EUROPEAN COMMISSION
DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY
Directorate HR.DS - Security
Informatics Security

Remote Access for Companies

Procedure for the creation and amendment of a Security Convention

Date:	07/07/2015
Version:	2.6
Ares Reg. number:	Ares(2015)2847392–07/07/2015
Contact:	EC-SECURITY-SECURITY-CONVENTIONS@ec.europa.eu

Document History

Version	Date	Notes
1.0	18/07/2005	CREATION
1.1	04/10/2005	CHANGED AMENDMENT PROCEDURE (PS)
2.0	10/07/2006	CHANGED FOLLOWING EVALUATION PERIOD
2.1	21/08/2006	COMMENTS FROM REVIEWERS INCORPORATED
2.2	27/09/2006	COMMENTS FROM REVIEWERS INCORPORATED
2.3	21/09/2007	DOCUMENT UPDATED BY K.KATMANN: - ADMINISTRATIVE INFORMATION UPDATED - ERRORS CORRECTED
2.4	03/10/2007	COMMENTS FROM REVIEWERS INCORPORATED
2.5	28/05/2010	DOCUMENT UPDATED BY K.KATMANN: - ADMINISTRATIVE INFORMATION UPDATED - ERRORS CORRECTED, REPETITIONS REMOVED - COMMENTS FROM REVIEWERS INCORPORATED
2.6	07/07/2015	DOCUMENT UPDATED BY K.KATMANN: - ADMINISTRATIVE INFORMATION UPDATED - ERRORS CORRECTED, REPETITIONS REMOVED

Table of Contents

1. BACKGROUND

The process of creation (or amendment) of a **security convention** is prerequisite for provision of the network access service called "Remote access for companies". The starting point of the process is the retrieval of the relevant documents from DIGIT Service Catalogue by the **DG requester**. In final, the security convention must reflect the tasks to be performed by the external companies and approved by all parties (i.e. DG, external company, HR.DS and DIGIT).

As a reminder, accesses to Commission resources (e.g. information systems, databases, etc.) can only be granted to an external company if a contractual framework is established (usually a **specific agreement** under a **framework contract**) and remote access is required to perform tasks under this contract. Nevertheless, it is important to stress that the established contractual relationship with the contractor is not prerequisite for the initial planning required for the remote access. The preparatory work for remote access can be initiated by the DG requester in parallel with the establishment of contract. **In fact the conditions and restrictions for remote access service are relevant to take into account already in the procurement phase.**

1.1. Security Convention

Security convention is a framework of authorisation for various types of Commission network access services, including remote access for companies.

Security convention is also a formal agreement defining the conditions and the accesses to/from a specific EC IT resource and consists of 2 parts:

- Part 1 describes the physical, logical and organisational protection measures and the network of the external company. The information provided by the external company is the subject of validation performed by HR.DS (hereafter referred to as DS).

- Part 2 defines the conditions for remote access and specifies the list of remote accesses required for the external company to fulfil their contractual obligations. This list of accesses is prepared and provided by the DG requester (e.g. IRM team, System Owner, System Supplier or LISO) and reviewed in the workflow by DS and DIGIT.

Each security convention has an expiry date which is linked to the duration of the contractual relationship between the external company and DG requester. After this date, the lists of accesses will not be possible anymore. It is the responsibility of the **DG requester to manage the validity of a security convention.**

The workflow used to create (i.e. service provisioning) or amend (i.e. service management) a security convention contains the following main phases: preparation, validation, signature and implementation.

1.2. Authentication/identification mechanisms for remote access

The authentication/identification is performed on two levels:

(a) Access to the EC network - the external company needs a token for their access in order to be authenticated at the perimeter of the European Commission network. Once the Part 2 of the security convention is signed and implemented by DIGIT, this token is ordered by the DG requester (or team in charge of token management at

DG) through the ordering tool for the tokens. A VPN client together with the token(s) is sent by DIGIT User Access Administration (hereafter referred to as DIGIT/UAA) to be installed on external company hosts. The validity of the token is one year by default and the DG requester must initiate the token renewal period whenever the token is needed for more than one year.

(b) Access to a Commission IT resource - additional access control mechanisms can be in place on each accessed resource.

1.3. Support and documentation

In order to provide help and clarifications during the process of establishing the security convention, the service description of remote access for companies and related documentation are available for consultation at the **DIGIT Service Catalogue**.

1.4. Incident handling

If the requested network accesses are already implemented but there are connectivity issues, DG requester needs to open a call via CHD towards DIGIT services. Beside the problem statement, provide always **the ID of the security convention** and **the ID of the related token(s).** Please consult DIGIT Service Catalogue for further instructions concerning the incident type, configuration item and supplementary information to be provided in the call.

2. CREATION PROCEDURE

2.1. Preparation phase

(1) DG requester retrieves the security templates Part 1 and Part 2 from **DIGIT Service Catalogue**.

(2) DG requester asks DS via functional mailbox: **EC-SECURITY-SECURITY-CONVENTIONS@ec.europa.eu** for the security convention number (<DG acronym>.<serial number>.T1) and indicates this number on the first page of both templates (i.e. Part 1 and Part 2).

(3) DG requester then submits Part 1 template to external company. From this point onwards Part 1 must only be handled between the external company and DS through electronic mail (functional mailbox: **EC-SECURITY-SECURITY-CONVENTIONS@ec.europa.eu**).

(4) DG requester fills in Part 2 with the support of the following partners:

(a) IF the machine is hosted at the Data Centre by DIGIT/C, DIGIT/C2/ISHS/CCOR team will provide support for mapping functional requirements on correct network flows related to the application which needs to be reached remotely. In this case, DG requester fills the following fields in Part 2 in order to specify his external access requirements and sends it to DIGIT/C2/ISHS/CCOR team (functional mailbox: **DIGIT-ISHS-CCOR@ec.europa.eu**):
- Application/Information System (and DC RFC Number if applicable)
- Environment (e.g. Production, Training, Acceptance, Test, Development, Maintenance)
- Component (e.g. WebLogic, Oracle)
- Protocol (e.g. HTTP, FTP)
- IP address(es) and Fully Qualified Name(s)
- Etc.

(b) ELSE if the machine is hosted at the DG, IRM team of DG, System Owner or System Supplier will provide support.

(c) External company (e.g. which is their client OS, how they will connect, administrative and support information, etc.).

(5) DG requester submits Part 2 electronically to DS for validation either via SMT ticket (preferable way) or via electronic mail (functional mailbox: **EC-SECURITY-SECURITY-CONVENTIONS@ec.europa.eu)**.

(6) External company encrypts and submits the draft version of Part 1 electronically to DS for validation (functional mailbox: **EC-SECURITY-SECURITY-CONVENTIONS@ec.europa.eu**).

2.2. Validation phase

(7) If systems are hosted by DIGIT/C, DS submits Part 2 to DIGIT/C2/ISHS/Service Desk via SMT in order to review and validate (within max 5 working days) the list of requested accesses (Annex V of Part 2).

(8) Thereafter, DS submits Part 2 via SMT to DIGIT/C4/SNET in order to review and validate (within max 3 working days) the list of requested accesses (Annex V of Part 2).

(9) When applicable, DIGIT/C2/ISHS/Service Desk and DIGIT/C4/SNET provide their feedback (e.g. corrections, comments) to DS within the above defined timeframe. The feedback is communicated by DS to DG requester.

(10) DS reviews the description of the security posture in Part 1 and when applicable sends its comments to external company.

When applicable, the validation with the concerned service(s) is repeated.

2.3. Signature phase

(11) Once both parts of the security convention (hereafter referred to as SC) are reviewed and validated, **DS initiates the signature phase:**

(a) DS sign Part 1 in Ares.

(b) Responsible people for DS, DIGIT and DG sign Part 2 in Ares.

(c) DS sends both Part1 and Part 2 to the company responsible for signing (by encrypted email). External company signs, keeps the signed SC and returns scan of duly signed Part 1 and Part 2 to DS (by encrypted email).

(d) DS distributes the copy of the duly signed Part 2 to DIGIT and DG via Ares.

2.4. Implementation phase

(12) When both Part 1 and Part 2 are signed, DS submits Part 2 via SMT ticket to DIGIT/C4/SNET for implementation.

(13) DIGIT/C4/SNET implements SC and assigns the ticket to DIGIT/UAA.

(14) DIGIT/UAA implements SC and reassigns SMT ticket to DS.

(15) DS informs the DG requester either via SMT ticket or the functional mailbox that the SC is implemented and provides DG requester an electronic copy of Part 2 for reference and future use (amendment). A progress report (with the reference to the SMT ticket) indicating the date each phase in workflow took place can be provided by DS upon the request from DG requester.

(16) DG requester orders a token through the ordering tool for the tokens.

(17) DIGIT/UAA performs the following actions:

(a) Activates token access and expiry dates (default is one year).

(b) Sends the token and the VPN client (either software or hardware) to the external company with a letter (en recommendé).

(c) Provides token pin-code once external company acknowledges the token delivery.

(18) External company is now able to perform a first connection to the European commission network.

3. AMENDMENT PROCEDURE

Amendment procedure can be initiated only if a security convention has been previously established. An amendment of a security convention is necessary for many reasons. Herewith the major ones:

- Changes of the contractual framework (e.g. specific agreements renewed, added).

- Changes in the list of authorised accesses (e.g. IP addresses and ports), in case of modification of the infrastructure hosting the services or enhancements of the functional needs.

- For any changes initiated by DIGIT/C2/ISHS (see p.3.2), DIGIT/C2/ISHS/CCOR will inform in due time the DG requester and will initiate an amendment to reflect the changes.

3.1. Procedure for a change initiated by the DG

The procedure is similar to the creation one described above.

3.1.1. Preparation phase

(1) DG requester modifies Part 2 document in order to reflect the changes.

(a) IF the machine is hosted at the Data Centre by DIGIT/C, DIGIT/C2/ISHS/CCOR team will provide support for mapping functional requirements on correct network flows related to the application which needs to be reached remotely. In this case, DG requester fills the following fields in Part 2 in order to specify his external access requirements and sends it to DIGIT/C2/ISHS/CCOR team (functional mailbox: **DIGIT-ISHS-CCOR@ec.europa.eu**):
- Application/Information System (and DC RFC Number if applicable)
- Environment (e.g. Production, Training, Acceptance, Test, Development, Maintenance)
- Component (e.g. WebLogic, Oracle)
- Protocol (e.g. HTTP, FTP)
- IP address(es) and Fully Qualified Name(s)
- Etc.

(b) ELSE if the machine is hosted at the DG, IRM team of DG, System Owner or System Supplier will provide support.

(c) External company (e.g. which is their client OS, how they will connect, administrative and support information, etc.).

(2) Once completed, DG requester submits Part 2 electronically to DS for validation either via SMT ticket or via the functional mailbox: **EC-SECURITY-SECURITY-CONVENTIONS**.

3.1.2. Validation phase

(3) If systems are hosted by DIGIT/C, DS submits Part 2 to DIGIT/C2/ISHS/Service Desk via SMT in order to review and validate (within max 5 working days) the list of requested accesses (Annex V of Part 2).

(4) Thereafter, DS submits Part 2 via SMT to DIGIT/C4/SNET in order to review and validate (within max 3 working days) the list of requested accesses (Annex V of Part 2).

(5) When applicable DIGIT/C2/ISHS/Service Desk and DIGIT/C4/SNET provide their feedback (e.g. corrections, comments) to DS within the above defined timeframe. The feedback is communicated by DS to DG requester.

When applicable, the validation with the concerned service(s) is repeated.

3.1.3. Signature phase

(6) Once Part 2 is reviewed and validated, **DS initiates the signature phase.**

(a) Responsible people for DS, DIGIT and DG sign Part 2 in Ares.

(b) DS sends Part 2 to the external company responsible for signing (by encrypted email). External company signs, keeps the signed SC and returns scan of duly signed Part2 to DS (by encrypted email).

(c) DS distributes the copy of the duly signed Part 2 to DIGIT and DG via Ares.

3.1.4. Implementation phase

(7) Once the duly signed Part 2 returns, DS submits Part 2 via SMT ticket to DIGIT/C4/SNET for implementation.

(8) DIGIT/C4/SNET implements SC and assigns the ticket to DIGIT/UAA.

(9) DIGIT/UAA implements SC and reassigns SMT ticket to DS.

(10) DS informs the DG requester either via SMT ticket or the functional mailbox that the SC is implemented and provides DG requester an electronic copy of Part 2 for reference and future use (amendment). A progress report (with the reference to the SMT ticket) indicating the date each phase in workflow took place can be provided by DS upon the request from DG requester.

(11) DG requester orders the prolongation of token(s) through the ordering tool for the tokens.

(12) External company is now able to perform a connection to the European Commission network.

3.2. Procedure for a change initiated by DIGIT/C2/ISHS

Please note that in the case of change initiated by DIGIT/C2/ISHS, the Part 2 of security convention will not follow the signing circuit, since it concerns changes to approved accesses, like upgrade of database, server migration to new infrastructure, etc.

3.2.1. Preparation phase

(1) DIGIT/C2/ISHS/CCOR requests from DS (via SMT ticket) the latest implemented version of Part 2 document impacted by the change.

(2) DIGIT/C2/ISHS/CCOR requester informs concerned DG about the planned change and modifies Part 2 document:

(a) Change the end-date of the concerned access impacted by the change with the migration date + "*n"* month(s) (the period "n" is variable depending on the planning of the migration).

(b) Insert new accesses with an end-date corresponding to the end-date of the accesses modified at point (a), i.e. the end-date of the security convention.

(3) DIGIT/C2/ISHS/CCOR requester submits Part 2 document electronically to DS via SMT ticket.

3.2.2. Validation phase

(4) DS submits Part 2 via SMT to DIGIT/C4/SNET in order to review and validate (within max 3 working days) the list of requested accesses (Annex V of Part 2).

(5) When applicable DIGIT/C4/SNET provides feedback (e.g. corrections, comments) to DS within the above defined timeframe. The feedback is communicated by DS to DIGIT/C2/ISHS/CCOR requester.

When applicable, the validation with the concerned service(s) is repeated.

3.2.3. Implementation phase

(6) Once Part 2 is reviewed and validated, DS submits Part 2 via SMT ticket to DIGIT/C4/SNET for implementation.

(7) DIGIT/C4/SNET implements SC and assigns the ticket to DIGIT/UAA.

(8) DIGIT/UAA implements SC and reassigns SMT ticket to DS.

(9) DS informs the DG and DIGIT/C2/ISHS/CCOR requester either via SMT ticket or the functional mailbox that the SC is implemented and provides DG requester an electronic copy of Part 2 for reference and future use (amendment). A progress report (with the reference to the SMT ticket) indicating the date each phase in workflow took place can be provided by DS upon the request from DG requester.

(10) External company is now able to perform a connection to the European Commission network.

(11) Once the date of expiration of old accesses is reached, DIGIT/C4/SNET removes obsolete accesses.