How to join ECHA's eDelivery network

October 2020

Disclaimer

This document aims to assist users in complying with their obligations under the CLP Regulation. However, users are reminded that the text of the CLP Regulation is the only authentic legal reference and that the information in this document does not constitute legal advice. Usage of the information remains under the sole responsibility of the user. The European Chemicals Agency does not accept any liability with regard to the use that may be made of the information contained in this document.

Version	Changes	
1.0	Initial publication	July 2019
1.1	Removed security requirements for eDelivery users	February 2020
1.2	Added information in the Test and Connection with ECHA phase	March 2020
1.3	Adaptations for SLA process	October 2020

How to join ECHA's eDelivery network

Reference: ECHA-2019-R-14-EN ISBN: 978-92-9020-698-9 Cat. Number: ED-04-19-513-EN-N DOI: 10.2823/906878

Reference: ECHA-2019-R-14-EN
ISBN: 978-92-9020-698-9
Cat. Number: ED-04-19-513-EN-N
DOI: 10.2823/906878
Publ.date: October 2020
Language: EN

If you have questions or comments in relation to this document please send them (quote the reference and issue date) using the information request form. The information request form can be accessed via the Contact ECHA page at:
http://echa.europa.eu/contact

European Chemicals Agency

Mailing address: P.O. Box 400, FI-00121 Helsinki, Finland
Visiting address: Telakkakatu 6, Helsinki, Finland

Table of Contents

Table of Figures

1. Introduction

1.1. Background

Under the Regulation (EC) No 1272/2008 on the classification, labelling and packaging of substances and mixtures (CLP Regulation), Article 45 and Annex VIII, companies placing hazardous mixtures on the European market have an obligation to provide information about these mixtures to the relevant national appointed bodies.

Appointed bodies, thus, need to accept dossiers in the PCN format and can use ECHA PCN systems to accept them if they wish to. Appointed bodies in each member state make this information available to poison centres so that they can provide rapid medical advice in the event of an emergency.

eDelivery is the automated solution provided by ECHA that appointed bodies can use to receive the PCN dossiers submitted to ECHA by industry. eDelivery is an AS4 specification of the ebMS protocol adopted by the European Commission to facilitate the secure communication amongst EC, European Institutions and Member States. EU DIGIT has released a sample implementation of the AS4 specification, Domibus, for which they offer support to member states and European institutions.

This service is provided by ECHA together with DIGIT under their Connecting Europe Facility (CEF).

1.2. Purpose

This document details the steps that appointed bodies need to take in order to start receiving poison centre notifications from ECHA using eDelivery.

1.3. References

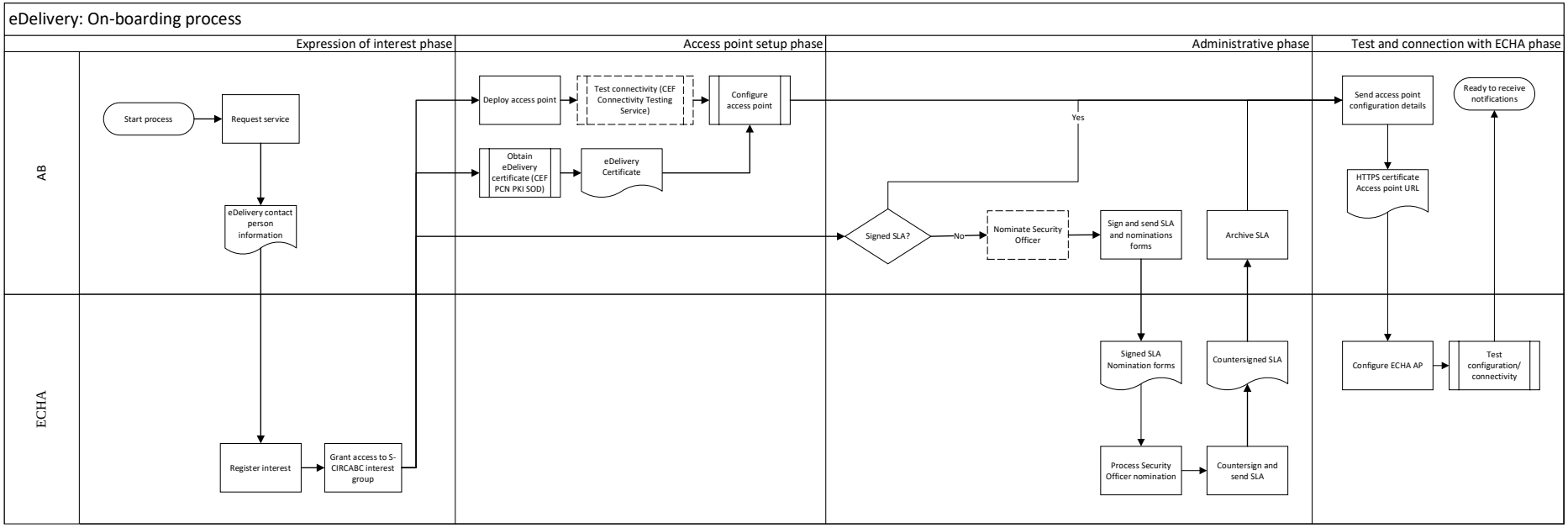
Title	Description
[REF1] CEF eDelivery use for PCN system: Solution Description Document	This document describes the technical implementation of eDelivery in the context of ECHA and PCN. It also gives recommendations for the implementation of eDelivery for appointed bodies.
[REF2] PKI for PCN: Public Key Infrastructure Service Offering Description	This document describes how appointed bodies can obtain a certificate from CEF that needs to be used for accessing ECHA's eDelivery network.
[REF3] CEF eDelivery Training and Deployment Service Offering Description	This document describes CEF's service for training and deployment of eDelivery.

Title	Description
[REF4] Access Point P-Mode Configuration ECHA	This document describes the configuration used to set up access point that are compatible with ECHA's eDelivery implementation.
[REF5] Connectivity Testing Service Offering Description	This document describes CEF's service to test the successful deployment of an eDelivery access point at the appointed body's side.
[REF6] Overview of eDelivery and PCN	This presentation gives an overview of eDelivery and how it is used in the context of PCN.
[REF7] Management Board Decision 59/2019 with Annexes	The MB Decision 59/2019 approved the specific security requirements in the context of PCN. Its annexes include 1) Declaration of Commitment by a Member State Competent Authority/Mandated National Institution/Designated National Authority of a Member State with respect to Security Aspects for ECHA's Information Systems 2) Standard security requirements for access to ECHA's Information Systems by Appointed Bodies ("AB") and the Poison Centres ("PC") identified by the Appointed Bodies
[REF8] Service Level Agreement (SLA)	The SLA defines the conditions under which ECHA provides services to the Appointed Body in the context of the CLP Art. 45 Annex VIII.

1.4. Glossary

Term	Definition
Access Point	Access points are eDelivery nodes that connect to ECHA's eDelivery network. ECHA access point is an installation of Domibus, the sample eDelivery implementation provided by DIGIT.
ECHA's eDelivery network	The network is composed of access points and it is accessed exclusively by ECHA's and its regulatory partners. Under the PCN project, it is used to forward PC notifications to appointed bodies.
Digital Certificate	The digital certificate is a set of files that serve to securely identify an access point to the other access points in the network. This certificate is obtained through CEF's PKI service as documented in 'PKI for PCN: Public Key Infrastructure Service Offering Description'. This certificate should not be confused with the one required for securing the communication at the HTTPS level, which should be handled and obtained independently by the networking team of the appointed body.
User administrator	User Administrator is in charge of access management (granting and revoking access rights) for authorised users to ECHA's Information systems. eDelivery does not require any extra users, but new users could potentially access other relevant systems, like the Interact Portal, where the Searchable Database of PC notification will be hosted.
Security officer	Security Officer is responsible for organisation's compliance with the specific Security Requirements for access to ECHA's Information Systems by appointed body. In addition, the officer is responsible for security awareness trainings and briefings for end-users before granting access to ECHA's Information Systems. He/she provides local security support for organisation's end-users and acts as a security contact point for ECHA.
Trust-store	File that contains the public digital certificate corresponding to ECHA's access point.

Figure 1 Diagram of the on-boarding process with the different phases



1.5. Roles and responsibilities

1.5.1. Appointed Body

Role: Organisation that is setting up eDelivery Access Point
Responsibilities:

- Sign the Service Level Agreement if not done already
- Ensure that the access point installation is secure
- Nominate personnel to represent appointed body at ECHA
- Obtain and install a security certificate from CEF PKI Service (T-System) to identify an access point in a secure way
- Independently obtain and install a SSL certificate to secure the HTTPS communication between the access points

1.5.2. ECHA

Role: Organisation to which the eDelivery Access Point connects to
Responsibilities:

- On-board appointed bodies
- Configure ECHA's Access Point

1.5.3. CEF Support

Role: Organisation that supports eDelivery standard and its correct implementation
Responsibilities:

- Support the installation of Domibus (eDelivery Sample Implementation) in Appointed Body's environment
- Provide digital certificate to Appointed Body

2. On-boarding process

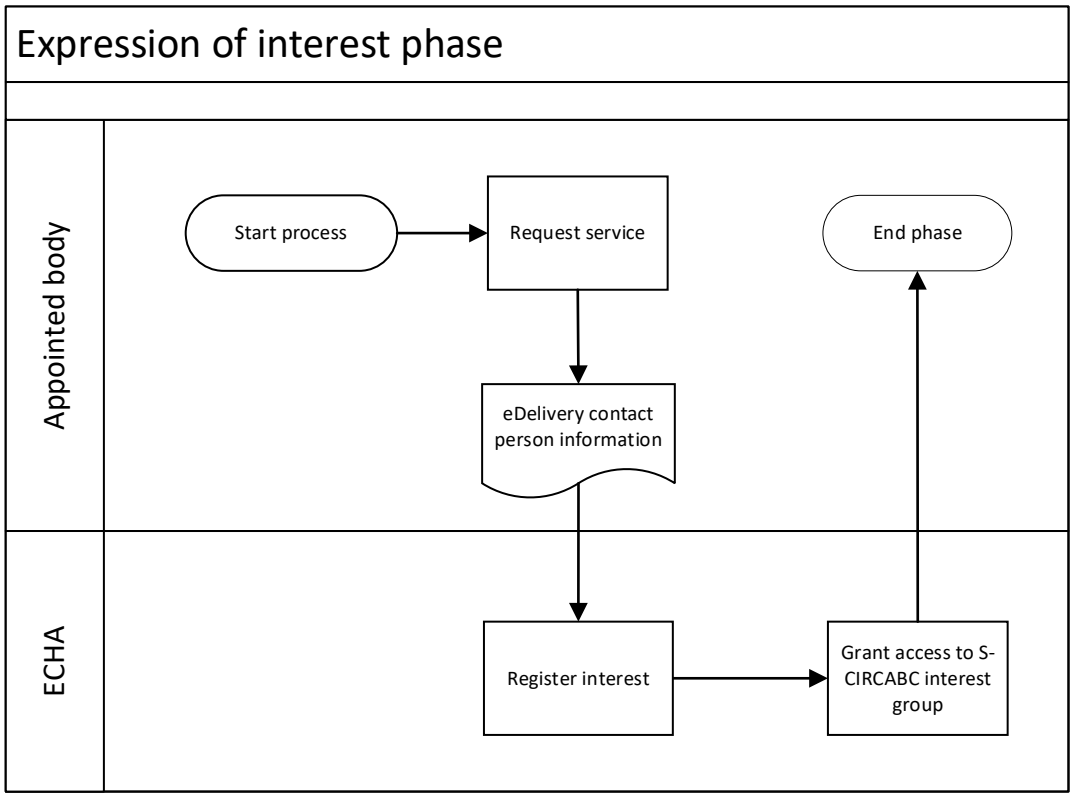
The on-boarding process starts by the appointed body expressing their interest in implementing eDelivery and requesting the latest version of the documentation package from ECHA via the Contact Form for Authorities.

The on-boarding process consists of 4 phases that are explained in the following sections.

Once appointed bodies have finished the expression of interest phase they can start in parallel the technical phase and administrative and security phase necessary to connect with ECHA's eDelivery access point.

2.1. Expression of interest phase

Figure 2 Diagram of Expression of interest phase



Purpose: Start the on-boarding of the appointed body into the ECHA's eDelivery network

Actors:

1. Appointed body
2. ECHA

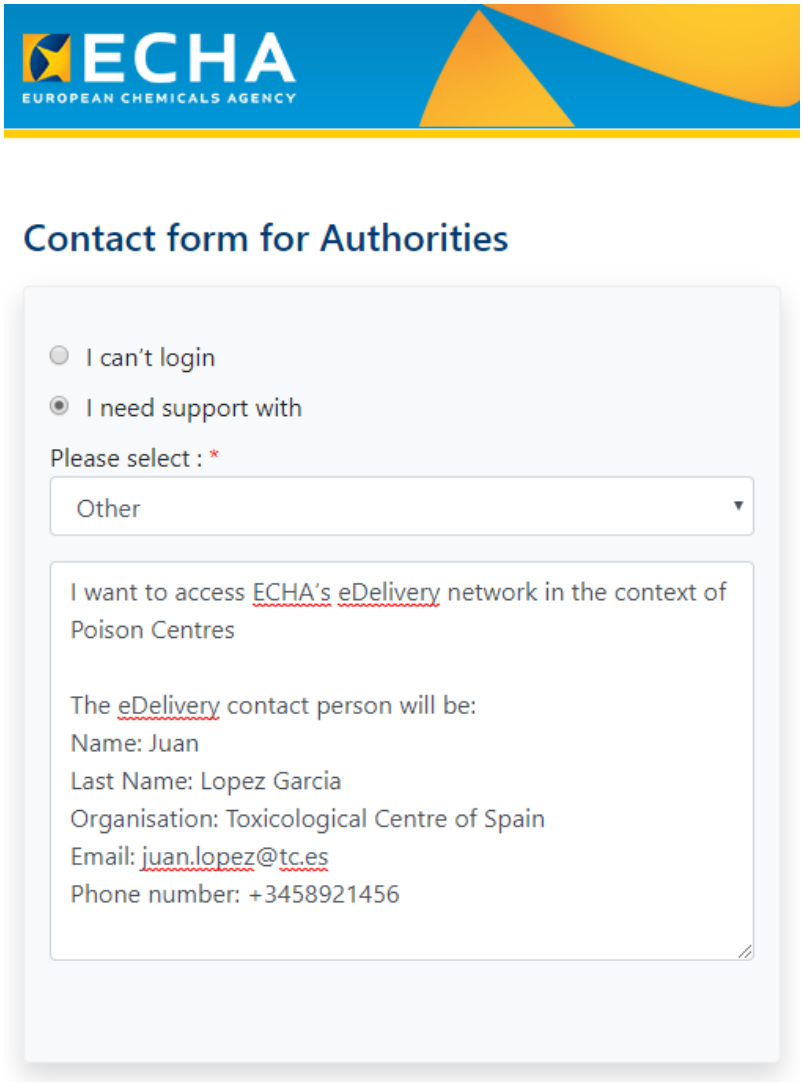
Process:

1. Request service
2. Register interest
3. Grant access to S-CIRCABC interest group for eDelivery contact points

2.1.1. Request service

Appointed bodies interested in connecting to ECHA's access point should start by requesting to be on-boarded to the service. To do that they should go to Contact Form for Authorities and complete the form as shown in the Figure 3 and explained below.

Figure 3 Authorities Contact Form with fields filled in for requesting to be on-boarded to eDelivery



1) 'I need support with'

2) Please select 'Other'

3) In the open comments field please state 'I want to access ECHA's eDelivery network in the context of Poison Centres'

4) In the open comments field please add the personal details for the eDelivery contact person. This person is responsible for the communication flow between ECHA and the appointed body:

    The eDelivery contact person will be:

    Name:

Last Name:

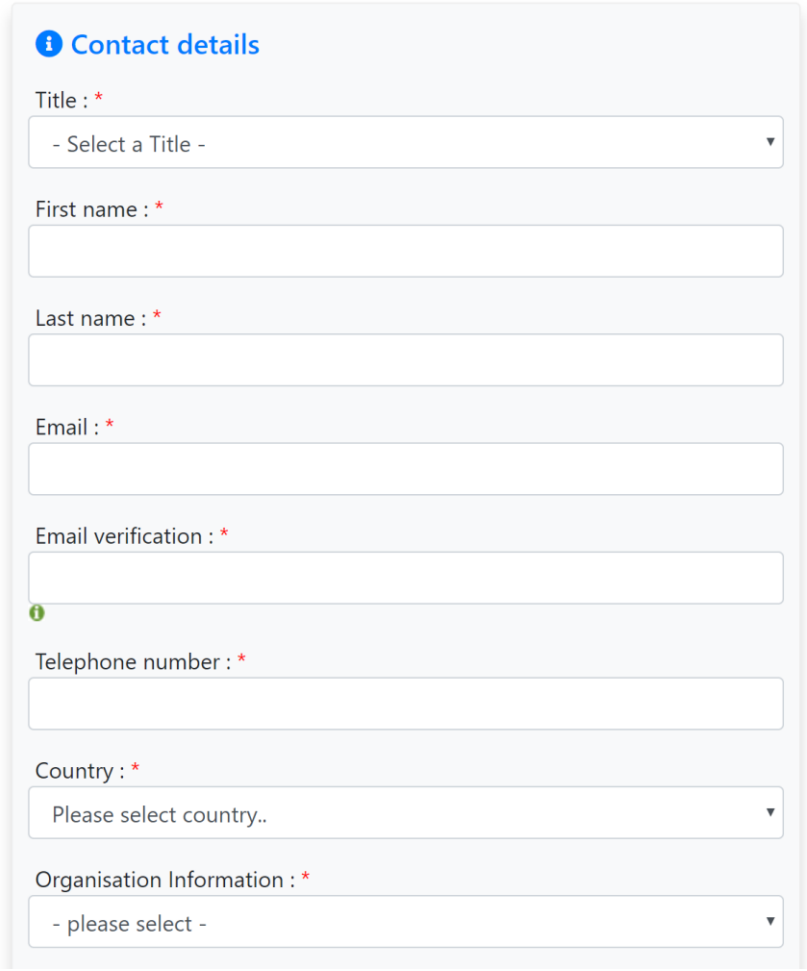
Organisation:

Email:

Phone number:

5) Fill in the contact details as shown in Figure 4. This contact details need to correspond to the appointed body's legal representative or the appointed body's contact person, body mentioned in the consolidated Commission list for appointed bodies.

Figure 4 Fields in the contact form to complete the contact details



2.1.2. Register interest

ECHA will register the interest and set up the communication channels with the appointed body.

2.1.3. Grant access to S-CIRCABC interest group

ECHA has set up an *interest group* in S-CIRCABC, a secure online platform provided by the commission. The interest group holds all the relevant documentation for connecting to ECHA's access point in its *library.* The interest group can also be used to host discussion amongst appointed bodies on topic specific to the eDelivery implementation.

ECHA will grant access to the interest group to the eDelivery contact person(s) nominated in the previous step.

The library of the interest group holds, among others, the following documents and files:

1) A PCN eDelivery Solution Description Document (SDD) detailing the implementation of the eDelivery in the PCN context;

2) A PMODE document describing the configuration parameters for ECHA's PCN eDelivery implementation;

3) A sample PMODE configuration file that can be used in Domibus with little changes

4) A eDelivery Training and Deployment Service Offering Document that details how to request and obtain support from CEF to install and use Domibus;

5) An eDelivery Connectivity Testing Service Offering Document (SOD) that describes the service provided by CEF to test the basic implementation of an eDelivery Access Point;

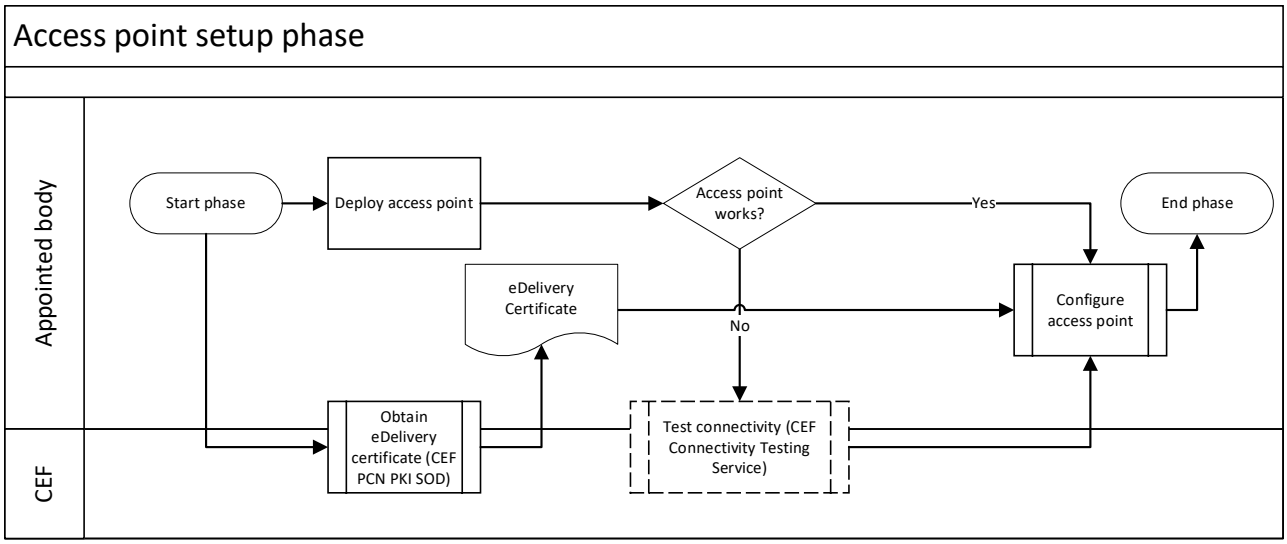
6) An eDelivery Private Key Infrastructure (PKI) for PCN Service Offering Document (SOD) that describes the service provided by CEF to obtain certificates to be used in the PCN eDelivery domain;

7) ECHA’s eDelivery public key file;

8) Couple of sample messages, as delivered by ECHA’s access point, which include sample dossiers.

2.2. Access point setup phase

Figure 5 Diagram of Access point setup phase



Purpose: The appointed body prepares an eDelivery access point to be able to connect to ECHA's eDelivery network.

Actors:

3. Appointed body
4. ECHA
5. CEF

Process:

1. Deploy access point
2. Obtain eDelivery certificate for PCN (can be done in parallel with step 1)
3. Test connectivity
4. Configure access point to process PCN messages

2.2.1. Deploy access point

The appointed body will install and configure an access point that complies with the eDelivery specification.

Appointed body can select an eDelivery solution provider to prepare their access point. It is recommended that they install Domibus in their own data centres.

Domibus installation and basic configuration are described in Documentation section of the Domibus webpage. Installation should be prepared and aligned to the requirements described in the PCN eDelivery Solution Description Document.

Appointed bodies can request training and deployment services from CEF to assist them in installing and configuring Domibus. More information can be found in its Service Offering Document.

2.2.2. Obtain eDelivery certificate for PCN

Communication with appointed bodies through eDelivery are secured via a digital certificate. The service requires appointed bodies to request the certificate from DIGIT's service provider. Details about the process are available in the PKI for PCN: Public Key Infrastructure Service Offering Description.

2.2.3. Test connectivity

The appointed body needs to successfully pass the connectivity test organized by CEF in their eDelivery Connectivity Testing service. More information about CEF's eDelivery Connectivity Testing can be found in its Service Offering Document.

Testing will ensure that installation has been done properly.

2.2.4. Configure access point to process PCN messages

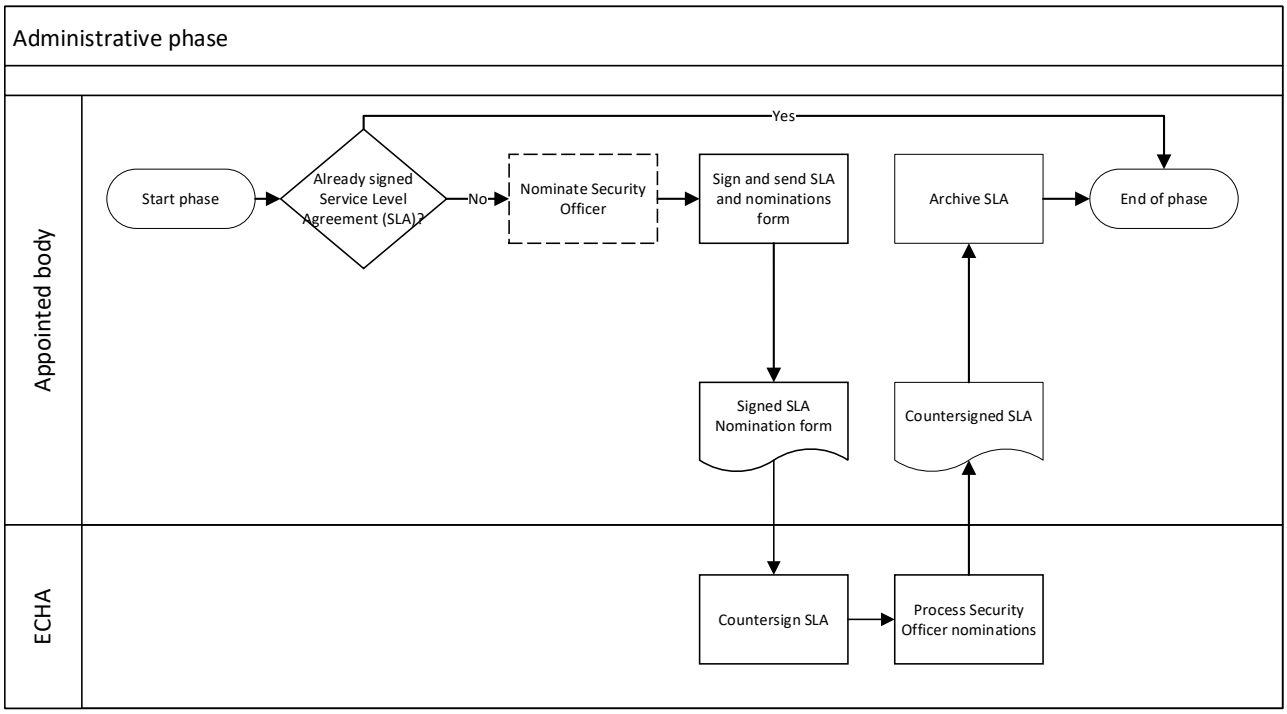
The eDelivery access point of the appointed body needs to process the PCN messages received from ECHA's access point. This processing needs to ensure that the dossier included in the message is stored in the appointed body's backend of choice.

To configure the access point, the appointed body needs to at least:

- Apply to the access point the configuration detailed in the PMode document.
    - If the appointed body is using Domibus, they can request a sample PMode file for their access point from ECHA
- Install the certificate obtained from CEF
    - If the appointed body is using Domibus, they can follow the instructions found in the eDelivery PKI for PCN Service Offering Document and in Domibus' administration guide.
- Install ECHA's eDelivery public key file
    - If the appointed body is using Domibus, they can follow the instructions found in the eDelivery PKI for PCN Service Offering Document and in Domibus' administration guide
- Connect their back-end system with their own eDelivery access point
    - If the appointed body is using Domibus, ECHA provides support for configuring Domibus' filesystem plugin. This plugin will copy the message attachment to a destination folder. Other Domibus' plugins can communicate directly with existing backend systems via, e.g., SOAP interface. Documentation for Domibus' plugins can be found in Domibus pages.

2.3. Administrative phase

Figure 6 Diagram of Administrative phase



Purpose: Appointed body have access to ECHA information systems

Actors:

6. Appointed body

7. ECHA

Process:

Appointed bodies that have signed the Service Level Agreement do not need to implement any additional requirements and can proceed with the technical implementation.

Appointed bodies that have not yet signed the Service Level Agreement shall:

1. Nominate a Security Officer (optional);

2. Sign and send the digital copy of the Service Level Agreement together with any nomination;

3. ECHA's Executive Director countersigns the Service Level Agreement;

4. Processing the nominations;

2.3.1. Nominate a Security Officer

The nomination of a Security Officer is optional for appointed bodies only connecting to the eDelivery network, and not to the other ECHA Information Systems. If the appointed body has already nominated a Security Officer for another EU Regulation, ECHA recommends nominating this same person for the CLP Regulation (Article 45, Annex VIII).

To nominate a Security Officer, the **appointed body's legal representative** (in other words, the person legally representing the appointed body mentioned in the consolidated Commission list for appointed bodies) needs to sign a nomination form specifying:

1. The institutional information of the appointed body (name and address) E.g.:

   "*Appointed body for Spain*

   - *National Institute of Toxicology and Forensics*
   - *Minister of Justice*
   - *Calle José Echegaray 4*
   - *Madrid, Spain*"

2. The contact information of the Security Officer

3. The starting date of the nomination for the Security Officer

2.3.2. Sign and send Service Level Agreement

Once the appointed body is ready to agree to the terms of the SLA, the appointed body director should sign it. A digital copy of the signed document should be sent to the poisoncentres@echa.europa.eu email. There is no need for the original paper version unless requested by the Poison Centres team.

2.3.3. Processing the nominations and setting up secure remote access;

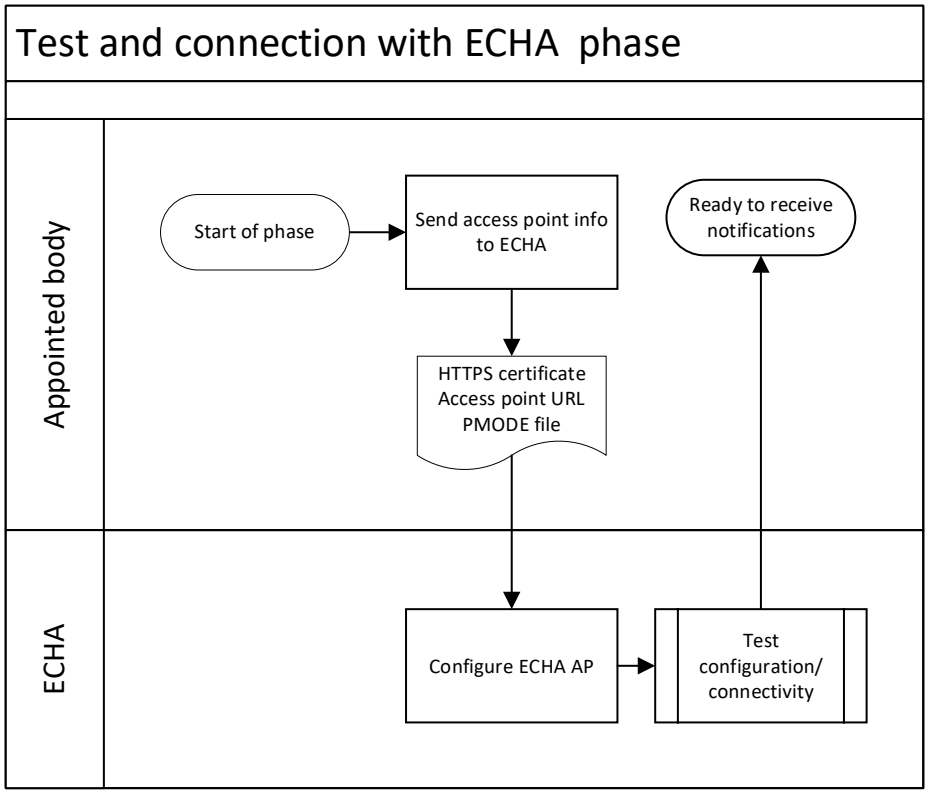
ECHA will process the nominations of Security Officer(s) and will grant access to the S-CIRCABC interest group of the Security Officers Network.

2.3.4. Countersign the Service Level Agreement

Upon receipt of the signed SLA, ECHA's Executive Director will countersign the SLA. ECHA will send a digital copy of the countersigned document back to the appointed body.

2.4. Test and connection with ECHA phase

Figure 7 Diagram of Test and connection with ECHA phase



Purpose: Check that all the requirements for connection to ECHA's access point are met and set up ECHA's access point

Actors:

8. Appointed body
9. ECHA

Process:

1. Send access point information to ECHA
2. Configure ECHA's access point
3. Test configuration and connectivity

2.4.1. Send access point information to ECHA

Once the appointed body has fulfilled the access point setup phase and the security and administrative phase, it is time to set up the connection with ECHA's access point. In order for ECHA to configure its access point, the eDelivery contact person of the appointed body needs to send the following information to ECHA using the Contact Form for Authorities:

- URL of the access point
- Certificate used to secure the HTTPS connection to the access point
- If using Domibus, the appointed body can also send the following information:
    - Their pmode.xml file (it can be downloaded from Domibus admin UI)
    - A screenshot or a list of the certificates installed in their Domibus truststore (it can be accessed through the Domibus Admin UI)

In the message, the contact person should suggest several time slots in which the connectivity test can be run. These timeslots should be of about 2 hours to allow for troubleshooting the connection. For that reason, it is important that engineers are available at the appointed bodies' side during that time. Final time will be agreed in step

2.4.2. Configure ECHA's access point

ECHA will set up the access point with the information provided. In particular:

- Set up access point truststore with appointed bodies public certificate for eDelivery obtained from T-Systems platform
- Set up its own Domibus' filesystem plugin to direct messages to the appointed body's access point as defined by the URL
- Set up eDelivery application server to recognize the HTTPS certificate provided by the appointed body

2.4.3. Test configuration and connectivity

This testing step will make sure that ECHA's and appointed body's access points can communicate with each other.

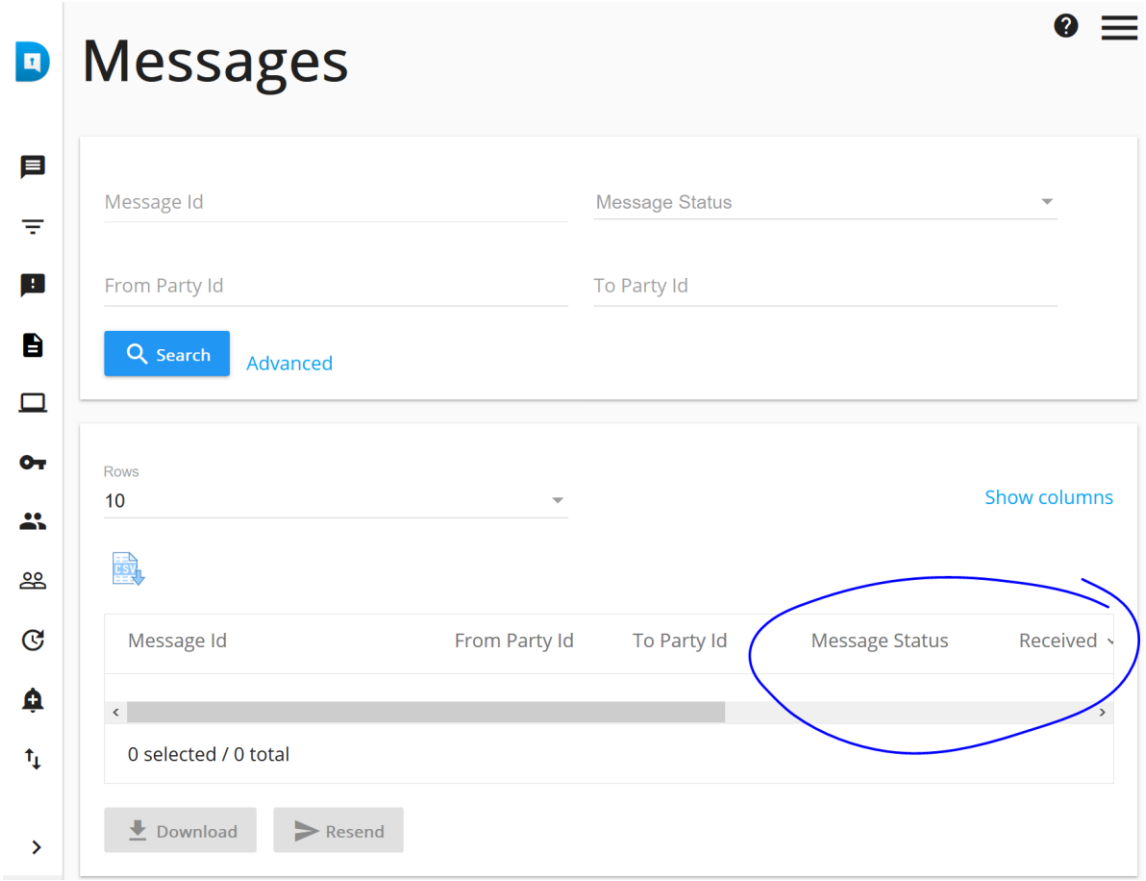
ECHA and the appointed body will arrange a suitable time for the testing session. This initial testing session will consist of sending and receiving a PCN message, as defined in the PCN eDelivery Solution Description Document.

The steps for the first message delivery are the following:

- ECHA copies the message content to the output folder of its Domibus installation
- ECHA checks from the administrator console of its access point that the message has been correctly sent
- ECHA informs the appointed body of the successful sending

Appointed body checks from the administrator console of its access point that the message has been received, see Figure 8.

Figure 8 Domibus administration console with Message Status and Received columns highlighted



- Appointed body informs ECHA of the successful receiving and processing of the message
- Appointed body informs ECHA in writing on the acceptance of the Terms and Conditions of the service and of the date they want to start receiving messages in production mode, and whether they want to receive the notifications sent to them before this date.

If more testing is required the appointed body can request via Contact Form for Authorities.

3. Service levels

ECHA eDelivery network aims to be operational 99.5% of the time, 24/7.

Planned downtime for upgrades will be communicated in advance to the eDelivery contact person for each appointed body.

Appointed body is requested to communicate planned downtime of their access point to ECHA via the Contact Form for Authorities. If the access point of the appointed body is down for unplanned reasons for more than 3 days, the appointed body should contact via the Contact Form for Authorities. In that cases, ECHA will temporarily stop sending messages to the appointed body's access point until they communicate that its access point is ready to receive messages again.

4. Termination of the service

Appointed body can create a request to be removed from ECHA's eDelivery network, and to stop receiving messages, by using the Contact Form for Authorities. The request needs to include the termination date.

5. Support mechanisms

Appointed bodies can contact ECHA or CEF depending on the issue.

5.1. ECHA

Contact ECHA if you have issues related to:

1) the connection to ECHA's eDelivery access point and

2) the delivery of eDelivery messages

Support can be requested via the Contact Form for Authorities.

ECHA's business hours are 09:00–18:00 (EET) from Monday to Fridays

5.2. CEF

Appointed bodies can get support in eDelivery implementation matters from CEF by requesting support service at their Service Desk webpage:

https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Service+Desk

CEF can also be reached by email at the address below:

cef-eDelivery-support@ec.europa.eu

CEF's business hours are 08:00–18:00 (CET) from Monday to Fridays

6. Questions and answers

6.1. What happens if the version of Domibus installed by the appointed body is no longer supported by CEF?

CEF supports each Long Term Support Domibus release for two years. Otherwise, CEF supports the rest of releases for one year. Appointed bodies are advised to upgrade to the most recent version of Domibus to guarantee support from CEF and to ensure found vulnerabilities are addressed.

The eDelivery network will continue to work independently of the version used by the appointed body, unless critical vulnerabilities need to be patched to maintain the security assurances of eDelivery.

6.2. What happens if an appointed body has technical issues with the backend that processes the messages?

The appointed body should communicate with ECHA to temporarily suspend the service while they address the technical issues using the Contact Form for Authorities.

6.3. What happens if the appointed body needs ECHA to re-send the messages?

If for some reason, the appointed body needs previously sent messages, they should create a request using the Contact Form for Authorities specifying which messages, e.g., resend those message within a timeframe. ECHA will consider the feasibility of the proposal and re-send those messages if possible.

6.4. What happens when the eDelivery certificate of the appointed body expires?

The appointed body has to renew their eDelivery certificate before it expires. To obtain the new certificate they need to follow the CEF PKI process described in 'PKI for PCN: Public Key Infrastructure Service Offering Description'. Once obtained, they need to inform ECHA of the successful renewal using Contact Form for Authorities.

6.5. How can I connect my backend system to the eDelivery access point?

Domibus provides several plugins to connect the access point to other systems. It also provides an API for the creation of new plugins. The Domibus webpage offers a 'Plugin Cookbook' with instructions and advice for plugin developers.

6.6. Can I reuse an existing installation of Domibus?

From version 4.0 onwards, Domibus supports multiple domains (multi-tenancy). This means a single installation of Domibus can connect to several eDelivery networks.

6.7. Can I reuse an existing certificate I obtained from CEF PKI service from another domain?

No, you cannot reuse an existing certificate to connect to ECHA's.

6.8. When is a notification considered accepted when using eDelivery?

eDelivery only informs to the notification submitter that a notification has been successfully downloaded by the appointed body. It is up to the appointed body to decide the acceptance process for the notifications. Appointed bodies can follow up a process with the submitter using the contact information found in the notification dossier.