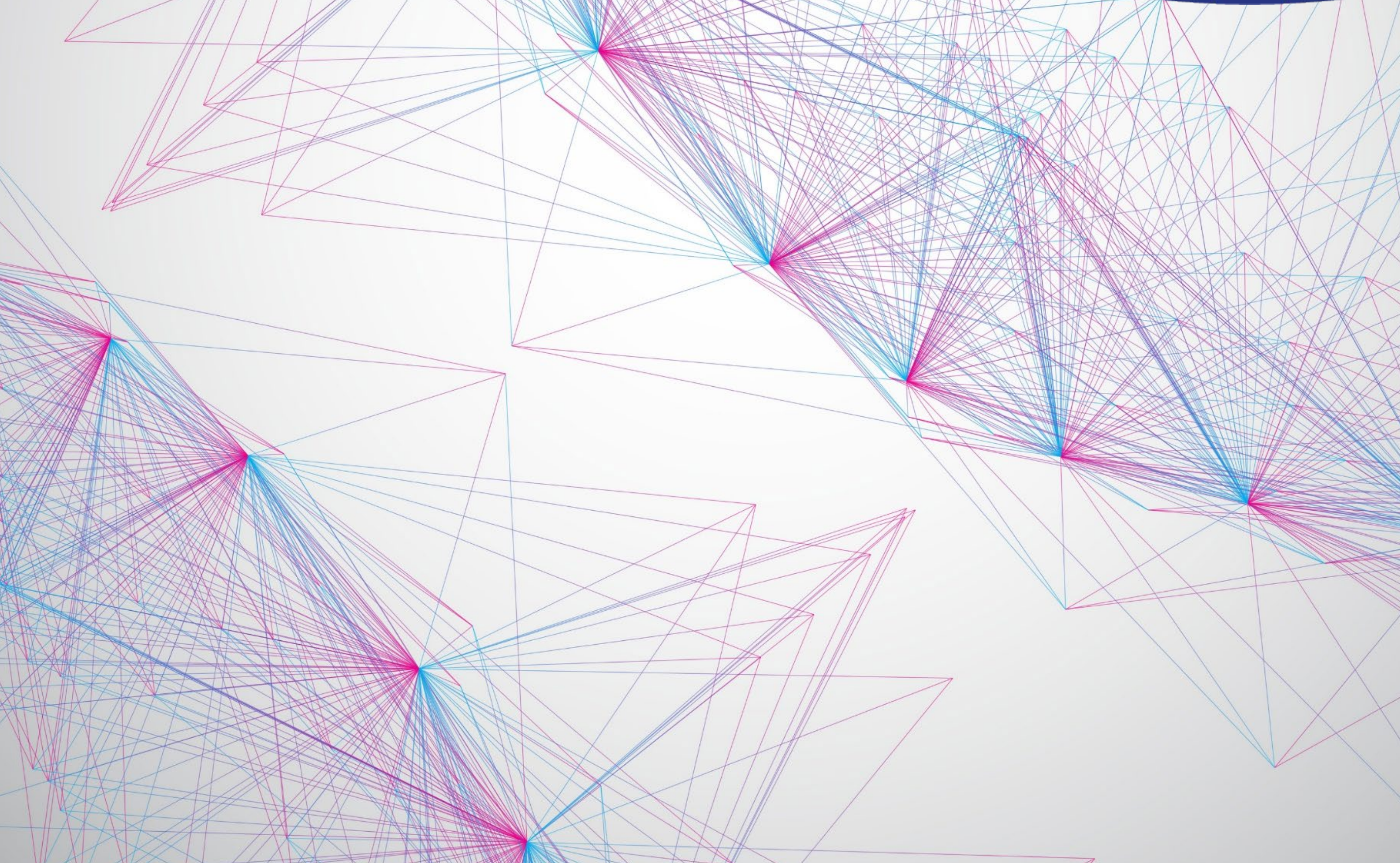
Recommendations on the operational and technical use of DubliNet

EASO Practical Guide Series

November 2020



Manuscript completed in November 2020

Neither the European Asylum Support Office (EASO) nor any person acting on behalf of the EASO is responsible for the use that might be made of the following information.

PDF ISBN: 978-92-9465-580-6 doi: 10.2847/8960 BZ- 08-21-342-EN-N

Cover page illustration, tigerstrawberry, ©iStock, 17 January 2020

About these recommendations

Why were these recommendations created? The mission of the European Asylum Support Office (EASO) is to support European Union Member States and Associated Countries (hereafter Member States[1]) through common training, common quality standards and common country of origin information, among others. According to its overall aim of supporting Member States in achieving common standards and high-quality processes within the Common European Asylum System (CEAS), EASO develops common practical tools and guidance. At a Thematic Expert Meeting on DubliNet and Dublin technical systems, held in Brussels on 26 September 2019, national DubliNet experts called upon EASO to support the drafting of a set of recommendations and good practices related to the use of DubliNet, the secure messaging system for the Member States. This is in order to promote a harmonised approach to the system in the Member States, and in order to ease the resolution of incidents. DubliNet is used by 31 Member States.[2]

What is the objective of this document? This document was developed to promote best practices for the operational use of DubliNet in the Member States. These recommendations should bring clarification for the use of and dealing with DubliNet on a daily basis, easing cooperation by providing common ground for the Member States as a starting point for the further harmonisation of the Dublin practice. This clarification and common ground should contribute to reducing incident resolution time.

What is in the scope of these recommendations? The nature of this document is to put forward recommended courses of action that can be taken by the Member States, either in the form of daily practice or in the form of practical policy. These recommendations should not restate existing documentation or guidance on the use of DubliNet. Rather, this document should provide unique content, focusing on daily use in the Dublin practice, as well as being a source of inspiration for Dublin managers and practical policy makers. These recommendations are predominantly workflow-centred, providing practical tips, exhibiting good practices and encouraging the adaptation of existing workflows with the use of good practices. These recommendations elaborate on best practices currently in use in the Member States, promoting a common standard the Member States can work towards.

Who should use these recommendations? This guide is primarily intended for Dublin case officers, working with DubliNet on a regular basis, as well as managers of Dublin units and policy advisors developing practical policies for the Dublin practice in their respective countries. Furthermore, these recommendations aim to inform other national officers, such as IT helpdesk professionals, as well as EU officers, such as experts working at eu-LISA, the European Commission or EASO, with a valuable insight in the daily practice of those working with DubliNet on a national level.

How were these recommendations developed? These recommendations were developed by Member State experts on DubliNet from Germany, Greece, the Netherlands, Romania, Sweden and Slovenia and with valuable input from officers working at eu-LISA. The development was facilitated and coordinated by EASO. Before its finalisation, a consultation on the guide was carried out with all Member States through the EASO Network of Dublin Units, consisting of 30 EU+ Member States and the European Commission, as well as eu-LISA.

[1] The 27 Member State of the European Union, complemented by Iceland, Liechtenstein, Norway and Switzerland.

[2] The situation as per 1 January 2021.

How should you read this document? This document starts with a standard workflow in working with DubliNet, delivering explanations, guidance and suggested courses for action for every step of this workflow. From Chapter Two onwards, further detailed recommendations are collected that cover certain topics of great importance further in-depth, such as Proof of Delivery and Security.

Wherever needed, recommendations are preceded by a legal reference in a box above the title of the recommendation. This document also contains, at strategic instances, boxes containing good practices, practical examples or additional remarks. Good practices are used to promote a certain way a Member State works, these are highlighted in orange in this document. Practical examples, highlighted in purple, are used to further illustrate and clarify certain topics for added clarification. Additional remarks, highlighted in green, are used to explain terminology used. The blue boxes refer to existing EASO products or other suggestions for further reading.

Contents

List of abbreviations and commonly used terms

CEAS Common European Asylum System

Dublin III regulation Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast)

DubliNet Secure electronic network of transmission channels between the national authorities dealing with asylum applications

EASO European Asylum Support Office

EID Exchange Infrastructure Document, describing the basis on which the exchange of messages can take place over DubliNet and listing the accompanying security measures

Eurodac European Asylum Dactyloscopy Database, established by the Eurodac regulation see 'Eurodac II regulation'

Eurodac II regulation Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast)

eu-LISA European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA)

Implementing regulation Commission Regulation (EC) No 1560/2003 of 2 September 2003 laying down detailed rules for the application of Council Regulation (EC) No 343/2003 establishing criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, as amended by Commission Implementing Regulation (EU) 118/2014 of 30 January 2014[3]

Member States Member States of the European Union and the Associated Countries (Iceland, Liechtenstein, Norway and Switzerland)

[3] For ease of reference, the consolidated version of these implementing regulations can be used.

Introduction

Dublin III regulation

Since 1 September 1997, Member States have been bound by a procedure known as the 'Dublin' procedure to determine which Member State is responsible for the examination of an application for international protection lodged in one of the Member States. The current Regulation (EU) No 604/2013 (Dublin III regulation), which entered into force in January 2014, lays down the criteria to determine which Member State is responsible for examining an application for international protection. The criteria for the determination of responsibility run, in hierarchical order, from family links in a Member State, to recent possession of a visa or residence permit in a Member State, to irregular entry into the EU. If none of these criteria apply, the first Member State in which the application was lodged is responsible.

Dublin procedure

As soon as a third-country national or stateless person lodges an application for international protection in one of the Member States, that Member State shall assess which Member State is responsible for examining that application. The ground rule of the Common European Asylum System (hereinafter: 'CEAS') is that Member States shall examine any application lodged by third-country nationals or stateless persons within the territory of the Member States, and the application shall be examined by a single Member State.

Member States may, on the basis of the Dublin III regulation, ask another Member State to take charge of the application for international protection of the person concerned. Examples include when that person has a spouse in that Member State who has already applied for international protection – or Member States may ask a Member State to take back the person concerned in case an application has already been lodged in that Member State.

Requests like these are sent to another Member State through a secure electronic transmission channel called 'DubliNet'. This secure messaging system lies at the heart of the Dublin system and is the subject of this set of recommendations.

Further reading

In case you are new to the Dublin procedure and wish to learn more about it, there are several ways to educate yourself. First of all, the ***EASO Practical guide on the implementation of the Dublin III Regulation: Personal interview and evidence assessment*** is an excellent starting point to read about the Dublin procedure, its operation in practice and some of its intricacies. This guide is available in multiple languages.

Another good way to start is with the ***EASO training module on the identification of potential Dublin cases*** which is a module offered by EASO to Member State asylum officers who may possibly come across a potential Dublin case. The module is available to help them determine how to proceed with those cases and refer those to the Dublin Unit.

A secure messaging system for the Member States

The European Commission developed DubliNet together with the Member States as an electronic secure network of channels for transmissions between the Member States. The system became operational on 1 September 2003.

The secure messaging system introduced many improvements that are common to the Dublin system as it is today. From this point on, Member States could work with a single 'national access point' in each Member State, considerably rationalising communications between the Member States. DubliNet also introduced the concept of common forms for the exchange of requests and information between the Member States. These electronic forms, still in use to this day, present information in a uniform and accessible manner, vastly simplifying procedures and runtimes. All exchanges over the system are encrypted, further protecting the personal data of applicants. This encryption, combined with having single access points for each Member State and standardised forms for the exchange of requests, heralded tremendous improvements for the Dublin procedure in the Member States. Since the introduction of the new secure messaging system, information exchanged over DubliNet is seen as reliable, correct and authentic.

What is the legal basis for DubliNet?

DubliNet was set up under Article 18 of Commission Regulation (EC) No 1560/2003, the Commission Implementing regulation complementing the Dublin II regulation. The Implementing regulation provides detailed rules for the setup and use of the system (see Articles 18-21 Implementing regulation). The Dublin III regulation prescribes that a system for the secure exchange of data pertaining to the Dublin III regulation shall exist (see Article 35(4) Dublin III regulation). The mandatory use of the system for all instances except for practical arrangements for transfers and time and place of arrival is mentioned in the Implementing regulation Article 15.

In addition to the aforementioned legal basis, an Exchange Infrastructure Document DubliNet (hereinafter: 'EID') was drafted by the European Commission, describing the basis on which the exchange of messages can take place over DubliNet and listing the accompanying security measures, which have to be considered by the Member States.

How does DubliNet work?

Member States have various ways to set up access to the network for their case officers. Some Member States choose to fully integrate DubliNet in their digital case management system, fencing off the Network from direct human interference. Other Member States operate access to the network through email clients, giving DubliNet the distinct appearance of an ordinary email exchange with an inbox, outbox, etc.

This appearance, however, is misleading: DubliNet relies on a so called 'mesh' of Member States directly communicating with each other without the interference of a central unit or database. The Network is neither linked to the internet in any way. Since there is no central point verifying the information exchanged, the Member States use certificates and encryption methods to verify the data exchanged with each other over the network.

What kind of data is exchanged over DubliNet?

All requests, replies and written correspondence that the Member States exchange which concern the application of the Dublin III regulation, are exchanged through DubliNet (see Article 15 Implementing regulation). DubliNet is used for the exchange of all personal data related to individual applicants that needs to be exchanged with other Member States. The exchange of information is not open-ended: each exchange of information needs to be justified in correspondence with the grounds for such an exchange in the Dublin III regulation.

DubliNet is most commonly used for the exchange of take-charge and take-back requests and replies to those requests, but also for the organisation of Dublin transfers, the exchange of health data of applicants before a Dublin transfer and for requests for information on grounds of Article 34 Dublin III regulation.

How is DubliNet maintained?

Since DubliNet is a decentralised system, maintenance predominantly falls to the Member States. They are required to ensure continued operation throughout the year. eu-LISA is tasked with the operational management of DubliNet[4], inter alia, supporting the Member States by generating the encryption certificates used by the Member States, providing support in case of issues and training on the technical use of DubliNet.

Mandatory use of DubliNet

All requests, replies and written correspondence pertaining to the Dublin procedure must be exchanged over DubliNet. The only exception to this rule is for correspondence regarding the practical arrangements for transfers, time and place of arrival, which may be exchanged through other means. The Member States are expected to ensure continuous operation of their national access point (see Article 21(1) Implementing regulation). Even in the case of unforeseen downtime, no alternative means of communication may be used. Deadlines for sending a request or reply (see e.g. Chapter VI Dublin III regulation) are not suspended during the interruption of service (see Article 21(3) Implementing regulation).

[4] Articles 1(4) and 8 of Regulation (EU) 2018/1726 outline the responsibilities of eu-LISA in relation to the operational management of DubliNET.

Chapter 1. Working with DubliNet

All Member States are obliged to exchange data pertaining to the application of the Dublin III regulation over DubliNet. This chapter suggests ways Member States can work with DubliNet in their daily practice.

To this end, a workflow is presented from section 1.2 onwards, depicting general steps taken when using DubliNet to send a message, starting from the preparation and the sending of a message up till the final steps after the message has been sent. Before a message can be sent through DubliNet, however, Member States need to ensure that all prerequisites are in place for the correct use of the system. These conditions for use can be found in section 1.1.

1.1 Conditions for use of DubliNet

Article 15(1) Implementing regulation

Always use DubliNet

- Since Member States are obliged to exchange all requests, replies and written correspondence with regards to the application of the Dublin III regulation through DubliNet, Member States are encouraged to inform officers with access to the system about the rationale behind this obligation in order to further ensure compliance.
- Member States should promote the consistent and correct use of DubliNet in their Dublin practice.
- Member States should never exchange messages through other means than DubliNet.
- Member States should refuse to accept requests, replies or other written correspondence sent through other means by another Member State.

Additional remark

All information exchanged through DubliNet is exchanged in the form of a message. Although in some Member States, DubliNet has the appearance of an email service, the word ‘email’ should not be used as a synonym for messages exchanged over DubliNet as the exchange of the message does not take place over the internet, but over a secure, separate network.

Further reading

In the ***EASO Guidance on the Dublin procedure: operational standards and indicators***, there is frequent mention of how Member States should implement and operate the DubliNet system in their Dublin practices.

Access to DubliNet

- Member States provide access to DubliNet for dedicated officers.
- Member States are encouraged to provide access to a sufficient number of officers to ensure that workloads can be shared evenly to avoid errors.

Good practice

Member States task a specialised unit or department to take care of the exchange of messages over DubliNet. This specialised unit monitors incoming messages and is tasked with ensuring appropriate follow-up to these messages. The unit gathers messages to be sent and makes sure messages are then sent in a uniform manner compliant with existing guidelines.

Training and instructions

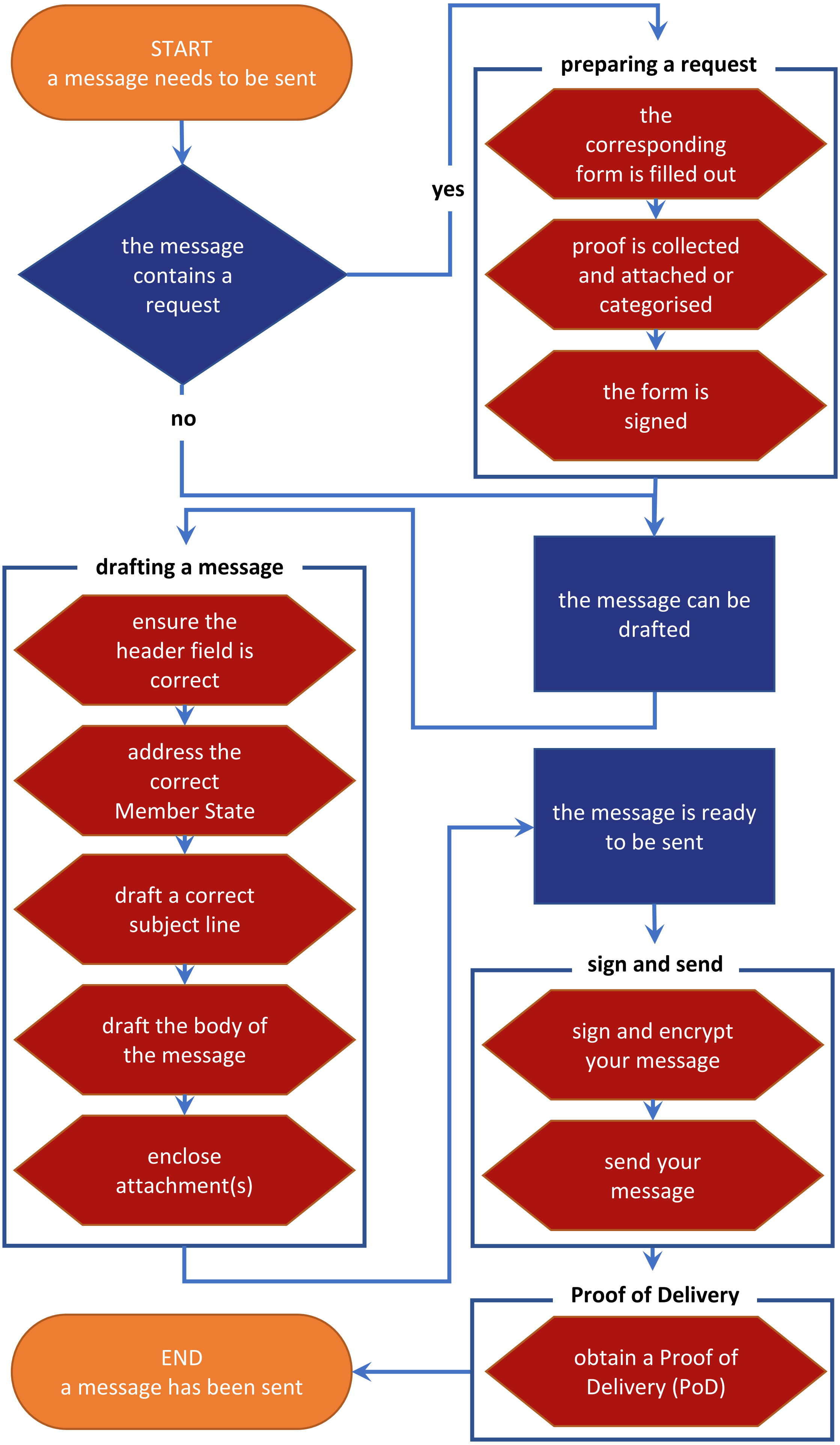
- Member States are advised to provide a training session to officers who will be working with DubliNet.
- Member States are advised to disseminate a manual with instructions for working with DubliNet to ensure a harmonised practical approach to the system on a national level.
- Member States are encouraged to regularly remind officers of the various rules and guidelines for conduct in working with DubliNet to ensure continued compliance.

Article 35(1) Dublin III regulation

Tools and workstations

- Member States are recommended to supply officers with sufficient (digital) tools to work with the network, such as a workstation with an office solution (for preparing textual answers), an ACROBAT-reader, either professional or standard (for filling the forms and converting answers and attachments to PDF format), the PKI (Public Key Infrastructure, i.e. the digital certificate) and proposed Adobe signing solution, and the client connected to the National Access Point for DubliNet.
- Member States may choose to grant new officers access to DubliNet and technical solutions for signing in segments, following their learning curve.

Standard DubliNet workflow for sending a message


START
a message needs to be sent
the message contains a request
yes
no
preparing a request
the corresponding form is filled out
proof is collected and attached or categorised
the form is signed
drafting a message
ensure the header field is correct
address the correct Member State
draft a correct subject line
draft the body of the message
enclose attachment(s)
the message can be drafted
the message is ready to be sent
sign and send
sign and encrypt your message
send your message
Proof of Delivery
obtain a Proof of Delivery (PoD)
END
a message has been sent

*This full workflow is clickable which leads to further clarification in the various other sections of this chapter

1.2 Preparing a request

Articles 1 and 2 Implementing regulation

Filling out the form

- When sending a take-back request, a take-charge request, transfer information or any other type of messages, the sending Member State always use the standard forms applicable for each situation.
- The case officers have access to these standard forms and should be instructed on their use, such as on how these forms are to be filled out.
- Case officers are advised to include as much information in their form as possible to allow for easier identification and faster proceedings.
- Case officers are recommended to write the information in their form in English if Member States have not agreed to a common language for use in the exchange.

Articles 1 and 2 Implementing regulation

Prepare and attach proof

- Case officers evaluate if, and what kind of proof should be included in the standard form or attached to the message to support the reply or request.
- Case officers are encouraged to include evidence in the standard forms as much as possible, for ease of reference.
- In case the request or other type of information requires one or more attachments to be sent separately, it is recommended that those attachments are named accordingly. This helps the receiving Member State to process the request faster.

Good practice

When naming attachments that are sent separately, short and snappy titles are given to each document so the receiver can easily determine the contents of each attachment. Titles used for attachments could look like ‘take-back request’, ‘abscondence info’, ‘Eurodac search result’, ‘fingerprints’, ‘passport’ etc.

Sign the form

- Before attaching any standard form, the standard form needs to be electronically signed by an officer who is authorised to do so.
- Case officers need to understand that standard forms need to be duly signed for them to be considered and processed by the requested Member State.

Further reading

For a case officer to be able to sign a form, and henceforth sign and encrypt a message to be sent through DubliNet, an adequate certificate is required.

The **Exchange Infrastructure Document**, the most recent version of which can be obtained from the DubliNet Single Point of Contact (SPoC) in each Member State, prescribes how these certificates need to be implemented in the Member States. This so-called ‘Public Key Infrastructure’ (PKI), which also concerns policies for hardware and software, ensures DubliNet is uniformly secured in all Member States.

1.3 Drafting a message

Article 15(2) Implementing regulation

Header fields

- Case officers need to make sure that a message is sent on behalf of the Member State.

Additional remark

Some Member States use an email client to make DubliNet accessible to case officers. In those countries, it may happen that the header field (the 'from' field) is not filled or selected with the national nap.testa domain by default. In those instances, case officers need to be extra cautious when sending a message. If this is not filled out correctly, the message risks bouncing back.

Address the correct Member State

- Case officers ensure to always address the correct Member State, for otherwise risking to not receive a reply to the message or a delivery error, which in turn could lead to exceeding the time limits established by the Dublin III regulation.
- Member States are encouraged to provide a (digital) address book containing solely NAP-addresses of all Member States for use with DubliNet.

Article 20(1) Implementing regulation

Drafting a subject line

- Messages are to be coded with the correct subject line, consisting of the correct code for each type of message.
- Case officers are advised to pay special attention to drafting the subject line since Member States can have set up automated rules and filters to handle and distribute incoming messages accordingly. The rules and filters only work correctly when the subject of the sent message complies with the commonly agreed specifications.

Additional remark

The subject line used in DubliNet is constructed by combining codes, file numbers and additional information so that it is clear to the requested Member State what the content of a message is.

1. The subject line starts with the country code of the Member State as given in ISO 3166, e.g. 'AT' or 'GR'
2. Then a 'DUB' to indicate the fact that there will be a Dublin exchange category referred to (see below)
3. Followed by the code corresponding with the category of the request (the 'type of exchange')
4. And finally, the national unique case reference number as defined by the sending Member State, which may contain characters ranging from A-Z, a-z, 0-9, slash, hyphen, dot and a blank inside

Additional remark

The codes for the different **types of exchange**:

DUB1	Request for taking charge
DUB2	Request for taking back
DUB3	Request for information
DUB4	Exchange of information on the child, sibling or parent of an applicant in a situation of dependency
DUB5	Exchange of information on the family, sibling or relative of an unaccompanied minor
DUB6	Transmission of information prior to a transfer
DUB7	Transmission of the common health certificate

- When replying to a message, case officers keep the original subject line of the message of the Member State to which the reply is sent, intact.

Additional remark

When replying to a message, case officers reflect the original subject line of the initial message, followed by an indication that the message that is being sent is a reply to that original message. The case officer does so by adding '+REPLY' to the subject line.

The case officer may choose to add to the subject line the reference number on other types of information or codes being used for the case in their Member State, to ease the identification of the case. Case officers can choose to put that information between brackets.

- Case officers are encouraged to make use of keywords in the subject line to point to peculiarities of the case that the message concerns.

Additional remark

Additional information can be added to the subject line as well as keywords. This is in order for the receiving Member State to be aware of the nature of the message from the moment of receiving the message and in order for the receiving Member State to proceed accordingly. Commonly accepted keywords are as follows:

'+abscondence' *indicating that the message concerns an absconded Dublin transferee*

'+detention' *indicating that the case concerns a third-country national or stateless person in detention*

'+family' *indicating that the message also concerns minors for whom the applicant is responsible*

'+suspensive effect' *indicating that the message contains information about suspensive effect. This information can be complemented with* 'appeal' *or* 'decision' *to indicate the beginning or the end of the injunction*

'+UAM' *indicating that the case concerns an unaccompanied minor*

Urgency

- In urgent cases, case officers add the keyword '+URGENT' to the subject line to draw the receiving Member States' attention to the message and to the need to provide follow up as soon as possible.
- The addition of '+URGENT' to the subject line is done at the discretion of the sending Member States', but generally this is done for cases in which a deadline is shortened, or in cases of extreme vulnerability.

Practical examples

The following practical examples are used to illustrate the aforementioned recommendations:

'DEDUB1########'
Germany is asking another Member State to take charge of the application for international protection of an alien with reference number ########

'GRDUB1######## +REPLY (#####)
A Member State sends an official reply to a take-charge request from Greece. The case identifier of the requested Member State can be found between brackets.

'SEDUB2######## +family'
Sweden is requesting another Member State to take back an alien with reference number ########. The request also covers one or more minors.

'ESDUB3####### +UAM'
Spain is asking for information another Member State might have about an unaccompanied minor who lodged an application for international protection in Spain.

'SIDUB2####### +FU (our ref. no. #####)'
A Member State follows up on an existing exchange regarding a third-country national or stateless person. Between brackets, the responding Member State included its own reference number.

'PLDUB6####### +URGENT (your ref. no. #####)'
Poland transmits information prior to a transfer to another Member State. The message is deemed urgent by Poland, most probably because of an upcoming deadline. Poland included the addressed Member State's own reference number to ease proceedings.

Article 16 Implementing regulation

Draft the body of the message

- A request sent through DubliNet should not contain a message body as all information about the contents of the message is in the subject line of the message and the request itself is in the electronic form.
- Any further exchanges taking place regarding the same topic are not bound by any form requirements. Therefore, case officers can use the body of the message to, for example, formally reply to a request.
- Member States are recommended to agree on a common language with their counterparts for the exchange of their messages to lessen confusion, misunderstanding or need for translations that might delay the process.
- If Member States did not agree on a common language for use in the exchange, case officers are recommended to send messages in English.

Enclosing attachments

- Case officers are advised to check all the attachments that will be sent to verify whether the correct request and attachments are being submitted.
- Case officers are requested to take the size of the message that will be sent into account before the message is sent. Member States might have a size limit in place for any incoming messages, blocking the delivery of the message which could ultimately result in receiving a delivery error message.
- Case officers can check the size of an electronic form by checking the properties of the file. Case officers should note that the encryption of the message roughly doubles the size of the message which can also result in exceeding message size limits.

Additional remark

In case Dublin officers need to adapt a message to meet the size limits for incoming messages some Member States have imposed, two recommended courses of action can be taken.

- **Compress the file using Adobe Acrobat**
  Through Adobe Acrobat, case officers can use the built-in option to compress the file which will lead to a smaller file size. Compressing should not impair the quality of the document in such a way that it renders the document useless or unreadable.
- **Create segments**
  Case officers can choose to send their message in different parts, separating attachments from the

electronic form, for example. In case the message is sent in parts, case officers should indicate this in the subject line of the message, for example by adding '(Part 1 of 2)', etc.

Member States are discouraged from enclosing compressed files such as .zip or similar with a message as these types of files can be flagged as potentially malicious content by Member States' security systems.

Further reading

The **Exchange Infrastructure Document** contains detailed and specific information on what the structure of messages exchanged through DubliNet should look like. The EID provides rules on the message header, subject, body and attachments exchanged.

Since the document provides the commonly agreed uniform standard for use of DubliNet in the Member States, all Member States must abide by the rules provided by the EID.

1.4 Sign and send

Article 15 Implementing regulation

Signing and encryption

- Case officers need to ensure that, before a message is sent, it is signed and encrypted as the exchange pertains to personal data of third-country nationals or stateless persons. Without the proper signature and encryption, the message might be refused by the receiving Member State.

Good practice

Member States choose to set up their DubliNet system in such a way that all outgoing messages are automatically signed and encrypted.

- Member States can disregard and delete all incoming messages that are not signed and encrypted.
- In case a Member State chooses to configure their exchange server in such a way that when an unencrypted and/or unsigned message is received, a warning message is sent instead of a Proof of Delivery, informing the sender of the fact that the message was not signed and/or encrypted and therefore deleted
  OR
- In case a Member States deletes unsigned and/or unencrypted messages manually at the national access point, the receiving Member State will notify the sender of the fact that an unsigned and/or unencrypted message was received.

Further reading

Chapter 4 of this document contains further recommendations on the security of DubliNet.

Article 15(2) Implementing regulation

Sending a message

- Any message sent to another Member State is deemed authentic by another Member State. Therefore, before sending any message, case officers are recommended to check whether all conditions for a valid message, and, if applicable, a request contained therein, are met. This includes the inclusion of the correct attachments and/or standard signed forms. Case officers might benefit from using the workflow in this document as a checklist.

1.5 Proof of Delivery

Articles 22(2), 25(1) and 35(4) Dublin III regulation
Articles 15(3), 19(3) and 21(3) Implementing regulation

Obtaining a Proof of Delivery

- The National Access Points of the Member States are responsible for issuing an acknowledgement that a message has been received. This acknowledgement is called the 'Proof of Delivery' (PoD) and functions as the starting point for calculating the time limits set by the Dublin III regulation.
- Member States are strongly recommended to use the standard text as put forward by the EID for the PoD.
- Case officers are advised to follow the recommended course for escalation in case no PoD is received following the sending of a message. Case officers are invited to refer to Chapter 3 of this document.
- In case no PoD is received and the addressed National Access Point experienced an interruption in its operation, Member States shall use the transmission log at the level of the central communication infrastructure as an alternative PoD.

Additional remark

As a last resort, Member States can ask eu-LISA to check the mail relay log of TESTA-ng for the delivery of a message. It should be noted that this is an exceptional back-up procedure which comprises of a manual check of the logs at hand. Therefore, sufficient technical details should be given when a request is filed, such as the address of the sender and recipient and the date range and time of when the message was sent and, preferably, the email subject.

- Case officers need to properly record the PoD received following the transmission of a message for the file.

Further reading

Chapter 2 of this document contains further recommendations on the Proof of Delivery.

1.6 Sending a reply

Handling incoming messages

- Case officers who need to reply to incoming messages, are advised the follow the aforementioned workflow for sending a reply.
- Member States are recommended to consistently monitor their National Access Point during working hours in order to ensure that incoming messages can be distributed to case officers for appropriate follow-up.

Good practice

In order to avoid a collective action problem, such as when a group of officers is responsible for a common shared task, resulting in the task not being done properly because responsibility is shared by too many people, Member States choose to task a single officer or a single team or unit to monitor the National Access Point and to process incoming messages. In some Member States, these tasks are fulfilled on a rotational basis.

In some Member States, these officers or teams take care of monitoring the whole procedure for following up on urgent messages, ensuring that case officers deal with the message in time and well within the given time limits.

Chapter 2. Proof of Delivery

As described in the previous chapter, National Access Points of the Member States are responsible for issuing an acknowledgement that a message has been received. In practice, these acknowledgements are known as a 'Proof of Delivery' which, in many Member States, will subsequently form an integral part of the case file of an applicant as the PoD proves the reception of a message concerning that applicant. Since certain time limits of the Dublin III regulation start running from the moment a message is received (see e.g. Article 25(1) Dublin III regulation), the PoD is an important piece of evidence as it proves the receipt of the message and thus the start of such time limits. In this chapter, recommendations on the PoD will be given in further detail.

2.1 Content of Proof of Delivery

Link to message

- It is important that the PoD is somehow linked to the original message the PoD pertains to. As per the EID, Member States should not alter the original subject line in order to allow the sending Member State to link the PoD to the original message.
- Member States can add an additional 'RE:' to precede the subject line to set the message clearly apart, or add 'Proof of Delivery' to the subject line.

Standard text

- Member States are strongly recommended to use the standard text as defined in Annex IV of the EID in order to clearly and uniformly state the use and content of the PoD.
- Member States should, when using this predefined text, fill the blank fields with their own contact details in order for them to be contacted in case of need.
- Member States are recommended to use general contact details at unit level for these fields to ensure that messages can be attended to at any given time.
- A PoD-message should be provided at least in English, for readability's sake, as the PoD will form part of the applicant's case file.

2.2 Organisation of Proof of Delivery

Automatic Proof of Delivery

- It is recommended that all Member States use automatic PoDs in order to ensure that a PoD is sent out in time, preventing unnecessary delays in the sending Member State.

Additional remark

The term 'automatic PoD' relates to the transmission of automated delivery receipts. Member States can choose to configure their network in such a way that upon receipt of a message, a delivery receipt is automatically issued without human intervention.

Good practice

As the sending of manual PoDs can lead to delays as it requires human intervention, which is usually only available during working hours, Member States prefer to adopt the automated issuing of delivery receipts.

- In the setup of automatic PoDs, Member States are strongly encouraged to prevent the sending of a PoD in reply to a PoD.

Additional remark

A known issue in the DubliNet practice is the sending of 'Double' PoDs. This happens when one Member State sends a message, the receiving Member State replies with a PoD and the first Member State, in its turn, replies to that PoD with another PoD. Issues like these should be possible to address depending on the technical setups in each Member State.

Manual Proof of Delivery

- Member States should send a PoD upon receipt of a message, preferably immediately, in order to prevent unnecessary delays, even in weekends and on holidays. Member States are therefore strongly recommended to abandon the practice of sending PoDs manually.
- Member States who continue to send manual PoDs are recommended to draft a workflow that permits the sending of a PoD on the same day as the original message was received, even in weekends and on holidays, and without substantial delays, as this would impede the Dublin practice in another Member States. Member States are advised to take note of the rule, per EID, that in case of a dispute, the time where a mail is received by the TESTA Central Services can be used as proof of delivery.

Additional remark

Some Member States have not (yet) automated the sending of PoDs following the receipt of a message. In those Member States, case officers send PoDs by manually drafting such acknowledgements of receipt for each incoming message.

Collection of Proof of Delivery

- Member States are recommended to enter any PoD received for a message concerning an individual applicant, in the applicant's (digital) case file for future reference.
- Member States that chose to collect PoDs in the (digital)case file of an applicant are advised to regularly train the case officers involved with exchanging messages over DubliNet of the importance of collecting a PoD for the case file as evidence.

Good practice

Member States have set up a way to automatically convert incoming PoDs into a file with a .pdf extension and to automatically upload it in the respective digital case file of the applicant in question, using the subject line of the PoD. As a result, case officers do not have to manually register a PoD into the case management system.

Good practice

The system is set up in such a way that it monitors whether a PoD is received. A notification is sent to the responsible case officers in case no PoD is recognised for the message sent, calling the case officer to action.

2.3 Interruption of service

Workflow in case Proof of Delivery is not sent or received

- Member States ensure that, as soon it becomes apparent that PoDs are not being received or sent properly, an adequate escalation procedure is followed to address the issue, such as in Chapter 3.
- Case officers are advised to actively and closely monitor the receipt of a PoD for each individual message sent over DubliNet, and to respond adequately in case no PoD is received.

Chapter 3. Business continuity

To expedite secure, fast and reliable communication regarding the Dublin III regulation, it is important that DubliNet in all Member States operates on a 24/7 basis. The Member States are required to operate their National Access Points without interruption (see Article 21(1) Implementing regulation). There are situations in which it is possible that DubliNet will not be operational in a Member State for a short or longer period of time. In case of an interruption, the other Member States need to be informed (see Article 21(2) Implementing regulation). This chapter describes how to act when a Member State has, or seems to have, an issue with DubliNet, what steps can be taken, how to appropriately escalate in case of an issue and how to notify other Member States in case of an interruption of service.

3.1 Dealing with downtime

Article 21 Implementing regulation

Planned downtime

- Member States keep planned downtime to a minimum. Scheduled maintenance should be combined with other necessary updates impairing the operation of DubliNet in order to minimise the impact on the Dublin procedure.

Additional remark

Planned downtime is a scheduled maintenance in a Member State with an expected loss of function of the National Access Point of DubliNet in that Member State, impacting the continued operation of the system. This is the case when a Member State, for example, performs technical maintenance, or updates software involved with the operation of DubliNet.

- Member States are recommended to schedule planned downtime for after working hours or on weekends to further ease any potential impact on the Dublin procedure.
- In case of any planned downtime, Member States should inform the other Member States impacted by this planned loss of service, preferably seven weekdays in advance, via the DubliNet Admin email, see 'communicating on downtime' below.
- In the case of planned downtime, Member States are encouraged to inform eu-LISA of any expected interruption of service.
- In instances of large-scale maintenance operations, Member States are recommended to plan ahead by drafting a downtime-plan with designated roles, escalation procedures and contingency plans.

Article 21(2) Implementing regulation

Unplanned downtime

- In case of unplanned downtime lasting more than seven working hours, the impacted Member State should inform the other Member States about its loss of service through the DubliNet admin email.

Additional remark

Unplanned downtime occurs when the National Access Point is down for reasons outside regular scheduled maintenance. Unplanned downtime could for example occur during a power blackout or loss of connection with a server, but also in instances in which software impairs the operation of the National Access Point, such as during a possible coordinated hostile attack.

- Member States are encouraged to also inform other Member States of unplanned downtime which will potentially impair the functioning of the National Access Point for less than seven hours, in order to notify Member States that PoDs might be delayed and any replies or other messages might be delivered in a delayed manner.

- Member States are recommended to develop an internal workflow, together with the responsible IT department and other users of DubliNet, to help ease addressing technical issues impairing the operation of the National Access Point, smoothen communications and encourage information sharing and cooperation in general by all units impacted by the downtime.
- In instances of unplanned downtime, the impacted Member State should also inform eu-LISA about the loss of service in order to allow eu-LISA, at their discretion, to offer assistance, monitor the status of the service unavailability and to inform other Member States through its own means of communication, such as the DubliNet Single Points of Contact (SPOCs) in each Member State.

Article 21(2) Implementing regulation

Communicating on downtime

- For communication about planned or unplanned downtime of DubliNet, the DubliNet admin email should be used since DubliNet can only be used for exchanging case-related messages.

Additional remark

Every Member State operates a separate and dedicated admin email address for communications on technical and other organisational matters that are not related to individual cases.

- Member States are recommended to grant (some) employees of the Dublin Unit in the Member State access to the DubliNet Admin email as some messages received can relate to the Dublin procedure.
- In case of any downtime, Member States should ensure that both the Dublin Unit and their national IT department are involved in the addressing of the planned or unplanned downtime to ensure that information about the disruption of service is correct and up-to-date.
- In the event of a full disruption of service of DubliNet and the DubliNet Admin email, direct communication to all Dublin Units is recommended. Member States are advised to contact the other Member States with the help of eu-LISA, but also through direct email, fax or telephone and by using the designated distribution lists operated by EASO. Such communication on a full disruption of all service should only pertain to the unplanned downtime, these alternative means for communication may not be used to exchange Dublin requests.
- For events of full disruption of service, Member States are advised to keep hard copies of aforementioned contact details used to inform the other Member States and eu-LISA.
- In case of any downtime, Member States should inform the other Member States with a message which at least includes information regarding:
    - the fact there is a (planned) downtime;
    - in case of planned downtime, time and date of the start and foreseen end of the downtime;
    - in case of unplanned downtime, the time and date of when the downtime was noticed and, where applicable, the time and date by which the Member State expects to resolve the issue;
    - which services are unavailable during the downtime;
    - if messages, which are sent from other Member States during the downtime, have to be sent again or whether messages were received and only the sending of PoDs is affected;
    - and whether PoDs will continue to be sent automatically.

Additional remark

Regarding the need to resend messages, it should be noted this is not always necessary. At central level, a central mail relay tries to deliver a message for several times. In case the delivery ultimately fails, a technical message notifies the sender of the non-delivery and the message needs to be sent again. Generally, short interruptions should only result in slight delays in the delivery of messages. Longer delays will result in the need to resend a message.

- Member States are encouraged to inform other Member States of the end of the downtime.

Good practice

At the end of (considerable) downtime, Member States send to each individual Member State a message announcing the end of the downtime, including the subject line of the message that was last received.

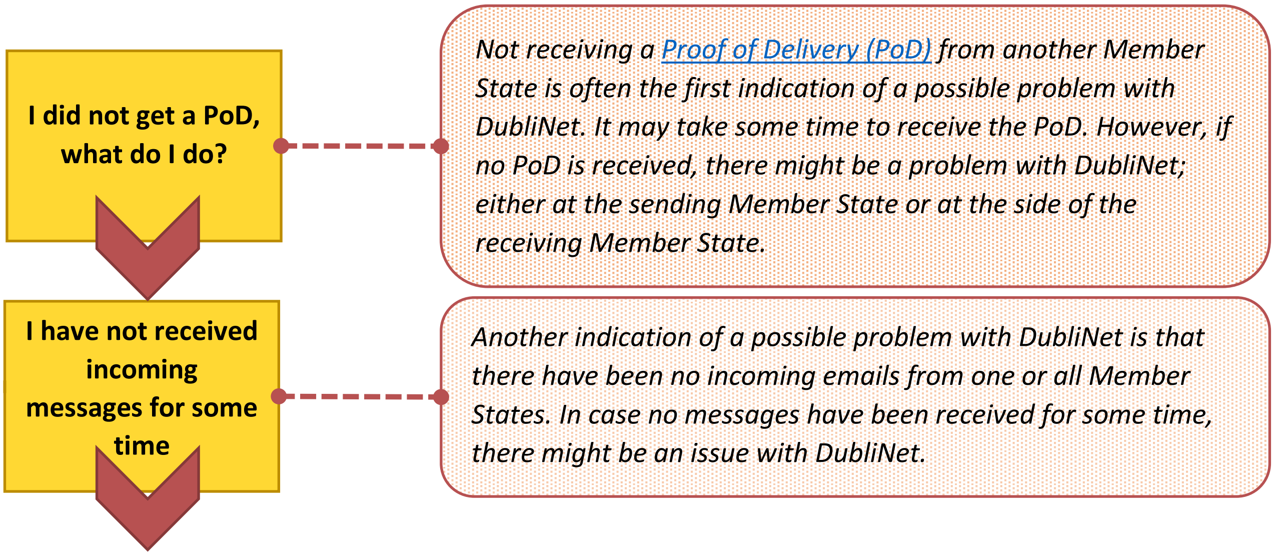
- In case unplanned downtime persists, Member States are encouraged to share a daily update to all Member States for as long as the problem is not resolved.
- In case of (an extended period of) downtime, Member States are advised to cooperate with eu-LISA on resolving the issue by providing information about the nature of the issue and by proactively communicating on the status of works to address the issue at hand.

Good practice

Member States have a manual at the ready to address instances of (unplanned) downtime which includes a template for informing Member States and eu-LISA. Member States regularly practice their crisis response in case of (unscheduled) downtime, together with all units and colleagues involved, in order to spot weak spots in their emergency procedures which will help ease addressing instances of downtime in the future.

3.2 Assessing and addressing issues in the operation of DubliNet

The below decision model should aid in determining the adequate course of action in case an issue occurs in the daily operation of DubliNet.



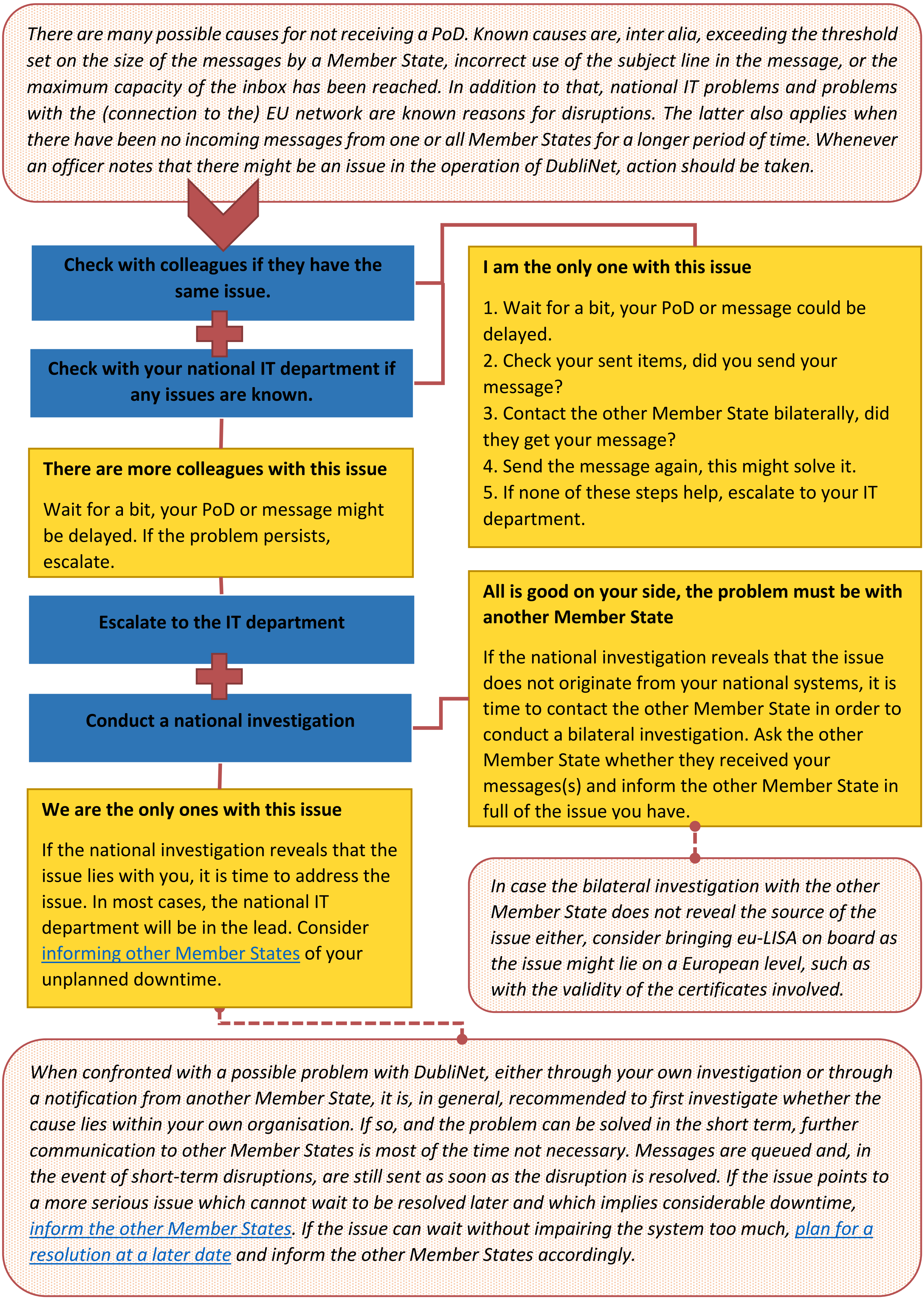
I did not get a PoD, what do I do?

Not receiving a Proof of Delivery (PoD) from another Member State is often the first indication of a possible problem with DubliNet. It may take some time to receive the PoD. However, if no PoD is received, there might be a problem with DubliNet; either at the sending Member State or at the side of the receiving Member State.

I have not received incoming messages for some time

Another indication of a possible problem with DubliNet is that there have been no incoming emails from one or all Member States. In case no messages have been received for some time, there might be an issue with DubliNet.

Model continues on following page.



There are many possible causes for not receiving a PoD. Known causes are, inter alia, exceeding the threshold set on the size of the messages by a Member State, incorrect use of the subject line in the message, or the maximum capacity of the inbox has been reached. In addition to that, national IT problems and problems with the (connection to the) EU network are known reasons for disruptions. The latter also applies when there have been no incoming messages from one or all Member States for a longer period of time. Whenever an officer notes that there might be an issue in the operation of DubliNet, action should be taken.

Check with colleagues if they have the same issue.

Check with your national IT department if any issues are known.

I am the only one with this issue

1. Wait for a bit, your PoD or message could be delayed.
2. Check your sent items, did you send your message?
3. Contact the other Member State bilaterally, did they get your message?
4. Send the message again, this might solve it.
5. If none of these steps help, escalate to your IT department.

There are more colleagues with this issue

Wait for a bit, your PoD or message might be delayed. If the problem persists, escalate.

Escalate to the IT department

Conduct a national investigation

All is good on your side, the problem must be with another Member State

If the national investigation reveals that the issue does not originate from your national systems, it is time to contact the other Member State in order to conduct a bilateral investigation. Ask the other Member State whether they received your messages(s) and inform the other Member State in full of the issue you have.

In case the bilateral investigation with the other Member State does not reveal the source of the issue either, consider bringing eu-LISA on board as the issue might lie on a European level, such as with the validity of the certificates involved.

We are the only ones with this issue

If the national investigation reveals that the issue lies with you, it is time to address the issue. In most cases, the national IT department will be in the lead. Consider informing other Member States of your unplanned downtime.

When confronted with a possible problem with DubliNet, either through your own investigation or through a notification from another Member State, it is, in general, recommended to first investigate whether the cause lies within your own organisation. If so, and the problem can be solved in the short term, further communication to other Member States is most of the time not necessary. Messages are queued and, in the event of short-term disruptions, are still sent as soon as the disruption is resolved. If the issue points to a more serious issue which cannot wait to be resolved later and which implies considerable downtime, inform the other Member States. If the issue can wait without impairing the system too much, plan for a resolution at a later date and inform the other Member States accordingly.

Chapter 4. Security rules

Because the information exchanged over DubliNet pertains to individual applicants, the use of the system does not only need to be limited for use by the relevant officers of the Member States, the system also needs to be securely operated by the Member State experts. In order to establish a high level of security of the data exchanged, all Member States need to abide by the unanimously agreed rules governing the system.

4.1 Security of procedure

Article 35(1) Dublin III regulation

Ensuring security on a daily basis

- Member States restrict the access to and operation of DubliNet to competent authorities only.
- Member States are advised to introduce an authorisation scheme to manage the access and operation of DubliNet by officers.
- Member States ensure, by way of adopting standard operating procedures and practical policies, that Dublin case officers and experts operating DubliNet follow the right steps of the procedure to ensure compliance with measures aimed at guaranteeing the security and confidentiality of DubliNet.
- Member States provide proper training and support to officers working with DubliNet on a daily basis, including training on the importance of compliance with security and confidentiality rules, and procedural safeguards such as how to act in case of irregularities in the operation of DubliNet.
- Member States are encouraged to hold regular ‘awareness’ sessions aimed at making case officers work with DubliNet in a compliant manner.
- Member States are advised to draft a procedural manual and small printouts and/or handouts, such as brief checklists, for use by case officers on a daily basis.

Good practice

Member States regularly remind case officers about the importance to follow procedures established to securely operate DubliNet, such as when and how to escalate issues in the daily operation, for example when no PoD is received. Instead of case officers trying to find a workaround or alternative means of communication for those instances, following proper escalation procedures ensures that personal data is kept safe, despite potential errors in the continued operation of DubliNet.

4.2 Data security

Article 15(1) Implementing regulation

Confidentiality and data protection

- Member States ensure that DubliNet can only be accessed and operated by Dublin case officers and staff members authorised for working with DubliNet.
- No personal information nor personal data should leave the network, such as by means of alternative communication.
- Any requests for information regarding (the case file of) a third-country national or stateless person should be dealt with in compliance with national rules and regulations governing such requests. These requests should be processed separately from DubliNet.
- Member States should not set up any gateway between the Dublin exchange infrastructure and external networks;
- Member States can ensure this, for example, by providing proper instructions and regular reminders, that case officers should not mix up DubliNet and their personal emails.

Additional remark

In some Member States, the local DubliNet client has the distinct appearance of a regular 'Outlook' inbox, which makes it hard to distinguish from a personal Outlook environment. In some instances, the two are integrated in one and the same program. It might therefore occur that case officers send their requests from their personal accounts and not via DubliNet, thus they are not secured or encrypted. This mainly happens in cases in which DubliNet is down, such as in instances of maintenance or because some Member States' mail connectivity is not only used for DubliNet purposes but also shared for Eurodac purposes and National Policy purposes, etc.

Article 34(8)-(12) Dublin III regulation

Data retention

- Member States will delete any information contained in their National Access Point if required to do so per the Dublin III regulation, such as when wrong or excessive information has been exchanged over DubliNet.
- Member States are encouraged to develop guidelines, in compliance with (inter)national data retention guidelines and regulations, on the retention of data within the DubliNet network, and any back-ups and archives.

Good practice

Member States retain data in the 'inbox' of their National Access Point for three months maximum. In the meantime, any incoming messages should have been processed by a dedicated colleague or unit and acted upon. In order to minimise unrestricted access to all data exchanged through DubliNet, officers are only granted access to their own 'inbox' within the National Access Point which only contains messages that fall within their own responsibility.

4.3 Security violations

What to do in cases of security violations

- Member States are advised to draft a standard operating practice to address cases of a breach of security.
- It is recommended that Member States immediately follow up and address any breach of security, including escalating to eu-LISA for technical support, follow-up and advice when required.
- Member States should also aspire to inform other Member States of a security breach as soon as possible, stating the nature of the breach, the impact, the consequences and, if applicable, a description of impacted messages that should be deleted by the receiving Member States or resent by the sending Member States.
- After a breach of security, Member States are recommended to work with eu-LISA to evaluate the incident and to follow-up on any recommendations made on their behalf to prevent a new incident from happening.

4.4 Certificate renewal

Renewing certificates at the level of Dublin units

- Member States collaborate proactively with eu-LISA during campaigns for certificate renewal. Member States respect the provided schedule and planning for the necessary actions.

Additional remark

The renewal of certificates is done every two years. The renewal process is initiated and coordinated by eu-LISA. Member States are properly informed about the process prior to the start of the renewal procedure.

- To allow for further easy cooperation, Member States ensure the appointment of a responsible and available contact person for communication with eu-LISA.
- When a new certificate is installed, the Member State disseminates a central message to all Member States reporting the (successful) installation of the new certificate. This message is usually sent by the national Dublin Unit.
- Dublin case officers that might be involved with the process of certificate renewal, are informed by the respective national authority about their roles and responsibilities.

Further reading

For the certificate renewal process, eu-LISA drafted an detailed guide on the process. This ***eu-LISA guide on certificate renewal*** can be obtained through the national DubliNet Single Point of Contact.

Chapter 5. System setups and workflows

Each Member State has set up their DubliNet National Access Point in their own way to meet requirements and demands from their national Dublin practice. This chapter lists some general recommendations regarding specific ways DubliNet is set up in the Member States.

Member States also work with DubliNet in various ways in their daily practice. This chapter therefore also lists various workflows that Member States prefer to use for working with DubliNet. These 'practical examples' of workflows function to display advantages and benefits of national system setups, and to provide valuable insights in ways other Member States work with DubliNet.

5.1 DubliNet clients used by Member States

In case Member States use an email client to host DubliNet: text formats

- Member States refrain from using HTML and/or Rich Text Format for sending messages as these might not be possible to read in some receiving Member States.
- Member States are advised to use a plain text format for sending messages.

Rules and filters

- When Member States create automatic rules and set up filters, it should be taken into account that those should comply with the specifications outlined in the applicable acquis. Rules related to DubliNet mailbox settings should not affect communication with other Member States.

Additional remark

The following filters and rules are most commonly used by the Member States:

- Automatic rule for sending out PoD
- Access to DubliNet inbox is only allowed when a message is received from the TESTA-ng domain
- Automatic rules for forwarding incoming messages to individual inboxes according to the subject for easier distribution of messages

5.2 Setting up remote access to DubliNet

Considerations for working with DubliNet out of the workplace

- When allowing case officers to access DubliNet remotely, such as through teleworking capacities, Member States should provide case officers with an adequately secure connection.
- Dublin case officers should take the physical security of their remote workplace into account. Case officers should prevent unauthorised access or views into their DubliNet client.

Additional remark

Remote access to DubliNet can be relevant for teleworking purposes. Telework staff require remote access to the internal IT infrastructure of their organisation. Organisations must make sure that their internal network remains safe and that remote access does not become a weak point in their IT security.

When setting up remote access, it is crucial to have a stable and safe internet connection, at least with WPA/WPA2-encryption, and the installation of a VPN (Virtual Private Network) or similar tunnelling protocols is recommended.

Ideally, individual business IT devices or a pool of devices are provided by the organisations for telework purposes. This ensures remote access to DubliNet via the national network.

5.3 Testing

Piloting new ways of working with DubliNet

- Member States refrain from using their National Access Points for testing new ways of working with DubliNet.
- When testing any new ways of working with DubliNet, such as a new DubliNet client, Member States refrain from using live data as to not impair the integrity of the network.

Additional remark

Currently, rules and regulations governing DubliNet do not allow the testing of a new working environment, client or workflow on the TESTA-ng network, thus through the live National Access Points. Simultaneously, no testing environment is available to pilot improvements, inventions and updates. Member States should therefore find alternative means to check whether any changes to their National Access Point of DubliNet client work.