

Poison Centres

System-to-system integration for industry

November 2019

ABC

Version	Changes
1.0	1 st version
	November 2019

Legal notice

This document aims to assist users in complying with their obligations under the CLP Regulation (EC) No 1272/2008 on classification, labelling and packaging of substances and mixtures and Annex VIII. 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.

Reproduction is authorised provided the source is acknowledged.

Title: Poison Centres: System-to-system integration for industry

Reference: ECHA-19-H-17-EN

ISBN: 978-92-9481-163-9

Cat. Number: ED-04-19-698-EN-N

DOI: 10.2823/573061

Publ.date: November 2019

Language: EN

© European Chemicals Agency, 2019

Cover page © European Chemicals Agency

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

Table of Contents

1 INTRODUCTION	5
1.1 Document references.....	5
1.2 Icons, abbreviations and terminology	5
2 REST API	8
2.1 Submit a dossier	8
2.1.1 Request.....	8
2.1.2 Response.....	8
2.2 Get submission report.....	9
2.2.1 Request.....	10
2.2.2 Response.....	10
2.3 Testing	13
2.3.1 Main objectives	13
2.3.2 Test scenario	13
3 SECURITY	14
3.1 General approach.....	14
3.2 HMAC-Signed JWT	15
3.2.1 Configuration	15
3.2.2 Usage	15
ANNEX A – LIST OF IMPLEMENTED VALIDATION RULES	17
ANNEX B – EXAMPLES	18
B.1 JWT	18
B.1.1 Without expiration date.....	18
B.1.2 With expiration date	18
B.2 Submit a dossier	19
B.2.1 Request in “test” mode	19
B.2.2 Request in “production” mode.....	19
B.2.3 Sample request.....	20
B.3 Get submission report	20
B.3.1 Request in “test” mode	20
B.3.2 Response in “test” mode	20
B.3.3 Request in “production” mode.....	21
B.3.4 Response in “production” mode.....	21
B.2.3 Sample request.....	22
B.4 Error responses.....	22
B.4.1 Legal entity not authorized by ECHA or JWT token is missing.....	22
B.4.2 JWT token malformed or expired	23

Table of Figures

Figure 1: S2S integration scenario	16
--	----

List of Tables

Table 1: Document references.....	5
Table 2: Terms and abbreviations.....	5
Table 3: Submit a dossier - Request headers	8
Table 4: Submit a dossier - Response status codes	8
Table 5: Submit a dossier - Response payload.....	9
Table 6: Get submission report – Request headers.....	10
Table 7: Get submission report – Response status codes	10
Table 8: Get submission report - Response payload	11
Table 9: Test flag in the HTTP Header	13
Table 10: S2S configuration for industry (per LE)	15
Table 11: JWT header	15
Table 12: HTTP Authorization header example (Bearer).....	16

1 Introduction

The goal of this document is to provide a technical guide to industry in order to consume REST services exposed by the ECHA Submission portal. More specifically:

1. It describes the REST API so that industry systems wishing to perform direct (system-to-system) submissions can integrate with;
2. It describes the security approach that will be implemented as part of the ECHA Submission portal authorisation checks. This will be a precondition for the system-to-system integration.

This document does not cover how to prepare a dossier compliant with the PCN format (see [1] for more support).

1.1 Document references

Table 1: Document references

Ref	Title
1	Poison Centres Notification format

1.2 Icons, abbreviations and terminology

This document uses various icons and specific abbreviations throughout. The icons are displayed to highlight useful or important information. The following icons are used:

 Useful information, guidance, assistance


 Very important note

Table 2: Terms and abbreviations

Term or Abbreviation	Explanation
API key	It is associated to Industry system accounts, managed in ECHA Accounts and is used to sign the JWT using the HS256 algorithm. The generated API key by the ECHA Accounts is Base64 encoded.
Dossier	A dossier or IUCLID dossier or PCN dossier represents the collection of all the scientific and administrative information at any given time (snapshot) fulfilling the legal data requirements (CLP Article 45 and Annex VIII) needed in order to notify and place the mixture in a specific market.

Term or Abbreviation	Explanation
ECHA Accounts	It is the family of applications used to manage companies' and users' information and provide authentication and authorisation services to integrating systems.
ECHA Submission portal	The portal used to submit Poison Centre notifications, which upon their successful processing and in case of no validation errors, are dispatched to the relevant market areas.
IDP	IDentity Provider is the system that creates, maintains, and manages identity information for principals while providing authentication services to relying applications within a federation or distributed network. In ECHA, IDP is considered an intrinsic part of the ECHA Accounts.
IUCLID	International Uniform Chemical Information Database, is a software application system for managing data on intrinsic and hazard properties of chemical substances and mixtures for accurate reporting to the regulatory authorities.
JSON	JSON (JavaScript Object Notation) is a lightweight data-interchange format.
JWT	JSON Web Token (JWT) is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed. JWTs can be signed using a secret (with the HMAC algorithm) or a public/private key pair using RSA or ECDSA.
Legal entity (LE)	A Legal Entity may represent anything between a complex business structure and a simple organised business (e.g. corporation, company, organisation) or a single natural person capable and having the right to engage into contracts or commercial transactions.
Mixture	A mixture or solution composed of two or more substances (Article 2(8) of CLP).
PCN	In the context of CLP Art.45 and Annex VIII, a notification or PCN (Poison Centre Notification) is the outcome of a valid and successful electronic submission (i.e. resulting in a positive outcome after processing) of the information required in a IUCLID dossier fulfilling the technical data requirements.
PCN number	PCN number is a UUID (Universally unique identifier), generated by industry for each initial submission of a Mixture and retained across submission of update dossiers. It is used as the correlation identifier of different submissions related to the same mixture. In case of significant change of composition of the mixture, a new PCN number must be generated to identify the new series of submissions.

Term or Abbreviation	Explanation
RESTful WS	The REST architectural style constrains an architecture to a client/server architecture and is designed to use a stateless communication protocol, typically HTTP. In the REST architecture style, clients and servers exchange representations of resources by using a standardized interface and protocol.
Shared secret	<i>see definition of "API key"</i>
Submission	A submission is an event resulting from the transmission of a Dossier prepared and submitted electronically to the ECHA Submission portal.
Submission number	A submission number is a unique number that is generated upon submission by any system receiving a dossier. The submission number can be used to uniquely identify each submission and get its submission report.
System account	It is used to represent an Industry software system integrating with the ECHA Submission portal and will be defined as follows: <ul style="list-style-type: none">- LE UUID: the company UUID in the ECHA Accounts- credential (the so-called API key): non-editable, auto-generated System accounts will be managed in ECHA Accounts A single system account will exist per LE.

2 REST API

This chapter describes the REST endpoints exposed by the ECHA Submission portal to facilitate the system-to-system integration from the industry systems and allow automatic submissions provided that the security requirements are met (see [3] Security for additional information).

2.1 Submit a dossier

This service is used to perform a submission to the ECHA Submission portal. This requires the IUCLID dossier file content bytes (the dossier to be submitted) and responds with the submission number, which can be later used to get the submission report.

Sample request/response pairs are provided in [B.2 Submit a dossier].

2.1.1 Request

Table 3: Submit a dossier - Request headers

Request Header	Description
Request URL	The request URL to submit the dossier, i.e. https://api.ecs.echa.europa.eu/submission
Request method	POST
Content-Type	application/vnd.iuclid6.archive; filename=<dossier-filename>.i6z
Accept	application/json, text/plain, */*
Authorization	This needs to be completed as described in [3. Security], e.g. Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MzI1MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c

The Request payload should include the IUCLID dossier (i6z file / attachment).

2.1.2 Response

Table 4: Submit a dossier - Response status codes

Status	Description
202	The IUCLID dossier file has been uploaded and submitted, the submission number has been returned in the response.
400	The server cannot process the request due to something that is perceived to be a client error such as malformed request syntax, e.g. Bearer token or request parameters not syntactically correct, Bearer token expired or revoked
401	The call failed the authentication checks

Status	Description
403	The call failed the authorisation checks
404	The service was not found
415	The server refused to accept the request because the payload format is in an unsupported format such as the Content-Type
500	It indicates that the server encountered an unexpected error that prevented it from accepting and processing the request.

Examples on response status codes are provided in [B.4 Error responses].

The response in JSON format includes the information described below.

Table 5: Submit a dossier - Response payload

Element	Description	Required
submissionNumber	The submission number generated upon submitting the provided IUCLID dossier file, e.g. "AAD678032-54"	Yes
statusUrl	The URL to retrieve the submission report through the S2S using the submission number, i.e. <a href="https://api.ecs.echa.europa.eu/submission/<submission-number>">https://api.ecs.echa.europa.eu/submission/<submission-number>	Yes
reportUrl	The URL that points to a human readable submission report page in the ECHA Submission portal (requires that a user has logged in first), i.e. <a href="https://ecs.echa.europa.eu/cloud/submissions/<submission-number>">https://ecs.echa.europa.eu/cloud/submissions/<submission-number>	Yes

2.2 Get submission report

This service is used to retrieve the submission report of a submission given a submission number. Naturally, it is performed after the submission of a dossier and can be used for the following purposes:

- To track the submission status, i.e. whether the submitted dossier identified by the submission number has passed or failed the validation checks and in case of failure to get the list of failed validations.
- To get the submitted dossier metadata, such as the submission number, the submission date, filename, dossier UUID, PCN number, link to submission report

Sample request/response pairs are provided in [B.3 Get submission].

2.2.1 Request

Table 6: Get submission report – Request headers

Request Header	Description
Request URL	The request URL including the submission number as a required path parameter, i.e. <code>https://api.ecs.echa.europa.eu/submission/<submission-number></code>
Request method	GET
Accept	<code>application/json, text/plain, */*</code>
Authorization	This needs to be completed as described in [3. Security], e.g. Bearer <code>eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c</code>

2.2.2 Response

Table 7: Get submission report – Response status codes

Status	Description
200	The relevant submission is found and the response includes its details
400	The server cannot process the request due to something that is perceived to be a client error such as malformed request syntax, e.g. Bearer token or request parameters not syntactically correct, Bearer token expired or revoked
401	The call failed the authentication checks
403	The call failed the authorisation checks
404	The service was not found, the submission information is not found, e.g. wrong submission number, submission number belongs to another company
415	The server refused to accept the request because the payload format is in an unsupported format such as the Content-Type
500	It indicates that the server encountered an unexpected error that prevented it from accepting and processing the request.


Examples on response status codes are provided in [B.4 Error responses].


The response in JSON format includes the submission report details, see next table.

Table 8: Get submission report - Response payload


Element	Description	Required
submissionNumber	The submission number of this submission, e.g. "AAD678032-54"	Yes
status	The submission status of this submission, i.e. <ul style="list-style-type: none"> - PENDING indicates that the submission is still being processed by the server, - VALIDATION_SUCCEEDED indicates that the submission has passed successfully the validation checks (although it may have failed some quality rules) and will be dispatched to the target market areas - VALIDATION_FAILED indicates that the submission has failed the validation checks (i.e. at least one submission rule has failed) and as a result of it the submitted dossier will not be dispatched to the target market areas. 	Yes
submissionDate	The creation datetime of this submission with an offset from UTC/Greenwich in the ISO-8601 calendar system e.g. "2007-12-03T10:15:30+01:00"	Yes
dossierUuid	The submitted IUCLID dossier UUID e.g. "20b78cc8-2594-4d12-b4b9-a4b5e5ab2cff"	No
filename	The specified IUCLID dossier filename during the submission e.g. PCNDossier.i6z	Yes
refType	The type of identifier used to correlate this submission with others/previous submissions for the same substance/mixture, used in case additional submission types are supported in the future, i.e. "PCN_NUMBER"	No
refValue	The PCN number value e.g. "e1131d0b-781f-4427-9a43-f5189dcb7918"	No
validations	In case of failed validation checks, this includes a list of identified validation failures (warnings or errors), e.g. <pre>[{ "level" : "FAIL", "code" : "BR553", "context" : "iuclid6:/3c13e517-2918-448d-9b68-ef804b009dea/CUSTOM_ENTITY.DOSSIER/3c13e517-2918-448d-9b68-ef804b009dea#SpecificSubmissions.PCNNumber" }, { "level" : "FAIL", "code" : "BR556", "context" : "iuclid6:/3c13e517-2918-448d-9b68-ef804b009dea/MIXTURE/282a1d61-d65c-460b-bb5f-493db041e9e0;section=CLP_PCN:1.1/MIXTURE/282a1d61-d65c-460b-bb5f-493db041e9e0#MIXTURE" }, { "level" : "WARN",</pre>	Yes

Element	Description	Required
	<pre>"code" : "BR508", "context" : "iuclid6:/0bda1005-201c-4a43-b776-3c748f5fd1cf/MIXTURE/282a1d61-d65c-460b-bb5f-493db041e9e0/FLEXIBLE_RECORD.ProductInfo/5ed5b5a2-dec4-446b-a343-3f89e2728932#ProductIdentifiers.TradeNames[0].TradeName" }]</pre> <p>Where</p> <ul style="list-style-type: none"> - "level" indicates the error level of this validation rule and may take the following values: <ul style="list-style-type: none"> a. FAIL indicates that the validation rule results in a submission with VALIDATION_FAILED status b. WARN indicates that this is a failed 'quality' rule that might trigger further manual checks but not sufficient to fail the submission c. EXCEPTION indicates that the validation rule could not be executed for technical reasons and as a result of it the submission remains in a PENDING status (it is expected that it will be fixed in the next application version and the submission will be resumed automatically without requiring re-submission from the company) - "code" is the identifier of the validation rule that failed - "context" indicates the path the current validation rule failed requiring from users to fix the reported error 	
reportUrl	<p>The URL that points to an HTML submission report page in the ECHA Submission portal (requires that a user has logged in first), i.e. <a href="https://ecs.echa.europa.eu/cloud/submissions/<submission-number>">https://ecs.echa.europa.eu/cloud/submissions/<submission-number></p>	Yes

 The list of validation error messages is provided in the Annex A of this document.

 When the processing status is PENDING (not final), the industry system needs to repeat the request until it receives a final status (either VALIDATION_SUCCESSFUL or VALIDATION_FAILED).

If the uploaded dossier fails the IUCLID file format checks, i.e. the ECHA Submission portal does not recognise the file as a IUCLID Dossier, the submission status will be VALIDATION_FAILED. In such case:

-  - submissionNumber, status, submissionDate, filename, and validations will be provided in the response; validations will provide the error cause, i.e. "Invalid IUCLID archive".
- dossierUuid, refType, refValue will not be provided, given that the dossier could not be properly processed and the respective fields to be extracted.

2.3 Testing

2.3.1 Main objectives

The main objectives of testing the system-to-system integration are the following:

- Ensure that industry system (client) passes connectivity and integration test (API compliance)
- ECHA Submission portal properly authorises, accepts the request and responds
- Industry system processes the response

2.3.2 Test scenario

The test scenario will work as follows:

1. Industry system submits a file (as described in [2.1.1 Request]) indicating that this is for testing purposes. For this purpose, a new HTTP Header needs to be provided in the Request:

Table 9: Test flag in the HTTP Header

Request Header	Description
X-ECHA-Mode	HTTP Header to indicate the "testing" operation mode, i.e. X-ECHA-Mode=test ; if not provided, the submission will be considered that it is for Production purposes.

2. ECHA Submission portal identifies that this is a "test" call and responds (as described in [2.1.2 Response]). Note that the test submissions will not be actually processed and a dummy response will be provided instead (e.g. answering with the same dummy submission number).
3. Industry system processes the response.
4. Industry system requests the submission report (as described in [2.2.1 Request]) by providing a submission number (the one received in the previous call) indicating that this is for testing purposes. For this purpose, the **X-ECHA-Mode=test** HTTP Header needs to be provided in the Request.
5. ECHA Submission portal identifies that this is a "test" call and responds (as described in [2.2.2 Response]). Note that a dummy response will be provided in this case that does not reflect the actual processing status; submitted dossiers are not further processed in "test" mode and the processing always remains in "PENDING" status.
6. Industry system processes the response and the scenario concludes.

3 Security

This chapter proposes a solution for the implementation of the security controls in the context of the system-to-system (S2S) integration.

3.1 General approach

The proposed solution is stipulated by the following main ideas/requirements:

1. Industry companies must be able to manage the credentials required for the S2S integration with the ECHA Submission portal services. In particular, they must be able to cancel or replace them with new ones, e.g. if they have doubts about their integrity.
2. ECHA needs to control which companies are allowed to submit data using the S2S integration in order to avoid malicious usage and for this purpose:
 - ECHA will setup a service
 - Interested companies will contact ECHA
 - ECHA will guide them on the process that needs to be followed
 - Upon ECHA's approval, companies will be able to access the system-to-system service (provided that they have implemented the REST API and the security requirements)



Details of this service will be separately described (not part of this document scope).

An outline of the solution for point #1 above is:

- Different credentials than the regular username and password credentials associated with user accounts in ECHA Accounts will be used. Industry will manage them independently from regular user passwords, and revoke them altogether without sacrificing any user accounts.
- A single system account per legal entity will be supported, i.e. it will not be possible to create multiple system accounts per legal entity (as this is the case for "human" accounts)
- An industry system may perform operations on behalf of multiple associated legal entities (as it is the case for most of the consultant companies/systems).
- For the management of the S2S credentials, a new user interface has been developed in the ECHA Accounts (LE management UI) where users can manage their API keys in all the companies in which they have the S2S account.
- The solution is based on the generation of the [HTTP Authorization](#) header, which is then added to the S2S service requests and verified by the system/gateway receiving the request.
- Industry system configures S2S credentials and generates S2S authentication headers to include in the service call. The configuration of the industry system should contain a list of two entries per LE:

Table 10: S2S configuration for industry (per LE)


Property	Description
LE UUID	The LE UUID (from the ECHA Accounts)
Credential	The shared secret, called "API key" (from ECHA Accounts)


3.2 HMAC-Signed JWT

An overview of the solution is that the client industry system generates a JWT containing its LE UUID and a timestamp for each batch of calls, and signs it using the HS256 (SHA-256 MAC) algorithm with a shared secret. The details are given in the next paragraphs.

3.2.1 Configuration

1. User generates an API key (by pressing a button), which is stored in ECHA Accounts (through the LE management UI).
2. The user copies the API key and pastes it in some configuration file of the industry system.

 The generated API Key, which is Base64 encoded, will be used as shared secret for signing the JWT.

 The API Key is never again displayed to the user; in case of loss, the only option is to generate a new one invalidating the previous one. In such case, the JWT has to be re-generated since the previous one is no longer valid.

3.2.2 Usage

1. The industry system creates a JWT with the following header and signs it using the HS256 (SHA-256 MAC) algorithm with the API key.

Table 11: JWT header

```
{
  "alg": "HS256",
  "typ": "JWT"
}
.
{
  "x-echa-party": "<le-uuid>"
  "exp": <now + 3h>
}
```

The `typ` field is optional information and can be omitted since it is not validated.

The `exp` field determining the JWT expiration date can be defined in either way:

- a. not provided at all, in that case the JWT never expires
- b. provided in seconds (e.g. 1569849550) since Unix epoch as defined here:

<https://tools.ietf.org/html/rfc7519#section-2> (see "NumericDate" in the terms)

Examples are provided in [B.1 JWT].

2. The Authorization header is set to type `Bearer` and the encoded JWT is as follows:

Table 12: HTTP Authorization header example (Bearer)

```
Authorization: Bearer  
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MzE2MjM1MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
```

3. The ECHA system receiving the S2S request from the industry system checks the presence of the Authorization header, extracts the JWT, and verifies it against S2S IDP Token Server (ECHA Accounts) using the API key stored for the system user claimed in the JWT.
4. Then
 - a. Upon successful verification, the S2S request reaches the Submission Services, which respond to the industry system.
 - b. Upon failed verification, there is Unauthorised error returned to the industry system.

The aforementioned steps are depicted in the following diagram (the happy-path scenario):

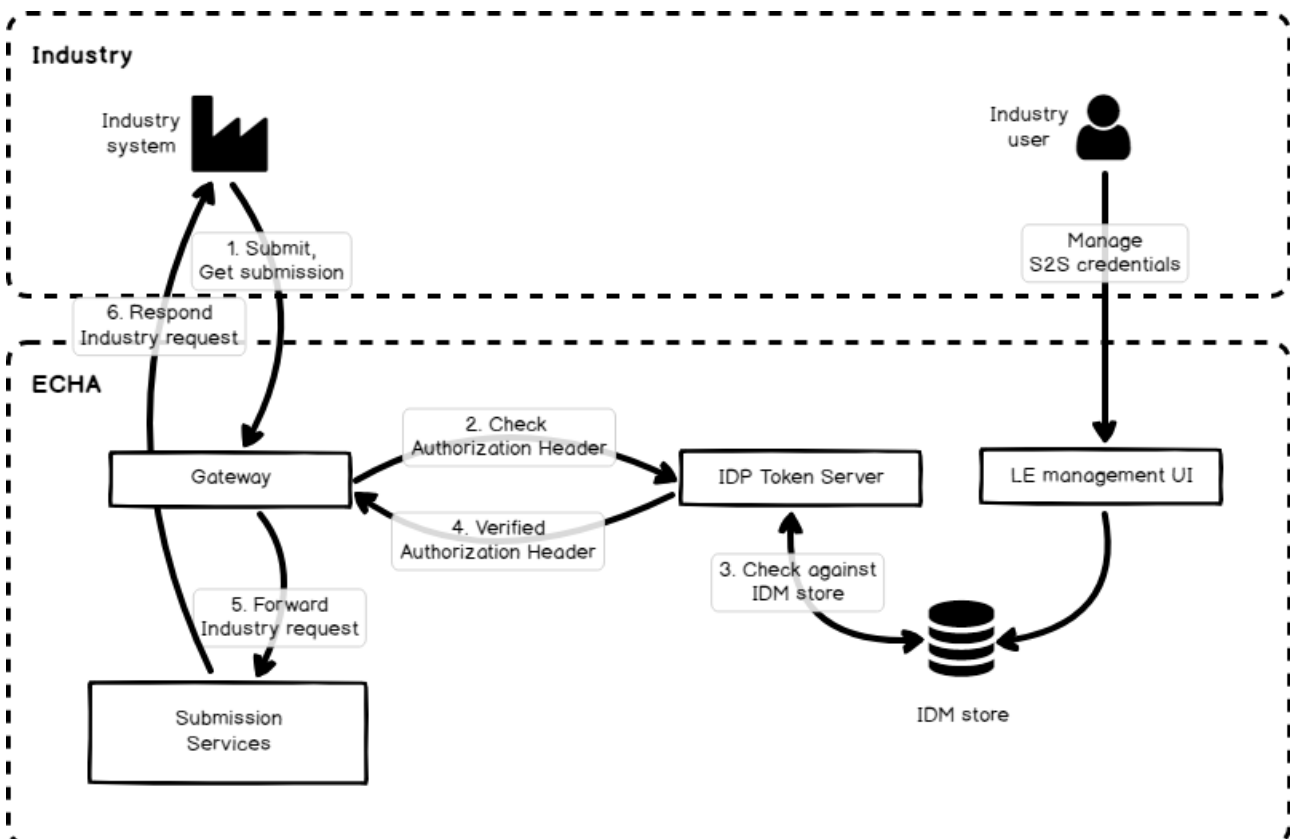


Figure 1: S2S integration scenario

Annex A – List of implemented validation rules

The following document provides short descriptions of the validation rules in IUCLID which are relevant for poison centres notifications (PCNs):

https://poisoncentres.echa.europa.eu/documents/22284544/28470089/PCN+Format+-+Annex+-+Validation+rules_v2.pdf/7eb924bd-234c-4bfd-4079-6f8be198b0d7

Annex B – Examples

B.1 JWT

B.1.1 Without expiration date

Optional `typ` is provided

```
{
  "alg": "HS256",
  "typ": "JWT"
}
.
{
  "x-echa-party": "ECHA-83a626b4-1d12-4a39-9832-20c97c1fba4d"
}
```

Optional `typ` is not provided

```
{
  "alg": "HS256"
}
.
{
  "x-echa-party": "ECHA-83a626b4-1d12-4a39-9832-20c97c1fba4d"
}
```

B.1.2 With expiration date

```
{
  "alg": "HS256"
}
.
{
  "x-echa-party": "ECHA-83a626b4-1d12-4a39-9832-20c97c1fba4d",
  "exp": 1601471928
}
```

B.2 Submit a dossier

B.2.1 Request in “test” mode

Request Header	Description
Request URL	https://api.ecs.echa.europa.eu/submission
Request method	POST
Content-Type	application/vnd.iuclid6.archive; filename=initial-dossier.i6z (<i>sent as multipart/form-data</i>)
Accept	application/json, text/plain, */*
X-ECHA-mode	test
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4bG9jaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTZkMTItNGEzOS05ODMyLTIwYzYzYzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11Uukai3fX4

B.2.2 Request in “production” mode

Just omit the X-ECHA-mode=test from the Request Headers of the example above

Request Header	Description
Request URL	https://api.ecs.echa.europa.eu/submission
Request method	POST
Content-Type	application/vnd.iuclid6.archive; filename=initial-dossier.i6z (<i>sent as multipart/form-data</i>)
Accept	application/json, text/plain, */*
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4bG9jaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTZkMTItNGEzOS05ODMyLTIwYzYzYzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11Uukai3fX4

B.2.3 Sample request

```
Sample request
```

```
POST /submission HTTP/1.1
X-ECHA-Mode: test
Content-Type: application/vnd.iuclid6.archive; filename=pcn_dossier.i6z
Accept: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LT
FkMTItNGEzOS05ODMyLTIwYzk3YzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11U
Ukai3fX4
Host: api.ecs.echa.europa.eu
Accept-Encoding: gzip, deflate
Content-Length: 72859
Connection: keep-alive
```

B.3 Get submission report

B.3.1 Request in "test" mode

Request Header	Description
Request URL	https://api.ecs.echa.europa.eu/submission/AAD678032-54
Request method	GET
Accept	application/json, text/plain, */*
X-ECHA-mode	test
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LT FkMTItNGEzOS05ODMyLTIwYzk3YzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11U Ukai3fX4

B.3.2 Response in "test" mode

```
Response
```

```
{
  "submissionNumber": "RMH652909-13",
  "status": "PENDING",
  "submissionDate": "2019-09-30T17:28:22.490982+03:00",
  "dossierUuid": "a6409333-e4d0-43c7-916a-83ce7a23e4c1",
  "filename": "TestIuclidDossier.i6z",
  "refType": "PCN number",
  "refValue": "49f3d053-336e-4e9a-a574-2c4f06146d42",
  "validations": [],
  "reportUrl": "https://echacs.trasys.gr/cloud/submissions/RMH652909-13"
}
```

B.3.3 Request in “production” mode

Just omit the X-ECHA-mode=test from the Request Headers of B.3 and provide a valid submission number submitted by your company.

Request Header	Description
Request URL	https://api.ecs.echa.europa.eu/submission/RMH652909-13
Request method	GET
Accept	application/json, text/plain, */*
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTFkMTItNGEzOS05ODMyLTIwYzYzYzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11UUKai3fX4

B.3.4 Response in “production” mode

Response
<pre>{ "submissionNumber": "RMH652909-13", "status": "VALIDATION_FAILED", "submissionDate": "2019-09-05T12:28:29.317171+03:00", "dossierUuid": "02d5ffce-bf9a-4017-ab3d-d7d6166ea34b", "filename": "s2s-update-1.i6z", "refType": "PCN number", "refValue": "1aab1d58-3050-4f7a-8d4d-d8079f84c089", "validations": [{ "level": "FAIL", "code": "BR564", "context": "" }, { "level": "FAIL", "code": "BR576", "context": "" }, { "level": "WARN", "code": "BR598", "context": "" }, { "level": "FAIL", "code": "BR553", "context": "iuclid6:/3c13e517-2918-448d-9b68-ef804b009dea/CUSTOM_ENTITY.DOSSIER/3c13e517-2918-448d-9b68-ef804b009dea#SpecificSubmissions.PCNNumber" }, { "level": "FAIL", "code": "BR556", </pre>

B.4.2 JWT token malformed or expired

Response

```
HTTP/1.1 400 Bad Request
Date: Tue, 08 Oct 2019 11:36:55 GMT
Content-Type: text/html
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 111
Connection: close
```

```
<html>
<head><title>400 Bad Request</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<hr><center>openresty</center>
</body>
</html>
```