ЕВРОПЕЙСКИ ПАРЛАМЕНТ PARLAMENTO EUROPEO EVROPSKÝ PARLAMENT EUROPA-PARLAMENTET
EUROPÄISCHES PARLAMENT EUROOPA PARLAMENT ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ EUROPEAN PARLIAMENT
PARLEMENT EUROPÉEN PARLAIMINT NA hEORPA EUROPSKI PARLAMENT PARLAMENTO EUROPEO
EIROPAS PARLAMENTS EUROPOS PARLAMENTAS EURÓPAI PARLAMENT IL-PARLAMENT EWROPEW
EUROPEES PARLEMENT PARLAMENT EUROPEJSKI PARLAMENTO EUROPEU PARLAMENTUL EUROPEAN
EURÓPSKY PARLAMENT EVROPSKI PARLAMENT EUROOPAN PARLAMENTTI EUROPAPARLAMENTET

Directorate-General for Innovation and Technological Support

Directorate for Development and Support

Unit ICT Evolution and Maintenance

WHITE PAPER ON THE VDI INFRASTRUCTURE IN THE CONTEXT OF THE EXTERNALISATION INITIATIVE

Purpose: This document is the result of the cooperation between the units (OPERATION, STANDARDS, CONCEPT and EVOLUTION) involved in the process of Externalization of intra-muros development teams. It clarifies and synthesizes the rules that are applied when granting access to the corporate working environments of the EP via VDI infrastructure.

According to the procedure for requesting firewall configuration, explained in the Procedural Guide document the official who is launching the request should first verify whether his/her request corresponds with the specified in this White Paper.

Document name	VDI_White Paper on VDI infrastructure_EN_v10_1B3B949.docx	Number of pages	12

Contents

1. Background

1.1. DG ITEC Needs

For accomplishing its objectives the DG ITEC relies on the expertise of external consultants, recruited by service providers of the European Parliament. The external consultants usually work within the premises of the EP (intramural).

The present external development teams are generally performing the following tasks:

1) Development, largest task considering the effort allocated to it, which includes encoding, building, unit testing and documenting.

2) Execution of integration tests.

3) Preparation of the load testing scenarios and monitoring of the results of the execution.

4) Preparation for the release deployments.

5) 2nd level support, including troubleshooting, investigation of issues, identification of problems, tracing logfiles, reproduction of incidents detected in production in a stable environment.

6) 1st Level support in the cases where the service has not been assigned to the IT Service Desk.

1.2. Access constrains

In 2013 in a note D(2013)46847 the Director-General of DG ITEC has given a mandate for reduction of the number of external consultants working within the EP offices.

According to the implementation plan it became clear that the majority of consultants will only be able to be externalised if they receive access for teleworking via VDI infrastructure to the Intranet systems of the Parliament.

As the current security policy adopted by STANDARDS unit determines the interdiction to access any pre-production or production system from outside the Parliament, it clearly reduces the tasks that can be a-priori carried out by the extra-muros teams. That means, in practice, that development teams could only be able to do encoding, building software, unitary testing and documenting. Thereby the execution of other tasks will have to be organised in a way to be done intra-muros.

1.3. Access needs in Production and Pre-production

However, the extra-muros development teams, besides the obvious access to the development environment, need also access to some components of our infrastructure in order to have the minimum working conditions to ensure the development tasks. These 2 categories of needs are:

Category 1: Supporting tools in production

Extra-muros development teams need access to ***web-based supporting tools*** and ***middle-ware components*** deployed in the production environments for the conventional development lifecycle.

Category 2: Corporate services in Pre-Production

The other category is access to ***corporate application web-services*** deployed in pre-production environments that are broadly used by a large number of applications. This is required to ensure the dependencies of applications on various common components that need to be accessible and running on a stable environment. Given that these components may have their own development life-cycle it would be a substantial complication if we had to establish the dependencies on the development environment rather than on the pre-production one. In some cases, the development teams have created their own mock web services to avoid the need to go to pre-production web-services. This principle has been encouraged to the teams as a best-practice. However, this approach is not applicable for all cases, especially where the business complexity is such that the effort to simulate the functionality of the existing pre-production services would be disproportional.

In consequence, it is requested to treat as exceptions to the norm the access to a reasonable number of tools in production and a reasonable number of corporate web services in pre-production to ensure the development tasks of the extra-muros teams.

2. Rules and Exceptions agreed

This chapter sets the rules what IT solutions are accessible through the VDI workstations, and to which the access is refused. In a separate section are listed the exceptions of these rules.

The rules and the exceptions are agreed by the Externalisation Task Force (mandated by the Head of Unit EVOLUTION) from Directorate DES and the Operations and Hosting Unit from Directorate ESIO.

The rules and the exceptions can only be changed upon a mutual agreement of the Document Owner and the Counterparty specified in section 4.1. Once the document ownership is changed from Directorate DES to Directorate ESIO, the document owner can update the document unilaterally. When the document is updated the document owner shall inform the Head of Service *IT Access & Asset Management & LSU*, and all Heads of Units in DES.

2.1. Rules agreed

For setting the rules the following terms are used:

- *IT solution* is any software application, component or database
- *Network location* is any shared folder or similar resource
- *Environment* is an IT landscape covering multiple IT solutions and Network locations. The Environments are qualified according to their purpose - development, integration etc.
- *Exceptions* can be agreed for specific IT solutions or Network locations, for which the granting of access overrules the below conditions.

The following rules have been agreed following the security policy adopted by STANDARDS:

1. The access from VDI to IT solutions or Network location residing in the *Development environment (DV)* is granted. However, some applications (e.g. CODICT) need a closer examination and validation because of the sensitive information they contain.
2. The access from VDI to any IT solution or Network location residing in the *Integration environment* is granted.
3. The access from VDI to any IT solution or Network location residing in the *Pre-Production environment (PP)* is denied.
4. The access from VDI to any IT solution or Network location residing in the *Training environment (FP)* is denied.
5. The access from VDI to any IT solution or Network location residing in the *Production environment* is denied.
6. Access is granted from VDI to TEFS servers which comply with the convention described in section 3.1 of the present document.

2.2. Exceptions agreed

The web-services exceptions from production and pre-production environments are the following:

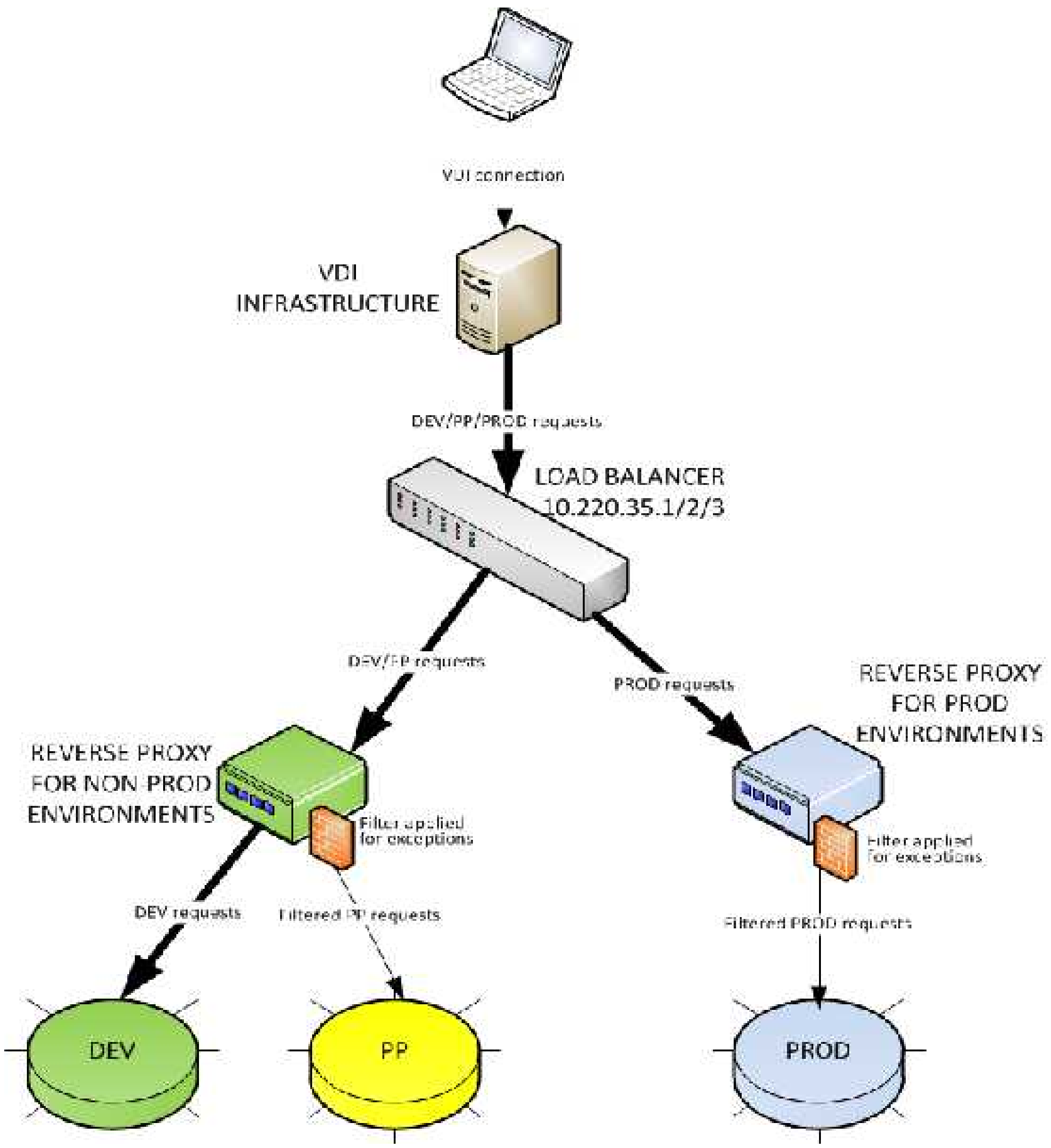
List of corporate web services running in PRE-PRODUCTION environments		
Component	**URL**	**IP address**
EWS web Service	http://www.bdmsewspp.ep.parl.union.eu	10.220.35.1
PrintShop	http://www.printshoppp.ep.parl.union.eu	10.220.35.1
Servlet EPADES	http://www.epadespp.ep.parl.union.eu	10.220.35.1
Application VISITSWS	http://www.visitswspp.ep.parl.union.eu	10.220.35.1
Vocal1 management application	http://eicilwp014.ep.parl.union.eu	136.173.57.68

List of supporting tools running in PRODUCTION environments		
Component	**URL**	**IP address**
Web ITO Apps portal	http://eicidevhttp.ep.parl.union.eu	10.220.35.1
CACTI	http://www.cacti-appli.ep.parl.union.eu	10.220.35.2
ADA	http://www.europarl.ep.ec/ada	10.220.35.3
BO server XI	http://boxi.ep.parl.union.eu	10.220.35.3
BO server	http://eicixzd265.ep.parl.union.eu	10.127.239.177
License server	http://MUSTLUXAHPLIC01-vdi.ep.parl.union.eu	136.173.22.236
License server (for HP UFT 12)	http://TESTLUXSLIC01-vdi.ep.parl.union.eu	10.21.29.212
EP Deploy	http://www.epdeploy.ep.parl.union.eu	10.220.35.3
EP Foundry SVN	http://www.ep-foundry.ep.parl.union.eu	10.220.35.3
Http Statistics	http://www.webstat.ep.parl.union.eu	10.220.35.3
Jira	http://www.jira.ep.parl.union.eu	10.220.35.3
MUSTI	http://www.musti.ep.parl.union.eu	10.220.35.3
Repo Maven	http://www.teles.ep.parl.union.eu	10.220.35.3
SIA Net	http://www.sianet.ep.parl.union.eu	10.220.35.3
SIAwiki (Confluence)	http://www.siawiki.ep.parl.union.eu	10.220.35.3
TEFS server - WEBCONTRACTS	http://www.tefs-bwc.ep.parl.union.eu	136.173.98.173
TEFS server INTRANET	http://epsvblp016-vdi.ep.parl.union.eu	136.173.22.236
TEFS server EVOLAD	http://epsvblp008-vdi.ep.parl.union.eu	136.173.98.178
TEFS EVOPARL	http://www.tefs-evoparl.ep.parl.union.eu	136.173.98.217
Repo Maven (TEFS)	http://epsvblp008.ep.parl.union.eu:8280	136.173.98.178

SIA Factory Nexus / Repo Maven (TEFS)	http://epsvblp008.ep.parl.union.eu	136.173.98.178
Sonar (TEFS)	http://epsvblp008.ep.parl.union.eu:8380	136.173.98.178
TestLink (test tool)	http://epsvblp020.ep.parl.union.eu	136.173.98.195
EPSD	http://www.epsd.ep.parl.union.eu	136.173.99.87

Nevertheless, it might be possible that additional exceptions will be requested when new development teams start working on extra-muros approach. These exceptions will mandatorily respect the same principles laid down in the previous paragraphs.

3. Technical solution


VDI connection
VDI INFRASTRUCTURE
DEV/PP/PROD requests
LOAD BALANCER 10.220.35.1/2/3
DEV/PP requests
PROD requests
REVERSE PROXY FOR NON-PROD ENVIRONMENTS
REVERSE PROXY FOR PROD ENVIRONMENTS
Filter applied for exceptions
Filter applied for exceptions
DEV requests
Filtered PP requests
Filtered PROD requests
DEV
PP
PROD

Any request to development, pre-production or production environments initiated by an extra-muros consultant through the VDI infrastructure will first be handled by a unique **load balancer**.

This architecture component is in charge of distributing workloads across multiple corporate computing resources, such as servers or network links aiming to optimize resource use, maximize throughput, minimize response time, and avoid overload of any one of the resources.

There is one IP address in the same subnet for each of the three environments: for development; for pre-production and for production servers.

The load balancer is dispatching the requests for development and pre-production (non-production environments) towards reverse proxy, while the requests for production are being dispatched to a different (second) reverse proxy.

Each reverse proxy will handle requests coming from the different clients to the private network or intranet. The reverse proxy in charge of the non-production environments will manage the requests addressing them to the development or pre-production areas. This provides a level of security that prevents some clients from having direct access to data on the corporate servers.

The **conceptual solution proposed** to manage the extra-muros requests to the different environments does rely on the following ideas:

- By default the VDI will have all the ports to the load balancer open, for the three environments. In consequence, there will be no any restrictions at this level.
- The ***reverse proxy for the non-production environments*** will let free access to development environments. However, for pre-production environments the access will be always refused except for the services considered as exceptions (see list above). A logical filter in the reverse proxy would be set up in order to enable this possibility.
- For the ***production reverse proxy*** the approach will be similar. All accesses to production will be refused by a logical filter except for the services/servers considered as exceptions (see list above).

This proposal appears to be the optimal solution for having a flexible, secure, efficient and controllable environment that could facilitate the operational activities. The technical aspects related to this conceptual proposal have to be addressed by the services in charge of the solution design (STANDARDS) and the hosting (OPERATIONS).

3.1. TEFS servers convention

The European Parliament has a standardized platform for enabling the software development process called *Technical Environment for Forge Software* (TEFS). The TEFS is hosted on a dedicated machine (TEFS server) which is accessed by the IT specialists for daily operations (building, deployment etc.).

The ALSA Service provides up to one TEFS server per department (Service). In order to comply with the best practices for IT landscape management, the Document Owner and the Counterparty have agreed on the following convention:

1. An Alias shall be configured for each TEFS server.
2. The Alias name will have the form: TEFS-*SERVICE, where:*
    a. TEFS is a constant 4 letters string
    b. - is the minus sign
    c. *SERVICE* is the mnemonic of the Service using the TEFS machine (e.g. EVOLAD).
3. The TEFS server shall be referred by its Alias (e.g. http://tefs-evolad.ep.parl.union.eu), and not by the server name itself (e.g. http://epsvblp008.ep.parl.union.eu).

4. Organisational aspects

In order to be as efficient and structured as possible it is necessary to **establish a minimum of governance level**.

4.1. Document Owner and Counterparty

From version 0.1 prior to version 1.0 this document:

a) Is owned by the Externalisation Task Force mandated by the Head of Unit ICT Evolution and Maintenance (Directorate DES).

b) The Counterparty is the Head of Service Capacity & Continuity mandated by the Head of ICT Operations and Hosting Unit (Directorate ESIO).

With version 1.0 the ownership of the document is suggested to the *Standards & ICT Security Unit* (Directorate ESIO).

4.2. Procedural guide

Moreover, *a complete procedure* has been established to register, verify, coordinate, harmonize and submit the diverse needs from the development and maintenance teams, including EVOLUTION and CONCEPT.

The Procedural Guide is now owned by the *IT Access & Asset Management & LSU service* in Unit Support. It describes the workflows for requesting and modification of resources (applications; access rights a.o.) needed for teleworking with the VDI solution.

It explains the procedures for how to request and maintain the VDI machines, used by teleworkers; how to request telework access for a new consultant or to change existing credentials. Standard procedures within the European Parliament (as user creation, group policies etc.) are not covered here.

The document shall be used as a reference by the Responsible Officials and Team Leaders.

4.3. VDI Firewall Dashboard

In order to support this process, a simple tool based on Excel spread sheet has been made as *a centralized register of the access needs* for external consultants working for the European Parliament. This dashboard is now maintained by the *IT Access & Asset Management & LSU service* in Unit Support.

4.4. Issue register

And last, *an issue register* (latest version named VDI_IssuesRegister_EN_v10) has been created to keep track of the different incidents and issues related to the accessibility, reliability and performance of the VDI solution. This excel sheet may be found at:

\\DITLUXA\RMSI-SIGA\PUBLIC\Externalisation\10 CoordinationVDI

5. Document control

5.1. Circulation

Direct.	Role/Position	Name/Initials		RACI[1] code
DES	Director DES	Steen Eilertsen	SE	I
DES	Head of Unit Evolution	Gerrit Potoms	GP	A
DES	ETF member	Ignacio Izquierdo	II	R
DES	ETF member	Todor Todorov	TT	R
DES	ETF member	Polya Markova	PM	R
DES	Head of Service IT Access & AM & LSU	Stephan Janssens	SJ	I
ESIO	VDI Technical Project Manager	Mark Williams	MW	C
ESIO	Head of Service Capacity & Continuity	Ingrid Schneider	IS	C
ESIO	Director ESIO	Pascal Paridans	PP	I
ESIO	Head of Unit Operations	Rafael Ruiz de la Torre	RRT	I
ESIO	Head of Unit Standards & Security	Luca Rettore	LR	C

5.2. Change history

Version number[2]	Status[3]	Date	Initials	Summary of changes
0.1	Draft	20/08/2014	II	Initial draft
0.4	Draft	10/10/2014	TT	Minor updates
0.5	Draft	09/01/2015	PM, TT	Information added, updates
0.6	Draft	10/02/2015	IS, PM	Comments, updates, added exceptions
1.0	Final	11/02/2015	TT	Promoted to final
1.0a	Final	13/02/15	PM	Small changes in URLs in exceptions table

5.3. Reference documents

N°	Document name	Description
[1]	*DRAFT* Proposal For reducing the IT activities that are performed by external consultants in SIA, working on the premises of the European Parliament (Intra Muros)	Proposal drafted in March 2012 X:\EVOLAD\Projects\Externalisation\01 Strategy & Plan\SIA extra-muros activities - DRAFT proposal 5-3-2012.pdf
[2]	Evolution Plan for reduction of EIM V1-2	X:\EVOLAD\Projects\Externalisation\04 Project documentation\20131031 EVOLUTION PLAN for reduction of EIM v1-2.pdf
[3]	EVOLUTION Implementation Plan v104	X:\EVOLAD\Projects\Externalisation\04 Project documentation\20140403_EVOLUTION Implementation Plan v104.pdf
[4]	VDI_ProceduralGuide_EN_v15	\\Ditluxa\rmsi-siga\PUBLIC\Externalisation\10

[1] **R**: Responsible, **A**: Approval, **C**: Contribution, **I**: Informed

[2] Naming convention: Procedure 'Program & Project naming convention' (Standards.net)

[3] Status: Draft, Final, Approved

N°	Document name	Description
		CoordinationVDI\20 Procedures\VDI_ProceduralGuide_EN_v14.pdf
[5]	VDI Firewall Dashboard	\\Ditluxa\rmsi-siga\PUBLIC\Externalisation\10 CoordinationVDI\VDI_FirewallDashboard_EN_v15.xlsx
[6]	Issue register	\\Ditluxa\rmsi-siga\PUBLIC\Externalisation\10 CoordinationVDI\VDI_IssuesRegister_EN_v10.xlsx

5.4. Glossary

Abbreviation	Description
VDI	Virtual Desktop Infrastructure
DEV	development
PP	pre-production
PROD	production