Directorate General for Innovation and Technological Support

Directorate for Development and Support

Directorate for Infrastructure and Equipment

Coordination of VDI requests and resources

Procedural Guide

Purpose:

This procedural guide describes the workflows for requesting and modification of resources (applications; access rights a.o.) needed for teleworking with the VDI solution.

The present document has been designed as a procedural guide of DG ITEC.

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.

TABLE OF CONTENTS

1. BACKGROUND

The European Parliament is the only directly-elected EU body and one of the largest democratic assemblies in the world. The Parliament is assisted by a Secretary-General (consisting of 11 General Directorates) for all core and support activities, including facility and inventory management. DG ITEC provides the European Parliament with information and communication technology services as well as printing and distribution services. 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).

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. In January 2014 the Head of Unit EVOLUTION has appointed an externalization task force (ETF) for drafting a more detailed implementation plan, which should cover all aspects of the process in order to achieve specific objectives for unit EVOLUTION until the end of 2014. The implementation plan was developed following the PMM4EP project management methodology adopted by the European Parliament. 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 to the Intranet systems of the Parliament.

The need of a reliable teleworking infrastructure caused involvement of the ETF team within the already existing initiative for implementing Virtual Desktop Infrastructure (VDI). The ETF has gathered the requirements for the VDI from Unit EVOLUTION and managed the communication related to the pilot phase.

Since the pilot phase is considered successfully closed (since November 2014) a strict procedure for management VDI requests is set for the industrial use of the infrastructure.

In January 2015 the unit SUPPORT has taken over from the unit EVOLUTION the maintenance of this Procedural Guide and the pre-processing of the firewall configuration requests.

2. OVERVIEW

This section describes the different actors involved and gives overview of the VDI infrastructure and specifies the resources being used.

2.1 Roles

For the purpose of this guide the roles recognised and referred within the workflows hereafter are listed below. These roles are not assigned to any specific person or position within the European Parliament, but the assignment is decided by the corresponding manager per project or team.

- Teleworker – a person who is authorised to access intranet resources of the European Parliament from Internet.
- Team Leader – a person coordinating one or more Teleworkers. The Team Leader could be internal or external for the European Parliament.
- Responsible Official – an internal employee of the European Parliament who acknowledges a requested access as necessary. The Responsible Official role could be also taken by a Head of Service.

2.2 Infrastructure

The infrastructure used for teleworking is designed by Unit STANDARDS in 2014. It is known as "Virtual Desktop Infrastructure" (VDI) and it is based on Citrix v7. It replaces an older technology known as "RDS" (based on Citrix v6). A simplified scheme of the VDI is shown on Figure 1. The VDI groups/categories represent a set of virtual workstations which have similar (or one and the same) configuration.

Categories of VDI machines:

- **Basic:** This category VDI machines is more properly referred to as a "group" because when a teleworker accesses to a machine of this category each time different virtual machine is assigned to him/her. There is no option for additional software to be configured on the Basic VDI machines, besides the software already provided. The characteristics of the workstations are given in Table 1.
- **Individual:** The individual VDI machines are similar to the Basic category in terms of the capacity and the software installed. The main difference is that a teleworker receives access always to the same VDI machine. Additionally there is a possibility for additional software to be configured for this category machines. However all requests for additional software must be justified. A need for an individual machine is justifiable for testing of a new software component. Justifications are checked periodically to confirm that the need of this software is still valid.
- **Development:** This category VDI machines has a greater capacity than the other ones, and these machines are always individually assigned to a developer. By default these machines are configured to have access to EP foundry where different

development tools are available for installation. Additional standard software could be also requested via MUSTi (see section 3.3).

Table 1: VDI machines characteristics

Virtual Desktop Type	Basic/Individual	Development
Number of VCPUs	2	4
Memory (GB)	4	8
Hard Drive (GB)	60	100

Virtual Desktop Infrastructure - Simplified overview

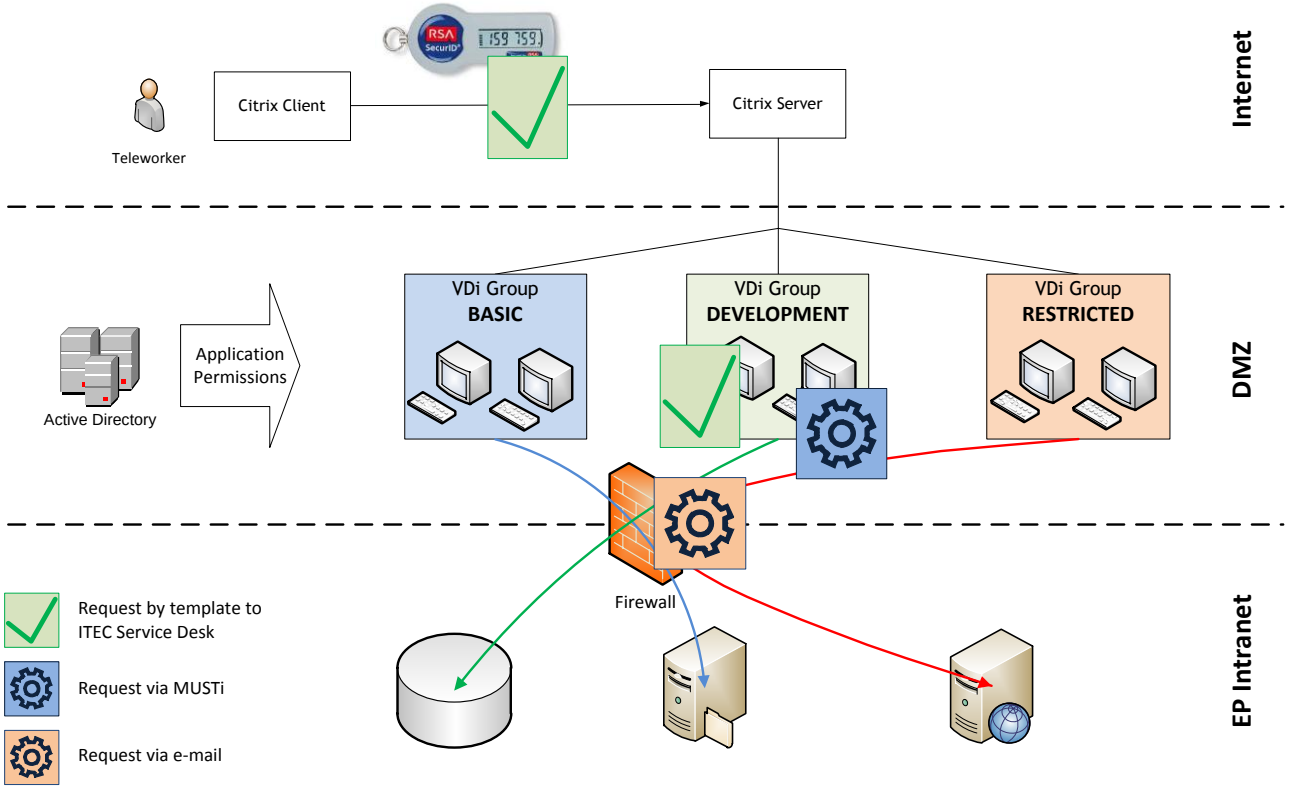

Figure 1 VDI Infrastructure Overview (simplified)

Each Teleworker is assigned to one or more "VDI Group" (e.g. Basic, Individual or Development). Once connected to the VDI infrastructure he/she must select the VDI Group to use. It is possible to concurrently use a BASIC and a DEVELOPMENT machine on the same computer (your user account just need to be authorized for both the VDI types. Then the teleworker is connected to a virtual workstation from the selected VDI Group. The virtual workstation is located in the DMZ network and it provides a set of resources defined for the VDI group – applications; access to network locations; access to databases etc.

Note: Although the Desktop applications are pre-installed on the virtual workstations, the user needs to have the corresponding rights in his/her Active Directory record in order to use them.

2.3 Comparison between the capabilities of VDI and RDS

Refer to table 2 when choosing the type of access (the teleworker machine) you need based on what resources are accessible via the different teleworking solutions

Table 2 VDI RDS capabilities

	RDS	VDI Development	VDI Individual	VDI Basic
Intranet	✓	Refer to VDI White Paper[1]	Refer to VDI White Paper[1]	Refer to VDI White Paper[1]
MS Office	✓	✓	✓	✓
MS Outlook	✓	✓	✓	✓
Additional Software	X	✓	X	X
TEFS server	✓	✓	✓	✓
Shared folders	✓	Refer to VDI White Paper[1]	Refer to VDI White Paper[1]	Refer to VDI White Paper[1]
Streamline (Prod/PP exceptions)	✓	Refer to VDI White Paper[1]	Refer to VDI White Paper[1]	Refer to VDI White Paper[1]
EP Foundry	X	✓	X	X

3. VDI REQUESTS

This section explains how to request or change access to the VDI machines. There are 7 types of requests concerning VDI resources, and most of them can only be raised by **an Official** (usually the Responsible Official). When a teleworker employed by an external company needs remote access **an Official must send a request**, providing information about the end date of the contract, the Head of the Service concerned and other relevant information as described further.

The following types of requests are processed:

1. NEW VDI MACHINE request - Teleworker needs access to a specific category VDI machine
2. A TOKEN DEVICE request – when a new teleworker needs access to VDI (or RDS or Mobile Office or all of them) infrastructure he must be provided with a token device
3. ADDITIONAL SOFTWARE request – when teleworkers need access to software that is not included in the standard configuration for their VDI machine
4. FIREWALL CONFIGURATION request – when a new set of rules must be configured for the firewall (e.g. to allow access to a new DB that would be used by the teleworker)
5. DECOMMISSIONING VDI MACHINE/ TOKEN request – Decommissioning of a token and/or VDI machine
6. REMOVING A FIREWALL CONFIGURATION request – removing the obsolete firewall configuration
7. INCIDENT request – reporting an issue that appears within using or accessing the VDI machine

These processes are shown on Figure 2 and are described in the following subsections.

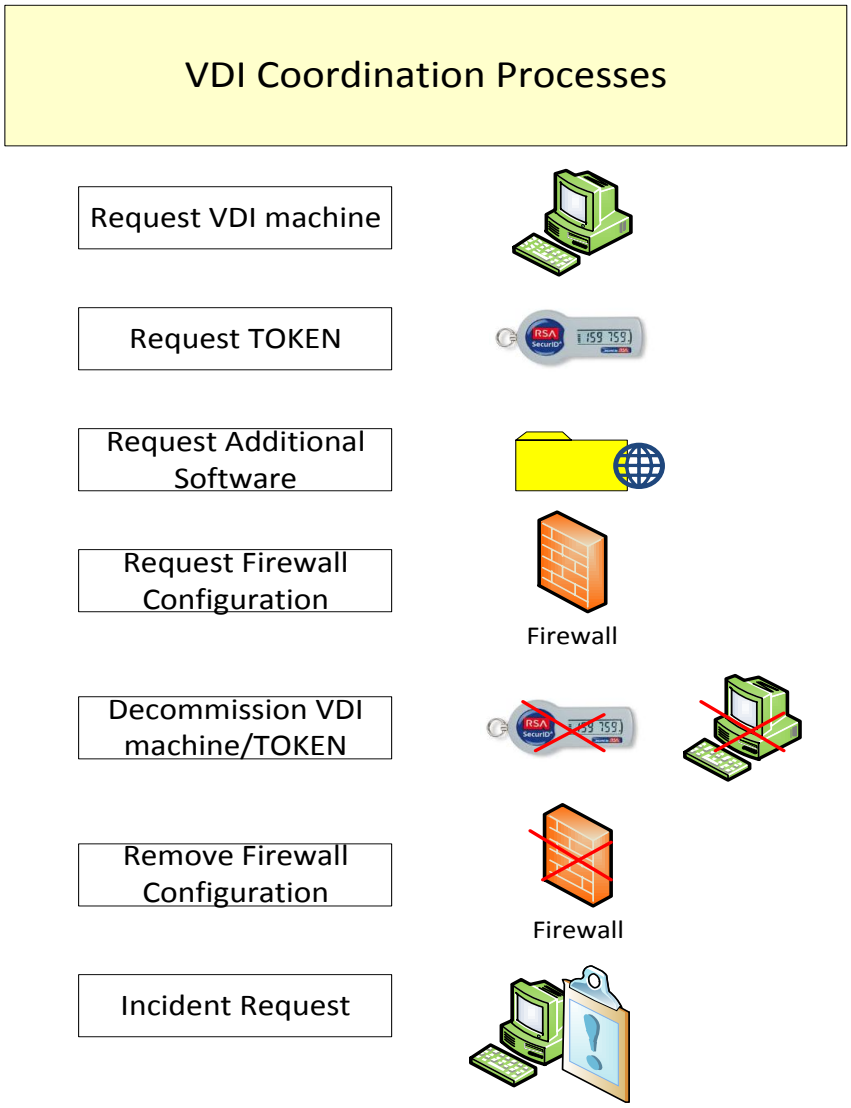

Figure 2 Overview of VDI Coordination processes

3.1 New VDI Machine Request

This process is initiated by an Official when a consultant needs to work as a teleworker, or in case the consultant needs access to an additional VDI Machines Category. Steps through the process:

If the future teleworker does not have an RSA token yet, RSA token should be requested first as explained in

1. 3.2 TOKEN Device Request.
2. The Official sends an email to ITEC Service Desk (itecservicedesk@europarl.europa.eu) using the template provided in section 6.1.
3. The ITEC Service Desk replies with an e-mail containing the EPSD ticket number of the request. This EPSD ticket number could be further used if additional software is needed for this VDI machine (section 3.3). **Note:** Additional software is not available for machines in the BASIC group.

4. When the VDI machine is configured an e-mail is sent to the requester, together with a "User Guide" for accessing the machine.

The procedure is depicted on Figure 3.

3.2 TOKEN Device Request

This process is initiated by an Official when a teleworker needs access to a VDI machine. A Token device is used for authentication each time a teleworker uses the VDI. Steps through the process:

1. The Official sends an email to ITEC Service Desk (itecservicedesk@europarl.europa.eu) using the template provided in 6.2
2. ITEC Service Desk returns an email contacting the EPSD ticket number of the request.
3. The Support Unit will process the request/s and inform the Responsible Officer when the token is ready to be picked up at one of the following locations:

   Brussels: the Computer Room in ASP 01E035
   Luxembourg: the Service Desk in KAD 05G006
   Strasbourg: the Support Unit office in WIC M0109

   The Teleworker must personally pick up the token!
4. Token must be returned if a teleworker is no longer part of the project

The procedure is depicted on Figure 4.

Note: The same Token could be also used for authentication in RDS and Mobile Office when filling in the template the requester must mark if so.

Note: When teleworker contract date expires, the token is no longer active. The responsible official should pro-actively request further extension of the token validity via ITEC SD.

Request for VDI Machine

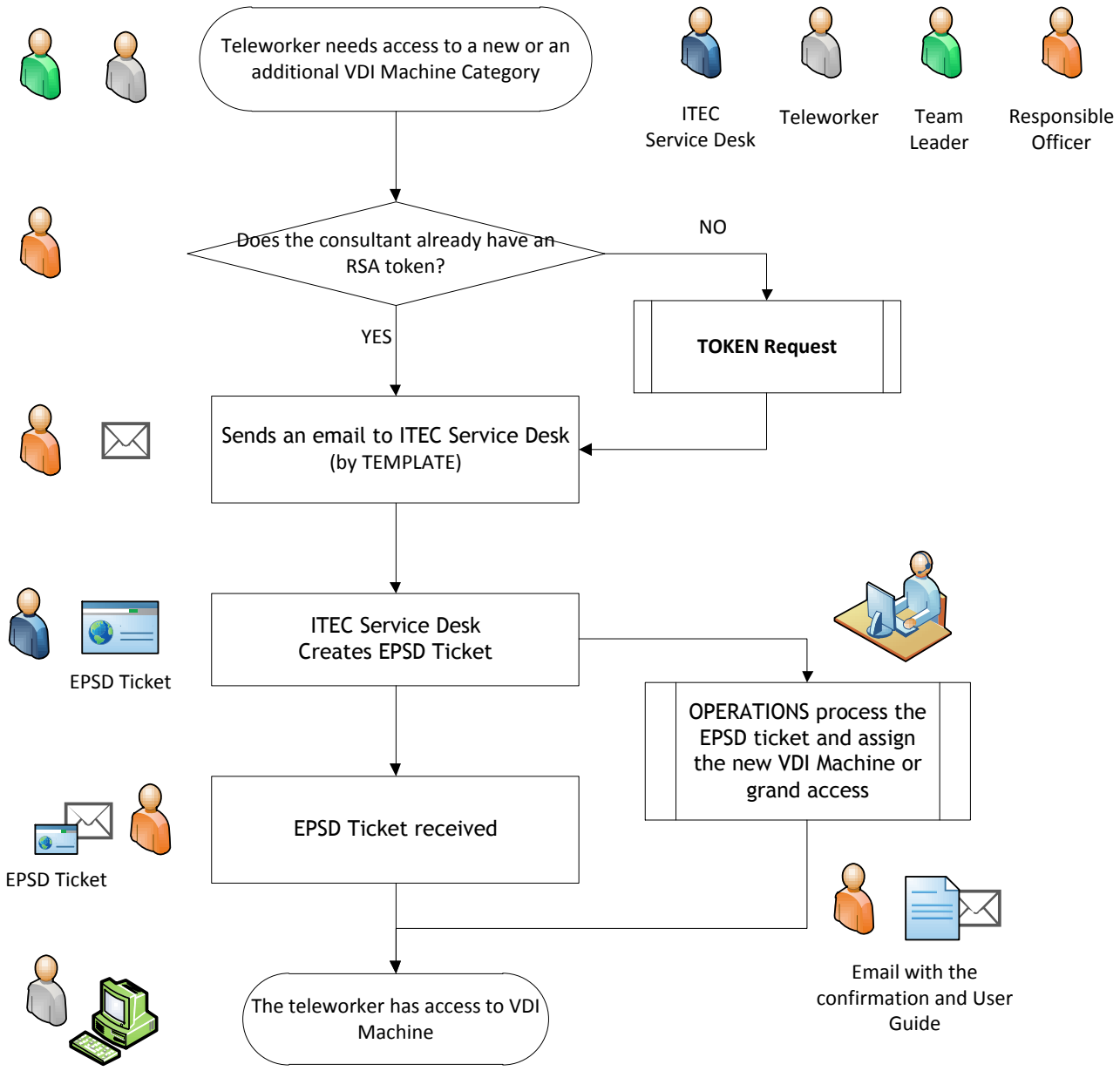

Figure 3 VDI workstation request process

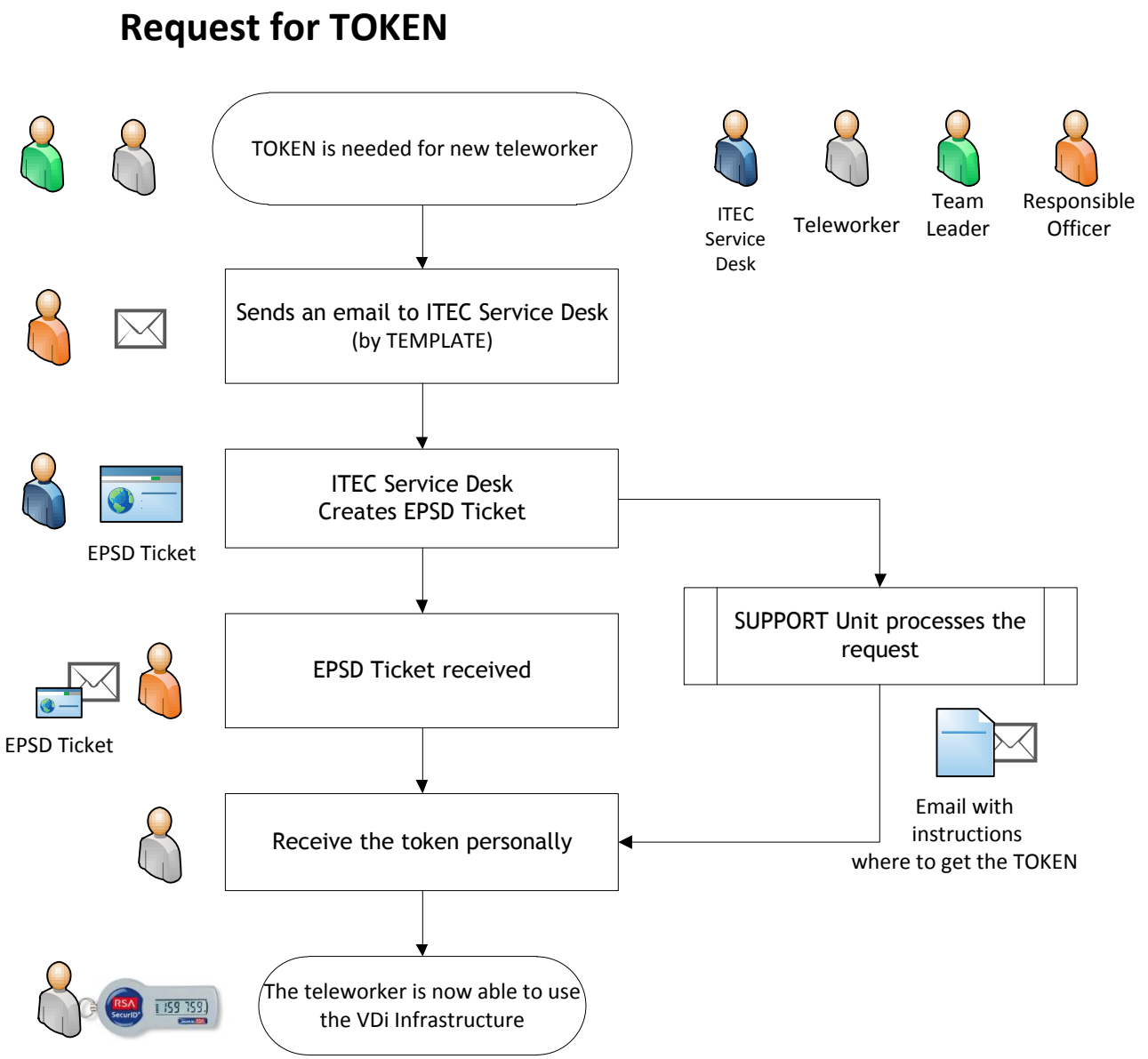

Figure 4 TOKEN request processes

3.3 Additional Software Request

Any software a developer might need that is not configured in VDI machine installation must be requested following this procedure.

A MUSTi request is for installing the software on the VDI workstation itself, but not for providing access between the workstation and the server hosting this software. If the requested software has already configured access the user should be able to access it without requesting FW configuration. In case the software is installed but there is no access, please refer to section 3.4 and follow the steps to request FW configuration.

This process is initiated by a Team Leader, when new type of software is needed for a specific VDI Machine. It consists of the following steps:

1. Team Leader creates a MUSTI Software request(http://www.musti.ep.parl.union.eu/)

2. In the MUSTI software request you have to check the “Yes” checkbox to specify that the request concern a Virtual VDI Win 7 workstation
3. Also in the field Head of Service you must put the name of the HoS for OPERATIONS to confirm with him the initial need of software

Figure 5 Snapshot of MUSTi header

4. The requester fills in the MUSTi request.
   He/she can ***select software from the provided list*** and/or ***specify software that is not available in the list*** (in the field *“Other Software or Comment”).*
   A strong justification is required in both cases!
   - The requester must fill in the filed *“Please, justify for EACH selected software”*- when software was chosen from the list.
   - Otherwise if the software you need is not in the list, please write the justification in the field *“Other Software or Comment”* after the statement for the software needed e.g. ***{name_of_the_VDI_machine} ITECLUXCVMVDI47***
     {name_of_the_requested_software} “Chrome” browser
     Justification: …..

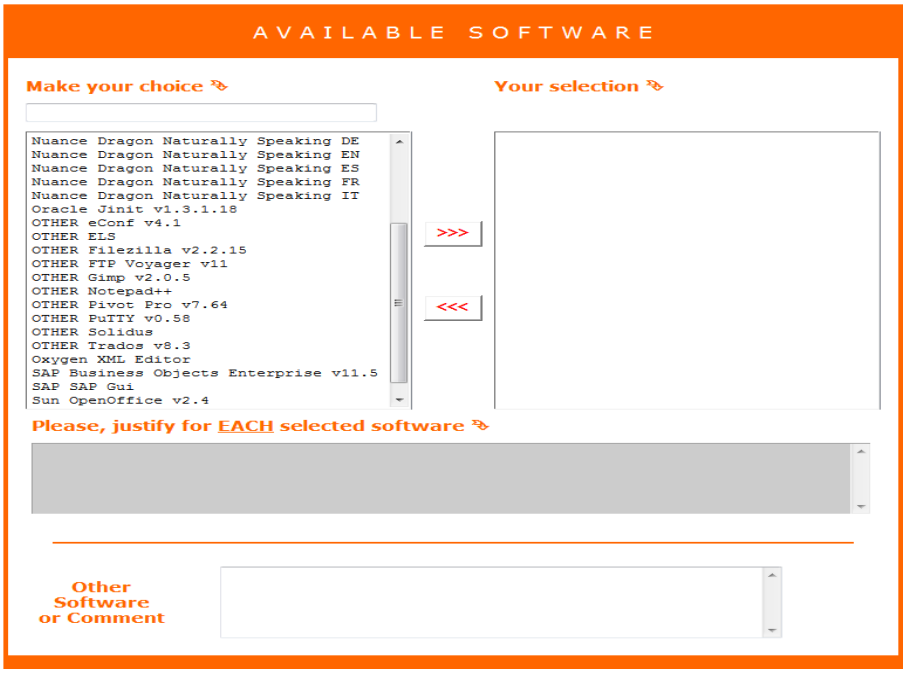

Figure 6 Snapshot of MUSTi details

5. The Support Unit will process the requests and inform the requester whether his/her request is accepted or denied
6. If the request is accepted the Support Unit will inform the requester when the software is available

The procedure is depicted on Figure 7.

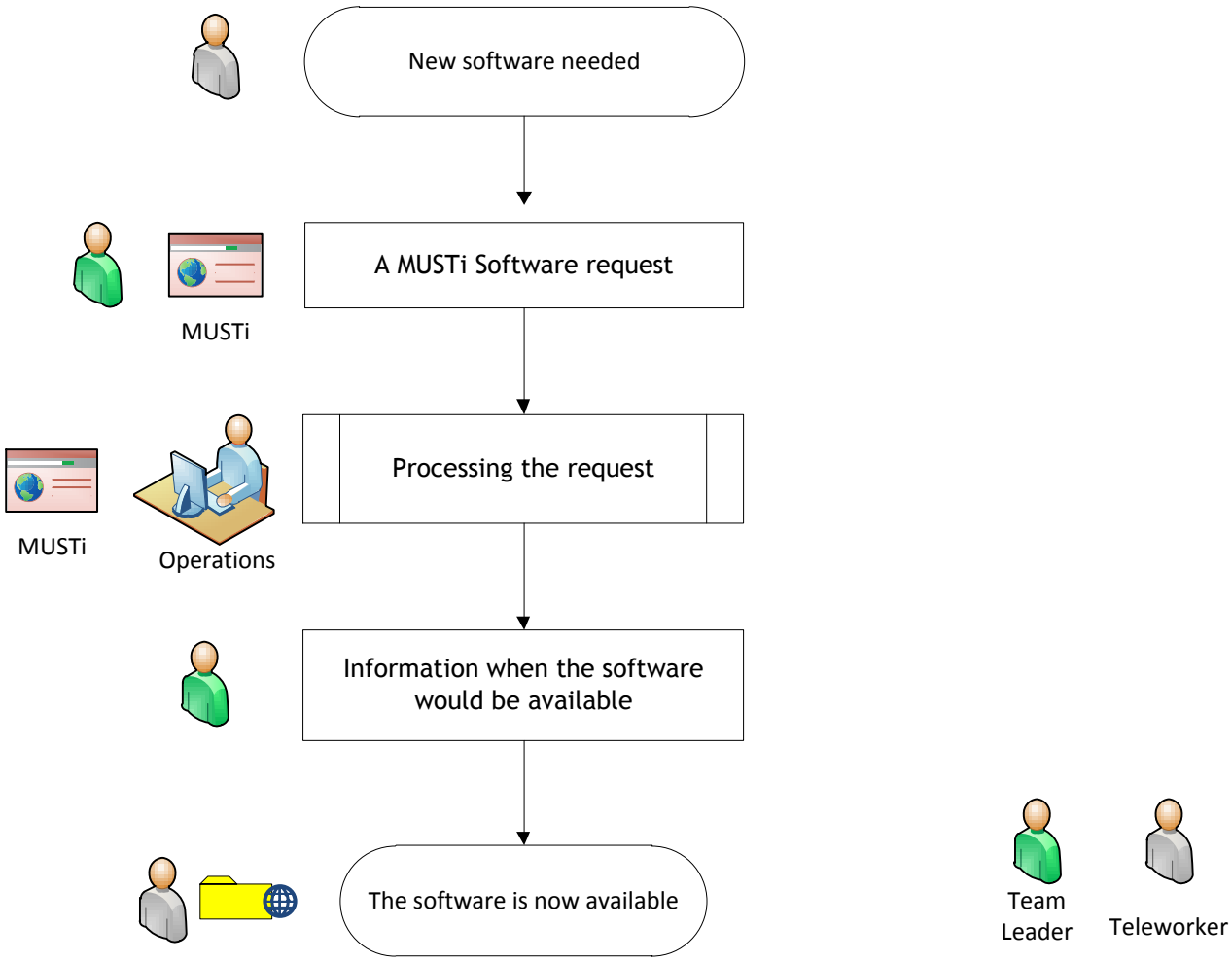

Figure 7 Additional software request coordination processes

3.4 Firewall Configuration Request

This is a process when a new rule must be set for the firewall or reverse proxy server. Usually is done to allow access to some components in EP corporate working environments. Firewall configurations are to be requested only for DEVELOPMENT environment with some already established exceptions from PP and PROD defined in "White paper on the VDI infrastructure" [1]

As regards the VDI machines, the firewall configurations apply to the entire VDI group (they are not individually set for a VDI machine). As regards the servers, the firewall configurations are individually set (a network port that has been opened for a specific server is not available for other servers).

Steps to be followed:

1. The Official sends an email to ITEC Service Desk (itecservicedesk@europarl.europa.eu) using the template provided in 6.3.
   A strong justification must be provided in order the request to be accepted.

2. The Support Unit will process the request and inform the requester whether his/her request is accepted or denied.

3. If the request is accepted the Support Unit will process the request and inform the requester when the new firewall configuration is active.

TEFS server requests are to be processed in the same way using the same template. However a list of dedicated/available TEFS machines is kept on the Wiki page:

http://www.ep-foundry.ep.parl.union.eu/wiki/display/ALSA/TEFS+-+Technical+Environment+for+Forge+Software

At future TEFS servers would be accessible via reverse proxy. For now OPERATIONS need an alias to be specified for details refer to [1].

3.5 Decommissioning VDI Machine/ TOKEN Request

This process is started by an Official (usually the team leader) in case a workstation and/or TOKEN is no longer needed. The procedure is depicted on Figure 8.

1. The Responsible Officer confirms which resource should be removed.
2. If the resource is still needed the Responsible Officer denies the request. The process stops here.
3. If no objection is received within 8 weeks, the Responsible Officer sends an email to ITEC Service Desk (itecservicedesk@europarl.europa.eu) using the template provided in 6.5 requesting the resources to be removed.
4. The operators execute the necessary configuration and close the EPSD ticket.

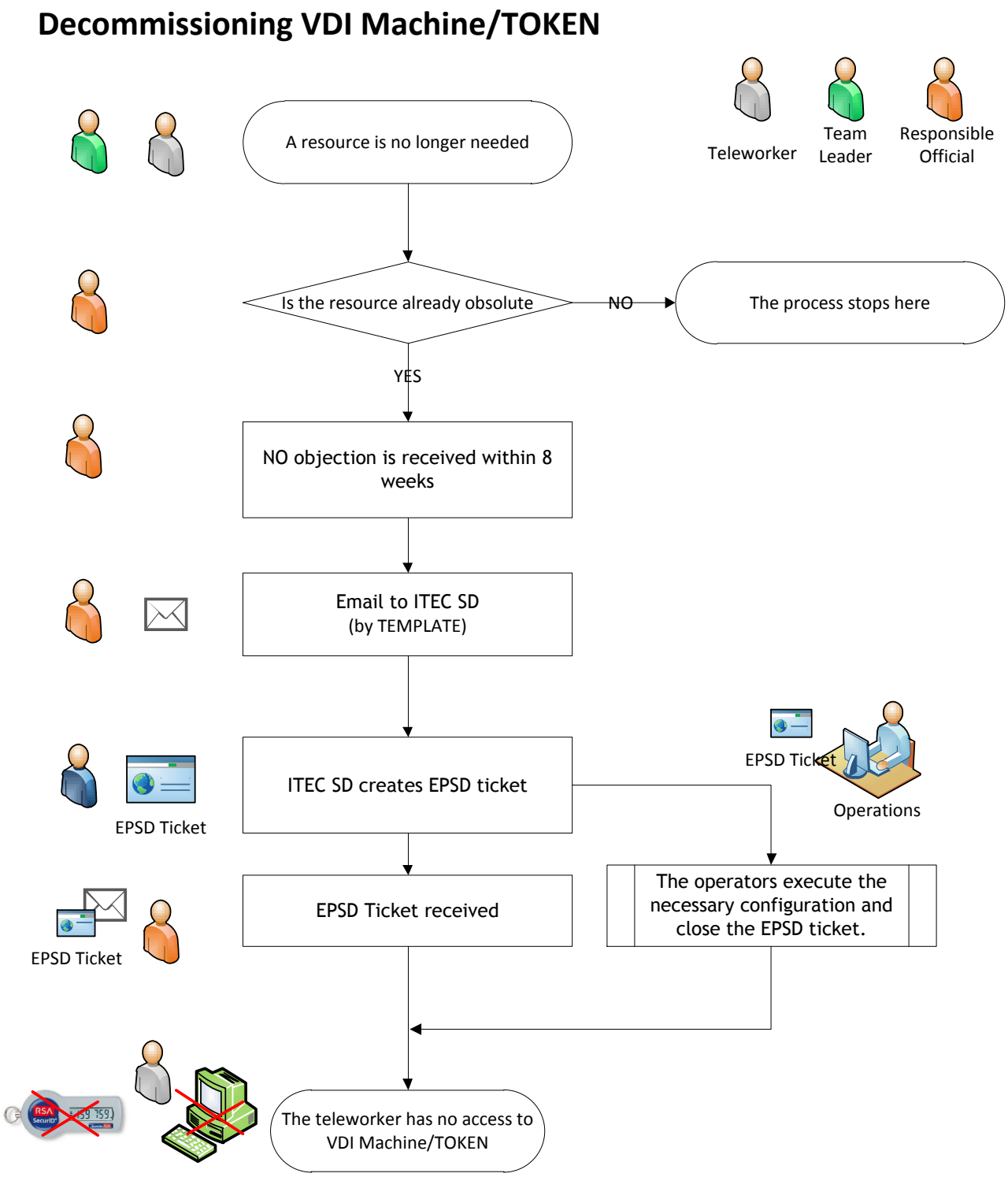

Figure 8 Decommissioning VDI machine request coordination processes

3.6 Removing a Firewall Configuration Request

This process is started by an Official in case a Firewall Configuration is no longer needed. In the template provided in 6.6 a brief description of the situation is needed (e.g. the firewall configuration was used to allow access to specific DB but this access is no longer needed since {describing the circumstances})

1. The Official sends an email to ITEC Service Desk (itecservicedesk@europarl.europa.eu) using the template provided in 6.6.
2. The Support Unit will process the request and inform the requester whether his/her request is accepted or denied.
3. If the request is accepted the Support Unit will process the request and inform the requester when the requested firewall configuration is completed.

The procedure is depicted on Figure 9.

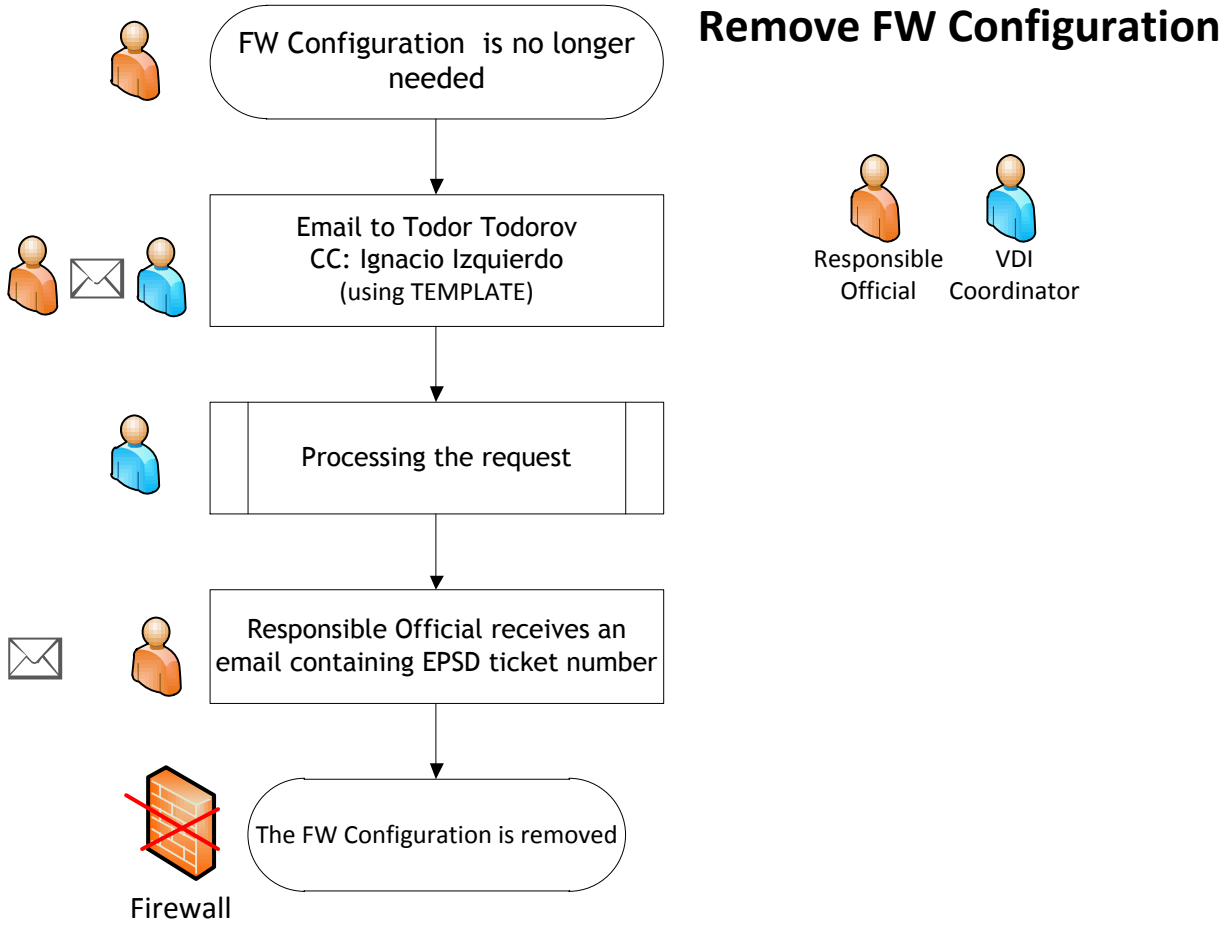

Figure 9 Remove FW configuration request coordination processes

3.7 Incident Request

This process is initiated when an existing VDI resource is not properly working.

1. The teleworker or his/her Team Leader sends an email to ITEC Service Desk (itecservicedesk@europarl.europa.eu) using the template provided in 6.4
2. ITEC Service Desk returns an email contacting the EPSD ticket number of the request.
3. The Support Unit will process the request and might contact the requester for additional details
4. The requester is informed for the resolution of the problem by ITEC Service Desk

The procedure is depicted on Figure 10.

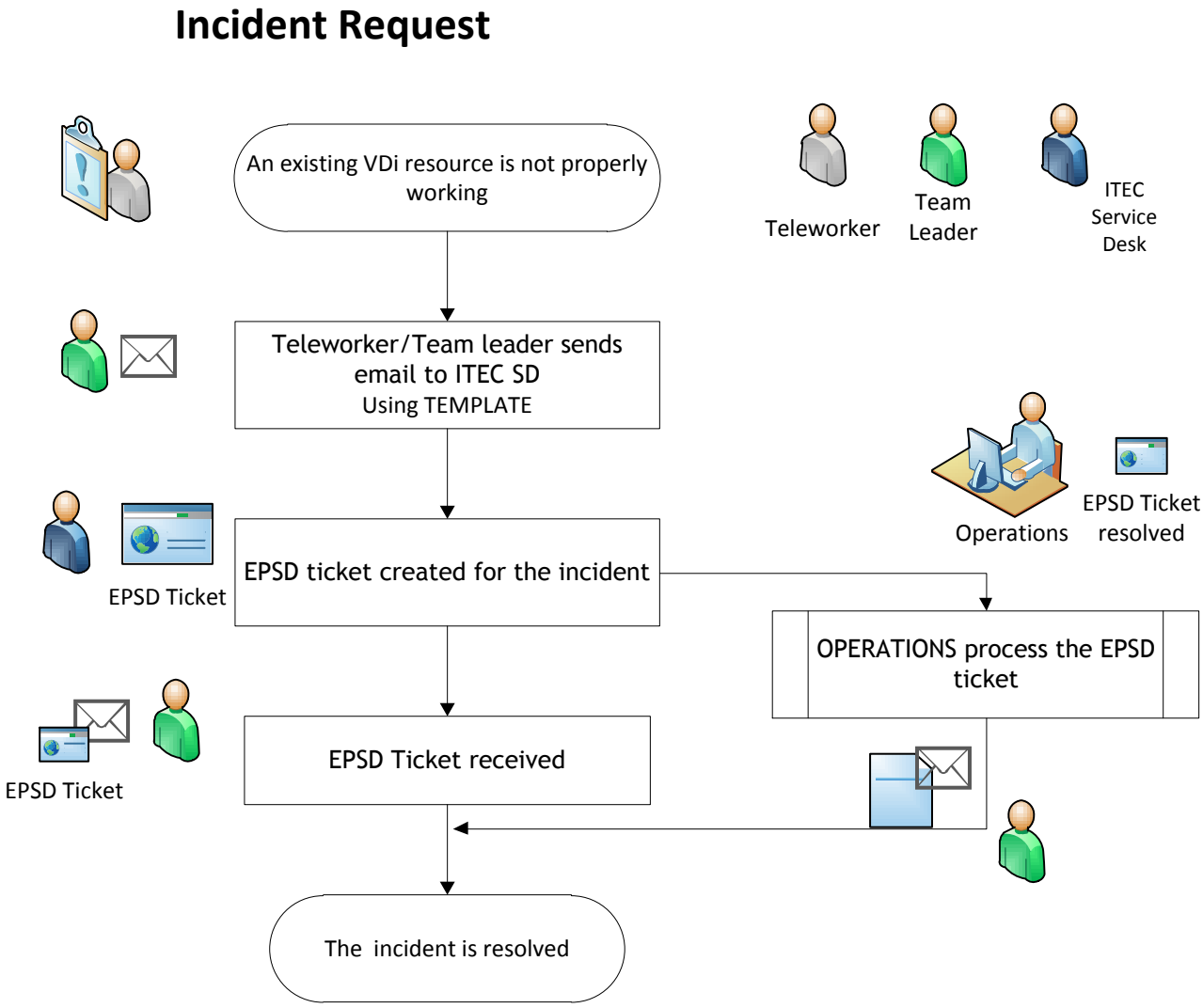

Figure 10 Incident request coordination processes

4. TELEWORKER'S WORKSTATION – SECURITY POLICIES

4.1 LSAs disable the local drives mapping

On the teleworker's local workstation, local drives could be: Hard-disks/partitions; USB memory sticks; External hard-disks; Memory cards (like those in Figure 11).

In short, any device that receives a drive letter once physically connected to the workstation.

There is the possibility to see all these local drives mapped in the Virtual Machine. It depends on the settings imposed by the LSAs.

The following picture shows a Virtual Machine with its C: and D: drives + a C/D/E drives that have been mapped from the teleworker's workstation.

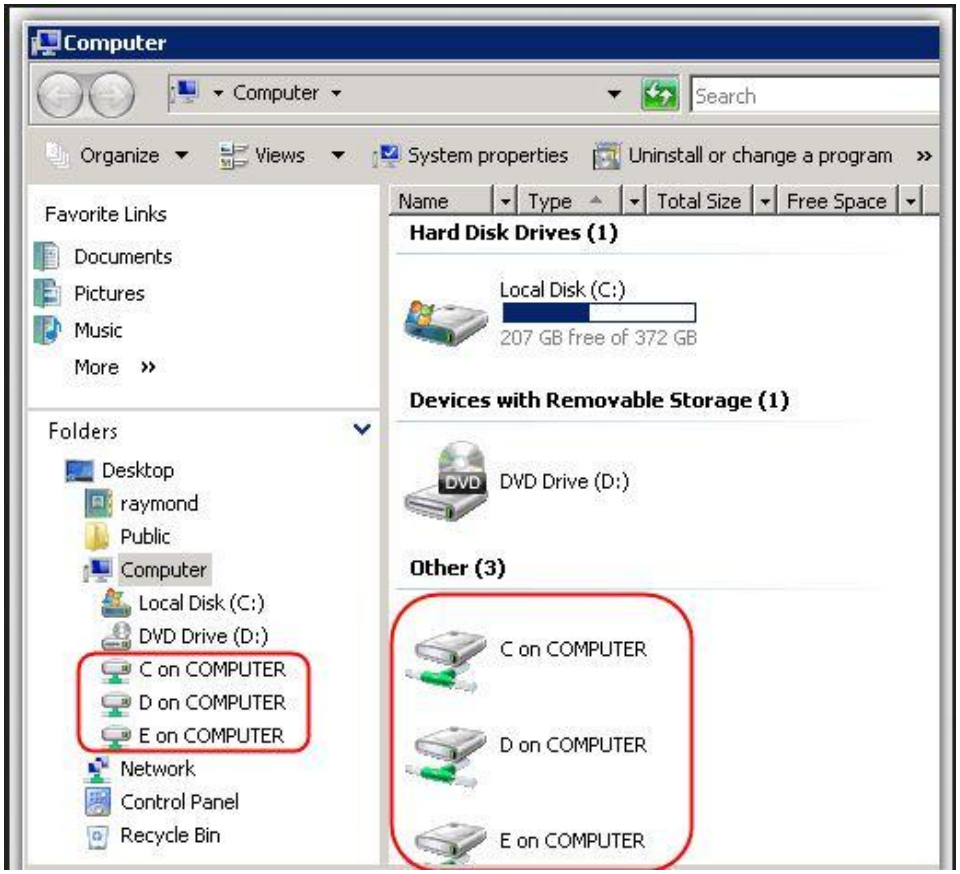

Figure 11 Local drives mapping

In this way it is easy for the teleworker to transfer a file from his/her workstation to the Virtual Machine: it is just a copy-&-paste from one of the local mapped drives to the C drive of the Virtual machine.

Why this scenario should be disabled by an LSA?

To improve security - Transferring a file in this way means that the only security check is made by the local anti-virus of the Virtual Machine.

If the LSAs disable the local drives mapping, the only way to copy a file from the teleworker's workstation to the Virtual Machine is sending it by e-mail as attachment.

In this way, the file can be double-checked: first by the anti-virus of the e-mail environment then by the anti-virus of the virtual machine. These anti-viruses are different products, in order to maximize the ability to detect any malware that could be embedded in the file.

5. FAQs

Q. Externals who've been declared offside in Conex no longer exist in Codict and EPDIR

The side effect of this is that they cannot use the applications using sso based on Codict information:

- no more access on EPSD (impossible to created USD, following the tickets of the team,...)

- no more access on KM Portal, the application they are working on...

A. Codict recently (6 January) changed its data main source for external consultants of DG ITEC. Information related to activity of external people now comes from CONEX application. It has been decided and communicated to concerned people that only Extra-Muros and Intra-muros contract types are transferred to CODICT. The different type of contract/activity, such as Ambulatory is no longer stored in CODICT, so the **teleworkers must be declared as Extramuros in CONEX**

Q. Token no longer works

A. Responsible Official should update the Token request information by sending an email to ITEC SD containing the new contract date for the teleworker

Q. Connection after authentication fails

A. In case of connection problem, user is able to restart his/her machine by right-clicking on the shortcut and then choosing 'Restart'.

6. ANNEX - DOCUMENT CONTROL

5.1 Change history

Version number[1]	Status[2]	Date	Initials	Summary of changes
0.1	Draft	16/04/2014	TT	Initial draft
0.2	Draft	23/04/2014	TT	Update after comments from TL
0.3	Draft	20/05/2014	TT	Update after meeting with MW and TL
0.4	Draft	28/10/2014	TT	Reflecting new updates, document shared with other services
0.5	Draft	05/11/2014	TT	Updates after a meeting with other services
0.6	Draft	10/11/2014	PM	Major updates after discussion with ACAS
0.61	Draft	10/11/2014	TT	Minor updates
0.7	Draft	11/11/2014	PM	Updated templates, procedures
0.8	Draft	12/11/2014	PM	Figures added
1.0	Final	12/11/2014	PM	Promoted to v1.0
1.2	Final	18/11/2014	PM	Changes in section 3.3
1.3	Final	24/11/2014	PM	Section 4 added
1.3	Update	02/12/2014	TT	Minor: Internal cross-references of figures updated
1.3	Update	02/12/2014	PM	Minor: template in 6.1
1.4	Update	16/12/2014	PM	Section 3.4 added information
1.5	Update	09/01/2015	PM	Section 3.3 added information
1.6	Update	21/01/2015	PM	Section 3.2 added information, Section 5 added
1.7	Update	26/01/2015	AQ	Minor updates for the VDI Coordination handover from EVOLUTION to SUPPORT

5.2 Reference documents

N°	Document name	Description
[1]	"20150112_VDI_White Paper on VDI infrastructure_EN_v05"	White Paper on the VDI Infrastructure

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

[2] Status: Draft, Final, Approved

7. OTHER ANNEXES

6.1 New VDI Machine Request TEMPLATE

VDI Machine Request
User logon name*: **Provide the logon name that will be associated with user account to access VDI**
User:
Responsible Official*:
Head of Service*:
Category VDI machine*: ☐ **Basic** ☐ **Individual** ☐ **Development** **Please, Choose one Checkbox**
DG concerned:
Unit and Service concerned:
Team leader:
Contract №:
Contract END DATE*:
Justification*: **Please, provide a complete justification for the assignment of VDI machine. It would be further used in the periodical resources checks to indicate if the recourses are managed properly**
*** All the fields marked are mandatory**

6.2 TOKEN Device Request TEMPLATE

TOKEN Device Request
User*:
Responsible Official*:
Head of Service*:
Authenticated Access to*: ☐ **VDI** ☐ **RDS** ☐ **Mobile Office**
DG concerned:
Unit and Service concerned:
Team leader:
Contract №:
Contract END DATE *:
*** All the fields marked are mandatory**

6.3 Firewall Configuration Request TEMPLATE

VDI CONFIGURATION - FIREWALL Request
Responsible Official*:
Application HOST*:
IP Address*:
Port*:
Type of environment: ☐ **Development** ☐ **Integration** ☐ **Pre-production** ☐ **Production** ☐ **Professional Training**
Application related:
Justification*: **Please, provide strong justification for the requested firewall rule configuration including how many people it affects and which tools/resources correspond**
*** All the fields marked are mandatory**

6.4 Incident Request TEMPLATE

VDI INCIDENT Request
User*:
Request Initiator*:
DG concerned:
Unit and Service concerned:
Contract №:
Contract END DATE *:
Incident description*: **Please, describe as detail as possible the incident occurred**
*** All the fields marked are mandatory**

6.5 Decommissioning VDI Machine/ TOKEN Request TEMPLATE

DECOMMISSIONING VDI Machine/TOKEN Request
User*:
Request Initiator*:
☐ **VDI Machine hostname:** ☐ **TOKEN serial number:** **Please, specify the number of the machine/TOKEN**
Reason:
*** All the fields marked are mandatory**

6.6 Removal of Firewall Configuration Request TEMPLATE

VDI FIREWALL REMOVAL Request
Responsible Official*:
Application HOST:*
IP Address*:
Port:*
Application related:
Justification*: **Please, briefly describe the situation**
*** All the fields marked are mandatory**