AGREED RECORD OF CONCLUSIONS BETWEEN THE EUROPEAN UNION AND NORWAY ON THE FLUX TRANSPORTATION LAYER

29 JUNE 2022

1. A European Union Delegation headed by Mr Eckehard Reussner and a Norwegian Delegation headed by Mr Thord Monsen met on 22 June 2022 to follow up the discussions between the Parties that took place during 2020, 2021 and 2022 on a revision of the Agreed Record of Conclusions of Fisheries Consultations between Norway and the European Union on a Transportation layer for electronic exchange of data of 20 June 2014.

2. The Delegations agreed to implement a business independent network to exchange data using the FLUX transportation layer developed by the European Union. The business content envisages in particular position reporting, electronic notifications and authorisations, electronic catch and activity data and sales notes. Specific Agreed records define the business rules to exchange business content.

3. The Delegations agreed to recommend to their respective authorities to implement the provisions related to the FLUX transportation layer as outlined in this Agreed Record. The implementation of the FLUX transportation layer shall be in effect between the parties no later than 1 November 2022. The use of the FLUX transportation layer shall be agreed between the parties for each specific business content.

4. The European Commission will host a webpage with all relevant documentation on the FLUX transportation layer.

5. The parties using the FLUX transportation layer nodes shall cooperate on keeping the security and confidentiality level of the nodes in the system in line with best practises and recommendations.

6. The Delegations noted that the FLUX transportation layer is a critical system. Therefore, the parties strive for ensuring at least 99.9% quality of service[1] by using appropriate technical and human resources and by monitoring the technical infrastructure 24/7. The European Commission offers a helpdesk for assistance to both parties, which can be reached during working days as well as during weekends.

7. The Delegations agreed on a business continuity plan (see Annex) which is triggered in case of unexpected downtime of the business IT systems connected to the FLUX transportation layer, or of the FLUX transportation layer itself.

[1] Measured as proportion of messages delivered by the FLUX transportation layer before expiring.

8. The Delegations agreed to implement an acceptance environment for testing purposes, in addition to the production environment. The acceptance environment shall be operational during normal office hours as a minimum and normally be identical to the production environment. If agreed during testing of new versions the acceptance environment can include only the version in test.

9. Norway and the European Commission will maintain an issue log sheet to have the possibility to do auditing and evaluate the system.

10. Before new versions of the FLUX transportation layer or new Data Flows are implemented in the production environment testing in the acceptance environment shall be conducted and the result accepted by the Parties.

11. The Delegations agreed that both parties are free to install new versions of the FLUX transportation layer if this new version is backward compatible. Installing a new version which is not backward compatible is subject to agreement of both parties.

12. The Delegations agree to mandate a permanent working group with the task to monitor the implementation of this Agreed Record and to put forward suggestions for improving it if deemed necessary.

13. By the date of its application referred to in section 14, this Agreed Record replaces the Agreed Record of Conclusions of Fisheries Consultations between Norway and the European Union on a Transportation layer for electronic exchange of data of 20 June 2014.

14. The Delegations agree to apply the arrangements in this Agreed Record as from the date of its signature.

29 June 2022

For the European Union Delegation
Eckehard REUSSNER

For the Norwegian Delegation
Thord MONSEN

EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR MARITIME AFFAIRS AND FISHERIES

Fisheries Policy Atlantic, North Sea, Baltic and Outermost Regions
The Director

ANNEX TO AGREED RECORD ON A TRANSPORTATION LAYER

EU-Norway FLUX Business Continuity plan

1. Overview

The Business Continuity plan describes how the communication between the Parties shall be organised in the situation when data communication channels are interrupted.

2. Terminology

Transportation layer (TL): the electronic network for fisheries data exchanges as made available by the European Commission to exchange data in a standardised way.

Central node: a node acting on the TL network as an intermediate node connecting several endpoints. Note that the EU Member States will be connected to the Norway node via the EU central node (operated by the European Commission).

Endpoint: a Party that is connected to the TL network and is active for exchanging data with other endpoints.

3. Fall-back procedure

3.1. Description

Any Party (sender or recipient) who becomes aware of any failure in the transmission of data, including non-receipt of messages or receipt of invalid reports, shall immediately initiate the fall-back procedure by informing the other party (recipient or sender) of the problem, using any communication means available.

The fall-back procedure shall also apply during maintenance periods of a central node or endpoint.

The party causing the problem must take the necessary actions to correct the situation without undue delay.

Once the problem has been resolved, the responsible Party shall immediately inform other involved Parties.

3.2. Circumstances

3.2.1. Problems on sender end-point

When a technical failure occurs on the sender endpoint and the sender can no more transmit messages, the sender shall store those messages that could not be delivered to the other Party until the problem is solved.

In case of urgency and on request by any Party receiving data, the Party responsible for sending data shall use other communication means (email, secured FTP, etc.) to transmit urgent messages.

After repair of the system the sender shall transmit all held messages as soon as possible over the Transportation layer.

3.2.2. Problems on receiver end-point

When a technical failure occurs on the receiver endpoint and the sender can no more transmit certain messages, the sender shall stop transmitting the messages concerned over the transportation layer and shall store all messages to the failing receiver until the problem is solved.

In case of urgency and only if agreed between Parties exchanging data, the Party responsible for sending data may use other communication means (email, secured FTP, etc.) to transmit urgent messages.

After repair of the system the sender shall transmit all held messages as soon as possible over the Transportation layer.

3.2.3. Problems of the EU central node

When a technical failure occurs on the EU central node and the sender can no more transmit certain messages, the sender shall stop transmitting the messages concerned over the transportation layer and shall store all messages concerned until the problem is solved.

In case of urgency and only if agreed between Parties exchanging data, the Party responsible for sending data can use other communication means (email, secured FTP, etc.) to transmit urgent messages.

After repair of the system the sender shall transmit all held messages as soon as possible over the Transportation layer.

3.2.4. Maintenance

3.2.4.1. Scheduled downtime

Normal scheduled system maintenance operations have to be performed regularly.

For the central node and because its availability is critical for all Parties on the TL, a normal maintenance operation should not cause an unavailability period of more than 3 hours.

For the endpoints a scheduled maintenance downtime should be no more than 6 hours.

Any Party scheduling the maintenance shall inform all other Parties at least 72 hours in advance by using any electronic means available.

In case of emergency or force majeure situations, the maintenance operation may be performed without respect of the prior notice delays mentioned here above. The notification in that situation needs to be sent prior to the downtime effectively taking place.

3.2.4.2. Unscheduled downtime

Unscheduled downtime occurs when the system goes down unexpectedly. These downtimes may occur at any time and vary in length depending upon the reason. The Parties should endeavour to restore the system concerned as quickly as possible. As far as possible, the responsible Party shall give an estimate of the expected downtime period. When the downtime is ended, the responsible Party shall immediately inform other involved Parties by using any electronic means available.

3.2.5. Invalid reports[2]

A Party receiving an invalid report must contact the sender using any communication means (email, phone, etc.) to clarify the problem. It is the responsibility of the Party sending the report to provide as soon as possible a solution.

3.2.6. Message incorrectly delivered

After the reception of the message, FLUX-TL may raise an error which is reported through the TL to the sender. The sender has to react by either resending the same message, resending a corrected message or not resending the message at all, as specified in the Appendix of this Business Continuity Plan.

4. COMMUNICATION

The communication procedure described here shall be followed to exchange information between Parties in case a fall-back procedure is initiated or there is a maintenance going on at a central node or end-point involved in the data exchange.

In these situations, human intervention is required and information is communicated by email. Contact details for each end node are available on (the FLUX TL wiki.) .

4.1. Communication between Parties

The communication should cover business and, if deemed necessary, also technical questions directly related to the data exchanged.

The contact point in Norway for business related questions is: FMC@fiskeridir.no

The contact point in Norway for technical questions is: FMC@fiskeridir.no

[2] Cfr FLUX Implementation Documents identifying circumstances when the fall back procedure must be applied for invalid reports.

The contact point in the European Commission for business related questions is: MARE-DATA-MANAGEMENT@ec.europa.eu

The contact point in the European Commission for technical questions is: FISH-FIDESINFO@ec.europa.eu

Contact points in the EU Member States will be listed on the FLUX TL wiki.

Each Party shall ensure that the first reply is given as soon as possible, but not later than within 1 working day. It can be a simple acknowledgment of the receipt, but should indicate an estimated timeframe, when the issue is expected to be resolved or addressed.

4.2. Communication with the DG MARE FIDES helpdesk

For practical reasons, the communication language is English.

FIDES Helpdesk email address is fish-fidesinfo@ec.europa.eu.

DG MARE FIDES helpdesk shall ensure that the first reply is given as soon as possible, but not later than within 1 working day. It can be a simple acknowledgment of the receipt.

DG MARE FIDES Helpdesk shall assign a unique business identifier to every request. All following email exchange shall maintain this subject line and the unique identifier.

For any email communication, please comply with the following instructions:

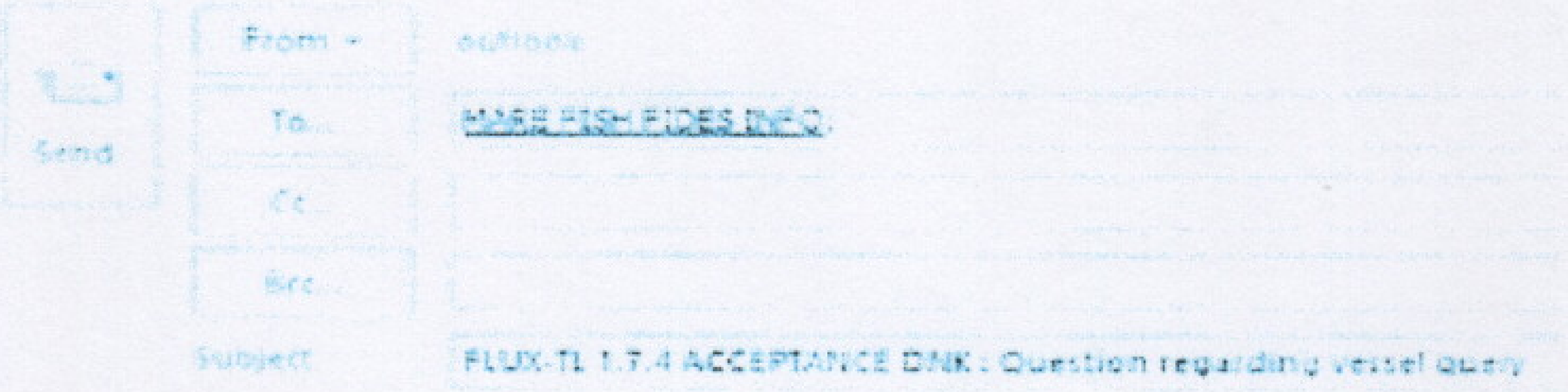
General Guideline:

For a ticket to be opened, fish-fidesinfo@ec.europa.eu needs to be in the TO field. If it is only in CC, it will consider the mail to be just for information.

Subject of the email: Please use the following structure:

- System (FLUX-TL, EU-ERS, NORERS, …)
- Version (1.7.4, 3.1, …)
- Environment (PROD or PRODUCTION, ACC or ACCEPTANCE)
- NODE: (e.g. "NOR") to avoid mistake on countries with multiple nodes and service providers managing multiple nodes
- Short Description: 50 Characters Maximum ideally

Example:



From: outlook

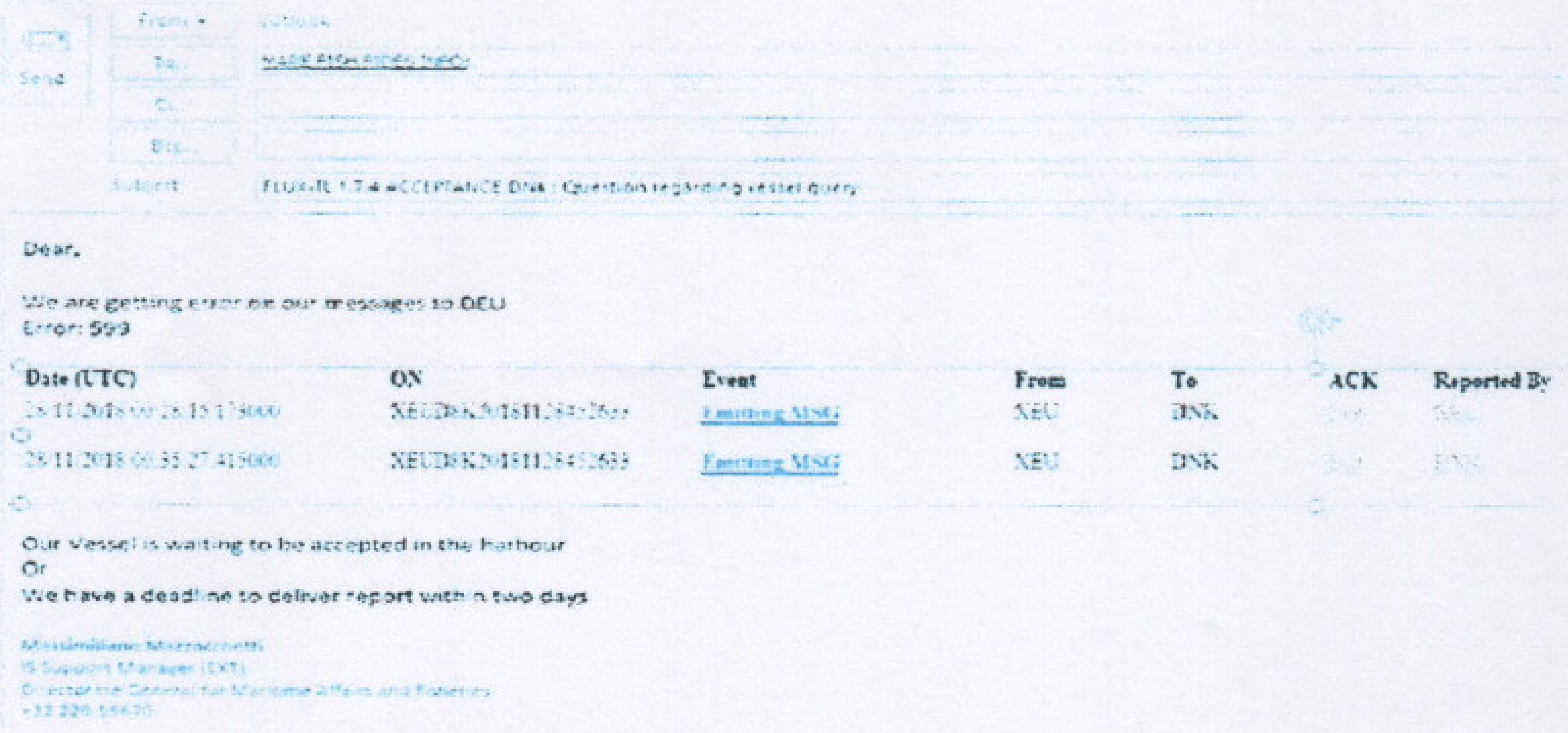
To: MARE FISH FIDES INFO;

Subject: FLUX-TL 1.7.4 ACCEPTANCE DNK : Question regarding vessel query

Content of the email:

- What is not working (e.g. Not able to send messages)
- Error: if applicable
- Screenshot or log of the system experiencing the issue (FLUX.LOG), to help us understand the nature of the issue
- Business Impact of the issue, to help us assessing the priority of to the ticket

Example:



From: outlook

To: MARE FISH FIDES INFO;

Subject: FLUX-TL 1.7.4 ACCEPTANCE DNK : Question regarding vessel query

Dear,

We are getting error on our messages to DEU
Error: 599

Date (UTC)	ON	Event	From	To	ACK	Reported By
28/11/2018 00:26:15.173000	XEUDNK20181128452622	Emitting MSG	XEU	DNK	[illegible]	[illegible]
28/11/2018 00:35:27.415000	XEUDNK20181128452633	Emitting MSG	XEU	DNK	[illegible]	DNK

Our Vessel is waiting to be accepted in the harbour
Or
We have a deadline to deliver report within two days

Massimiliano Mezzacchetti
IS Support Manager (EXT)
Directorate-General for Maritime Affairs and Fisheries
+32 229 56620

5. Appendix - Policy about resending FLUX TL messages

In principle, messages not correctly delivered by FLUX TL should be resent until they arrive at their intended destination.

However, some error messages require a different action:

Don't resend messages if :

- **201** - Final status. Message has been delivered correctly.
- **202** – Non-final status. The message will be tried again until expiration. Don't resend until you have final status
- **500-598** – Non-final status. Don't resend. The message will be retried by itself until expiration.

Fix and Resend messages if :

Wait for a configuration change / fix and then resend in the following cases:

- **4xx** statuses. They're final statuses but something needs to be changed either in the recipient configuration or on the outgoing message before resends can be done.
    - **400** – Bad Request. Message needs to be reviewed by sender. Modify it and resend.
    - **401** – Node needs to be whitelisted. Wait for whitelisting at XEU and then resend.
    - **403** – Node needs to be authorised. Wait for authorisation at XEU and then resend.
    - **404** – Unknown dataflow. Wait for configuration at XEU and then resend.
    - **406** – Bad envelope. Message needs to be reviewed by sender. Modify it and resend.
    - **412** – Unknown return route. Wait for configuration at XEU and then resend.
    - **413** – Message too large. Configuration needs to change either at sender
    - **--*** or at XEU before resending.

Always Resend:

- **599** – Time Out. Resend. In principle, resends should be done until the message is successfully delivered.