



Council of the  
European Union

Brussels, 12 December 2018  
(OR. en)

---

---

**Interinstitutional File:**  
**2018/0422(NLE)**

---

---

15503/18  
ADD 1

FISC 558  
N 67  
ECOFIN 1197

#### COVER NOTE

---

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	12 December 2018
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	ANNEXES 1 to 6 to COM(2018) 832 final
Subject:	ANNEXES to the Proposal for a Council Decision on the position to be taken on behalf of the European Union in the Joint Committee established in accordance with Article 41(1) of the Agreement between the European union and the Kingdom of Norway on administrative cooperation, combating fraud and recovery of claims in the field of the value added tax

---

Delegations will find attached ANNEXES 1 to 6 to COM(2018) 832 final.

---

Encl.: ANNEXES 1 to 6 to COM(2018) 832 final



Brussels, 12.12.2018  
COM(2018) 832 final

ANNEXES 1 to 6

## **ANNEXES**

**to the Proposal for a**

**Council Decision**

**on the position to be taken on behalf of the European Union in the Joint Committee established in accordance with Article 41(1) of the Agreement between the European union and the Kingdom of Norway on administrative cooperation, combating fraud and recovery of claims in the field of the value added tax**

## ATTACHMENT 1

### Draft

#### **DECISION No 1/[date] of the Joint Committee of [date] adopting the Rules of Procedure of the Joint Committee**

THE JOINT COMMITTEE,

Having regard to the Agreement between the European Union and the Kingdom of Norway on administrative cooperation, combating fraud and recovery of claims in the field of the value added tax (hereinafter referred to as the "Agreement") and in particular Article 41(1) thereof,

Whereas:

- (a) It is necessary to lay down rules on composition and chairmanship, observers and experts, convening of meetings, agenda, secretarial support, drafting and adoption of minutes, procedure for the adoption of decisions and recommendations and expenses.
- (b) It is necessary to adopt practical arrangements for the implementation of Article 41(3) of the Agreement,

HAS ADOPTED THE FOLLOWING RULES OF PROCEDURE:

#### *Article 1*

##### **Composition and chairmanship**

- (1) The Joint Committee shall be composed of representatives of the European Union and representatives of the Kingdom of Norway (the Parties).
- (2) The European Union shall be represented by the European Commission. The Kingdom of Norway shall be represented by [.....].
- (3) The Joint Committee shall be chaired alternately by each of the Parties for two calendar years. The first period ends on 31 December of the year following the year of the entry into force of the Agreement. The first chair will be the European Union.

#### *Article 2*

##### **Observers and Experts**

- (1) Representatives of the Member States of the European Union may participate as observers.
- (2) The Joint Committee may also admit other persons as observers to its meetings.
- (3) Observers may be permitted by the chair to take part in the discussions and provide expertise. However, they shall not have voting rights and shall not participate in the formulation of the decisions and recommendations of the Joint Committee.
- (4) Experts with special expertise may also be invited with regard to specific agenda items.

### *Article 3*

#### **Convening a meeting**

- (1) Meetings of the Joint Committee shall be convened by the chair at least once every two years. Either Party may request that a meeting be convened.
- (2) The date and place of each meeting shall be determined and agreed between the Parties.
- (3) Meetings may also be held by means of teleconferencing / videoconferencing.
- (4) The chair shall communicate the invitation to the other Party, to the observers referred to Article 2(2) and the experts at least 15 working days before the meeting. The European Commission shall invite the representatives of the Member States of the European Union referred to Article 2(1).
- (5) The meetings shall not be public unless otherwise agreed. The Joint Committee's deliberations shall be confidential.

### *Article 4*

#### **Agenda**

- (1) The chair shall draw up the provisional agenda for each meeting and submit it to the Parties no later than 6 months before the meeting. The final agenda shall be agreed between the Parties no later than 15 working days before the meeting and circulated by the chair.
- (2) Reference papers and supporting documentation shall be sent to the Parties no later than the date on which the provisional agenda is sent.
- (3) For agenda items referring to decisions of the Joint Committee, the request for inclusion in the agenda and any related documents shall be sent to the Joint Committee at least 7 months in advance of the meeting.

### *Article 5*

#### **Secretarial support**

- (1) The chair shall carry out the tasks of secretary of the Joint Committee. All correspondence to the Joint Committee, including requests for items to be included or removed from the agendas, must be addressed to the chair.
- (2) Notwithstanding the above, the Commission shall act as secretary for the communication of the statistics, provided under Article 20 and Article 39 of the Agreement.

### *Article 6*

#### **Minutes of the meeting**

- (1) The chair shall draft the minutes of each meeting. The chair shall circulate the minutes without delay and no later than one month after the meeting. The minutes shall be subject to mutual agreement between the Parties.

- (2) The chair shall send the adopted minutes to the Parties.

#### *Article 7*

#### **Adoption of decisions and recommendations**

- (1) Any decisions and recommendations of the Joint Committee shall be subject to prior discussion between the Parties.
- (2) Decisions and recommendations of the Joint Committee shall be adopted during its meetings by unanimity.
- (3) Decisions or recommendations may be adopted by written procedure provided both Parties agree.
- (4) Under the written procedure the chair shall send the draft decisions and recommendations to the Parties and shall lay down a time limit to express their position. Any Party which does not oppose the draft acts before the expiry of that time limit, shall be regarded as having tacitly agreed to the draft acts.
- (5) The chair shall inform the Parties of the outcome of the written procedure without delay, and no later than 14 calendar days after the expiry of the time limit.

#### *Article 8*

#### **Expenses**

Each Party, and when applicable each observer, shall bear the expenses it incurs in taking part to the meetings of the Joint Committee.

*Date*

## **ATTACHMENT 2**

### **Draft**

#### **DECISION No 2/[date] of the Joint Committee of [date] adopting the standard forms, the transmission of communication and the practical arrangements for the organisation of the contacts between the central liaison offices**

THE JOINT COMMITTEE, established in accordance with Article 41(1) of the Agreement between the European Union and the Kingdom of Norway on administrative cooperation, combating fraud and recovery of claims in the field of the value added tax, hereinafter referred to as the "Agreement",

Whereas:

- (1) (a) Tools for transmission of communication, such as standard forms and electronic communication systems are already implemented within the framework of Council Regulation (EU) No 904/2010 on administrative cooperation and combating fraud in the field of value added tax<sup>1</sup> and Council Directive 2010/24/EU concerning mutual assistance for the recovery of claims relating to taxes, duties and other measures<sup>2</sup> and they are fully compatible with the administrative cooperation framework of the Agreement.
- (2) (b) It is necessary to adopt practical arrangements for the implementation of points (d), (e), (g) and (h) of Article 41(2) of the Agreement,

HAS ADOPTED THIS DECISION:

#### *Article 1*

##### **Standard Forms**

Pursuant to Articles 21(1) and 40(1) of the Agreement, for the communication of information under Titles II and III of the Agreement, the competent authorities shall make use of the standard forms adopted for the implementation of Council Regulation (EU) No 904/2010 and Council Directive 2010/24/EU.

The structure and lay-out of the standard forms may be adapted to any new requirements and capabilities of the communication and information exchange systems, provided that the data and information contained therein are not substantially altered.

#### *Article 2*

##### **Transmission of communication**

All information communicated pursuant to Titles II and III of the Agreement shall be transmitted only by electronic means via the CCN/CSI network, unless this is impracticable for technical reasons.

---

<sup>1</sup> Council Regulation (EU) No 904/2010 of 7 October 2010 on administrative cooperation and combating fraud in the field of value added tax (OJ L 268, 12.10.2010, p.1).

<sup>2</sup> Council Directive 2010/24/EU of 16 March 2010 concerning mutual assistance for the recovery of claims relating to taxes, duties and other measures (OJ L 84, 31.3.2010, P. 1).

### *Article 3*

#### **Organisation of the contacts**

- (1) In order to organise the contacts between the central liaison offices and liaison departments referred to in Article 4(2)(b) and Article 4(3)(b) of the Agreement, the competent authorities shall make use of the rules adopted for the implementation of Council Directive 2010/24/EU.
- (2) The central liaison offices designated pursuant to Article 4(2) of the Agreement, shall keep the list of liaison departments and competent officials designated pursuant to Article 4(3) and Article 4(4) up-to-date and make it available to the other central liaison offices via electronic means.

*Date*

## **ATTACHMENT 3**

### **Draft**

#### **DECISION No 3/[date] of the Joint Committee of [date] adopting the procedure for the conclusion of Service Level Agreement**

THE JOINT COMMITTEE, established in accordance with Article 41(1) of the Agreement between the European Union and the Kingdom of Norway on administrative cooperation, combating fraud and recovery of claims in the field of the value added tax, hereinafter referred to as the "Agreement",

Whereas:

- (3) (a) A service level agreement ensuring the technical quality and quantity of the services for the functioning of the communication and information exchange systems shall be concluded according to the procedure established by the Joint Committee.
- (4) (b) It is necessary to adopt practical arrangements for the implementation of Article 5 of the Agreement,

HAS ADOPTED THIS DECISION:

#### *Sole Article*

- (1) The Service Level Agreement, referred to in Article 5 of the Agreement, shall be concluded by the Joint Committee and shall be binding on the Parties from the day following its approval by the Joint Committee.
- (2) Each Party may request a revision of the Service Level Agreement by sending a request to the chair of the Joint Committee. Until the Joint Committee decides on the proposed changes, the provisions of the last concluded Service Level Agreement will remain in force.

*Date*



## ATTACHMENT 4

### Draft

#### **DECISION No 4/[date] of the Joint Committee of [date] adopting the Service Level Agreement for the systems and the applications for administrative cooperation and recovery of claims in the area of VAT**

### **1. REFERENCE AND APPLICABLE DOCUMENTS**

#### **1.1. APPLICABLE ACTS**

This Service Level Agreement ('SLA') takes into account the list of agreements and applicable decisions listed below.

[AD.1.]	Agreement between the Union and the Kingdom of Norway on administrative cooperation, combating fraud and recovery of claims in the field of value added tax ('the Agreement')(OJ L 195, 01.08.2018, p. 3)
[AD.2.]	Decision of the XX Joint Committee implementing points (d), (e), (g) and (h) of Article 41(2) of the Agreement with regard to the standard forms, the transmission of communication and the organisation of the contacts of [date]

Table 1: Applicable acts

#### **1.2. REFERENCE DOCUMENTS**

This SLA takes into account the information provided in the following reference documents. Applicable versions of the documents are published on CIRCABC or ITSM Web Portal.

[RD.1.]	CCN Mail III User Guide for NAs ( <i>ITSM Web Portal</i> )
[RD.2.]	CCN Intranet – Local Network Administrator Guide ( <i>ITSM Web Portal</i> )
[RD.3.]	Statistics – Guidelines and instructions (ANNEX rev1) to SCAC No 560
[RD.4.]	VAT e-Forms – Functional Specifications
[RD.5.]	VAT e-Forms – Technical Specifications
[RD.6.]	Recovery e-Forms – Functional Specifications
[RD.7.]	Recovery e-Forms – Technical Specifications
[RD.8.]	CCN/CSI General Security Policy ( <i>ITSM Web Portal</i> )
[RD.9.]	CCN Gateway Management Procedures ( <i>ITSM Web Portal</i> )
[RD.10.]	CCN/CSI Baseline Security Checklist ( <i>ITSM Web Portal</i> )

Table 2: Reference Documents

## 2. **TERMINOLOGY**

### 2.1. **ACRONYMS**

<b>ACRONYM</b>	<b>DEFINITION</b>
CCN/CSI	Common Communication Network/Common System Interface
CET	Central European Time
CIRCABC	Communication and Information Resource Centre Administrator
CLO	Central Liaison Office
CT	Conformance Testing
DG	Directorate General
EoF	Exchange of Forms
FAT	Factory Acceptance Tests
HTTP	HyperText Transfer Protocol
ITIL <sup>3</sup>	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
Party	Within the scope of this SLA, "party" shall mean either Norway or the Commission.
VAT	Value Added Tax

Table 3: Acronyms

### 2.2. **DEFINITIONS**

<b>EXPRESSION</b>	<b>DEFINITION</b>
CET	Central European Time, GMT+1 and during summer time GMT+2 hours.
Working days and hours (ITSM service desk)	7:00 to 20:00 (CET), 5 days a week (Monday to Friday including holidays)

Table 4: Definitions

## 3. **INTRODUCTION**

This document consists of a SLA between the Kingdom of Norway ('Norway') and the European Commission ('the Commission'), collectively referred as 'the Parties to the SLA'.

### 3.1. **SCOPE OF THE SLA**

Article 5 of the Agreement specifies that "A service level agreement ensuring the technical quality and quantity of the services for the functioning of the communication and information exchange systems shall be concluded."

This SLA sets out the relationship between the Kingdom of Norway and the Commission concerning the use of the systems and applications for administrative

<sup>3</sup>

ITIL:

- <http://www.ital-officialsite.com>
- [http://www.best-management-practice.com/gempdf/itSMF\\_An\\_Introductory\\_Overview\\_of\\_ITIL\\_V3.pdf](http://www.best-management-practice.com/gempdf/itSMF_An_Introductory_Overview_of_ITIL_V3.pdf)

cooperation and recovery of claims in the area of VAT, and between the Kingdom of Norway and the Member States concerning the exchange of forms.

The following systems are operational and are subject to the terms of the SLA:

- Exchange of Forms (EoF);
- Monitoring, statistics and testing.

The Commission determines the process to achieve agreement for the administrative cooperation by means of information technology. This involves standards, procedures, tools, technology and infrastructure. Assistance to Norway is provided to ensure data exchange systems are available and are properly implemented. The monitoring, supervision and evaluation of the overall system is also provided by the Commission. Furthermore the Commission provides Norway with guidelines to be respected in relation to this exchange of information.

All targets referred to in the SLA will be applicable under normal working conditions only.

In case of events of Force Majeure, the applicability of the SLA for Norway will be suspended for the duration of these Force Majeure conditions.

Force Majeure represents an unpredictable event or occurrence outside the control of Norway or the Commission, and which is not attributable to any act or failure to take preventive action by the responsible party. Such events shall refer to government actions, war, fire, explosion, flood, import or export regulations or embargoes and labour disputes.

The party invoking the Force Majeure shall inform the other party without delay about the impossibility to provide services or to accomplish the SLA targets due to Force Majeure incidents, setting out the affected services and targets. When the incidence of Force Majeure has ceased the affected party shall likewise inform the other party without delay.

### **3.2. AGREEMENT PERIOD**

The SLA is binding on the Parties from the day following its approval by the Joint Committee established by Article 41 of the Agreement ('the Joint Committee').

## **4. RESPONSIBILITIES**

The purpose of this SLA is to ensure the quality and quantity of the services to be delivered by the Commission and by Norway in order to make the specified systems and applications for administrative cooperation and recovery of claims in the area of VAT available to Norway and to the Commission.

### **4.1. SERVICES PROVIDED BY THE COMMISSION TO NORWAY**

The **Commission** shall make the following services available:

- Operational services as follows:
  - Helpdesk and operations:
    - (a) Helpdesk Support;
    - (b) Incident Handling;
    - (c) Monitoring and Notification;

- (d) Training;
  - (e) Security Management;
  - (f) Reporting and statistics;
  - (g) Consulting.
- Reference centre:
- (a) Information management;
  - (b) Documentation centre (CIRCABC);

In order to provide these services, the Commission shall maintain the following applications:

- Statistical applications;
- CIRCABC;
- Service desk tool.

#### **4.2. SERVICES PROVIDED BY NORWAY TO COMMISSION**

Norway shall make the following services available:

- Norway shall communicate to the Commission any available information relevant to their application of the Agreement;
- Norway shall communicate to the Commission any exceptional conditions;
- Norway shall provide annually the statistics regarding the communication of information set out in Article 20 of the Agreement.

### **5. SERVICE LEVEL REVIEW**

This chapter provides a detailed description of the quantitative and qualitative aspects of the services to be provided by the Commission and by Norway as described above.

#### **5.1. COMMISSION SERVICE LEVELS**

##### **5.1.1. Service desk**

###### **5.1.1.1. *Agreement***

The Commission shall make available a Service Desk in order to respond to any questions and to report any problems which Norway experiences with the systems and applications for administrative cooperation and recovery of claims in the area of VAT or any component that could affect them. This Service Desk will be operated by ITSM and its operating hours shall be the same as the ITSM working hours.

The availability of the ITSM Service Desk shall be ensured in at least 95% of the operating hours. All questions or problems can be communicated to the service desk during the ITSM working hours by telephone, fax or e-mail and outside those working hours by E-mail or fax message. Where these questions or problems are sent outside the working hours of the ITSM they shall be automatically deemed to have arrived at 8:00 CET on the next working day.

The Service Desk shall register and classify the service calls in a Service Management Tool and shall inform the reporting party of any change in status regarding their service calls.

The ITSM shall deliver a first line support to the users and shall dispatch any service call, which is the responsibility of another party (e.g. developer's team, ITSM contractors) within the specified time. ITSM shall ensure compliance with the registration deadlines in at least 95% of the cases occurring over a reporting month.

The ITSM shall monitor the resolution procedure for all service calls and shall start an escalation procedure by informing the Commission where the resolution period exceeds a predefined threshold, which will depend on the type of problem.

The priority level shall determine both the response and the resolution times. This is set by ITSM, but Member States or the Commission may require a specific priority level.

The *registration time* is the maximum time interval that is allowed to pass between the time of the receipt of the email and the sending of the acknowledgment email.

The *resolution time* is the time interval between the registration of the incident and the resolution information being sent to the issuer. This also includes the time involved in closing the incident.

These shall not be absolute deadlines as they take into account only the time when ITSM acts on the service call. When a service call is dispatched to Norway, the Commission or another party (e.g. developer's team, ITSM contractors) then this time does not form part of the resolution time of ITSM.

ITSM shall ensure the compliance with the registration and resolution deadlines in at least 95% of the cases occurring over a reporting month.

PRIORITY	REGISTRATION TIME	RESOLUTION TIME
P1: Critical	0.5h	4h
P2: High	0.5h	13h (1 day)
P3: Medium	0.5h	39h (3 days)
P4: Low	0.5h	65 h (5 days)

Table 5: Registration times and resolution times (working hours / days)

#### 5.1.1.2. Reporting

The Commission shall report on all service calls related to the systems and applications for administrative cooperation and recovery of claims in the area of VAT as follows:

- All the service calls closed during the month for Norway;
- All the service calls created during the month for Norway;
- All the service calls pending at the reporting date and time for Norway.

## 5.1.2. Statistical Service

### 5.1.2.1. *Agreement*

The Commission shall generate statistics about the number of exchanged forms in the VAT and recovery domain using CCN/Mail, which are available on the ITSM Web portal.

### 5.1.2.2. *Reporting*

The Commission shall produce a report on the conformance test reports, where applicable, and shall make them available to Norway.

## 5.1.3. Exchange of Forms

### 5.1.3.1. *Agreement*

The following table illustrates the maximum transmission deadline or answer time for the exchange of forms as defined in the legislation.

<b><i>CCN/Mail mailbox</i></b>	<b><i>Form</i></b>	<b><i>Deadline</i></b>
VIESCLO	Exchange of Information under Articles 7, 10, 12 and 18 of the Agreement 0  General exchanges	The time limit for providing information is as quickly as possible, and no later than <u>3 months following the date of the request</u> ( <b>Article 8 of the Agreement 0</b> ).  However when the requested authority is already in possession of the information the time limit shall be reduced to a maximum period of <u>one month</u> ( <b>Article 8 of the Agreement 0</b> ).
VIESCLO	Exchange of Information under Articles 7, 10, 12 and 18 of the Agreement 0  Request for notification	Request for notification with immediate answer ( <b>Article. 12 0 of the Agreement</b> ).
TAXFRAUD	Exchange of Information under Articles 7, 10, 12 and 18 of the Agreement 0  Anti-fraud exchanges	Missing trader information shall be sent <u>as soon as the information becomes available</u> .
TAXAUTO	Automatic exchanges	The categories of information subject to automatic exchange, in accordance with Article 11 of the Agreement, are to be determined by the Joint

<i>CCN/Mail mailbox</i>	<i>Form</i>	<i>Deadline</i>
		Committee.
REC-A-CUST; REC-B-VAT; REC-C-EXCISE; REC-D-INCOME-CAP; REC-E-INSUR; REC-F-INHERIT-GIFT; REC-G-NAT-IMMOV; REC-H-NAT-TRANSP; REC-I-NAT-OTHER; REC-J-REGIONAL; REC-K-LOCAL; REC-L-OTHER; REC-M-AGRI	Request for information under Art. 22 of the Agreement 0,  Request for notification under Art. 25 of the Agreement 0  Request for recovery under Art. 27 of the Agreement 0  Request for precautionary measures under Art. 33 of the Agreement 0	Request for information:  - acknowledgment of receipt within 7 calendar days;  - update at the end of 6 months from the date of acknowledgment  Request for notification:  - acknowledgment of receipt within 7 calendar days;  Request for recovery and request for precautionary measures:  - acknowledgment of receipt within 7 calendar days;  - update at the end of every 6 months from the date of acknowledgment

Table 6: Performance EoF

### 5.1.3.2. *Reporting*

Norway shall also provide on an annual basis to the Commission statistical data via e-mail regarding to the communication of information as set out in Articles 20 and 39 of the Agreement [RD.3.].

### 5.1.4. **Problem Management**

#### 5.1.4.1. *Agreement*

Norway shall maintain an adequate problem registration<sup>4</sup> and follow-up mechanism for any problems affecting their application host, system software, data and applications software.

Problems with any part of the CCN network (Gateways and/or Exchange Mail servers) shall be reported to ITSM immediately.

#### 5.1.4.2. *Reporting*

Norway shall inform the ITSM where they have an internal problem with the technical infrastructure related to their own systems and applications for administrative cooperation and recovery of claims in the area of VAT.

Where Norway considers that a problem reported to ITSM is not being addressed or resolved or was not addressed or resolved in a satisfactory way, it shall report this to the Commission as soon as possible.

<sup>4</sup> Linked to Problem and Change management processes of ITIL.

### 5.1.5. Security Management

#### 5.1.5.1. *Agreement*<sup>5</sup>

Norway shall protect its systems and applications for administrative cooperation and recovery of claims in the area of VAT against security violations and shall keep track of any security violations and of any security improvements made.

Norway shall apply the security recommendations and/or requirements specified in the following documents:

Name	Version	Date
https security recommendations of CCN /Mail III Webmail access – Ref. CCN /Mail III User Guide for NAs	3.0	15/06/2012
Security recommendations of CCN /Mail III Webmail access – Ref. CCN Intranet – Local Network Administrator Guide	4.0	11/09/2008

#### 5.1.5.2. *Reporting*

Norway shall on an ad-hoc basis report to the Commission on any security violations and on any measures taken.

## 5.2. NORWAY'S SERVICE LEVELS

### 5.2.1. All Service Level Management Areas

#### 5.2.1.1. *Agreement*

Norway shall register any unavailability problems or changes<sup>6</sup> regarding to the technical, functional and organisational aspects of Norway's systems and applications for administrative cooperation and recovery of claims in the area of VAT.

#### 5.2.1.2. *Reporting*

Norway shall inform the ITSM where necessary in relation to any unavailability problems or changes regarding the technical, functional or organisational aspects of their system. ITSM shall always be informed for any changes regarding the operating personnel (operators, system administrators).

### 5.2.2. Service desk

#### 5.2.2.1. *Agreement*

Norway shall make available a service desk for responding to incidents assigned to Norway, for giving assistance and to carry out testing. The working hours of the service desk should be the same as the working hours of the ITSM Service Desk during ITSM working days. Norway's service desk shall operate at a minimum between 10:00-16:00 CET during working days, except on its national holiday. It is recommended that Norway's service desk follows the ITIL service support guidelines in handling the questions and incidents.

<sup>5</sup> These are the documents versions available at the time of writing this SLA. The reader is invited to check any subsequent updates on the CCN/CSI Portal (<http://portal.ccntc.ccnsci.int:8080/portal/DesktopDefault.aspx?tabid=1>).

<sup>6</sup> Use of principles described in the incident management in ITIL is recommended.



#### 5.2.2.2. *Reporting*

Norway shall inform the ITSM where necessary in relation to any availability problem related to its service desk.

### **6. QUALITY MEASUREMENT**

#### **6.1. AGREEMENT**

The Commission shall evaluate the reports (activity reports generated by ITSM, notifications, statistics, other information) received from the ITSM and Norway, shall determine the levels of adherence to this SLA and in case of problems shall contact Norway in order to solve the problem and to ensure that the quality of the service is in line with this agreement.

#### **6.2. REPORTING**

The Commission shall report on a monthly basis to Norway the level of the service as defined in Section 5.1.2.

### **7. APPROVAL OF THE SLA**

The Service Level Agreement has to be approved by the Joint Committee in order to be applicable.

### **8. CHANGES TO THE SLA**

The Service Level Agreement will be reviewed following a written request from the Commission or Norway to the Joint Committee.

Until the Joint Committee decides on the proposed changes, the provisions of the current SLA remain in force. The Joint Committee acts as the decision making body for the present agreement.

### **9. CONTACT POINT**

For any questions or remarks regarding this document, feel free to contact:

SERVICE PROVIDER - SERVICE DESK

[support@itsmtaxud.europa.eu](mailto:support@itsmtaxud.europa.eu)

*Date*

## ATTACHMENT 5

### Draft

### DECISION No 5/[date] of the Joint Committee of [date] adopting the Service Level Agreement for the Common Communication Network/Common System Interface services ('CCN/CSI SLA')

#### 1. REFERENCE AND APPLICABLE DOCUMENTS

##### 1.1. APPLICABLE ACTS

This CCN/CSI SLA takes into account the list of agreements and applicable decisions provided below.

[AD.1.]	Agreement between the Union and the Kingdom of Norway on administrative cooperation, combating fraud and recovery of claims in the field of value added tax ('the Agreement')(OJ L 195, 01.08.2018, p. 3)
[AD.2.]	Decision of the XX Joint Committee implementing points (d), (e), (g) and (h) of Article 41(2) of the Agreement with regard to the standard forms, the transmission of communication and the organisation of the contacts of [date]

Table 7: Applicable acts

##### 1.2. REFERENCE DOCUMENTS

This CCN/CSI SLA takes into account the information provided in the following reference documents. Applicable versions of the documents are those available at the time of signing this agreement.

ID	REFERENCE	TITLE	VERSION
<a href="#">RD1</a>	CCN-COVW-GEN	CCN/CSI & SPEED2 Systems Overview	EN18.01
<a href="#">RD2</a>	CCN-CMPR-GW	CCN Gateways Management Procedures	EN19.20
<a href="#">RD3</a>	CCN-CSEC-POL	CCN/CSI General Security Policy	EN05.00
<a href="#">RD4</a>	CCN-CSEC-BSCK	CCN/CSI Baseline Security Checklist	EN03.00
<a href="#">RD5</a>	CCN-CLST-ROL	Description of CCN/CSI	EN02.10
<a href="#">RD6</a>	CCN-CNEX-031	External note 031 - Procedure for the Move of a CCN/Site	EN06.20
<a href="#">RD7</a>	CCN-CNEX-060	External Note 060 - Installation of new CCN Site	EN02.20
<a href="#">RD8</a>	CCN/CSI-PRG-AP/C-01-MARB	CCN/CSI-PRG-AP/C-01-MARB-Application Programming Guide (C Language)	EN11.00

Table 8: Reference Documents

## 2. TERMINOLOGY

### 2.1. ACRONYMS

ACRONYMS	DEFINITION
ACT	Application Configuration Tool
AIX	IBM Unix OS
CBS	Central Backup Site
CCN	Common Communication Network
CCN/CSI	Common Communication Network / Common System Interface
CCN/WAN	Framework service for the provision of network services to CCN
CI	Configuration Item
CIRCABC	Communication and Information Resource Centre for Administrations, Businesses and Citizens
COTS	Common Off The Shelf
CPR	Customer Premises Router
CSA	CCN Security Administrator
CSI	Common System Interface
DG	Directorate General
DMZ	De-Militarised Zone
EC	European Commission
ESTAT	Eurostat
FW	Firewall
HPUX	Hewlett Packard Unix Operating System
HTTP	Hyper Text Transport Protocol
HTTPS	Hyper Text Transport Protocol - Secure
HVAC	Heating, Ventilating, and Air-Conditioning
HW	Hardware
ICT	Information and Communication Technology
IMAP	Internet Message Access Protocol
IP	Internet Protocol
ITCAM	IBM Tivoli Composite Application Manager
ITS	IT Services
ITSM	IT Service Management
LAN	Local Area Network
LSA	Local System Administrator
MQ	IBM MQ Series SW
MVS	Multiple Virtual Storage
N/A	Not Applicable
NA	National Administration
NDI	National Domain Interface
OBS	Orange Business Services
OLA	Operational Level Agreement
OLAF	Office de Lutte Anti-Fraude
OS	Operating System
OSP	Obligation of Service Provider
OSR	Obligation of Service Requesters
POL	Policy

PoP	Point of Presence
PRG	Program
QA	Quality Assurance
RAP	Remote API Proxy
RD	Reference Document
REV	Revision
RFA	Request For Action
ROL	Role
SFI	Submit For Information
SMTP	Simple Mail Transport Protocol
SQI	Service Quality Indicator
SSG	Secure Services Gateways (Juniper Encryption box)
SW	Software
TAXUD	Taxation and Customs Union
TCP	Transmission Control Protocol
UPS	Uninterruptible Power Supply
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network

Table 9: Acronyms

## 2.2. DEFINITIONS OF TERMS FOR THE PURPOSE OF THE CCN/CSI SLA

TERM	DESCRIPTION
<b>Reporting period</b>	The elapsed time covered is one month.
<b>Working day</b>	The working days are the working days of the Service Provider Service Desk. These are 7 days a week including public holidays.
<b>Working hour</b>	The working hours are the working hours of the Service Provider SD. These are 24/24 during the working days.
<b>Duty Period</b>	<p>The Service Provider's "Duty Period" is the hours of coverage of the Service Desk function. The duty is ensured by Service Provider SD from 24/24, 7 days a week including public holidays.</p> <p>Depending of the CI's Service Window, there is an immediate action (24*7) or the intervention is scheduled for the next day. Letter, fax, e-mails and electronic requests (through the ITSM Portal) are accepted at any moment. Incoming requests are registered as "Service Calls" in the Service Provider Service Desk management system.</p>

Table 10: Definitions

## 3. INTRODUCTION

This document consists of a Common Communication Network/Common System Interface Service Level Agreement (CCN/CSI SLA) between the European Commission ('Service Provider') and the Kingdom of Norway ('Service Requester'), collectively referred as 'the Parties to the SLA'.

In particular the 'Service Provider' includes the organisational units of DG TAXUD, as listed below:

- DG TAXUD B2 unit coordinating all CCN/CSI activities;
- ITSM3 Operations providing operational services;
- CCN2DEV providing CCN software (evolutionary and corrective maintenance services);
- Trans-European Backbone network provider (CCN/WAN, currently OBS).

Based on the nature of the requested service, one of the Service Providers will fulfil the task.

The 'Service Requester' is the national tax administration (NA) of Norway. The concerned organisational units within the NA are:

- The **National CCN Support Centre** in charge of the support and management of the DG TAXUD CCN Infrastructure equipment located at NA premises as well as the national infrastructure supporting the applications running over the CCN/CSI infrastructure;
- The **National Application Support Centre** in charge of the national support of the EC applications running in the National Domain and using the CCN/CSI infrastructure services;
- The **National Application Development Teams** in charge of the development of applications using the CCN/CSI infrastructure including their sub-contractors.

### 3.1. SCOPE OF THE CCN/CSI SLA

Article 5 of the Agreement specifies that "A service level agreement ensuring the technical quality and quantity of the services for the functioning of the communication and information exchange systems shall be concluded."

This CCN/CSI SLA sets out the relationship between and the Commission (Service Provider) and the Kingdom of Norway (Service Requester), concerning the operational phase of the Common Communication Network/Common System Interface system ('CCN/CSI system').

It defines the required level of the service provided to the Service Requester. It also provides for a mutual understanding of service level expectations and the responsibilities of the involved Parties to the SLA.

This document describes the services and service levels provided currently by the Service Provider.

All targets referred to in the CCN/CSI SLA will be applicable under normal working conditions only.

In case of events of Force Majeure, no Party shall be liable for any failure to perform its obligations where such failure is as a result of natural disaster (including fire, flood, earthquake, storm, hurricane or other natural disaster), war, invasion, act of foreign enemies, hostilities (whether war is declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation, terrorist activities, nationalisation, government sanction, blockage, embargo, labour dispute, strike, lockout or interruption or long-term failure of the commercial electricity grid.

### 3.2. CCN/CSI SERVICE DEFINITION AND CHARACTERISTICS

The Common Communication Network/ Common System Interface is a tool for exchange of tax information between the National Administrations in the field of Taxation and Anti-Fraud. The main characteristics of the CCN/CSI system infrastructure are listed hereafter:

<b>TRANS-EUROPEAN</b>	CCN/CSI offers a global WAN access to Service Requesters through a number of Points of Presence (PoP) in every Member State, acceding countries and Norway. The CCN/CSI network backbone offers the required capacity and resilience to provide the Service Requesters with a high availability rate.
<b>MULTI-PLATFORM</b>	Allows the interoperability between heterogeneous platforms (Windows, Linux, Solaris, AIX, HPUX, SVR4, IBM MVS, etc.) through a highly portable communication stack (CSI) installed on standard national Application Platforms.
<b>MULTI-PROTOCOL</b>	<p>Supports various protocols and exchange paradigms:</p> <ul style="list-style-type: none"> <li>▪ CSI protocol supporting asynchronous and synchronous (request/response) communication paradigms (CCN/CSI channel);</li> <li>▪ HTTP/S protocol for interactive access to CCN Intranet services (CCN Intranet channel);</li> </ul> <p>POP, IMAP, SMTP protocols for the exchange of e-mail between NA users but also between applications (CCN Mail III channel).</p>
<b>SECURE</b>	<p>Information exchanges over the CCN/CSI network are protected to ensure optimal confidentiality and data integrity. Security services include:</p> <ul style="list-style-type: none"> <li>▪ Site-to-site IPsec256-bits encryption and protection against unwanted accesses enforced by Firewall/encryption devices deployed at every CCN/CSI site;</li> <li>▪ Access control mechanisms (authentication, authorisation, accounting) at site level enforced at CCN Gateway and supported by local administration tools (ADM3G);</li> </ul> <p>Session-level security enforced by message-level encryption (CSI secure), SSL v.3 mutual authentication and encryption (HTTPS), POP-S and IMAP-S (secure e-mail transport).</p>
<b>MANAGED</b>	<p>The CCN/CSI infrastructure also provides Service Requesters with managed services including:</p> <ul style="list-style-type: none"> <li>▪ Central Monitoring;</li> <li>▪ Event logging;</li> <li>▪ Production of statistics on CSI and CCN Mail III message exchanges (size, number of messages, matrix) and statistics on CCN gateways and CCN Mail III;</li> </ul>

	<ul style="list-style-type: none"> <li>▪ User management (ADM3G) and directory services;</li> <li>▪ CSI stacks validation;</li> <li>▪ Portal services: <ul style="list-style-type: none"> <li>○ CCN Portal: on-line access to statistics, on-line remote API proxies (RAP) management;</li> <li>○ ITSM Portal: on-line Newsletter, on-line documentation and CSI stack packages, CCN Frequently Asked Questions (FAQ)</li> </ul> </li> <li>▪ ACT (Application Configuration Tool);</li> </ul> <p>Services calls tracking and on-line support.</p>
--	---

Table 5: Characteristics of the services provided by CCN/CSI

### 3.3. AGREEMENT PERIOD

The CCN/CSI SLA is binding on the Parties from the day following its approval by the Joint Committee established by Article 41 of the Agreement ('the Joint Committee').

## 4. RESPONSIBILITIES

### 4.1 DUTIES OF THE SERVICE PROVIDER (OSP)

The Service Provider shall:

[OSP1]	Operate the CCN/CSI network infrastructure in order to achieve the Service Levels described in section 8.
[OSP2]	Select the various CCN/CSI Infrastructure and Software components.
[OSP3]	Provide Hardware and Software maintenance for the DG TAXUD CCN infrastructure equipment (e.g. CCN Gateways) installed at the Service Requesters premises as well as the central CCN Mail III servers.
[OSP4]	Provide monitoring of the DG TAXUD CCN Infrastructure equipment installed at the Service Requesters premises.
[OSP5]	Manage the CCN/CSI audit files.
[OSP6]	Manage the CCN/CSI addressing plan.
[OSP7]	Respect the rules and recommendations put forward in the "Security documents": <ul style="list-style-type: none"> <li>▪ CCN/CSI General Security Policy <a href="#">RD3</a>;</li> </ul> CCN/CSI Baseline Security Checklist <a href="#">RD4</a> ;
[OSP8]	From time to time, the Service Requester needs to make sure that the network availability will not be reduced due to maintenance or other expected unavailability's. In that case, the Service Requester will notify the

	Service Provider at least 1 month in advance. If the Service Requester cannot respect this delay, DG TAXUD will arbitrate the situation.
[OSP9]	All software licenses running on the CCN gateways will be provided by DG TAXUD.
[OSP10]	Respect the CCN/CSI site backup policy (cfr. RD2).
[OSP11]	Audit the system as defined in RD2.
[OSP12]	Regularly proceed with the System Security Checkup as defined in RD2

Table 6: Obligations of the Service Provider (OSP)

#### 4.2. DUTIES OF SERVICE REQUESTER (OSR)

The Service Requester shall:

<b>Technical and Infrastructure level</b>	
[OSR1]	House the DG TAXUD CCN Infrastructure equipment provided by the DG TAXUD and provide appropriate: <ul style="list-style-type: none"> <li>▪ Rack/Storage space;</li> <li>▪ electrical power supply;</li> </ul> HVAC;
[OSR2]	Make sure that the CCN/CSI components are "electrically" connected to the UPS. Specific adaptations to local standards (e.g. plug adapters) have to be provided by the Service Requester
<b>Operational and Organisation level</b>	
[OSR3]	Assign personnel in charge of the roles listed in RD5.
[OSR4]	Ensure presence outside of normal working hours whenever deemed necessary and requested by the Service Provider.  For some operations performed by the backbone carrier or by the Service Provider, the coordination and/or the presence of the LSA from the Service Consumer may be required. There will be at least one-month notice in order to plan these activities; full cooperation is necessary in order to respect the complex planning due to the number of sites.
[OSR5]	Never stop any of the DG TAXUD CCN Infrastructure equipment without formal authorisation from the Service Provider.
[OSR6]	Ask for the formal authorisation from the Service Provider before installing on the DG TAXUD CCN Infrastructure equipment additional hardware or



	software components that do not belong to the standard delivery package.
[OSR7]	Provide a clear description of the perceived/reported incidents, reported by the service requester.
[OSR8]	Collaborate actively with the Service Provider and/or his representatives when required for the delivery of services.
<b>Communication level</b>	
[OSR9]	Use exclusively the contact points at the Service Provider and inside their own organisation.
[OSR10]	Notify the Service Provider of any absence of the contact points during the opening hours of the Service Provider, or, at least, provide a backup able to replace the contact points.
[OSR11]	Notify the Service Provider of any modification of its own contact points, at least 5 working days before this modification becomes effective.
[OSR12]	Notify the Service Provider of any scheduled INFRASTRUCTURE maintenance potentially affecting the DG TAXUD CCN Infrastructure equipment hosted at the Service Consumer premises (at least one week in advance for all equipment).  e.g.: planned power or network infrastructure outages, DC move, ip-address changes, ....
[OSR13]	Notify the Service Provider of any external problem such as power failure affecting the good running of the CCN Gateways and application platforms.
[OSR14]	Notify Service Provider, through a formal request, at least six months in advance for any moving of DG TAXUD CCN Infrastructure equipment. The Service Requester takes in charge the costs of the moving operations. Refer to <a href="#">RD6</a> for more details about the procedure.
[OSR15]	Notify the Service Provider of any outage of the secured links between the DG TAXUD CCN Infrastructure and the Service Requester (NA or peer DG).
[OSR16]	Notify the Service Provider of any outage of the Application Platforms.
[OSR28]	The service requester is requested to communicate any planned local DC/Computer room outage (incl. WAN) 1

	(one) working week upfront. This in order for DG TAXUD to be able to put in place the necessary communication to any other involved stakeholders.
<b>Security and User Management level</b>	
[OSR17]	Manage the local user accounts on the CCN Gateway (cf. <a href="#">RD2</a> ).
[OSR18]	Grant physical access permission to the equipment and staff mandated by the Service Provider when required.
[OSR19]	Authorise the appropriate TCP ports in the Service Consumer network (National Domain) (cfr. <a href="#">RD2</a> ).
[OSR20]	Ensure that the Network Encryption Devices (currently Juniper SSG) at the Service Requester site is located in an access-controlled area.
[OSR21]	Restrict access to all devices of the DG TAXUD CCN Infrastructure to authorised personnel. The access shall be allowed only on request from the CSA. Unwanted access to these devices can jeopardise the security or at least cause network outages.
[OSR22]	Respect the rules and recommendations put forward in the “Security documents”: <ul style="list-style-type: none"> <li>▪ CCN/CSI General Security Policy <a href="#">RD5</a>;</li> <li>▪ CCN/CSI Baseline Security Checklist <a href="#">RD6</a>;</li> </ul>
<b>Application Management Development</b>	
[OSR27]	The Service Requester is sole responsible for the development, support and management of its applications. They must conform to the rules defined in <a href="#">RD8</a>

Table 7: Obligations of the Service Requesters (OSR)

### 4.3. SERVICES PROVIDED BY THE SERVICE PROVIDER

#### 4.3.1. IT Service Desk

The Service Provider offers a consolidated IT Service Desk with Incident and Problem Management. The IT Service Desk extends the range of classical help desk services and offers a more global-focused approach, allowing business processes to be integrated into the CCN/CSI service management.

Indeed, the IT Service Desk not only handles incidents, problems and questions, but also provides an interface for other activities such as change requests, maintenance contracts, software licences, service level management, configuration management, availability management, security management and IT service continuity management.

The IT Service Desk also spontaneously notifies the Service Requester of any urgent information, thus acting as an information-dispatching centre for the Service Requester.

A Notification is defined as a message issued by the Service Provider warning Service Requester of an event that may affect the CCN/CSI operations: gateway unavailability, system outage, malfunctions, infrastructure maintenance or software update.

The IT Service Desk interface to Service Requester is achieved through the Service Provider contact point or through the ITSM Web portal, which provides on-line services to the Service Requester such as service call tracking; ACT tool and the CCN Web portal which provides CSI packages download area, access to statistics and monitoring information, etc.

#### 4.3.1.1. *Incident and problem management*

This service deals with incidents originating from Service Desk users (including system operations). An incident may be defined as a simple request for information or clarification, but may also be categorized as the reporting of non-compliant behaviour of a specific component.

An incident is defined as an unexpected event that is not part of the standard operation of the infrastructure or a failure that degrades an operational CCN/CSI service. An incident is solved when the service is restored.

The incident can be related to the following Configuration Items (CI):

- The hardware under responsibility of the Service Provider: CCN gateways, security devices, Customer Premises Routers (CPR) and other network connectivity devices on the EuroDomain (DG TAXUD CCN Infrastructure) LAN;
- The software running on the encryption devices;
- The system software running on the gateways: Operating System, basic communication software such as TCP/IP, etc.;
- The third-party software running on the gateways such as Tuxedo, MQSeries, Sun ONE Directory Server, PostgreSQL, Apache, etc.;
- The CCN Mail III;
- The CCN/CSI software running on the gateways;
- The CSI software running on the Application Platforms;
- SIAP (Secure Internet Access Point) – Unified Defence.

A problem is identified either from a single incident which has an extremely adverse impact on the user service and for which the cause is unknown, or from multiple incidents exhibiting common symptoms. A problem is solved when the cause is identified and removed.

When an incident occurs, the situation is investigated in order to restore the operational CCN/CSI services (if needed) and to find the root cause of the incident. The Service Provider helps to resolve incidents in the NA application software, at the level of the interface with CCN/CSI, as long as this has no impact on the other services to be provided by the Service Provider. The Service Provider assistance

consists in providing information about the correct usage of CCN/CSI. **It does not consist in participating in the debugging of NA application software.**

#### **4.3.2. Tools supporting the Service Management**

The monitoring of the CCN gateway infrastructure, applications and CCN queues is supported by the IBM® Tivoli Monitoring (Tivoli Monitoring) and IBM Tivoli Composite Application Manager (ITCAM) product family.

The CCN Tivoli Monitoring and Reporting service, based on IBM Tivoli Monitoring suite, provides the following functionalities:

- Monitor the applications queues located on the CCN Gateways (WebSphere MQ);
- Monitor the operating system status of the CCN Gateways;
- CPU usage, Disk space, Memory usage, Network usage, Processes;
- Out of Band HW monitoring;
- Monitor the running processes of the CCN components located on the CCN Gateways;
- Monitor the CCN Mail III infrastructure;
- Provide to the CCN Tivoli users a view on the previous monitored information;
- Generate pre-defined alerts on the previous monitored components;
- Provide reports based on collected historical data (CCN Tivoli Data Warehouse);
- Give information about the availability and performance of the CCN/CSI infrastructure over time, reporting important trends in a consistent and integrated manner.

#### **4.3.3. ICT Infrastructure Management and Operations**

The Service Provider is called upon to install, operate, and maintain the CCN/CSI operational infrastructure so as to guarantee the agreed availability levels.

The CCN/CSI operational infrastructure is composed of the EuroDomain relay devices (CCN Gateways), security devices, customer premises router and telecommunications.

This service covers:

- Availability Management;
- Contingency Management;
- Application Configuration Data management;
- Security Management.

And also includes:

- The coordination of the moving of CCN/CSI equipment;
- The coordination of deployment of new sites;
- The capacity planning of the CCN infrastructure;

- Follow-up of the above-requested activity during the monthly progress meeting. This meeting is QA'ed and consists of all contracting parties contributing to the CCN/CSI service;
- Facilitation of 'freeze' requests. These can be requested only by authorized users to a DG TAXUD dedicated official;
- Design, planning, deployment, operations, technical support & retirement of HW, OS and COTS;
- Network Services;
- HW& OS & COTS Services;
- Backup & Restore;
- Job Management Service;
- Production & Maintenance of ICT Infrastructure Management Related Plans i.e. ICT Infrastructure Plan, Availability Plan, Capacity Plan, Continuity Plan;
- Feasibility Studies linked to Infrastructure.

#### 4.3.3.1. *Availability Management*

The main service that the Service Provider has to provide is to ensure that the CCN/CSI system is "up and running" at the required availability level.

The Service Provider ensures that all CCN/CSI sites are interconnected through a Wide Area Network (WAN) offering the necessary resilience and capacity to ensure the proper functioning of critical business applications using the CCN/CSI infrastructure and services.

The availability management service covers the following items:

- Global access in all connected NAs;
- The provision of the local loop (+ a backup line) between the WAN local access point (PoP) and the National Administration premises;
- The Customer Premises Router (CPR) installation, configuration, and maintenance;
- The Security Device (i.e. SSG encryption-firewall box) installation and maintenance;
- Communication gateways located on the DMZ, at every local site (i.e. CCN Gateways);
- The central CCN Mail III system.

The Service Provider also provides statistical information on the availability collected under operational circumstances and a monitoring service, both for proactive problem tracking and statistical purposes.

#### 4.3.3.2. *Contingency Management*

The Service Provider is responsible for the CCN/CSI components located in the DG TAXUD CCN Infrastructure at each CCN/CSI site.

The Contingency service aims at restoring the agreed service levels within an agreed timeframe in case of partial or complete dysfunction or destruction of the CCN/CSI system by providing the Service Requesters with help and items such as:

- Software backup of CCN gateways (at every site);
- Central CCN backup site;
- Redundant encryption devices;
- Switching capabilities between production and backup gateways;
- Spare units for hardware devices;
- Dual telecom access lines to the CCN backbone (at every site);
- Assistance in installation and configuration of CCN/CSI items in the DG TAXUD CCN Infrastructure;
- Recovery procedures.

#### 4.3.3.3. *Application Configuration Data Management*

This service concerns the management of configuration data, required by CCN/CSI applications, by the Service Provider.

These configuration data are stored in the central CCN/CSI Directory. The central CCN/CSI Directory management is shared between the Service Provider and the National Administrations. Each National Administration is in charge of the management of its local CCN/CSI users. The rest is managed by the Service Provider.

Examples of configurations subject to an Administration Service Request are:

- Definition of a local admin profile;
- Registration of an application service;
- Registration of an application queue;
- Registration of a message type;
- Validation of application configuration data;
- Registration of administration roles;
- Contact list management.

#### 4.3.4. **Security Management**

This service concerns the management of the security items, required by CCN/CSI environment, by the Service Provider.

Security is managed as well on the level of the involved server equipment (OS), network equipment and on operational level.

- Information exchanges over the CCN/CSI network are protected to ensure optimal confidentiality and data integrity.
- Security services include:
  - Site-to-site encryption and protection against unwanted accesses enforced by firewall/encryption devices.

- Access control mechanisms (authentication, authorisation, accounting) at site level enforced at CCN Gateway and supported by local administration tools (ADM3G).
- Session-level security enforced by message-level encryption (CSI secure), SSL mutual authentication and encryption (HTTPS & NJCSI), POP-S and IMAP-S (secure e-mail transport).
- SIAP unified defence mechanism for secured internet access to CCN services.

#### **4.3.5. Documentation management**

The Service Provider maintains the whole CCN/CSI technical documentation (i.e. technical document, user guides, frequently asked questions, newsletters, upcoming events, etc.) up-to-date, which acts as Documentation Centre.

This includes the documentation related to the CCN/CSI infrastructure: Oracle-Tuxedo, IBM-MQ, CCN Gateways, CCN Mail III, CSI software, procedures, reports, history of communication with partners, etc.

The Service Provider manages a list of documentation, related to the CCN/CSI that can be communicated to Service Requester. These documents are available on CIRCABC, and the ITSM Portal.

The Service Provider automatically updates the list with the newly approved version of the documents.

#### **4.3.6. Reporting and statistics**

The Service Provider provides the Service Requester with the following reporting facilities through the CCN and ITSM Web Portal:

- On-line availability figures for CCN Gateways and CCN Mail III servers;
- On-line newsletters;
- Statistics on CCN/CSI exchanges.

The Service Provider also regularly holds IT Tech & Infra meeting, where the reporting and statistics are presented.

#### **4.3.7. Training**

The Service Provider works out courses and performs training related to the technical aspects of the CCN/CSI system. The standard courses are organised in training packages divided into modules. As a general rule, training sessions are organised every year. The standard training packages are distributed twice a year via DG TAXUD and available online on the ITSM Portal.

## **5. SERVICE LEVEL MEASUREMENT**

### **5.2. SERVICE LEVEL**

The Service Level is a measure of the quality of the services provided by the Service Provider. It is computed by a Service Quality Indicator or SQL.

It is expected that the Service Requester complies with its obligations (see §0) to achieve the agreed Service Level.

### **5.2. APPLICABLE SERVICE QUALITY INDICATORS**

### 5.2.1. Individual CCN/CSI Site Availability

This Quality indicator provides the lowest measured availability of an individual site during the « Full Period », i.e. 24\*7, for a given month. The CCN/CSI SLA limit is defined as follows:

<b>LIMIT</b>	>= 97,0 % availability
--------------	------------------------

### 5.2.2. Quality Indicator on the Duty Period

The Service Provider's "Duty Period" is the hours of coverage of the Service Desk function. The duty is ensured by the Service Provider SD 24/24, 7 days a week including public holidays.

Depending of the CI's Service Window, there is an immediate action (24\*7) or the intervention is scheduled for the next Service Window. Letter, fax, e-mails and electronic requests (through the ITSM Portal) are accepted at any moment. Incoming requests are registered as "Service Calls" in the Service Provider Service Desk management system.

The SLA limit is defined as follows:

<b>LIMIT</b>	Service Desk shall not be unreachable during the duty period more than 2 times / month
--------------	--

### 5.2.3. Quality Indicator on the Notification Service

The Service Provider provides notifications services to the Service Requester.

There are two types of notifications, for Urgent Notifications and for Normal Notifications:

- URGENT NOTIFICATIONS (when there isn't enough time to notify the CCN/CSI community at least 7 calendar days in advance): the notifications are disseminated to the appropriate audience at the latest, 2 hours after reception of an urgent notification request.
- NORMAL NOTIFICATIONS (or planned interventions): the notifications are disseminated to the appropriate audience at least one week (7 calendar days) before the interventions and a reminder is sent at least 24 hours before the events.

This indicator measures the respect of deadline for announcement (via mass mails) of scheduled unavailability.

### 5.3.4. Quality Indicator on the Contingency Management

**Cold Standby** (Switch Procedure, Backup & Restore or CCN over Internet)

The appropriate type of switch to be performed depends on a thorough analysis of the specific national administration setup and the problem at hand.

The maximum delay to switch from any national administration Production Gateway to an appropriate CCN Backup Gateway solution is defined as follows:

<b>LIMIT</b>	Max 5 working hours following the agreement with the Service Requester to perform the switch
--------------	--



### 5.3.5. Quality Indicator on the Application Configuration Data management

The maximum delay to implement an Application Configuration Request via the ACT (Application Configuration Tool) for a single site is defined as follows:

<b>LIMIT</b>	5 working days
--------------	----------------

### 5.3.6. Quality Indicator on the Acknowledgment Delay

The maximum delay between the time a request is received by the Service Desk and the time an acknowledgment (i.e. Service Call number) is sent to the service requester, is defined as follows:

<b>LIMIT</b>	30 minutes
--------------	------------

Incidents are classified according to their **priority levels**.

The priority of an incident is a number between 1 and 4:

<b>1</b>	<b>CRITICAL</b>
<b>2</b>	<b>HIGH</b>
<b>3</b>	<b>MEDIUM</b>
<b>4</b>	<b>LOW</b>

### 5.3.7. Quality Indicator on the Resolution Delay

The resolution delay is the elapsed time between the moment the incident is acknowledged by the Service Provider and the moment the Service Provider repairs the root cause of the incident or implements a workaround.

According to the Priority, the resolution delay is defined as follows:

<b>PRIORITY</b>	<b>RESOLUTION DELAY</b>
<b>CRITICAL</b>	5 Working Hours
<b>HIGH</b>	13 Working Hours
<b>MEDIUM</b>	39 Working Hours
<b>LOW</b>	65 Working Hours

Table 8: Resolution Delays

<b>PRIORITY</b>	<b>LIMIT</b>
<b>CRITICAL</b>	>= 95.00% of CRITICAL incidents must be solved within the agreed resolution delay (5 Working Hours).
<b>HIGH</b>	>= 95.00% of HIGH incidents must be solved within the agreed resolution delay (13 Working Hours).

<b>MEDIUM</b>	>= 95.00% of MEDIUM incidents must be solved within the agreed resolution delay (39 Working Hours).
---------------	---

Table 9: Limit of Resolution Delays for Incidents

**6. APPROVAL OF THE SLA**

The Service Level Agreement has to be approved by the Joint Committee in order to be applicable.

**7. CHANGES TO THE SLA**

The CCN/CSI SLA will be reviewed following a written request from the Commission or Norway to the Joint Committee.

Until the Joint Committee decides on the proposed changes, the provisions of the CCN/CSI SLA in force are applicable. The Joint Committee acts as the decision making body for the current CCN/CSI SLA.

**8. CONTACT POINT**

For all operational services, the ITSM3 Operations acts as single point of contact. Its coordinates are provided below:

ITSM3 Operations - IBM

☎ Toll free: + 800 7777 4477

📞 Caller paid: + 40 214 058 422

✉ support@itsmtaxud.europa.eu

🌐 <http://portal.ccntc.ccncsi.int:8080/portal>  
(CCN Web Portal - for CCN Registered users)

🌐 <https://itsmtaxud.europa.eu/smt/ess.do>  
(ITSM Web Portal - For Service Calls)

*Date*

## ATTACHMENT 6

### Draft

#### **DECISION No 6/[date] of the Joint Committee of [date] adopting the amount and modalities of the financial contribution to be made by Norway to the general budget of the Union in respect of the cost generated by its participation in the European Information Systems**

THE JOINT COMMITTEE, established in accordance with Article 41(1) of the Agreement between the European Union and the Kingdom of Norway on administrative cooperation, combating fraud and recovery of claims in the field of the value added tax, hereinafter referred to as the "Agreement",

Whereas:

- (a) Regulation (EU) No 1286/2013 of the European Parliament and the Council of 11 December 2013 establishing an action programme to improve the operation of taxation systems in the European Union for the period 2014-2020 (Fiscalis 2020) lays down the rules for the development, operation and maintenance of the European Information Systems.
- (b) The Common Communication Network/Common System Interface and the electronic forms to be adopted pursuant Article 41(2)(d) of the Agreement are Union components of the European Information Systems referred to in point A of the Annex of Regulation (EU) No 1286/2013.
- (c) Pursuant to Article 9(3) of Regulation (EU) No 1286/2013 the use of the Union components of the European Information Systems by non-participating countries shall be subject to agreements with those countries to be concluded in accordance with Article 218 of the Treaty on the Functioning of the European Union.
- (d) It is necessary to adopt practical arrangements for the implementation of Article 41(2)(f) of the Agreement;

HAS ADOPTED THIS DECISION:

#### *Article 1*

##### **Installation costs**

The initial costs to be paid by the Kingdom of Norway for the establishment of the Virtual Private Network access is 20 000 EUR.

The amount shall be paid within 60 days following adoption of this decision.

#### *Article 2*

##### **Yearly financial contribution**

The yearly financial contribution that the Kingdom of Norway shall pay to the General Budget of the Union shall be 20 000 EUR. The amount shall be paid each year by 1 September.

The contribution shall cover the expenditures related to the development, maintenance and upgrade of IT solutions (Common Communication Network/Common System Interface, e-Forms).

*Article 3*

**Method of payment**

The contributions under Articles 1 and 2 shall be paid in euro to the euro denominated bank account of the Commission that will be indicated in the debit note.

*Date*