ECHA
EUROPEAN CHEMICALS AGENCY

ECHA Submission portal

System-to-System submission for industry

February 2020

Version	Changes	
1.0	1st version	November 2019
1.1	Updated to incorporate: - Testing modes (connectivity and integration) - SCIP supported as a new submission type	February 2020

Legal notice

This document aims to provide duty holders needing to submit data to ECHA a technical guide to consume REST services exposed by the ECHA Submission portal.

Users are reminded that 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.

Title: ECHA Submission portal: System-to-system submission for industry

Reference: ECHA-20-H-01-EN
ISBN: 978-92-9481-163-9
Cat. Number: ED-04-19-698-EN-N
DOI: 10.2823/573061
Publ.date: February 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

Table of Contents

Table of Figures

List of Tables

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.

It should be noted that only submission types supported by the ECHA Submission portal will pass the business checks, while any others will fail during their processing.

Additionally, some submission types, such as the SCIP article notification, may only be supported in test mode until official support is enabled.

1.1 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 1: 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 represents the collection of all the scientific and administrative information at any given time (snapshot) fulfilling the legal data requirements.
ECHA Accounts	It is the family of applications used to manage companies' and users' information and provide authentication and authorisation services to integrating systems.

Term or Abbreviation	Explanation
ECHA Submission portal	The portal used to submit Poison Centres (PCN) and SCIP notifications, which upon their successful processing and in case of no validation errors, - are dispatched to the relevant market areas (PCN notifications) - are disseminated in the ECHA website (SCIP notifications)
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, mixtures and articles 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.
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.
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.
SCIP primary article identifier	SCIP primary article identifier is defined by the notifying Company by a type (according to a predefined list) and a value for each initial submission of an Article. The same identification should be retained in subsequent submissions of the same article to be considered as an update.

Term or Abbreviation	Explanation
Shared secret	*see definition of "API key"*
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: - 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 model for additional information). The exposed API can operate both in regular, production, mode, and in test mode to allow the verification of the connectivity and integration of industry systems without creating confusion with their actual legal obligations.

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 2: 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, */*
Authorisation	This needs to be completed as described in [3. Security model], e.g. Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c

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

2.1.2 Response

Table 3: 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, "test" HTTP Headers not correctly set

Status	Description
401	The call failed the authentication checks
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 4: 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. 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. 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. Naturallly, 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, link to submission report

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

2.2.1 Request

Table 5: Get submission report – Request headers

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

2.2.2 Response

Table 6: 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, "test" HTTP Headers not correctly set
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 7: 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. - 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. myDossier.i6z	Yes
refType	The type of identifier used to correlate this submission with others/previous submissions for the same substance/mixture/article, i.e. - For PCN dossier "PCN_NUMBER" is the only applicable value - For SCIP dossier, Primary article identifier, "ECHA Article ID" or "GTIN (Global Trade Item Number)" are two examples of the applicable types.	No
refValue	The value of the identifier used (see also above) 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.
	[{
	"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",
	"code" : "BR508",
	"context" : "iuclid6:/0bda1005-201c-4a43-b776-3c748f5fd1cf/MIXTURE/282a1d61-d65c-460b-bb5f-
		Yes

Element	Description	Required
	493db041e9e0/FLEXIBLE_RECORD.ProductInfo/5ed5b5a2-dec4-446b-a343-3f89e2728932#ProductIdentifiers.TradeNames[0].TradeName" }] Where - "level" indicates the error level of this validation rule and may take the following values: 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	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. https://ecs.echa.europa.eu/cloud/submissions/<submission-number>	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.

3 Security model

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 8: 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 9: 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 10: HTTP Authorization header example (Bearer)

```
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4
gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.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):

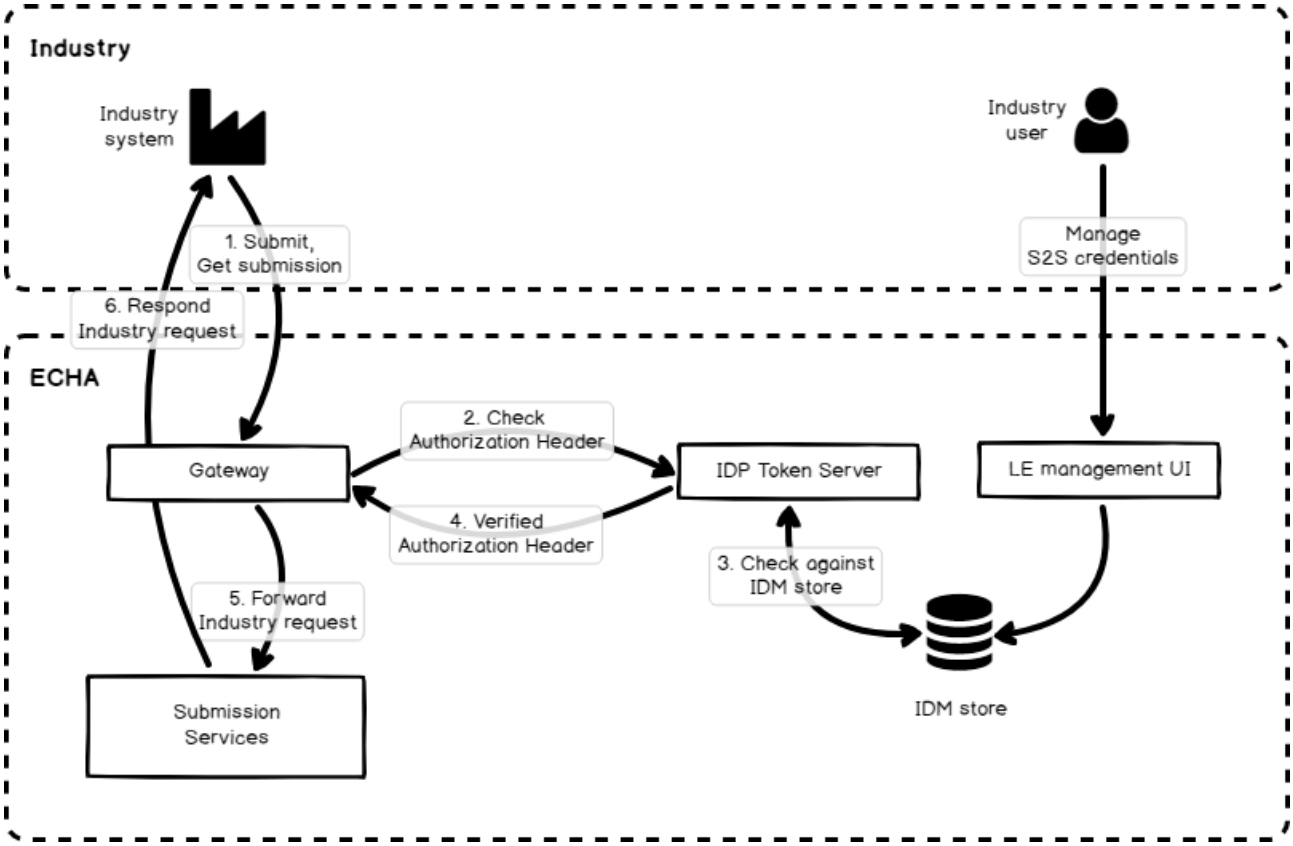

Figure 1: S2S integration scenario

4 Testing instructions and switch to production mode

4.1 Main objectives

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

- Ensure that industry system (client) passes the ECHA Submission portal connectivity and integration test and it is ready to switch to real operational mode.
- ECHA Submission portal properly authorises, accepts, processes the request and responds

4.2 Test flags

ECHA Submission portal supports the aforementioned testing phases by using two HTTP Header elements that have to be provided while testing in every request performed by the industry system:

Table 11: Test flags in the HTTP Header

Request Header	Description
X-ECHA-Mode	HTTP Header to indicate the mode of operation, i.e. - X-ECHA-Mode=test while testing; - X-ECHA-Mode must be omitted when switching to Production mode. ⚠ In case it is provided and takes a value other than "test", it causes a 400 - Bad request.
X-ECHA-Test-Run	A test run identifier effectively provides an isolated testing environment, both from regular production submissions, but also from test submissions with a different test run identifier. It allows grouping multiple submissions, potentially from different legal entities, into a single test run, in order, in particular, to verify cross-submission and even cross-legal entity portal business rules. As a consequence, the same dossiers (and associated UUIDs, UFI, etc) can be reused in different test runs, without interfering with each other. The expected structure of the identifier consists of two parts separated by a dash "-" character: a globally unique alphanumeric "company" prefix, and an incremental number. Note that the uniqueness of the prefix is not ensured by technical means. Integrators are advised to use a characteristic acronym or name that has little chance to be selected by another company or group e.g. the legal entity key. Obviously, generic choices such as "test", "pilot", "echa", should be avoided. ⚠ This must be only provided when X-ECHA-Mode=test, otherwise it causes a 400 - Bad request

The aforementioned test flags should be used as follows:

Table 12: Test flags per testing phase/scenario

X-ECHA-Mode	X-ECHA-Test-Run	Testing phase/purpose
test	(absent)	Connectivity tests - no actual processing of the submitted file - dummy responses
test	(absent)	Authentication and authorisation tests - no actual processing of the submitted file - dummy responses
test	mycompanyid-001 (example)	Integration tests - actual processing of the submitted file - actual response
(absent)	(absent)	Production mode - actual processing of the submitted file - actual response - valid dossiers are dispatched - valid dossiers become available in Remote Access portal

⚠ Any other combination of values not listed in the table above will lead to 400 - Bad request error.

⚠ Expiration of run-tests is not provided at the moment. However, depending on the usage and the volume of test data received, ECHA retains the right to clean them up periodically.

4.3 Testing phases

4.3.1 Connectivity test

The purpose of the connectivity test is to assure companies that they have been able to call successfully the ECHA Submission portal exposed services passing the security checks. During this phase, it is verified whether the Security model has been properly implemented and the basic request-response scenario passes.

The happy-path scenario should work as follows:

1. Industry generates a Bearer token, e.g. X (see [3 Security model])
2. Industry system performs **all requests** indicating in the HTTP Header:
    a. X-ECHA-Mode=test
    b. Authorization=Bearer X (see [2 REST API])
3. Industry system performs a "Submit a dossier" request
4. ECHA Submission portal identifies that this is a "test" call and provides a dummy response, while the submitted dossier is not processed by the system
5. Industry system receives and processes the dummy response

6. Industry system performs a "Get submission report" request by providing a submission number (the one received in the previous call)
7. ECHA Submission portal identifies that this is a "test" call and provides a dummy response
8. Industry system receives and processes the dummy response

The scenario can be repeated as many times as it is necessary, until there are no errors. When the connectivity tests have been completed successfully, the industry system may switch to integration test mode.

4.3.2 Integration test

The purpose of the integration test is to offer companies a realistic dossier submission and processing experience. It should be noted that the submissions made in the context of the integration tests will not be further processed, i.e. will not dispatched to the ABs in the case of PCN dossiers and will not be disseminated to the ECHA website in the case of SCIP article notifications (when SCIP will be officially supported).

The happy-path scenario should work as follows:

1. Industry generates a Bearer token, e.g. X (see [3 Security model])
2. Industry system performs **all requests** indicating in the HTTP Header:
    a. X-ECHA-Mode=test
    b. X-ECHA-Test-Run=mycompanyid-run001 (example)
    c. Authorization=Bearer X (see [2 REST API])
3. Industry system performs a "Submit a dossier" request
4. ECHA Submission portal identifies that this is a "test" call and the "test-run" has been also provided, so processes the request and provides a "real" response
5. Industry system receives and processes the response
6. Industry system performs a "Get submission report" request by providing a submission number (the one received in the previous call)
7. ECHA Submission portal identifies that this is a "test" call and the "test-run" has been also provided, so processes the request and provides a "real" response including any validation errors
8. Industry system receives and processes the response.

In the context of the integration testing, ECHA Submission portal supports actual processing of the submitted dossiers as it happens in production mode.

The scenario can be repeated as many times as it is necessary. When the integration tests have been completed successfully, the industry system may switch to Production mode. SCIP notifications can not be submitted as a real data in production mode before Autumn 2020.

Any submission performed in the context of the integration tests is visible in the ECHA Submission portal. As a result, users are able to verify the outcome of their testing

relying on the response sent by the ECHA Submission portal
- The URL for viewing the results in the portal is part of the standard response (see [2.1.2] and [2.2.2])
- For test runs, the URL is scoped to the test run identifier, with each test run effectively defining a separate virtual subdomain.

4.4 Switching to production mode

Once the testing phases have been concluded successfully, companies may switch to real operational mode, i.e. production. Any submissions made will be processed and, depending on their outcome, may be further processed as per the submission type specific needs.

The happy-path scenario should work as follows:

1. Industry generates a Bearer token, e.g. X (see [3 Security model])
2. Industry system performs **all requests** without providing any of the X-ECHA Mode and X-ECHA-Test-Run headers, but only the Authorization header:
    a. Authorization=Bearer X (see [2 REST API])
3. Industry system performs a "Submit a dossier" request
4. ECHA Submission portal identifies that this is a "real" call, so processes the request and provides a response
5. Industry system receives and processes the response
6. Industry system performs a "Get submission report" request by providing a submission number (the one received in the previous call)
7. ECHA Submission portal identifies that this is a "real" call, so processes the request and provides a response including any validation errors
8. Industry system receives and processes the response

Annex A – List of implemented validation rules

- **Poison centres notifications**: 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

- **SCIP notifications**: The validation rules implemented for SCIP will be published in the ECHA website under the Waste Framework Directive (WFD), SCIP Database section: https://echa.europa.eu/scip-support

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 "connectivity" 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 *(sent as multipart/form-data)*
Accept	application/json, text/plain, */*
X-ECHA-Mode	test
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTFkMTItNGEzOS05ODMyLTIwYzk3YzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8lRifaub1XjsG11UUkai3fX4

B.2.2 Response in "connectivity" test mode

Response

{
"submissionNumber": "AAD678032-54",
"statusUrl": "https://api.ecs.echa.europa.eu/submission/AAD678032-54",
"reportUrl": "https://ecs.echa.europa.eu/cloud/submissions/AAD678032-54"
}

B.2.3 Request in "integration" 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 *(sent as multipart/form-data)*
Accept	application/json, text/plain, */*
X-ECHA-Mode	test
X-ECHA-Test-Run	mycompanyid-run001
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTFkMTItNGEzOS05ODMyLTIwYzk3YzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8lRifaub1XjsG11UUkai3fX4

B.2.4 Response in "integration" test mode

Response

{
"submissionNumber": "RMH562417-19",
"statusUrl": "https://api.ecs.echa.europa.eu/submission/RMH562417-19",
"reportUrl": "https://test-mycompanyid-run001.ecs.echa.europa.eu/cloud/submissions/RMH562417-19"
}

B.2.5 Request in "production" 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 *(sent as multipart/form-data)*
Accept	application/json, text/plain, */*
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTFkMTItNGEzOS05ODMyLTIwYzk3YzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8lRifaub1XjsG11UUkai3fX4

B.2.6 Response in "production" mode

Response

{
"submissionNumber": "RMH562417-19",
"statusUrl": "https://api.ecs.echa.europa.eu/submission/RMH562417-19",
"reportUrl": "https://ecs.echa.europa.eu/cloud/submissions/RMH562417-19"
}

B.2.7 Sample request

Sample request
POST /submission HTTP/1.1 X-ECHA-Mode: test Content-Type: application/vnd.iuclid6.archive; filename=initial_dossier.i6z Accept: application/json Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTFkMTItNGEzOS05ODMyLTIwYzk3YzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8lRifaub1XjsG11UUkai3fX4 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 "connectivity" 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.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTFkMTItNGEzOS05ODMyLTIwYzk3YzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8lRifaub1XjsG11UUkai3fX4

B.3.2 Response in "connectivity" test mode

Response


```
{
  "submissionNumber": "AAD678032-54",
  "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://ecs.echa.europa.eu/cloud/submissions/AAD678032-54"
}
```


B.3.3 Request in "integration" test mode

Request Header	Description
Request URL	https://api.ecs.echa.europa.eu/submission/RMH904851-07
Request method	GET
Accept	application/json, text/plain, */*
X-ECHA-Mode	test
X-ECHA-Test-Run	mycompanyid-run001
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTFkMTItNGEzOS05ODMyLTIwYzk3YzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8lRifaub1XjsG11UUkai3fX4

B.3.4 Response in "integration" test mode

Response


```
{
  "submissionNumber": "RMH904851-07",
  "status": "VALIDATION_FAILED",
  "submissionDate": "2019-12-05T12:46:11.202978+02:00",
  "dossierUuid": "005056b7-b57b-4ed9-b1ae-c979eb74a1e7",
  "filename": "s2s-update-1.i6z",
  "refType": "PCN number",
  "refValue": "005056b7-b57b-4ed9-b1ae-c99fb9dec1e7",
  "validations":    [
        {
      "level": "WARN",
      "code": "QLT505",
      "context": "FLEXIBLE_RECORD-MixtureComposition-005056b7-b57b-4ed9-b1ae-
ca3149ab41e7, Mixture composition, Components, (3)"
    },
        {
      "level": "WARN",
      "code": "QLT505",
      "context": "FLEXIBLE_RECORD-MixtureComposition-005056b7-b57b-4ed9-b1ae-
ca3149ab41e7, Mixture composition, Components, (6)"
    },
        {
      "level": "WARN",
      "code": "QLT505",
      "context": "FLEXIBLE_RECORD-MixtureComposition-005056b7-b57b-4ed9-b1ae-
ca3149ab41e7, Mixture composition, Components, (11)"
    },
        {
      "level": "FAIL",
      "code": "BR570",
      "context": ""
    }
  ],
  "reportUrl": "https://test-mycompanyid-
run001.ecs.echa.europa.eu/cloud/submissions/RMH904851-07"
}
```


B.3.5 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, */*

Request Header	Description
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTFkMTItNGEzOS05ODMyLTIwYzk3YzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8lRifaub1XjsG11UUkai3fX4

B.3.6 Response in "production" mode

Response


```
{
  "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",
      "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",
      "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"
```

```
    }
  ],
  "reportUrl": "https://ecs.echa.europa.eu/cloud/submissions/RMH652909-13"
}
```


B.3.7 Sample request

Sample request
GET /submission/RMH652909-13 HTTP/1.1 X-ECHA-Mode: test Accept: application/json, text/plain, */* Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTFkMTItNGEzOS05ODMyLTIwYzk3YzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8lRifaub1XjsG11UUkai3fX4 Host: api.ecs.echa.europa.eu Accept-Encoding: gzip, deflate Connection: keep-alive

B.4 Error responses

B.4.1 Legal entity not authorised by ECHA or JWT token is missing

Response
HTTP/1.1 401 Unauthorized Date: Tue, 08 Oct 2019 11:32:34 GMT Content-Type: text/html Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 124 Connection: Keep-Alive <html> <head><title>401 Authorization Required</title></head> <body>   401 Authorization Required   <hr> openresty </body> </html>

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

{
  "error": "invalid_request",
  "error_description": "JWT signature does not match locally computed signature. JWT validity cannot be asserted and should not be trusted."
}
```

B.4.3 JWT token includes a wrong LE UUID

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

{
  "error": "invalid_request",
  "error_description": "No signing key could be found for ECHA-83a626b4-1d12-4a39-9832-20c97c1fba4d."
}
```

B.4.4 JWT token 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

{
  "error": "access_denied",
  "error_description": "JWT expired at 1970-01-01T02:00:00Z. Current time: 2020-01-09T12:32:37Z, a difference of 1578565957774 milliseconds.  Allowed clock skew: 0 milliseconds."
}
```

B.4.5 Incorrect “test” Headers

Example: X-ECHA-Mode=mytest (instead of ‘test’)

Response

```
HTTP/1.1 400 Bad Request
Date: Thu, 05 Dec 2019 10:31:39 GMT
```

```
Content-Type: text/plain
Strict-Transport-Security: max-age=15768000;includeSubDomains
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 94
Connection: close

Invalid operation mode: mytest. Should be either set to 'test' or not set at all
```

Example: X-ECHA-Test-Run=mycompanyid-run001, but X-ECHA-Mode is not provided at all

Response

```
HTTP/1.1 400 Bad Request
Date: Thu, 05 Dec 2019 10:35:43 GMT
Content-Type: text/plain
Strict-Transport-Security: max-age=15768000;includeSubDomains
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 98
Connection: close

Invalid operation mode: if X-ECHA-Test-Run is set then X-ECHA-Mode should be set to 'test'
```

EUROPEAN CHEMICALS AGENCY
ANNANKATU 18, P.O. BOX 400,
FI-00121 HELSINKI, FINLAND
ECHA.EUROPA.EU