transfer, remote access services via Windows Terminal Services, application servers;
  - E-mail, Europarl Intranet/Internet;
- **UNIX servers**:
  - Database servers (Oracle, Adabas), file servers, web servers, application servers, backup servers;
  - DNS and LDAP directory services;
  - SSO authentication and authorization;
  - Europarl Intranet/Internet, centralised-application hosting.
- **LINUX servers**:
  - RedHat Enterprise Linux (RHEL).

The computer centre also has NAS and SAN storage infrastructure.

The following table sets out Parliament's standard hardware and software configurations for servers and gives some indication of trends:

Hardware	Current minimum configurations	New configurations / developments
VMware servers:	x86 (Intel) 10-Core Quad-processor	New processor generation with higher clock rates
Windows servers:	x86 (Intel) 8-Core Dual-processor Blade x86 (Intel) 8-Core Dual-processor	New processor generation with higher clock rates
UNIX servers:	SPARC64 VII Intel Xeon 6-Core Dual-processor AMD Opteron Quad-core Dual-processor	No extension planned

Software	Current configurations	Developments / Trends
Operating system:	Windows 2008 r2 Enterprise 64 Bits Windows 2012 r2 Enterprise 64 Bits	Windows 2016 r2 Enterprise 64 Bits
	RHEL 6 (phase out) RHEL 7	
	SUN Solaris 10 SPARC and X86	X86
Database Management System (DBMS):	Oracle 11g R2 * including Binary XML * including Semantic Technologies (Triple Store) PostgreSQL 9.1 CouchDB 1.5.1	Oracle 12c PostgreSQL 9.4+ CouchDB 1.5.1+

	Adabas V6.2.1	No extension planned
Application server:	Tomcat 7.0.x (phase out) Tomcat 8	Tomcat 9.0.x
Search engine	ElasticSearch 2.x	ElasticSearch 5.x
Messaging server	HornetQ 2.2.x (phase out) Apache ActiveMQ Artemis 1.4.x	Apache ActiveMQ Artemis 2.x
Web server:	IIS 6 (Windows 2003) (Phase out) IIS 7 (Windows 2008 R2) IIS 8 (Windows 2012 R2)	
Reverse Proxy	Apache HttpD 2.4.x (Phase out) NGINX 1.8	NGINX 1.10
Reporting and analysis tool:	SAP BI 4.1	SAP BI 4.2
Business Process Management (BPM):	ARIS Connect Platform 9.x: • ARIS Connect server • ARIS Connect viewers • ARIS Architect • ARIS Publisher • ARIS Process Governance • ARIS Architect for SAP	

Unified Modeling Language 2.1 tool (UML)	MagicDraw 18. x	
McAfee Anti-virus solution	Viruscan Enterprise 8.8	HIPS 8.0 for server and future evolutions of Viruscan Enterprise
Document conversion	Adlib Express Server 4.12 OpenOffice 4.x	Adlib Express Server 5.3

3.3.2 Servers to cover departmental needs

Windows, UNIX and LINUX servers are accommodated in the DGs and political groups, to cover departmental needs. The servers provide the following services:

- **Windows servers**:
- Database servers (Oracle), file servers, print servers, web servers, application servers;
- **LINUX servers**:
  - RedHat Enterprise Linux (RHEL),
  - Database servers (Oracle, PostgreSQL, Apache CouchDB)
  - Application servers, Web servers (Apache HttpD, Tomcat)
  - File servers, Print servers (samba, nfs, cups)

Hardware	Current minimum configurations	New configurations / developments
Windows and Linux servers:	x86 (AMD and Intel) 10 Cores Dual-processor, x86 (AMD and Intel) 10 Cores Quad-processor	New dual processor generation with higher clock rates

Software	Current configurations	Developments / Trends
Operating system:	Windows 2003 SP2 (phase out) Windows 2008 r2Enterprise 64 Bits (phase out)	Windows 2016 r2 Enterprise 64 Bits

	Windows 2012 r2 Enterprise 64 Bits	
	RHEL 6 (phase out) RHEL 7	
Database Management System (DBMS):	Oracle 11g R2 * including Binary XML * including Semantic Technologies (Triple Store) PostgreSQL 9.1 CouchDB 1.5.1	Oracle 12c PostgreSQL 9.4+ CouchDB 1.5.1+
Application server:	Tomcat 7.0.x (phase out) Tomcat 8	Tomcat 9.0.x
Search engine	ElasticSearch 2.x	ElasticSearch 5.x
Messaging server	HornetQ 2.2.x (phase out) Apache ActiveMQ Artemis 1.4.x	Apache ActiveMQ Artemis 2.x
Web server:	IIS 6 (Windows 2003) (Phase out) IIS 7 (Windows 2008 R2) IIS 8 (Windows 2012 R2) Apache HttpD 2.4.x (restricted use)	

With regard to software, Parliament is taking an **open source solution** approach whenever possible. Special arrangements governing the acquisition and use of open source software are submitted for validation.

Tools are used for server administration, supervision and backup at central and departmental level.

As part of departmental projects, Parliament provides:

- Physical and virtual servers

- Operating systems

- WSUS to update security patches

- Antivirus

These servers will have to be maintained, according to the standards of Parliament.
The developments and software must be compatible with the supported operating systems

3.4 Workstations

Parliament's workstations run in a Windows environment. Users and resources are managed through one specific Active Directory domain. A DNS structure is used for name resolution.

In order to meet specific needs with regard to applications, together with management, security and portability requirements, Parliament has defined a standard configuration seeking to make workstations totally user-independent and give users an enhanced level of service based on the portability of their parameters and documents.

The following table sets out Parliament's standard hardware and software configurations for work stations and gives some indication of trends:

Hardware	**Current minimum configurations**	**New configurations / developments**
	Intel Pentium G3440 (3,3GHz); 8 GB, SSD 128GB, NIC 10/100/1000, DVD-ROM, USB	evolution of the standard PC configuration

Software	**Current configurations**	**New configurations / developments**
Operating system:	Windows Seven 64 bits SP1	Windows 10 64Bits 1607 CBB
Office suite:	Office 2013 32 bits	Office 2016 32 bits
Mail user agent:	Outlook 2013 32 bits	Outlook 2016 32 bits
Web client:	Internet Explorer 11 Firefox ESR 45	Edge Internet Explorer 11 Firefox ESR 52
McAfee anti-virus solution	VSE 8.8 and HIPS 8.0 for Workstations	Evolutions of VSE and HIPS

3.5 Mobile devices

The European Parliament is introducing mobile devices (more precisely tablets) within the Institution, the main objective is to implement the 3 following technologies: IOS, Android and Windows.

4 Environments for development of centralised applications

For centralised applications hosted at the ESIO's computer centre, the following environments are provided:

4.1 Development environment

A development environment with the following components:

- **Servers**: server development instances (for application servers, Oracle database servers and source management servers), development of servers shared by various environments (LDAP directory);
- **Developer stations**: work stations with a standard configuration including the development platform.

4.2 Pre-production environment

A dedicated pre-production environment for tests to validate an application (user acceptance tests and integration tests, applications load tests and vulnerabilities tests) before any move to go into production. This environment, which is similar to the production environment, is made up of the following components:

- **Servers**: server pre-production instances (for application servers, Oracle database servers and source management servers), development of servers shared by various environments (LDAP directory); the move from the development environment to the pre-production environment, where an application is deployed on pre-production servers, is handled by the computer centre;
- **Tester stations**: work stations with a standard configuration including tools for validating an application before any move to go into production.

4.3 Production environment

A production environment fully managed by the computer centre, with the move from pre-production to production environment, where an application is deployed on production servers, being handled by the computer centre.

4.4 Other environments

A dedicated training environment is also available, as is a data warehouse.

At the server end and at the developer/user work station end, the configuration parameters for each environment and their upgrades are defined by the computer centre and by the ESIO's STANDARDS Unit respectively.

5 Directorates' recommendations and strategic guidelines

In general, the applications base is evolving in a light web client direction. Heavy client applications are being phased out in favour of the light client model. Man-machine interfaces must comply with the ergonomic standards laid down by DG ITEC.

5.1 Main standards

The main standard facilities opted for by DG ITEC are:

- Oracle (DBMS used at central and departmental levels),
- PostgreSQL,
- Apache CouchDB
- Apache Tomcat (Servlet 3.1 / JSP 2.3)
- ElasticSearch
- EP Foundry Eclipse Platform (standard IDE for JEE development based on Eclipse and a standard set of add-ons),
- UML 2.1 modeler MagicDraw,
- ARIS Design Platform (Business Process Management and Modelling Tool),
- SAP Business Intelligence (reporting and analysis tool),
- Jahia (multilingual application portal server/ CMS),
- Atlassian Confluence (WiKi),
- Atlassian JIRA (Project tracking),
- Atlassian FishEye/Crucible
- RedHat Enterprise Linux,
- McAfee anti-virus solution: VSE 8.8 and HIPS 8.0,
- Adlib express server,
- OpenOffice (server side),
- SharePoint 2013 using only Out Of The Box features restricted to collaborative needs of European Parliament.

DG ITEC pays the utmost attention to multi-platform usability of applications and to compliance with the methodologies, rules and standards it lays down.

5.2 Methodological recommendations

DG ITEC has implemented the following:

- A methodological framework (**EPMF**) which includes a set of specific methods:
- - A modeling and business analysis method (**BPMM4EP**)
    - **BPMM4EP** is supported by a set of templates, guides or procedures and by specific workshops.
  - A method for the program management (**PP04EP**) based on " The standard for Program Management Second Edition";
    - **PPO4EP** is supported by a set of templates, guides or procedures and by specific workshops.
  - A method for the project management **(PMM4EP)** based on the PMBok (Project Management Body of Knowledge) of **PMI** (Project Management Institute); a version Agile based on **SCRUM** is available;
    - **PMM4EP** describes several lifecycles in function of the initial risk level;
    - **PMM4EP** is supported by a set of templates, guides or procedures and by specific workshops.
  - A method for infrastructure project management **(IPM4EP)** based on the PMBok (Project Management Body of Knowledge) of **PMI** (Project Management Institute);
    - **IPM4EP** describes several lifecycles in function of the initial risk level;
    - **IPM4EP** is supported by a set of templates, guides or procedures and by specific workshops.
  - A method for the Workload Estimation (**WEM4EP)** based on ISO standards (Function Point Analysis (FPA), NESMA, IFPUG). The first implementation of **WEM4EP**, "indicative estimation", is based on the 'Business Case' that comes out of the BPM phase and is obtained by completing an on line form.
  - An approach for the **Risk Management** during the whole project lifecycle (**PMM4EP**), based on the PMBok principles;
    - The risk Management is supported by specific tools at the various moments of the risk lifecycle: Initial Risk Assessment (**IRA**) when the project global risk is assessed for the first time, and **Project dashboard** for a qualification and a rigorous follow-up of each individual risk all along the project. A **guide** on the risk management is also available.

All necessary information on the DG ITEC 's recommendations and strategic guidelines will be provided to the successful bidder.

5.3 Security at EP

The end-point security solution working at EP is:

1. McAfee ViruscanEnterprise8.8. The software is an anti-virus including access protection feature and the classical file scanning.
2. HIPS 8.0 from McAfee. This software is a Host Intrusion Prevention System which completes the anti-virus.

Optional security software is also available in specific cases:

- McAfee file and removable media protection (FRP), v.4.3.1;
- McAfee Endpoint Encryption for PC version 7.0.3;
- Symantec PGP encryption desktop version 10.3.2;

These pieces of software are a compulsory part of EP the Standard Configuration. The compatibility of any software with the McAfee solution must be checked as a pre-condition of any new project.

It is also highly recommended to consider the group policies (GPO) in force at the European Parliament. These policies require a set of rules. For example, for a Web application, it is not possible to download a font if it is not installed on an EP-domain.

All applications and servers connected to the EP infrastructure are subject to regular ICT security assessments (vulnerability scans, pentests...) using various tools.