AGREED RECORD OF CONSULTATIONS BETWEEN THE UNITED KINGDOM AND NORWAY ON THE FLUX TRANSPORTATION LAYER

19 JUNE 2024

1. A United Kingdom Delegation headed by Mr James Windebank, and a Norwegian Delegation headed by Mr Thord Monsen, have consulted on an Agreed Record on the Fisheries Language for Universal Exchange Transportation Layer (FLUX TL) for electronic exchange of data between the United Kingdom and Norway.

2. The Delegations decided to implement a business independent network to exchange data using the FLUX TL. The business content envisaged: position reporting, electronic notifications and authorisations, electronic catch and activity data and sales notes etc. Specific Agreed records will define the business rules to exchange business content.

3. The Delegations decided to recommend to their respective authorities to implement the provisions related to the FLUX TL as outlined in this Agreed Record. The implementation of the FLUX TL shall be in effect between the Parties no later than 1 December 2024. The use of the FLUX TL shall be decided between the Parties for each specific business content.

4. The Parties using the FLUX TL nodes shall cooperate on keeping the security and confidentiality level of the nodes in the system in line with best practises and recommendations.

5. The Delegations noted that the FLUX TL 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.

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

7. The Delegations decided 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 may include only the new version in test.

8. The Delegations will maintain an issue log sheet to have the possibility to do auditing and evaluate the system.

---

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

9. Before new versions of the FLUX TL 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.

10. The Delegations decided that both Parties are free to install new versions of the FLUX TL if this new version is backward compatible. Installing a new version which is not backward compatible is subject to agreement of both Parties.

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

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

Date: 19/6/24

Place: BRUSSELS

For the United Kingdom Delegation
James WINDEBANK

Date: 19/6/24

Place: Brussels

For the Norwegian Delegation
Thord MONSEN

ANNEX TO AGREED RECORD ON A TRANSPORTATION LAYER

UK-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 software for the Transportation Layer for fisheries data exchanges would conform to the UN/CEFACT standard.

Endpoint: the UK node and the Norway node constitutes the endpoints for exchanging data.

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 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 longer transmit messages, the sender shall store the 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 longer 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. Maintenance

3.2.3.1. Scheduled downtime

Normal scheduled system maintenance operations have to be performed regularly.

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

Any Party scheduling the maintenance shall inform the other Party 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.

3.2.3.2. 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 the other Party by using any electronic means available.

3.2.4. 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.

---

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

3.2.5. 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 an end-point involved in the data exchange.

In these situations, human intervention is required, and information is communicated by email.

4.1. Communication between Parties

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

Business related inquiries:

Norwegian FMC	**UKFMC**
fmc@fiskeridir.no	UKFMC@gov.scot
Directorate of Fisheries, Bergen	The Marine Directorate of the Scottish Government, Edinburgh *and* ops@marinemanagement.org.uk Marine Management Organisation, Newcastle

Technical inquiries:

Norwegian FMC	**Cefas**
fmc@fiskeridir.no	atoperations@cefas.gov.uk
Directorate of Fisheries, Bergen	Centre for Environment Fisheries and Aquaculture Science, Suffolk

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.

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 GBR/NOR and then resend.
    - **403** – Node needs to be authorised. Wait for authorisation at GBR/NOR and then resend.
    - **404** – Unknown dataflow. Wait for configuration at GBR/NOR 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 GBR/NOR and then resend.
    - **413** – Message too large. Configuration needs to change either at sender or receiver before resending.

Always Resend:

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