EUROPEAN COMMISSION
DIRECTORATE-GENERAL
INFORMATICS
Directorate C - Infrastructure services provisions
Infrastructure Services Coordination and Customer Relationship

DIGIT

Infrastructure Services Provision Service Catalogue

Remote access for companies

Date:	30.08.2012
Version:	1.04
Reference Number:	

Commission européenne, B-1049 Bruxelles / Europese Commissie, B-1049 Brussel - Belgium. Telephone: (32-2) 299 11 11.
Commission européenne, L-2920 Luxembourg. Telephone (352)43 01-1

Document History

Version	Date	Comment	Modified Pages
1.00	24/06/2009	Document created by HVH and revised by DIGIT C4.	All
1.01	20.07.2010	Document links updated	
1.02	03.02.2011	Document updated	All
1.03	07.11.2011	Links updated	All
1.04	30.08.2012	Remote access kit and SMT ticket creation	All

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Service Purpose

The aim of this service is to give the business partners[1] (with a contractual obligation) within the European Commission (EC) IT department's secured access to specific EC Information Technology resources.

1.2. Document purpose

This document specifies the current service provided by DIGIT.C.

1.3. Document organisation

The document is organised as follows:

- Description of the service element
  - who is this service for
  - scope of the service
  - technical description
  - pre-requisites, i.e. what must be respected to benefit from the service
  - Features
  - Security
  - Service provisioning
  - Limits of the service, i.e. what is not provided by the service
  - roles and responsibilities, i.e. who does what
  - service management
- Related documents and web sites

1.4. Document Audience

The target audience of this document are:

- The DG's and entities of the EC such as PMO & OIB & OIL who intend to grant an external company access to EC Information Technology resources.
- Any company (via a contractual obligation) that need to access EC Information Technology resources.
- Any other person involved in the preparation, validation and signing of a security convention preceding to the activation of the access permissions.

The audience must be covered by the appropriate confidentiality clauses including:

- Commission officials
- Contractors
- Applicants for Calls for Tenders[2]

[1] Business partners also called in this document 'external companies'

[2] this document can be sent outside the European Commission to organisations that have signed a Non Disclosure Agreement.

1.5. Definitions, Acronyms and Abbreviations

HR DS: Security Directorate, part of DG HR which is in charge of defining the information systems security policy of the EC.

AES-256: The Advanced Encryption Standard (AES) is an encryption standard developed by two Belgian cryptographers

DC: Data Centre of the European Commission

DIGIT: Directorate of Informatics at the European Commission

DIGIT C1 ISHS: Information System Hosting Services Unit

DIGIT C2 NS: Section dealing with Network Services

DG: Directorate General

EC: European Commission

IP: Internet Protocol, a data-oriented protocol used for communicating data across a packet-switched network.

IRM: Informatics Resources Manager

Security Convention: a document describing the conditions under which a user or service of the EC can install and make use of a specific connectivity, not allowed by the Security Policy of the EC in normal circumstances

SLA: Service Level Agreement

SNET: service owned by the DIGIT.C, in charge of the design, management and support of the IP internal network and the Telecom Centre

TCP: The Transmission Control Protocol (TCP) is one of the core protocols of the Internet Protocol Suite.

Token: A security token (or sometimes hardware *token*, *authentication token*) is a physical device that an authorized user of computer services is given to perform the authentication.

1.6. Glossary

A glossary of DIGIT.C terms can be found at
http://www.cc.cec/home/dgserv/digit/tools/glossary/index_en.htm

2. SERVICE ELEMENT DESCRIPTION

2.1. Who is this service for?

- The owner of information systems hosted at either the Data Centre or in a DG and who wants to grant their business partners remote access to their information system(s) to allow them to fulfil their contractual obligations.

- The DG's who have contracts with business partners for remote maintenance on servers/appliances.

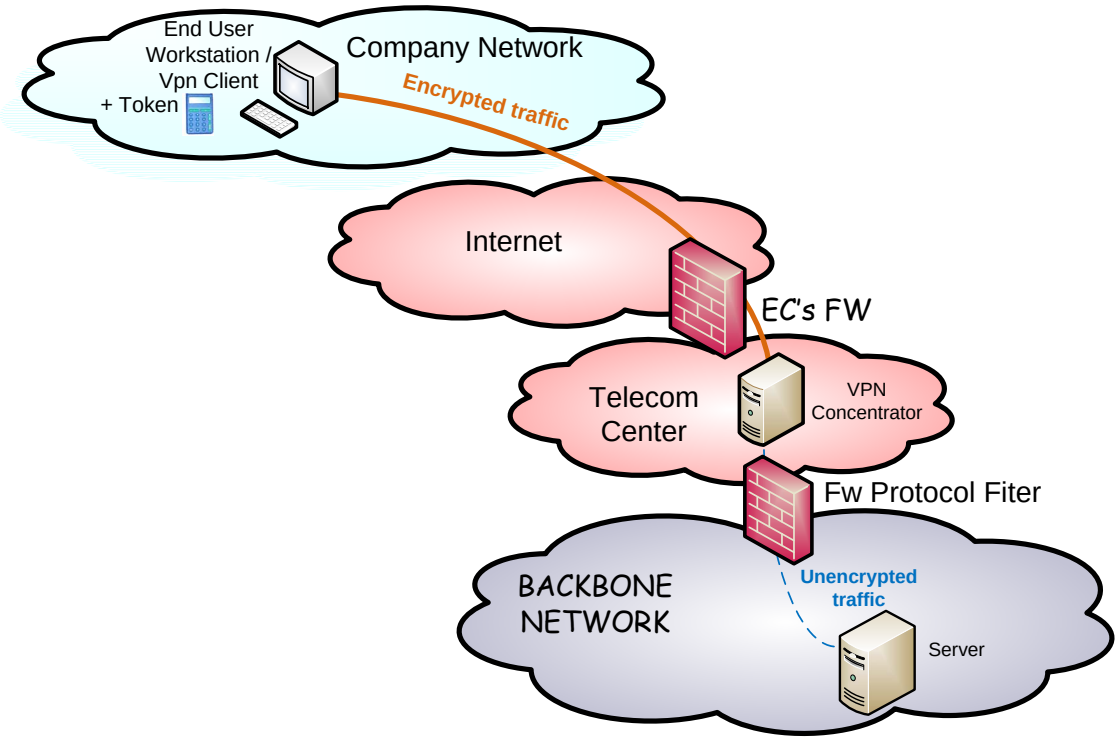
2.2. Service Scope

The scope of the service offered by DIGIT C2-NS is to filter IP traffic at the boundary of the European Commission intranet before it enters the European Commission network.

There is always a strong authentication from the company and each authenticated source has its own set of Firewall rules allowing access to a restricted list of destinations until a specific end date.

2.3. Technical description

2.3.1. Architecture



There is always a strong authentication from the company via a "token[3]" device. The actual authentication is carried out from inside the EC telecom centre.

The network traffic between the remote-end workstation and the VPN concentrator is tunnelled and encrypted (AES-256) once the remote user is successfully authenticated[4].

Any TOKEN device assigned to a specific company (security convention) can be used for the remote-end authentication. All those Tokens are linked to the authorised list of accesses.

The protocol filtering is performed by firewall equipments configured with a set of rules. Each rule has an expiry date that matches the expiry date of the security convention to which it refers to. In addition - each firewall rule has a set of parameters which are:

- Source IP address / Source port number
- Destination IP address / Destination port number
- IP protocol number
- End Date

[3] TOKEN device used for one time password authentication

[4] One timepassword generated by a TOKEN device

- Maximum session duration = 10h
- Idle time out is 30 minutes

2.3.2. Software products

Software VPN client for Windows OS.

2.3.3. Hardware products

The token device used to authenticate the user.

Harware VPN client for all non Windows OS.

2.4. Pre-requisites

This section describes the constraints that must be respected by the client before using the service.

2.4.1. Security convention

A security convention is a formal agreement defining the conditions under which the external company shall perform the remote interventions on the specific EC Information Technology resources. A security convention is concluded between the representatives of ADMIN DS, DG[5] or service of EC and the external company.

A security convention is divided in 2 parts:

- A first part (**Part 1**) describes the physical and logical protection measures and the sub-network of the external company. The information provided by the external company is the subject of validation performed by ADMIN DS.

- A second part (**Part 2**) defines the conditions for remote intervention and specifies the list of remote accesses required for the external company to fulfil their contractual obligations. The list of requested accesses is the subject of validation performed by ADMIN DS and DIGIT.

The validity of a security convention is linked to the duration of the contruactual relationship, including a list of deliverables between the external company and the DG or service of EC.

The workflow used to establish a security convention is coordintated by ADMIN DS and contains the following 4 main phases: preparation, validation, signature and implementation. More information about this procedure is available on "Procedure for the creation and amendment of a Security Convention".

[5] IRM and LISO

2.4.2. Token and VPN client software

The external company needs a token for their access in order to be authenticated at the border of the EC network. Once the security convention is duly signed by all parties and implemented by DIGIT, the IRM team of the requester DG can order one (or more) token device(s). This device together with a VPN client will be sent to the external company.

2.4.3. Technical knowledge

During the preparation phase:

- The requester DG together with the external company shall be able to provide detailed information about network flows related to the applications they want to reach. DIGIT ISHS shall be consulted in case the application is hosted at the Data Centre.

For the remote access to the EC domain:

The external company must know **how to install the** Remote Access Kit for External Companies (SE) available on http://www.cc.cec/digitline/r/products/ntpref/rak/index_en.htm#raklap

- and must know **how to use a TOKEN device**.

2.5. Features

2.5.1. Environments

Upon receipt of the request for implementing the security convention from ADMIN DS, the requested accesses are configured in the production firewalls. There is no test (firewall) environment available.

2.5.2. Service resiliency

The network path between the remote-end workstation and the remote WAN access (typical internet) is out of control of the EC. The EC internet access, the VPN concentrator and the connectivity between the EC telecom centre and the internal network are fully redundant. The network patch between the EC internal information technology resources and the internal network could be redundant. This will be checked on a case by case basis.

2.5.3. DNS name resolution

No DNS service is offered.

2.5.4. Protocols allowed

Only the protocols listed in the security convention are allowed till the end date of the security convention.

2.6. Security

2.6.1. Data integrity

The data integrity is not altered by the service

2.6.2. Personal Data

Every external access is logged in the firewall management system. The log files are kept for duration 6 months.

2.6.3. Encryption

The communication between the remote end and the EC boundary is encrypted[6] once the remote user is successfully authenticated.

2.7. Limits of the service

2.7.1. Compliance with the rules

For all remote interventions, the external company must comply with the rules defined in the **security convention**.

2.7.2. Access restrictions

At the remote end (companies network), access to the internet or any other network either local or remote is not permitted[7] when the VPN tunnel to the EC network is established.

2.7.3. List of authorised accesses

Only the list of authorised accesses specified in the security convention is allowed for the remote intervention. By default all IP traffic is blocked[8] except the IP traffic listed in a valid/active security convention. The goal is to limit TCP/IP traffic between a specific individual external company and specific EC internal information technology resources. Keeping this to a minimum will still allow companies to fulfil their contractual obligations they have with the EC. Certain "IP" protocols that could jeopardise the other EC internal information technology resources are not allowed.

2.7.4. Authentication/Identification mechanism

At the boundary of the Commission´s network, the mechanism is a token. In addition, specific access controls[9] are in place for each resource in the list of authorised accesses.

---

[6] AES-256

[7] Is blocked by the VPN client

[8] http/HTTPs access to public EC webservers is always allowed

[9] See annexe V in Part2 of security convention

2.7.5. Limited period of validity

A security convention, as a prerequisity for this service, is active as long as there is a contractual relationship, including a list of deliverables[10] between the external company and one of the EC services.

2.8. Service Provisioning

2.8.1. Service primitives

The different service primitives are;

- Service provisioning;
  - Request for a ***new*** TOKEN.
  - Request to set-up a ***new*** 'remote access for an external company'.
- Standard Service operations (once the service is 'provisioned');
  - Request to ***change*** an existing security convention.
  - Request to ***keep*** an existing security convention.
  - Request to ***keep*** a TOKEN for another year[11].
  - Request for ***assistance*** (restore of the service) in the case of a problem on the 'remote access for an external company'.
  - Request for ***information*** in the case the scope of the service is not understood.

[10] Specific agreements

[11] Maximum one year depending on the life time of the security convention

2.9. Roles & Responsibilities

Multiple services are involved in the service delivery process. Each of them has its specific role and responsibility. The services involved are:

- The Company who is using the service,
- The Companies IT department who must install the VPN client and perform incident management of incidents on the companies local (remote) network,
- The requester DG[12] who is for the service provisioning process - the interface between the company and the EC,
- The IRM team who is (during working hours) the interface between the company and the EC IT departments,
- The CHD who is (outside working hours) accepting and registering incident tickets,
- HR for the information systems security policy of the EC and the security convention,
- DIGIT ISHS; If the information system is hosted in DIGIT/C, DIGIT C1-ISHS ***can*** provide hosting-related technical information[13].
- DIGIT.C3 (UAA) for the TOKEN management and the distribution of the VPN software client and a VPN hardware client,
- DIGIT C2 SNET for the incident handling on the EC IT domain and the implementation of the security mechanism.

2.9.1. IRM team specific tasks (during working hours);

The IRM performs the first level support and use SMT to escalate incidents.

IRM specific tasks are;

- In the case of a problem (during working hours) or a need for clarifications, diagnose problems and create a SMT ticket when deemed necessary.
- Create a SMT ticket for standard service request like;
  - a request for a new remote access,
  - Change on an existing access,
  - keep the access later than the end date of the security convention
- Use SMT-ES for a request for a new TOKEN or for a prolongation of an existing TOKEN.

Each DG (IRM) has access to his security conventions. Those security convention documents are stored and maintained by HR. Adding the security-convention-ID to the SMT ticket will have a positive effect on the time to resolve an incident or the time to implement a change.

[12] IRM

[13] During the preparation phase (Change Coordinators: DIGIT ISHS CCOR)

Important SMT information fields to take into account for each type of request are;

SMT ticket created when:	Incident type	CI	Supplementary info.
Req. access for a new company	Req. for service	Security Convention-T01	
problem on an existing TOKEN	Incident	TOKEN-ID	RAS troubleshooting.XLS
Problem on a remote access	Incident	security-convention ID	
Request For Information	Req. For Info.	security-convention ID	
Request For Change for an access	Req. for change	security-convention ID	
prolongation of a sec. Conv.	Req. for change	security-convention ID	
SMT-ES			
request for a new TOKEN	request to be made via SMT-ES		
keep a Token for another year	request to be made via SMT-ES		

2.9.2. Processing of SMT requests during working hours

Multiple services are involved in the service delivery and operational phase.

- The IRM must use the CI's defined for this service "TOKEN service' or 'Security-concvention-T01' or the “security convention ID”. This CI together with the SMT 'skill match'  function will make sure that the ticket is directly assigned to the concerned service.

- The local support desk should fill out the RAS troubleshooting.XLS guide before assigning the SMT ticket.

- Any other SMT request will be analysed first by the Central Helpdesk service before it is assigned to the concerned services.

2.9.3. Processing of SMT requests outside working hours.

- The company must (for **critical or urgent** incident management only) make a telephone call to the Central help desk that will, when needed, dispatch the call to the concerned service.

2.10. Service management

2.10.1. Point of contact

During working hours, see 2.9.2.

Outside working hours, see 2.9.3.

2.10.2. Service Desk Opening hours.

HR, SNET, UAA and the Central Help Desk, the IRM and the external company are collaborating during the service management process.

HR, SNET, UAA and the CHD have a Service Desk function at the EC premises with dedicated working hours. CHD and SNET are on-call outside working hours. The time to intervene, during business hours and during on-call hours, will depend on the specific contractual OLA.

	Service desk working hours		
	Week		
	From	**To**	**Week-end**
CHD	7h	20 h	Not Applicable
SNET	7h	19 h	Not Applicable
UAA	8h30	17 h	Not Applicable

HR	8h30	17 h	Not Applicable

	on-call hours		
	week		
	from	to	Week-end
CHD	20h	7h	24h/24h
SNET	19h	7h	24h/24h
UAA	not applicable		
HR	not applicable		

2.10.3. SLA: Incident handling.

	restore time	
	Incident priority	SNET
working hours	Normal calls	9 h 00
	Urgent calls	2 h 15
	Critical calls	1 h 15
on-call	Urgent calls	4 h 30
	Critical calls	2 h 30

3. DOCUMENTATION AND USEFUL LINKS

- Service Catalogue page http://myintracomm.ec.europa.eu/corp/digit/en/isp_service_catalogue/pages/isp_service_catalogue.aspx
- SICMOB application containing the exhaustive list of GBI : http://sicmob.cc.cec.eu.int:9000/