

System-to-System submission service manual

January 2024



Version	Changes	Date
1.0	1 st version	November 2019
1.1	Updated to incorporate: <ul style="list-style-type: none"> - Testing modes (connectivity and integration) - SCIP supported as a new submission type 	February 2020
1.2	Updated to incorporate the new endpoint allowing companies to retrieve the list of events related to their submissions	May 2020
1.3	Updated to incorporate the version 2 changes of the public API	August 2020
1.4	Updated to include recommendations and best practices for successful S2S integration	February 2021
1.5	Updated to incorporate the version 3 changes of the public API	July 2021
1.6	This current document merges the previous manuals 'How to join ECHA's system-to-system service' and 'ECHA Submission portal: System-to-system submission for industry' Updated to incorporate the version 4 changes to the public API	July 2022
1.7	Corrections in 2.6 and C.6 for Disable submission	August 2022
1.8	Updates to onboarding process and removal of v2 information	January 2024

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: System-to-system submission service manual

Reference: ECHA-22-H-14-EN

ISBN: 978-92-9481-163-9

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

DOI: 10.2823/573061

Publ.date: Jan 2024

Language: EN

© European Chemicals Agency, 2024
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

Reproduction is authorised provided the source is acknowledged.

Table of Contents

1 INTRODUCTION	8
1.1 Icons, abbreviations and terminology	8
2 REST API	11
2.1 Versioning scheme and retention policy	11
2.2 Submit a dossier	11
2.2.1 Request.....	11
2.2.2 Response.....	12
2.3 Get submission report.....	14
2.3.1 Request.....	14
2.3.2 Response.....	14
2.4 Get list of events.....	19
2.4.1 Request.....	19
2.4.2 Response.....	20
2.5 Submit by reference (simplified SCIP notifications).....	23
2.5.1 Request.....	23
2.5.2 Response.....	24
2.6 Disable submission (only for PCN)	25
2.6.1 Request.....	25
2.6.2 Response.....	26
3 SECURITY MODEL	28
3.1 General approach	28
3.2 HMAC-Signed JWT	29
3.2.1 Configuration	29
3.2.2 Usage	29
4 TESTING INSTRUCTIONS AND SWITCH TO PRODUCTION MODE	31
4.1 Main objectives	31
4.2 Test flags	31
4.3 Testing phases.....	32
4.3.1 Connectivity test	32
4.3.2 Integration test	33
4.4 Switching to production mode.....	34
ANNEX A LIST OF IMPLEMENTED VALIDATION RULES	35
ANNEX B RECOMMENDATIONS FOR SUCCESSFUL INTEGRATION	36
B.1 Performing submissions	36
B.2 Getting the submission report.....	37
B.3 Getting the list of events.....	37
ANNEX C EXAMPLES	38
C.1 JWT	38

C.1.1	Without expiration date	38
C.1.2	With expiration date	38
C.2	Submit a dossier	39
C.2.1	Request in "connectivity" test mode	39
C.2.2	Response in "connectivity" test mode	39
C.2.3	Request in "integration" test mode	39
C.2.4	Response in "integration" test mode	40
C.2.5	Request in "production" mode	40
C.2.6	Response in "production" mode	40
C.2.7	Request in "production" mode (CLP notification)	41
C.2.8	Sample request	41
C.3	Get submission report	42
C.3.1	Request in "connectivity" test mode	42
C.3.2	Response in "connectivity" test mode	42
C.3.3	Request in "integration" test mode	43
C.3.4	Response in "integration" test mode	43
C.3.5	Request in "production" mode	43
C.3.6	Response in "production" mode	44
C.3.7	Sample request	44
C.4	Get list of events	44
C.4.1	Request in "connectivity" test mode	44
C.4.2	Response in "connectivity" test mode	44
C.4.3	Request in "integration" test mode	45
C.4.4	Response in "integration" test mode	45
C.4.5	Request in "production" mode	46
C.4.6	Response in "production" mode	46
C.4.7	Sample request	46
C.5	Submit by reference (simplified SCIP notification)	46
C.5.1	Request in "connectivity" test mode	46
C.5.2	Response in "connectivity" test mode	47
C.5.3	Request in "integration" test mode	47
C.5.4	Response in "integration" test mode	47
C.5.5	Request in "production" mode	47
C.5.6	Response in "production" mode	48
C.5.7	Sample request	48
C.6	Disable submission	48
C.6.1	Request in "connectivity" test mode	48
C.6.2	Response in "connectivity" test mode	49
C.6.3	Request in "integration" test mode	49
C.6.4	Response in "integration" test mode	49
C.6.5	Request in "production" mode	50
C.6.6	Response in "production" mode	50
C.6.7	Sample request	50
C.7	Error responses	51
C.7.1	Legal entity not authorised by ECHA or JWT token is missing	51
C.7.2	JWT token malformed or expired	51
C.7.3	JWT token includes a wrong LE UUID	51
C.7.4	JWT token expired	52
C.7.5	Incorrect "test" Headers	52
ANNEX D	GUIDELINES FOR SUBMITTING A C&L NOTIFICATION	53
D.1	Group of manufacturers or importers (MI group)	53

D.2	Contact person	56
D.3	IUCLID format versions accepted in the S2S.....	58
ANNEX E HOW TO ONBOARD TO ECHA'S SYSTEM-TO-SYSTEM SERVICE.....		59
E.1	Step 1 – Request access to System-to-System service.....	59
E.2	Step 2 – Assign access roles.....	60
E.3	Step 3 – Create S2S keys.....	61
E.4	Step 4 – Test the implemented setup	64

Table of Figures

Figure 1: S2S integration scenario	30
Figure 2: "Manage group of manufacturers or importers" in REACH-IT menu.....	53
Figure 3: "Create new group" of manufacturers or importers in REACH-IT	54
Figure 4: Provide a group name during the creation of a new group of manufacturers or importers in REACH-IT	54
Figure 5: Manufacturers' or importers' group details and members in REACH-IT	54
Figure 6: Manufacturers or importers group help link in REACH-IT	55
Figure 7: Manufacturers or importers group help pages in REACH-IT	55
Figure 8: "Contacts" in REACH-IT menu.....	56
Figure 9: Managing contacts in REACH-IT	57
Figure 10: Viewing contact assignments and Contact UUID in REACH-IT.....	57
Figure 11 - Onboarding overview	59
Figure 12 - S2S request form	60
Figure 13 - ECHA Account S2S access right.....	61
Figure 14 - S2S Key management in ECHA accounts page	62
Figure 15 - Accepting T&Cs	63
Figure 16 - Key creation pop up window	63

List of Tables

Table 1: Terms and abbreviations	8
Table 2: Submit a dossier - Request parameters.....	11
Table 3: Submit a dossier - Response status codes	12
Table 4: Submit a dossier - Response payload.....	13
Table 5: Get submission report - Request parameters.....	14
Table 6: Get submission report - Response status codes	14
Table 7: Get submission report - Response payload	15
Table 8: Get list of events - Request parameters.....	19
Table 9: Get list of events - Response status codes	20
Table 10: Get list of events - Response payload.....	20
Table 11: Submit by reference - Request parameters	23
Table 12: Submit by reference - Response status codes.....	24
Table 13: Submit by reference - Response payload	24
Table 14: Disable submission - Request parameters	25
Table 15: Disable submission - Response status codes.....	26
Table 16: Disable submission - Response payload.....	26
Table 17: S2S configuration for industry	28
Table 18: JWT header	29
Table 19: HTTP Authorization header example (Bearer)	29
Table 20: Test flags in the HTTP Header	31
Table 21: Test flags per testing phase/scenario	32
Table 22: Recommendations - Performing submissions	36
Table 23: Recommendations - Getting the submission report.....	37
Table 24: Recommendations - Getting the list of events.....	37
Table 25: Roles required per S2S service (endpoint)	60

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 authentication and authorisation checks. This will be a precondition for the system-to-system integration.

In addition, the document explains the steps industry needs to take to start using the ECHA's S2S service (see Annex E for more details).



It should be noted that only certain submission types supported by the system-to-system submission services (i.e. PCN, SCIP and C&L notifications) and will pass the business checks, while any others will fail during their processing.

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 Base64URL encoded.
C&L	Classification and Labelling
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	<p>The portal used to submit Poison Centres (PCN) and SCIP notifications, which upon their successful processing and in case of no validation errors,</p> <ul style="list-style-type: none"> - are dispatched to the relevant market areas (PCN notifications) - are disseminated in the ECHA website (SCIP notifications)
IDP	<p>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.</p>
IUCLID	<p>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.</p>
JSON	<p>JSON (JavaScript Object Notation) is a lightweight data-interchange format.</p>
JWT	<p>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.</p>
Legal entity (LE)	<p>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.</p>
MI group	<p>Manufacturers and/or Importers group used in C&L notifications.</p> <p>Manufacturers / Importers who place a hazardous substance on the market will have to notify the classification and labelling of the substance to ECHA. Notifications can be done individually by a manufacturer or importer or by a group of them.</p>
PCN number	<p>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.</p>

Term or Abbreviation	Explanation
PSSI	<p>Persistent system sequence identifier is used to correlate different submissions pertaining to the same "thing", e.g. same mixture or article.</p> <ul style="list-style-type: none"> • For PCN, this is provided by the company in the submitted dossier and called PCN number; • For SCIP, this is generated by the portal for the first submission of an article notification and called SCIP number; updates get assigned the same SCIP number as their first initial successful submission.
REACH-IT	The IT system used to submit REACH and CLP dossiers, including C&L notifications.
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 by the same notifying Company in subsequent submissions of the same article in order to be considered as an update.
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	<p>It is used to represent an Industry software system integrating with the ECHA Submission portal and will be defined as follows:</p> <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 <p>System accounts will be managed in ECHA Accounts</p> <p>A single system account will exist per LE.</p>



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 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 Versioning scheme and retention policy

Whenever the ECHA Submission portal introduces changes in the exposed REST API, it ensures backwards compatibility so that it gives sufficient time to companies to upgrade. This is achieved by supporting the last two versions of the API in parallel, i.e. the previous one available (for 1 year) and the new API version. The previous version always remains intact in terms of request parameters and the URL it is available by, while the new API version is provided through a different URL indicating its version. Assuming that the current version is v3, the new version is v4 and provided through <https://api.ecs.echa.europa.eu/submission/v4>.

In terms of description:

- Whenever an endpoint is altered, the tables describing its parameters are further expanded with two additional columns, the first to cover the previous version (e.g. v3), the second to provide details about the new version (v4);
 - The URLs of both versions are provided for all exposed services.
-  Companies are recommended to upgrade the soonest possible to the new API version and benefit from the latest offered features.
-  v2 is decommissioned after the release of v4.
v3 will be decommissioned 1 year after the release of v4.

2.2 Submit a dossier


This service is used to perform direct system-to-system submissions to ECHA . 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 [C.2 Submit a dossier].

2.2.1 Request

Table 2: Submit a dossier - Request parameters

Request Param	Description
Request URL	The request URL to submit the dossier, i.e. v3: https://api.ecs.echa.europa.eu/submission/v3 v4: https://api.ecs.echa.europa.eu/submission/v4
Request method	POST
Content-Type	application/vnd.iuclid6.archive; filename=<dossier-filename>.i6z

Request Param	Description
Accept	application/json, text/plain, */*
Authorisation	This needs to be completed as described in [3. Security model], e.g. Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
X-ECHA-MI-Group-Id	Manufacturers or importers group UUID optionally provided (whenever a MI group applies) for C&L notifications (supported as of v3)
X-ECHA-Contact-Id	Contact UUID always required for C&L notifications (supported as of v3)
X-Correlation-Id	<p>Industry provided optional identifier, which may be used to correlate submission requests between the company system and the ECHA Submission portal. The correlation identifier is returned through the list of events (see [2.4.2 Response]).</p> <p>This must be always provided in lower case, digits being allowed, while special characters must be avoided (with the exception of '-'), otherwise, it causes a HTTP 400 – Bad request response.</p>
X-ECHA-Legislation	<p>The submitted dossier's legal context (supported as of v4), which may take one of the following values:</p> <ul style="list-style-type: none"> - CLP_PCN for PCN notifications - SCIP for SCIP notifications - CLP_NOTIF for CLP notifications <p>Although this information exists in the submitted dossier, ECHA Submission portal needs it prior to its processing in order to assign the relevant priority.</p> <p> It this value does not match with the content of the dossier the submission will be failed.</p>

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

2.2.2 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
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 [C.7 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. v3: <a href="https://api.ecs.echa.europa.eu/submission/v3/<submission-number>">https://api.ecs.echa.europa.eu/submission/v3/<submission-number> (in case the request was made in v3) v4: <a href="https://api.ecs.echa.europa.eu/submission/v4/<submission-number>">https://api.ecs.echa.europa.eu/submission/v4/<submission-number> (in case the request was made in v4)	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. v3: <a href="https://ecs.echa.europa.eu/cloud/submissions/v3/<submission-number>">https://ecs.echa.europa.eu/cloud/submissions/v3/<submission-number> (in case the request was made in v3) v4: <a href="https://ecs.echa.europa.eu/cloud/submissions/v4/<submission-number>">https://ecs.echa.europa.eu/cloud/submissions/v4/<submission-number> (in case the request was made in v4)	Yes

-  In case of CLP notifications, the link to the REACH-IT submission report can be retrieved either by accessing REACH-IT directly or by accessing the ECHA Submission portal's submission report (according to the *reportUrl* returned above).

2.3 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, link to submission report

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

2.3.1 Request

Table 5: Get submission report – Request parameters

Request Param	Description
Request URL	The request URL including the submission number as a required path parameter, i.e. v3: <a href="https://api.ecs.echa.europa.eu/submission/v3/<submission-number>">https://api.ecs.echa.europa.eu/submission/v3/<submission-number> v4: <a href="https://api.ecs.echa.europa.eu/submission/v4/<submission-number>">https://api.ecs.echa.europa.eu/submission/v4/<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.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MzIyODUyLjFkXwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c

2.3.2 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

Status	Description
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 [C.7 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	
		v3	v4
submissionNumber	The submission number of this submission, e.g. "AAD678032-54"	Yes	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 portal - 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 in case of PCN submissions, or disseminated in case of SCIP submissions - VALIDATION_FAILED indicates that the submission has failed the validation checks (i.e. at least one submission rule has failed) and as a result the submitted dossier will not be dispatched to the target market areas in case of PCN submissions, or disseminated in case of SCIP submissions 	Yes	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	Yes
dossierUuid	The submitted IUCLID dossier UUID e.g. "20b78cc8-2594-4d12-b4b9-a4b5e5ab2cff"	No	No
submittedFilename	The specified IUCLID dossier filename during the submission e.g. myDossier.i6z	No	No
refType	The type of identifier used to correlate this submission with other/previous submissions for the same	n/a ¹	n/a ²

¹ n/a indicates that the element has been removed in the relevant version

Element	Description	Required	
		v3	v4
	substance/mixture/article, i.e. <ul style="list-style-type: none"> - For PCN dossier "PCN_NUMBER" is the only applicable value - For SCIP dossier, Primary article identifier, "catalogue number" or "GTIN (Global Trade Item Number)" are two examples of the applicable types. 		
refValue	The value of the identifier used (see also above) e.g. "e1131d0b-781f-4427-9a43-f5189dcb7918"	n/a	n/a
validations	In case of failed validation checks, this includes a list of identified validation failures (warnings or errors), e.g. <pre>[{ "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" }]</pre> Where <ul style="list-style-type: none"> - "level" indicates the error level of this validation rule and may take the following values: <ol 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 	Yes	Yes
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.	Yes	Yes

Element	Description	Required	
		v3	v4
	https://ecs.echa.europa.eu/cloud/submissions/<submission-number>		
events	<p>A list of events related to this submission in the following structure:</p> <pre>[{ "eventType": "SUBMITTED", "eventData": {}, "timestamp": "2020-04-08T07:55:05.362305+03:00" }, { "eventType": "PASSED", "eventData": {}, "timestamp": "2020-04-08T07:55:07.089871+03:00" }, { "eventType": "DISPATCHED", "eventData": { "recipients": "FI,GR,BE" }, "timestamp": "2020-04-08T07:55:15.379869+03:00" }, { "eventType": "DOWNLOADED", "eventData": { "country": "FI" }, "timestamp": "2020-05-22T09:52:45.939339+03:00" }]</pre> <p>See also [2.4 Get list of events]</p>	Yes	Yes
pssi	<p>The so-called Reference number, which stands for:</p> <ul style="list-style-type: none"> - The PCN number for PCN dossiers - The SCIP number for SCIP dossiers - An identifier generated by the ECHA Submission portal for CLP notifications for correlation purposes (may be ignored by the Industry systems). The REACH-IT Reference number is returned by the <i>identifiers</i> elements, see next item 	No	No
identifiers	<p>A list of identifiers extracted from the submitted dossier:</p> <ul style="list-style-type: none"> - For PCN dossiers, it includes the UFIs as follows: <pre>[{ "label": "Unique formula identifier (UFI)", "value": "W000-A0PG-U00U-2K6S", "other": {} }, { "label": "Unique formula identifier (UFI)", "value": "GJA0-K0KA-H00Q-EK9M", "other": {} }]</pre> 	Yes	Yes

Element	Description	Required	
		v3	v4
	<ul style="list-style-type: none"> - For SCIP dossiers, it includes the main/root Article primary identifier as shown below: <pre>[{ "label": "serial number", "value": "131313", "other": {} }]</pre> - For CLP notifications, it includes the REACH-IT Reference number as shown below: <pre>[{ "label": "Reference number", "value": "02-2114090355-48-0000", "other": {} }]</pre> 		
variant	<p>The element indicating the type of submission:</p> <ul style="list-style-type: none"> - DOSSIER: submission performed through a submitted dossier - SBR: submission performed as simplified SCIP notification - DISABLE (as of v4): submission concerns a request to disable another submission. Previous versions of the API do not return at all DISABLE submissions. 	Yes	Yes
referencedPssi	In case of SBR (refers to SSNs), it returns the referenced PSSI (SCIP number used to submit the SSN) included in the submission.	No	No
disabled	<p>Indicates whether the submission has been disabled or not:</p> <ul style="list-style-type: none"> - true: submission has been disabled - false: submission is active 	n/a	No
disableReason	<p>Applicable only to DISABLE variants, indicates the reason for disabling the submission and is one of the following:</p> <ul style="list-style-type: none"> - DISABLE_BY_MISTAKE: Submission made unintentionally - DISABLE_WRONG_COMPANY: Submission made by a wrong company - DISABLE_WRONG_INFO: Submitted dossier contains wrong information - DISABLE_TEST_DATA=Submitted dossier contains test data 	n/a	No
referencedSubmission	Applicable only to DISABLE variants, indicates the submission number to be disabled, e.g. RMH431110-36	n/a	No

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



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.
- C&L notifications failing the IUCLID file format checks will not be visible in REACH-IT.

In some cases (when the system is under load), it is possible that the submission report returns 404, when the request is made shortly after the dossier submission. For this purpose, it is recommended that Industry systems get the list of events (as described in 2.4) and when the status of the submission is final (VALIDATION_SUCCEEDED or VALIDATION_FAILED), they may get the submission report, which includes additional information.



2.4 Get list of events

This service is used to retrieve events related to submissions made by a company. It is typically performed after the submission of one or more dossier and can be used for the following purposes:

- To track the submission status of multiple submissions using a single call as an alternative of issuing multiple calls to the "Get submission report" per submitted dossier.
- To track the download status of PCN dossiers, which are dispatched and downloaded by the ABs. This information is not currently available in the "Get submission report".

Sample request/response pairs are provided in [C.4 Get list of events].

2.4.1 Request

Table 8: Get list of events – Request parameters

Request Param	Description
Request URL	The request URL including the offset and limit as optional query parameters, i.e. v3: <a href="https://api.ecs.echa.europa.eu/submission/v3/events?offset=<offset>&limit=<limit>">https://api.ecs.echa.europa.eu/submission/v3/events?offset=<offset>&limit=<limit> v4: <a href="https://api.ecs.echa.europa.eu/submission/v4/events?offset=<offset>&limit=<limit>">https://api.ecs.echa.europa.eu/submission/v4/events?offset=<offset>&limit=<limit> where: <ul style="list-style-type: none"> • offset (default value is '0'): it defines the starting event • limit (default value is '1000'): it defines the maximum number of events returned in the response. When not provided or provided value exceeds '1000', the default value applies.
Request method	GET
Accept	application/json, text/plain, */*
Authorization	This needs to be completed as described in [3. Security model], e.g. Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MzE1MjM1MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c

2.4.2 Response

Table 9: Get list of events – Response status codes

Status	Description
200	The service is found and the response includes the list of events
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, offset or limit parameters less than 0
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 [C.7 Error responses].

The response in JSON format includes one entry per event related to a submission, while the order of events provided in the response is by ascending offset.



Table 10: Get list of events - Response payload

Element	Description	Required
Submission ID	The submission number of this submission, e.g. "AAD678032-54"	Yes

Element	Description	Required v4
c	The dossier type of the related submitted dossier, e.g. CLP_PCN, SCIP, CLP_NOTIF	No
e	The type of the event, one of <ul style="list-style-type: none"> - SUBMITTED - PASSED - FAILED - DISPATCHED - DOWNLOADED - DISABLED (as of v4, not returned in previous version of the API) 	Yes
e	It is populated in certain cases, i.e. <ul style="list-style-type: none"> - for DISPATCHED events to include the list of recipient countries, e.g. "eventData": {"recipients": "FI,DE"} - for DOWNLOADED events to include information on countries that have downloaded the submitted dossier, e.g. "eventData": {"country": "FI"}. One country per event is included. 	Yes
t	The timestamp when the event was generated e.g. "2007-12-03T10:15:30+01:00"	Yes
c	The "position" of this event in the list	Yes


E I r e r t	Description	Required v v4 :
s e t		
s t a t u s	<p>The URL to retrieve the submission report through the S2S using the submission number, i.e.</p> <p>v3: <a href="https://api.ecs.echa.europa.eu/submission/v3/<submission-number>">https://api.ecs.echa.europa.eu/submission/v3/<submission-number> (in case the request was made in v1)</p> <p>v4: <a href="https://api.ecs.echa.europa.eu/submission/v4/<submission-number>">https://api.ecs.echa.europa.eu/submission/v4/<submission-number> (in case the request was made in v2)</p>	Y e s
U r l I d e n t i f i c a t o r	<p>The submitted IUCLID dossier UUID e.g. "20b78cc8-2594-4d12-b4b9-a4b5e5ab2cff"</p>	N o
U r l I d e n t i f i c a t o r	<p>The so-called Reference number, which stands for:</p> <ul style="list-style-type: none"> - The PCN number for PCN dossiers - The SCIP number for SCIP dossiers - An identifier generated by the ECHA Submission portal for CLP notifications for correlation purposes (may be ignored by the Industry systems) 	N o
I n d i c a t o r	<p>This flag indicates whether a successful (PASSED) submission has failed any quality rules. In case it is 'true', it serves as an indication that the relevant submission report should be fetched by the Industry system in order to identify the rules that failed.</p>	N o
I n d i c a t o r	<p>It returns the correlation identifier value provided in the submission request (see [2.2.1 Request])</p>	N o

E l e m e n t	Description	Required
a t t r i b u t e		v4 :

-  ECHA Submission portal does not perform any offset book-keeping; it is the client’s responsibility to keep track of the event offsets already consumed.
-  It is possible that the “same” event type (e.g. DISPATCHED) related to one submission is received more than once. In such cases, the former event should be considered as containing the correct timestamp.

2.5 Submit by reference (simplified SCIP notifications)

This service is used to submit a list of Reference numbers as an alternative of submitting a physical file/dossier; the service currently supports the simplified SCIP notifications (SSN) and expects a list of valid SCIP numbers. Please see following website for additional information: <https://echa.europa.eu/scip-support>

-  Ensure that the SCIP number you are providing has not been already provided by the same Legal Entity in the context of another SSN.

Sample request/response pairs are provided in [C.5 Submit by reference (simplified SCIP notification)].

2.5.1 Request

Table 11: Submit by reference – Request parameters

Request Param	Description
Request URL	The request URL to submit by reference v3: https://api.ecs.echa.europa.eu/submission/v3/sbr v4: https://api.ecs.echa.europa.eu/submission/v4/sbr
Request method	POST
Accept	application/json, text/plain, */*

Request Param	Description
Authorization	This needs to be completed as described in [3. Security model], e.g. Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
(list of SCIP numbers)	This should be provided in the body and include the list of PSSI numbers (list of SCIP numbers, the SSN is made for), e.g. ["ff89396f-3974-4888-8791-bef8bad67698","c4a422e1-5aa7-44d7-b9ea-c3ca11fae2e9"]

2.5.2 Response

Table 12: Submit by reference – Response status codes

Status	Description
202	The provided list of SCIP numbers has been submitted and the response includes the status of each of them.
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
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 [C.7 Error responses].

The response in JSON format includes the information described below.

Table 13: Submit by reference - Response payload

Element	Description	Required
submissionRequests	A list including the response per provided PSSI number (SCIP number), where each entry includes the following:	Yes

status	The status of the submission request, i.e. <ul style="list-style-type: none"> • SUBMITTED indicates that the submission has been performed successfully • FAILED indicates that the submission has not been performed 	Yes
submissionNumber	The Submission number generated for the provided <i>referencedPssi</i> , e.g. "AAD678032-54"	No
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/v4/<submission-number>">https://api.ecs.echa.europa.eu/submission/v4/<submission-number>	No
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/v4/<submission-number>">https://ecs.echa.europa.eu/cloud/submissions/v4/<submission-number>	No
referencedPssi	The PSSI the submission refers to, e.g. 38843e3e-60ce-458a-bf7b-3289fb272402	Yes

2.6 Disable submission (only for PCN)

This service is used to disable the latest succeeded and non-disabled submission performed in the context of one PCN number. It should be used by PCN notifiers whenever they realise that the submission contains invalid information and cannot be corrected through an updated submission (like errors in the mixture composition).

Sample request/response pairs are provided in [C.6 Disable submission].

2.6.1 Request

Table 14: Disable submission – Request parameters

Request Param	Description
Request URL	The request URL to disable the last succeeded submission submit by reference, i.e. (supported as of v4) v4: <a href="https://api.ecs.echa.europa.eu/submission/v4/<pssi>/disable">https://api.ecs.echa.europa.eu/submission/v4/<pssi>/disable <u><pssi>: this should be replaced by the PCN number, for which that last succeeded non-disabled submission will be disabled.</u>
Request method	POST
Accept	application/json, text/plain, */*

Request Param	Description
Authorization	This needs to be completed as described in [3. Security model], e.g. Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
{"reason": "<REASON>"}	This should be provided in the body and indicate the reason for disabling the selected submission. One of the following reasons has to be provided: <ul style="list-style-type: none"> - <i>DISABLE_BY_MISTAKE</i>: Submission made unintentionally - <i>DISABLE_WRONG_COMPANY</i>: Submission made by a wrong company - <i>DISABLE_WRONG_INFO</i>: Submitted dossier contains wrong information - <i>DISABLE_TEST_DATA</i>: Submitted dossier contains test data <p>Example: {"reason": "DISABLE_BY_MISTAKE"}</p>

2.6.2 Response

Table 15: Disable submission – Response status codes

Status	Description
202	The request to disable one submission has been submitted and the submission number of the request 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
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 [C.7 Error responses].

The response in JSON format includes the information described below.

Table 16: Disable submission - Response payload

Element	Description	Required
submissionNumber	The submission number generated upon submitting the Disable, e.g. "AAD678032-54"	Yes
statusUrl	The URL to retrieve the submission report through the S2S using the submission number, i.e. v4: <a href="https://api.ecs.echa.europa.eu/submission/v4/<submission-number>">https://api.ecs.echa.europa.eu/submission/v4/<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. v4: <a href="https://ecs.echa.europa.eu/cloud/submissions/v4/<submission-number>">https://ecs.echa.europa.eu/cloud/submissions/v4/<submission-number>	Yes

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 (see further details in Annex E. How to onboard to ECHA's System-to-System 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)

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.
- Multiple system accounts per legal entity will be supported, so it will be possible to have "personal" keys per company (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 personal 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 three entries per LE:

Table 17: S2S configuration for industry

Property	Description
Username	The username of the S2S account (from the ECHA Accounts)
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 username (of the system account), 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 Base64URL 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 18: JWT header

```
{
  "alg": "HS256",
  "typ": "JWT"
}
.
{
  "sub": "<username>",
  "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 [C.1 JWT].

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

Table 19: HTTP Authorization header example (Bearer)

```
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.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):

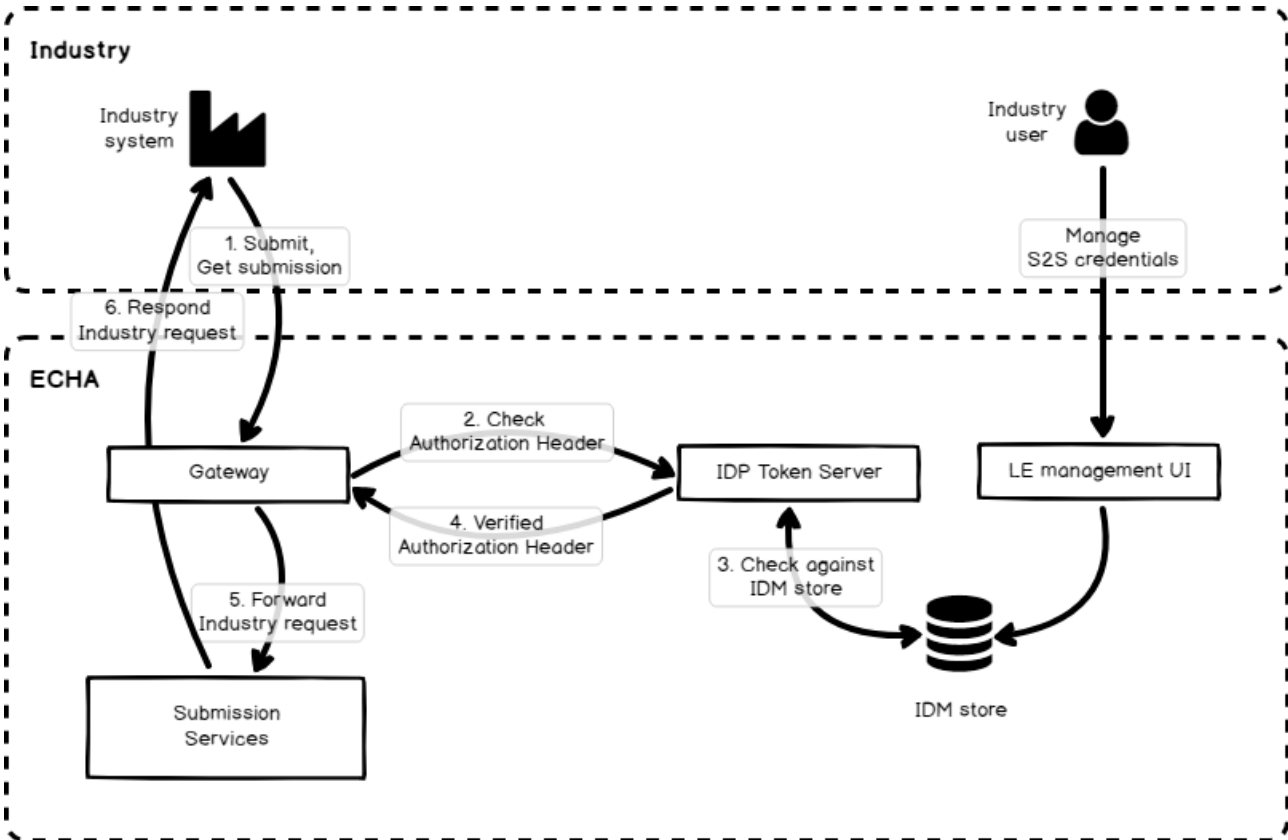


Figure 1: S2S integration scenario

! In order to ensure backwards compatibility with the previous tokens (generated at the Legal entity level), the S2S service accepts those ones as well, provided that they are valid and have not expired. However, it is not possible to manage them through the ECHA Accounts user interface any longer.

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 in every request performed by the industry system:

Table 20: Test flags in the HTTP Header

Request Param	Description
X-ECHA-Mode	<p>HTTP Header to indicate the mode of operation, i.e.</p> <ul style="list-style-type: none"> - X-ECHA-Mode=test while testing; - X-ECHA-Mode must be omitted when switching to Production mode. <p>⚠ In case it is provided and takes a value other than "test", it causes a 400 - Bad request.</p>
X-ECHA-Test-Run	<p>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.</p> <p>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.</p> <p>⚠ This must be only provided when X-ECHA-Mode=test, otherwise it causes a 400 - Bad request.</p> <p>⚠ This must be always provided in lower case, digits being allowed, while special characters must be avoided (with the exception of '-'), otherwise, the submission report is not visible through the ECHA Submission portal.</p>

The aforementioned test flags should be used as follows:

Table 21: Test flags per testing phase/scenario

X-ECHA-Mode	X-ECHA-Test-Run	Testing phase/purpose
test	(absent)	Connectivity tests <ul style="list-style-type: none"> - no actual processing of the submitted file - dummy responses
test	(absent)	Authentication and authorisation tests <ul style="list-style-type: none"> - no actual processing of the submitted file - dummy responses
test	mycompanyid-001 (example)	Integration tests <ul style="list-style-type: none"> - actual processing of the submitted file - actual response
(absent)	(absent)	Production mode <ul style="list-style-type: none"> - 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 list of events" request

7. ECHA Submission portal identifies that this is a "test" call and provides a dummy response
8. Industry system performs a "Get submission report" request by providing a submission number (the one received in step 4)
9. ECHA Submission portal identifies that this is a "test" call and provides a dummy response
10. 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 be dispatched to the ABs in the case of PCN dossiers and will not be disseminated to the ECHA website in the case of C&L and SCIP article notifications.

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 list of events" request
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
8. Industry system performs a "Get submission report" request by providing a submission number (the one received in step 4)
9. 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
10. 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 necessary. When the integration tests have been completed successfully, the industry system may switch to Production mode.

Any submission performed in the context of the integration tests is visible in the ECHA Submission portal Trial. 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 [2.2.2] and [2.3.2]).

For test runs, the URL is scoped to the test run identifier, with each test run effectively defining a separate “virtual” subdomain.

- ! The ECHA Submission portal and its Trial version should be solely used for integration testing purposes. Other types of testing like load, stress, security, penetration testing are responsibility of the companies and should be performed in their own test infrastructure.

4.4 Switching to production mode

Once the testing phases have been successfully concluded, 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 list of events” request
7. ECHA Submission portal identifies that this is a “real” call, so it processes the request and provides a response
8. Industry system performs a “Get submission report” request by providing a submission number (the one received in step 4)
9. ECHA Submission portal identifies that this is a “real” call, so processes the request and provides a response including any validation errors
10. Industry system receives and processes the response

Annex A List of implemented validation rules

- **Poison centres notifications:** The validation rules implemented for PCN are available on the dedicated Poison Centres Notification format page: [PCN Validation rules annex](#)
- **SCIP notifications:** The validation rules implemented for SCIP are available on the dedicated SCIP support webpage, [Validation rules for SCIP notifications](#)
- **CLP notifications:** The validation rules implemented for CLP notifications are available on the dedicated C&L notifications section within the System-to-system submission service, [Validation rules for CLP notifications](#)

Annex B Recommendations for successful integration

This annex provides some recommendations to ensure the optimum integration between the Industry systems and the ECHA Submission portal. Apart from the main flows, it addresses some exceptional situations (e.g. slow response times, system becomes unresponsive, etc.), which the Industry systems are expected to handle.

B.1 Performing submissions

Table 22: Recommendations – Performing submissions

#	Description
1.	Avoid the submission of big volumes in peak hours, which are between 10.00 and 17.00 Helsinki time. S2S submissions pose additional load to the system on the top of the user activity, such as manual submissions in the ECHA Submission portal and the use of the ECHA Cloud services (IUCLID instances).
2.	Wait until you get a response from the ECHA Submission portal and do not abort the connection. Set a sufficiently long timeout in your requests (e.g. 30sec or 1min), allowing ECHA Submission portal to respond when the system is heavily used.
3.	Do not set an unlimited number of retries when submitting, instead set a small and configurable number of retries (e.g. 2 retries).
4.	Avoid consecutive submission retries without allowing a sufficient time to receive a response, instead retry after 1hour and if that fails, try the next day. When the maximum number of retries is exhausted, contact ECHA.
5.	Avoid submitting all the dossiers in one go. It is preferable to send in batches and verify the status of submissions before moving on with the next batch. This ensures that Industry systems do not have a large amount of submissions failing for the same reason, while the issue could have been spotted since the first failure.
6.	Avoid fully unattended submissions, monitor your systems and block further automated submissions when a threshold of failed submissions is reached.
7.	Avoid the resubmission (e.g. the same file or an updated file) when the reason for failure of a previous submission pertaining to the same entity (PCN mixture or SCIP Article) has not been identified. It is possible that the new dossier will fail once more due to the same reason.
8.	Differentiate between technical and business errors (BR failures), since the corrective actions are different (e.g. the first one may relate to connectivity/technical issues, the latter to information requirements).
9.	Classify differently the response codes and retry when the status code indicates a recoverable situation, e.g. HTTP 500 indicates a server error, so need to retry in such cases, while HTTP 400 indicates a Bad request that will also fail in subsequent retries.
10.	Failed submissions indicate a final status and requires human intervention in most of the cases for the correction of data. Do not automatically retry in such cases and check the error message given first.

#	Description
11.	Avoid unnecessary submissions, ensure the quality of the data before submitting your notification (e.g. by validating 'representative' dossiers) and avoid submitting updates to correct minor mistakes.
12.	If you are submitting an SSN, ensure that the SCIP number you are providing has not been already provided by the same Legal Entity in the context of another SSN.

B.2 Getting the submission report

Table 23: Recommendations – Getting the submission report

#	Description
1.	Avoid polling for getting the submission report to identify the status of each submission, instead get the list of events related to your submissions (where the submission status is also depicted).
2.	Get the submission report when the status is final (either successful or failed) in order to fetch the information related to this submission. Submission reports for pending submissions (being processed) do not include dossier information.

B.3 Getting the list of events

Table 24: Recommendations – Getting the list of events

#	Description
1.	Prefer getting the list of events to determine the submission status since each event conveys the submission status information.
2.	Polling for events should have a different configuration to the submission service. Polling may be continuously performed without any upper limit on a scheduled basis. The schedule is to be defined by the Industry systems depending on the number of submissions they perform (e.g. could be 1 min, 1hour, 6 hours, 1day).
3.	During periods of high levels of activity, you may experience longer processing times, during which the submissions will appear with pending status. As a result, polling should continue until the final status of the relevant submissions is shown. If certain submission still appear as pending after a period (few days), contact ECHA via the ECHA Contact form providing the necessary details (LE UUID, submission number).

Annex C Examples

C.1 JWT

C.1.1 Without expiration date

Optional `typ` is provided

```
{
  "alg": "HS256",
  "typ": "JWT"
}
.
{
  "sub": "s2s-user",
  "x-echa-party": "ECHA-83a626b4-1d12-4a39-9832-20c97c1fba4d"
}
```

Optional `typ` is not provided

```
{
  "alg": "HS256"
}
.
{
  "sub": "s2s-user",
  "x-echa-party": "ECHA-83a626b4-1d12-4a39-9832-20c97c1fba4d"
}
```

C.1.2 With expiration date

```
{
  "alg": "HS256"
}
.
{
  "sub": "s2s-user",
  "x-echa-party": "ECHA-83a626b4-1d12-4a39-9832-20c97c1fba4d",
  "exp": 1601471928
}
```

C.2 Submit a dossier

C.2.1 Request in "connectivity" test mode

Request Param	Description
Request URL	https://api.ecs.echa.europa.eu/submission/v4
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.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTlkMTItNGEzOS05ODMyLTIwYzYzYzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11UUKai3fX4
X-ECHA-Legislation	CLP_PCN

C.2.2 Response in "connectivity" test mode

Response
<pre>{ "submissionNumber": "AAD678032-54", "statusUrl": "https://api.ecs.echa.europa.eu/submission/v4/AAD678032-54", "reportUrl": "https://ecs.echa.europa.eu/cloud/submissions/AAD678032-54 ?leUuid=ECHA-83a626b4-1d12-4a39-9832-20c97c1fba4d" }</pre>

C.2.3 Request in "integration" test mode

Request Param	Description
Request URL	https://api.ecs.echa.europa.eu/submission/v4
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

Request Param	Description
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTfkMTItNGEzOS05ODMyLTIwYzYzYzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11UUKai3fX4
X-ECHA-Legislation	CLP_PCN

C.2.4 Response in "integration" test mode

Response
<pre>{ "submissionNumber": "RMH562417-19", "statusUrl": "https://api.ecs.echa.europa.eu/submission/v4/RMH562417-19", "reportUrl": "https://test-mycompanyid-run001.ecs.echa.europa.eu/cloud/submissions/RMH562417-19?leUuid=ECHA-83a626b4-1d12-4a39-9832-20c97c1fba4d " }</pre>

C.2.5 Request in "production" mode

Just omit both X-ECHA-Mode and X-ECHA-Test-Run from the Request Parameters.

Request Param	Description
Request URL	https://api.ecs.echa.europa.eu/submission/v4
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.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTfkMTItNGEzOS05ODMyLTIwYzYzYzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11UUKai3fX4

C.2.6 Response in "production" mode

Response
<pre>{ "submissionNumber": "RMH562417-19", "statusUrl": "https://api.ecs.echa.europa.eu/submission/v4/RMH562417-19", "reportUrl": "https://ecs.echa.europa.eu/cloud/submissions/RMH562417-19?leUuid=ECHA-83a626b4-1d12-4a39-9832-20c97c1fba4d" }</pre>

C.2.7 Request in “production” mode (CLP notification)

Sample request for CLP notification including the relevant HTTP headers for MI Group and Contact person.

Request Param	Description
Request URL	https://api.ecs.echa.europa.eu/submission/v4
Request method	POST
Content-Type	application/vnd.iuclid6.archive; filename=clp-dossier.i6z (<i>sent as multipart/form-data</i>)
Accept	application/json, text/plain, */*
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTZkMTItNGEzOS05ODMyLTlwYzYzYzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11UUKai3fX4
X-ECHA-MI-Group-Id	66534afc-1af0-493b-9065-3f927690c1d2
X-ECHA-Contact-Id	0d5953ef-680b-43ed-985a-e5dc4be8420b
X-ECHA-Legislation	CLP_NOTIF

C.2.8 Sample request

Sample request
<pre> POST https://api.ecs.echa.europa.eu/submission/v4 HTTP/1.1 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTZkMTItNGEzOS05ODMyLTlwYzYzYzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11UUKai3fX4 X-ECHA-Mode: test X-ECHA-Legislation: CLP_PCN Content-Type: application/vnd.iuclid6.archive; filename=initial_dossier.i6z Accept: application/json Host: api.ecs.echa.europa.eu Accept-Encoding: gzip, deflate Content-Length: 72859 Connection: keep-alive -----=_Part_0_934668894.1612436191150 Content-Type: application/octet-stream; name=SCIPDossierFile1.i6z Content-Transfer-Encoding: binary Content-Disposition: form-data; name="SCIPDossierFile1.i6z"; filename="SCIPDossierFile1.i6z" <the binary content...> </pre>

C.3 Get submission report

C.3.1 Request in "connectivity" test mode

Request Param	Description
Request URL	https://api.ecs.echa.europa.eu/submission/v4/AAD678032-54
Request method	GET
Accept	application/json, text/plain, */*
X-ECHA-Mode	test
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4bWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTFFkMTItNGEzOS05ODMyLTlwYzYzYzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11UUKai3fX4

C.3.2 Response in "connectivity" test mode

Response
<pre>{ "submissionNumber": "AAD678032-54", "status": "VALIDATION_SUCCEEDED", "submissionDate": "2022-06-08T10:04:00.301182+03:00", "dossierUuid": "10319994-41c0-4d3c-b810-94ecf432137e", "submittedFilename": "10319994-41c0-4d3c-b810-94ecf432137e.i6z", "validations": [{ "level": "WARN", "code": "QLT507", "context": "Classification and labelling information.001, Classification of the mixture and label elements" }], "reportUrl": "https://api.ecs.echa.europa.eu/cloud/submissions/RMH645371-08?leUuid=ECHA-dfba30d1-ae5f-4450-83c0-4b258aba4125", "events": [{ "eventType": "SUBMITTED", "eventData": {}, "timestamp": "2022-06-08T10:04:00.301182+03:00" }, { "eventType": "PASSED", "eventData": {}, "timestamp": "2022-06-08T10:04:01.692840092+03:00" }, { "eventType": "DISPATCHED", "eventData": {"recipients": "FI,GR,BE,AT,BG"}, "timestamp": "2022-06-08T10:04:45.036+03:00" }, { "eventType": "DISABLED", </pre>

Response

```

    "eventData": {},
    "timestamp": "2022-06-08T10:18:50.413746655+03:00"
  }
],
"pssi": "84565abd-1c33-491e-8226-5280b7c31c3b",
"identifiers": [ {
  "label": "CLP unique formula identifier (UFI)",
  "value": "CQ37-NCKQ-G001-TV56",
  "other": {}
}],
"variant": "DOSSIER",
"disabled": true
}

```

C.3.3 Request in "integration" test mode

Request Param	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.eyJ4bG9jaGEtcGFydHkiOiJFQ0hBLTgzYTUyNmI0LTZkMTItNGEzOS05ODMyLTIwYzYzYzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11Uukai3fX4

C.3.4 Response in "integration" test mode

Same as in C.3.2

C.3.5 Request in "production" mode

Just omit both X-ECHA-Mode and X-ECHA-Test-Run from the Request Parameters and provide a valid submission number submitted by your company.

Request Param	Description
Request URL	https://api.ecs.echa.europa.eu/submission/RMH652909-13
Request method	GET
Accept	application/json, text/plain, */*
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4bG9jaGEtcGFydHkiOiJFQ0hBLTgzYTUyNmI0LTZkMTItNGEzOS05ODMyLTIwYzYzYzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11Uukai3fX4

C.3.6 Response in “production” mode

Same as in C.3.2

C.3.7 Sample request

```

Sample request

GET https://api.ecs.echa.europa.eu/submission/RMH652909-13 HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LT
FkMTItNGEzOS05ODMyLTIwYzYzYzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11U
Ukai3fX4
X-ECHA-Mode: test
Accept: application/json, text/plain, */*
Host: api.ecs.echa.europa.eu
Accept-Encoding: gzip, deflate
Connection: keep-alive

```

C.4 Get list of events

C.4.1 Request in “connectivity” test mode

Request Param	Description
Request URL	https://api.ecs.echa.europa.eu/submission/v4/events?offset=0
Request method	GET
Accept	application/json, text/plain, */*
X-ECHA-Mode	test
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LT FkMTItNGEzOS05ODMyLTIwYzYzYzFmYmE0ZCJ9.Q Nkrbc_eUeKA7k2i4DV8IRifaub1XjsG11UUkai3fX4

C.4.2 Response in “connectivity” test mode

```

Response

[
  {
    "submissionNumber": "AAD678032-54",
    "eventType": "SUBMITTED",
    "eventData": {},
    "timestamp": "2020-04-13T08:27:56.756322+03:00",
    "offset": 0,
    "statusUrl": "https://api.ecs.echa.europa.eu/submission/v4/AAD678032-54"
  },
  {
    "submissionNumber": "AAD678032-54",
    "dossierType": "CLP_PCN",
    "eventType": "PASSED",

```

Response

```

"eventData": {},
"timestamp": "2020-04-23T08:27:56.756322+03:00",
"offset": 1,
"statusUrl": https://api.ecs.echa.europa.eu/submission/v4/AAD678032-54,
"dossierUuid": "bc4a478d-73f8-4193-ae37-783123cf34ad",
"pssi": "f17532c0-5caf-4689-8db7-e2474b2a42d6"
},
{
"submissionNumber": "AAD678032-54",
"dossierType": "CLP_PCN",
"eventType": "DISPATCHED",
"eventData": {"recipients": "DE,FI,GR"},
"timestamp": "2020-05-03T08:27:56.756322+03:00",
"offset": 2,
"statusUrl": "https://api.ecs.echa.europa.eu/submission/v4/AAD678032-54",
"dossierUuid": "bc4a478d-73f8-4193-ae37-783123cf34ad",
"pssi": "f17532c0-5caf-4689-8db7-e2474b2a42d6"
},
{
"submissionNumber": "AAD678032-54",
"dossierType": "CLP_PCN",
"eventType": "DOWNLOADED",
"eventData": {"country": "DE"},
"timestamp": "2020-05-08T08:27:56.756322+03:00",
"offset": 3,
"statusUrl": "https://api.ecs.echa.europa.eu/submission/v4/AAD678032-54",
"dossierUuid": "bc4a478d-73f8-4193-ae37-783123cf34ad",
"pssi": "f17532c0-5caf-4689-8db7-e2474b2a42d6"
}
]

```

C.4.3 Request in "integration" test mode

Request Param	Description
Request URL	https://api.ecs.echa.europa.eu/submission/events?offset=0&limit=10
Request method	GET
Accept	application/json, text/plain, */*
X-ECHA-Mode	test
X-ECHA-Test-Run	mycompanyid-run001
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTUyNmI0LTFFkMTItNGEzOS05ODMyLTlwYzkyZmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11UUKai3fX4

C.4.4 Response in "integration" test mode

Same as in C.4.2.

C.4.5 Request in “production” mode

Just omit both X-ECHA-Mode and X-ECHA-Test-Run from the Request Parameters.

Request Param	Description
Request URL	https://api.ecs.echa.europa.eu/submission/events?offset=0&limit=10
Request method	GET
Accept	application/json, text/plain, */*
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTZkMTItNGEzOS05ODMyLTIwYzYzYzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11Uukai3fX4

C.4.6 Response in “production” mode

Same as in C.4.2.

C.4.7 Sample request

Sample request
<pre>GET https://api.ecs.echa.europa.eu/submission/events?offset=0&limit=10 HTTP/1.1 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTZkMTItNGEzOS05ODMyLTIwYzYzYzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11Uukai3fX4 X-ECHA-Mode: test Accept: application/json, text/plain, */* Host: api.ecs.echa.europa.eu Accept-Encoding: gzip, deflate Connection: keep-alive</pre>

C.5 Submit by reference (simplified SCIP notification)

C.5.1 Request in “connectivity” test mode

Request Param	Description
Request URL	https://api.ecs.echa.europa.eu/submission/v3/sbr
Request method	POST
Accept	application/json, text/plain, */*
X-ECHA-Mode	test
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTZkMTItNGEzOS05ODMyLTIwYzYzYzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11Uukai3fX4

Request Param	Description
["6e89878c-eb2e-476a-a4ae-06c96b1488cf"]	List of PSSI numbers (SCIP numbers) as a comma-separated list

C.5.2 Response in "connectivity" test mode

Response
<pre>{ "submissionRequests": [{ "status": "SUBMITTED ", "submissionNumber": "AAD678032-54", "statusUrl": "https://api.ecs.echa.europa.eu/submission/v2AAD678032-54", "reportUrl": "https://ecs.echa.europa.eu/cloud/submissions/v3/AAD678032-54" "referencedPssi": "6e89878c-eb2e-476a-a4ae-06c96b1488cf" }] }</pre>

C.5.3 Request in "integration" test mode

Request Param	Description
Request URL	https://api.ecs.echa.europa.eu/submission/v4/sbr
Request method	POST
Accept	application/json, text/plain, */*
X-ECHA-Mode	test
X-ECHA-Test-Run	mycompanyid-run001
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4Ij40LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTFkMTItNGEzOS05ODMyLTIwYzk3YzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11UUKai3fX4
["6e89878c-eb2e-476a-a4ae-06c96b1488cf"]	List of PSSI numbers (SCIP numbers) as a comma-separated list

C.5.4 Response in "integration" test mode

Same as in C.5.2.

C.5.5 Request in "production" mode

Just omit both X-ECHA-Mode and X-ECHA-Test-Run from the Request Parameters.

Request Param	Description
Request URL	https://api.ecs.echa.europa.eu/submission/v3/sbr

Request method	POST
Accept	application/json, text/plain, */*
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTZkMTItNGEzOS05ODMyLTIwYzk3YzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11Uukai3fX4
["6e89878c-eb2e-476a-a4ae-06c96b1488cf","38843e3e-60ce-458a-bf7b-3289fb272402"]	List of PSSI numbers (SCIP numbers) as a comma-separated list

C.5.6 Response in "production" mode

Same as in C.5.2.

C.5.7 Sample request

Sample request
<pre>POST https://api.ecs.echa.europa.eu/submission/v3/sbr Accept-Encoding: gzip, deflate Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTZkMTItNGEzOS05ODMyLTIwYzk3YzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11Uukai3fX4 Content-type: application/json X-ECHA-Mode: test Accept: application/json, text/plain, */* Host: api.ecs.echa.europa.eu Connection: keep-alive ["ff89396f-3974-4888-8791-bef8bad67698","22499eb4-25e7-401b-9b30-06bfa11052c"]</pre>

C.6 Disable submission

C.6.1 Request in "connectivity" test mode

Request Param	Description
Request URL	https://api.ecs.echa.europa.eu/submission/v4/20354d7a-e4fe-47af-8ff6-187bca92f3f9/disable
Request method	POST
Accept	application/json, text/plain, */*
X-ECHA-Mode	test

Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTFkMTItNGEzOS05ODMyLTIwYzk3YzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11Uukai3fX4
{"reason": "DISABLE_BY_MISTAKE"}	Reason for disabling one submission (provided in the body)

C.6.2 Response in "connectivity" test mode

Response
<pre>{ "submissionNumber": "AAD678032-54", "statusUrl": "https://api.ecs.echa.europa.eu/submission/v4/AAD678032-54", "reportUrl": "https://ecs.echa.europa.eu/cloud/submissions/AAD678032-54 ?leUuid=ECHA-83a626b4-1d12-4a39-9832-20c97c1fba4d" }</pre>

C.6.3 Request in "integration" test mode

Request Param	Description
Request URL	https://api.ecs.echa.europa.eu/submission/v4/20354d7a-e4fe-47af-8ff6-187bca92f3f9/disable
Request method	POST
Accept	application/json, text/plain, */*
X-ECHA-Mode	test
X-ECHA-Test-Run	mycompanyid-run001
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTFkMTItNGEzOS05ODMyLTIwYzk3YzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11Uukai3fX4
{"reason": "DISABLE_BY_MISTAKE"}	Reason for disabling one submission (provided in the body)

C.6.4 Response in "integration" test mode

Same as in C.6.2.

C.6.5 Request in “production” mode

Just omit both X-ECHA-Mode and X-ECHA-Test-Run from the Request Parameters.

Request Param	Description
Request URL	https://api.ecs.echa.europa.eu/submission/v4/20354d7a-e4fe-47af-8ff6-187bca92f3f9/disable
Request method	POST
Accept	application/json, text/plain, */*
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTFlkMTItNGEzOS05ODMyLTIwYzk3YzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11Uukai3fX4
{"reason": "DISABLE_BY_MISTAKE"}	Reason for disabling one submission (provided in the body)

C.6.6 Response in “production” mode

Same as in C.6.2.

C.6.7 Sample request

Sample request
<pre>POST https://api.ecs.echa.europa.eu/submission/v4/20354d7a-e4fe-47af-8ff6-187bca92f3f9/disable Accept-Encoding: gzip, deflate Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ4LWVjaGEtcGFydHkiOiJFQ0hBLTgzYTYyNmI0LTFlkMTItNGEzOS05ODMyLTIwYzk3YzFmYmE0ZCJ9.QNkrbc_eUeKA7k2i4DV8IRifaub1XjsG11U Ukai3fX4 Content-type: application/json X-ECHA-Mode: test Accept: application/json, text/plain, */* Host: api.ecs.echa.europa.eu Connection: keep-alive {"reason": "DISABLE_BY_MISTAKE"}</pre>

C.7 Error responses

C.7.1 Legal entity not authorised by ECHA or JWT token is missing

Response
<pre>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> <center><h1>401 Authorization Required</h1></center> <hr><center>openresty</center> </body> </html></pre>

C.7.2 JWT token malformed or expired

Response
<pre>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." }</pre>

C.7.3 JWT token includes a wrong LE UUID

Response
<pre>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",</pre>

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

C.7.4 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."
}
```

C.7.5 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'
```

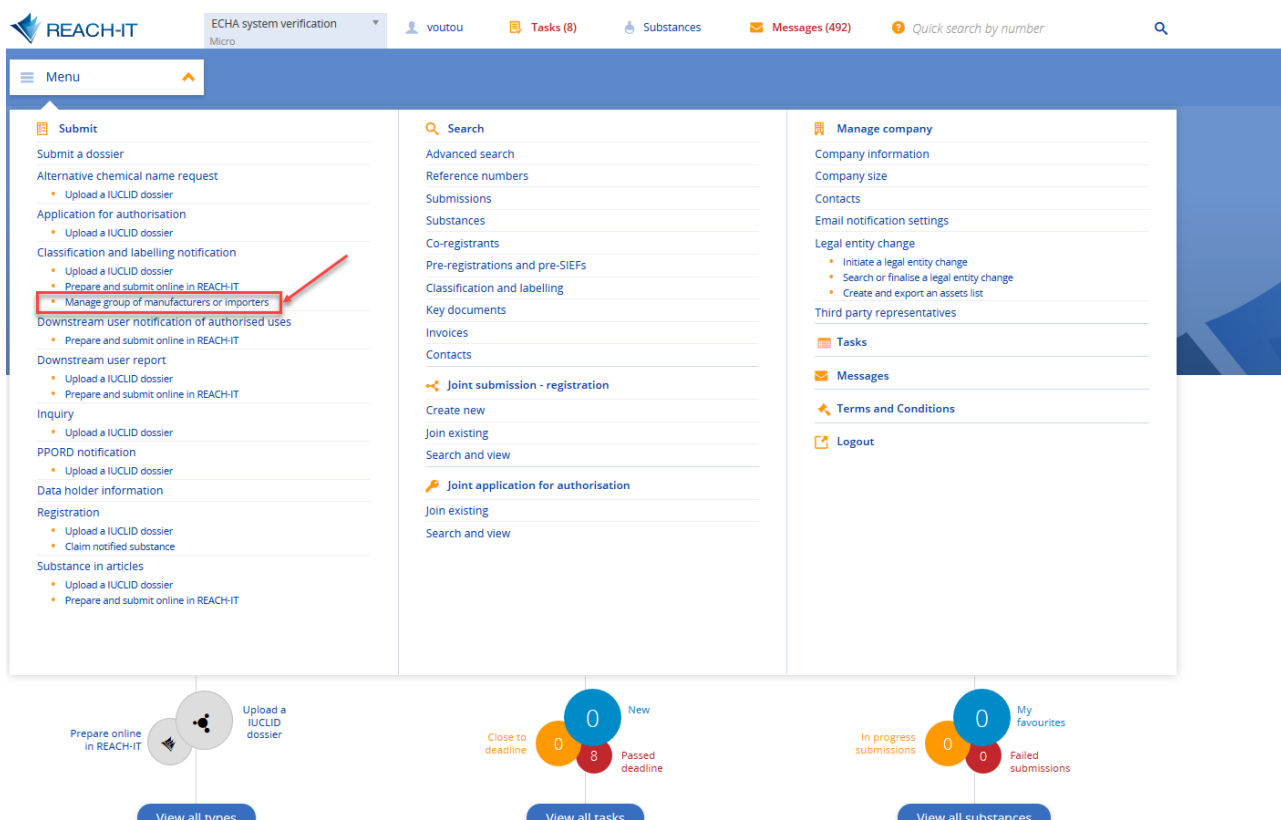
Annex D Guidelines for submitting a C&L notification

Systems integrating with the exposed REST API may submit C&L notifications on behalf of a group of manufacturers and importers. Apart from the submitted dossier, the service requires information about the Group of manufacturers or importers and Contact person; both elements are mandatory information that needs to be provided in the request, see [2.2 Submit a dossier] for further details on this.

D.1 Group of manufacturers or importers (MI group)

Before submitting a C&L notification on behalf of a group of manufacturers and importers via S2S, users need to find or create the MI group information in REACH-IT.

Step 1: Choose the option "Manage group of manufacturers or importers" from the main menu in REACH-IT.



The screenshot shows the REACH-IT user interface. At the top, there is a navigation bar with the REACH-IT logo, a dropdown menu for 'ECHA system verification' (set to 'Micro'), a user profile 'voutou', and notification counts for 'Tasks (8)', 'Substances', and 'Messages (492)'. A search bar is also present. Below the navigation bar is a main menu with three columns. The left column is titled 'Menu' and contains various options such as 'Submit', 'Alternative chemical name request', 'Application for authorisation', 'Classification and labelling notification', 'Downstream user notification of authorised uses', 'Downstream user report', 'Inquiry', 'PPORD notification', 'Data holder information', 'Registration', and 'Substance in articles'. The option 'Manage group of manufacturers or importers' is highlighted with a red box and a red arrow. The middle column is titled 'Search' and contains options like 'Advanced search', 'Reference numbers', 'Submissions', 'Substances', 'Co-registrants', 'Pre-registrations and pre-SIEFs', 'Classification and labelling', 'Key documents', 'Invoices', and 'Contacts'. The right column is titled 'Manage company' and contains options like 'Company information', 'Company size', 'Contacts', 'Email notification settings', 'Legal entity change', 'Third party representatives', 'Tasks', 'Messages', 'Terms and Conditions', and 'Logout'. At the bottom of the page, there are three circular widgets: 'Prepare online in REACH-IT' with a 'View all boxes' button, 'Close to deadline' with a 'View all tasks' button, and 'In progress submissions' with a 'View all substances' button.

Figure 2: "Manage group of manufacturers or importers" in REACH-IT menu

Step 2: You may start the creation of a new group by clicking on "Create a new group". In case there are already groups in your account, this page shows the list of the existing ones, where you may edit them, e.g. by updating the composition of the group, or even delete them.

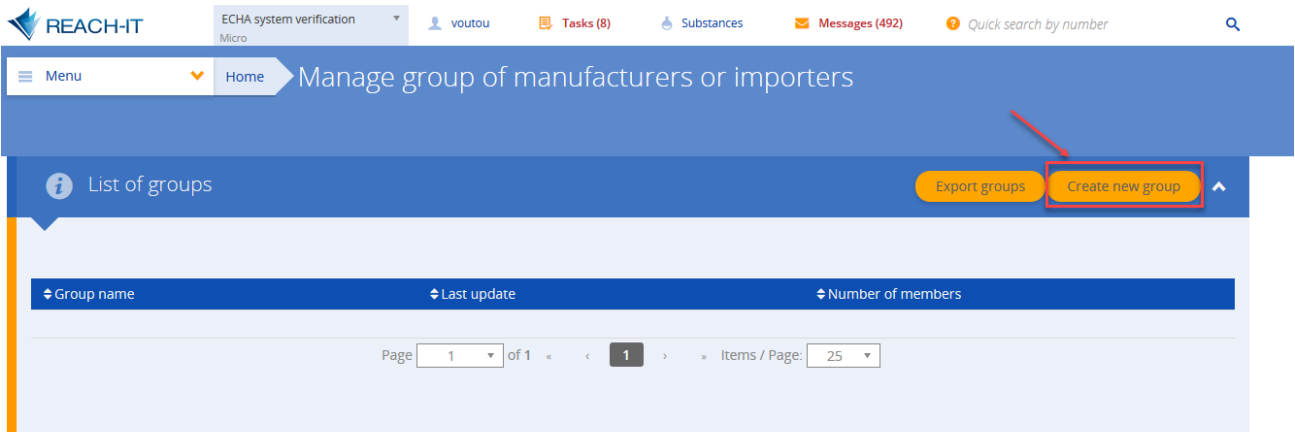


Figure 3: "Create new group" of manufacturers or importers in REACH-IT

Step 3: After providing a name for the new group, you will be prompted to provide additional information, add the members and finalise the group creation.

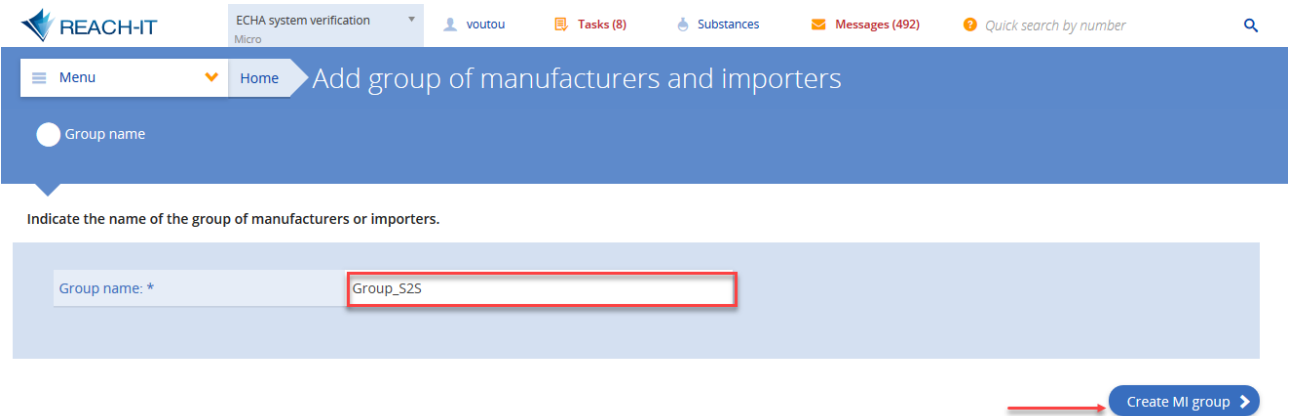


Figure 4: Provide a group name during the creation of a new group of manufacturers or importers in REACH-IT

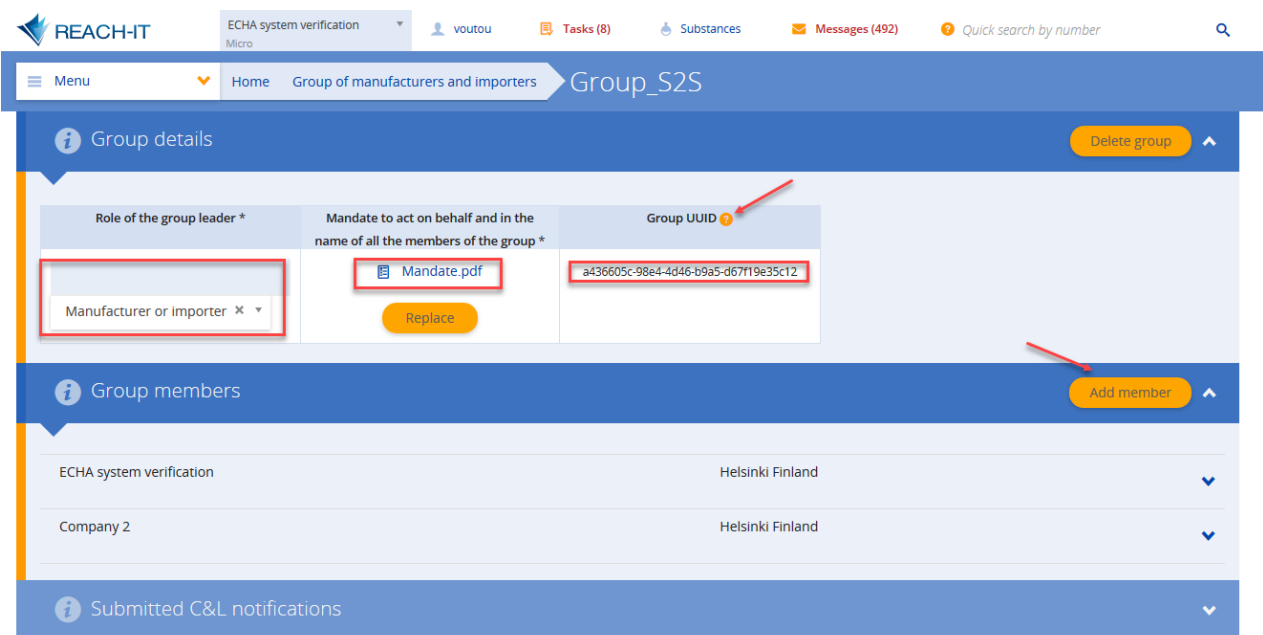


Figure 5: Manufacturers' or importers' group details and members in REACH-IT

The MI group UUID, shown above, has to be provided in the S2S request. The UUID is shown in the screen once the group creation has been finalised.

Additional practical help on the creation of a group of manufacturers or importers can be found also directly in REACH-IT via its help pages.

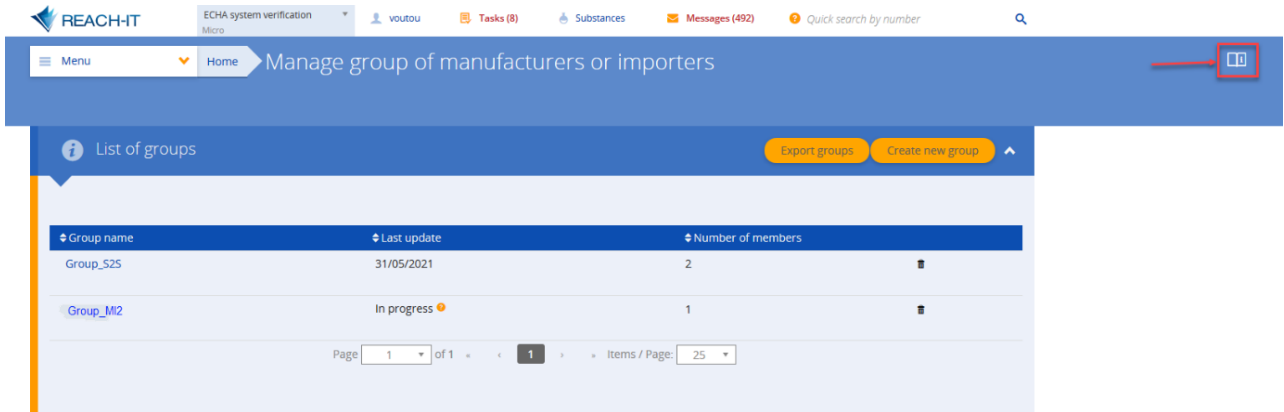


Figure 6: Manufacturers or importers group help link in REACH-IT

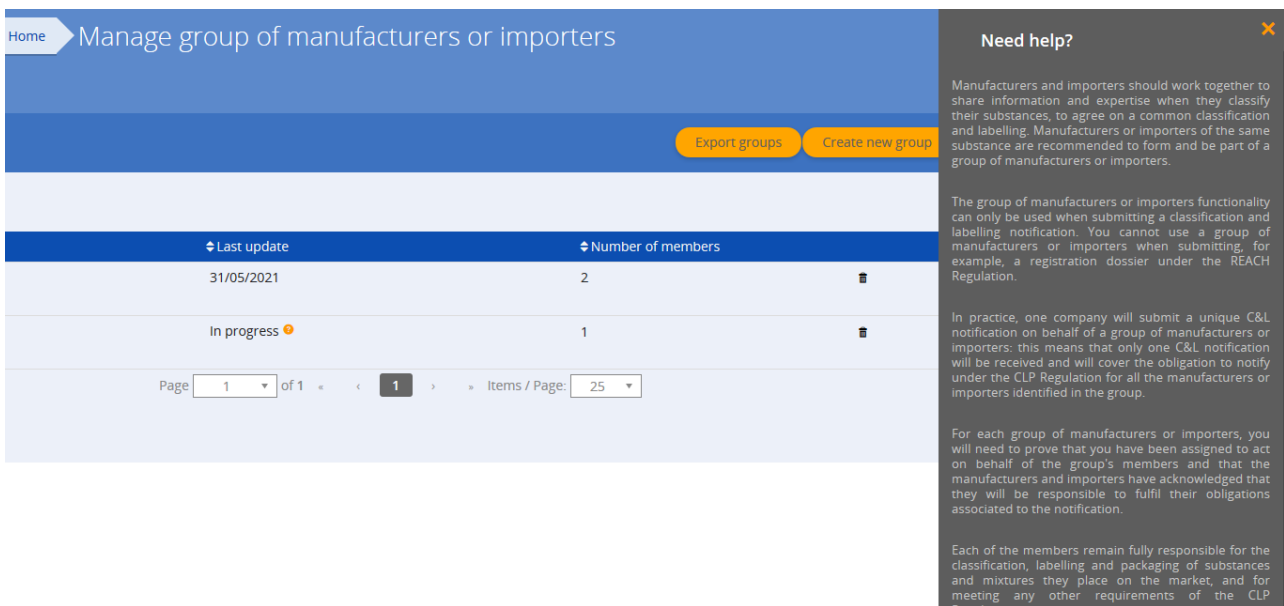


Figure 7: Manufacturers or importers group help pages in REACH-IT

D.2 Contact person

For every submission of a C&L notification, a contact person must be also assigned. Contacts are managed in REACH-IT; you may use a contact already existing in the system, or create a new one.

Step 1: Choose the “Contacts” from the main menu in REACH-IT

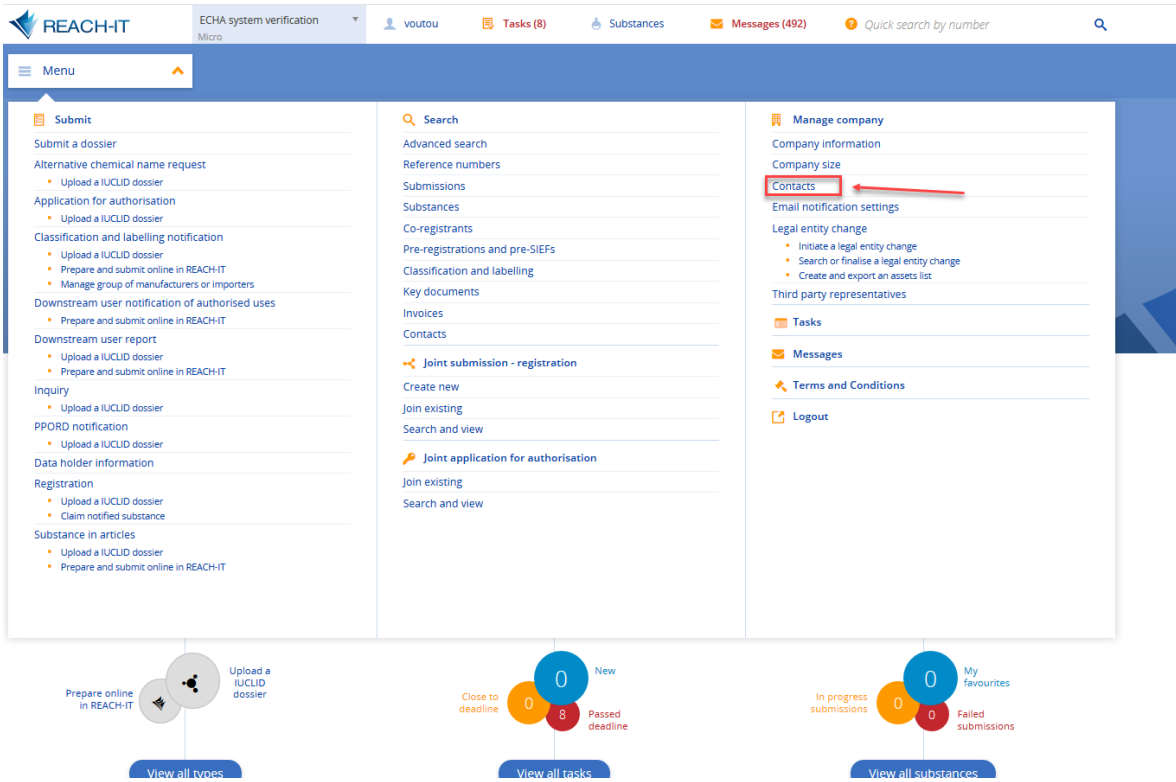


Figure 8: “Contacts” in REACH-IT menu

Step 2: You can search for the existing contact persons or add new contacts. You may also delete a contact but only if they do not have any assignments or after you have transferred their assignments to another contact.

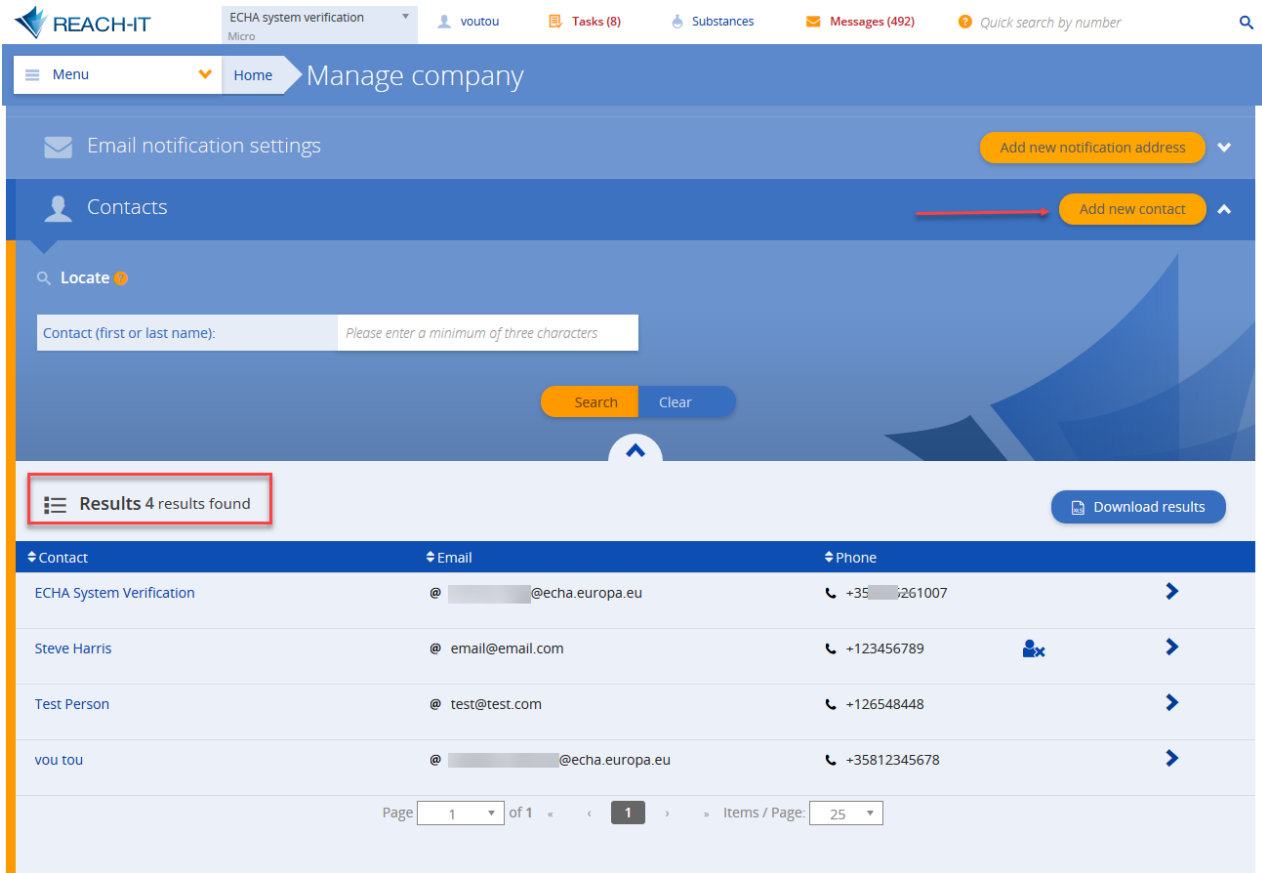


Figure 9: Managing contacts in REACH-IT

Step 3: By clicking on the contact person, you can see their details and assignments and the contact UUID which you need for your S2S submission. On this page, you can also edit the details and assignments of the contact person. By clicking on the assignment, you will be directed to the corresponding page, where you can change the assigned contact person.

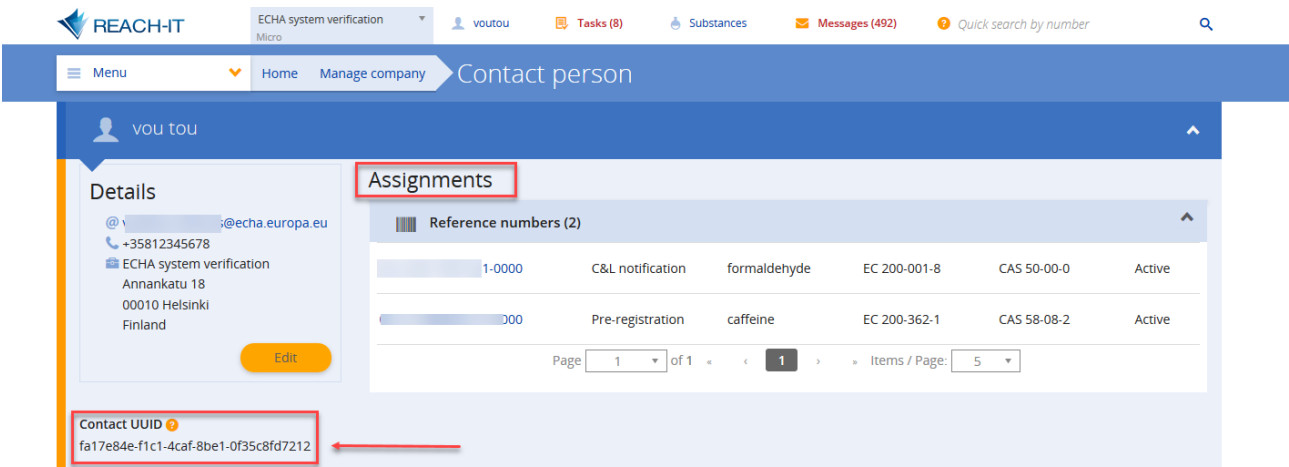


Figure 10: Viewing contact assignments and Contact UUID in REACH-IT

Remember to keep the contact details up to date, as they may be used by ECHA and other authority users to send communications to your company or enquire about the specific submission.

D.3 IUCLID format versions accepted in the S2S



Submissions of C&L notifications through the S2S interface should be performed in IUCLID format version **6.3 or higher**.

Annex E How to onboard to ECHA's System-to-System service

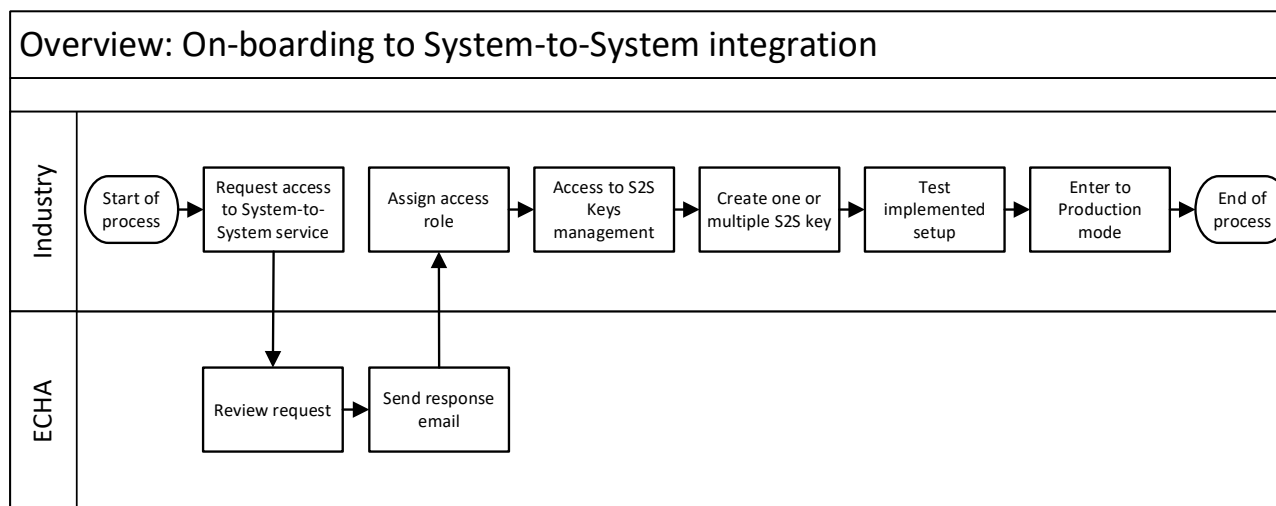


Figure 11 - Onboarding overview

E.1 Step 1 – Request access to System-to-System service

The LE manager needs to submit a request to be part of the System-to-System service via ECHA's contact form - http://comments.echa.europa.eu/comments/cms/Contact_S2S.aspx

Request type:

Select "Access request"

Username:

Enter your ECHA account username

Legal Entity UUID:

Enter the Legal Entity UUID that wants to submit dossiers

Question:

In the open textbox for 'Question', the following information needs to be provided:

- Legal entity name
- Software used to connect to ECHA system (if using own, specify 'self-developed')

The LE manager can use a text like the one shown below:

' I want my Legal Entity to have access to the System-to-System service provided by ECHA.

Legal Entity Name: XXXXX

Our S2S API requests will be performed by: XXXXX '

Your contact details

In 'Your contact details' section, the email address meant to receive the email containing the response to the service request has to be provided.

Figure 12 - S2S request form

E.2 Step 2 – Assign access roles

Once ECHA approves the request, the LE manager will be able to assign its user(s) a new role called "S2S Keys Manager". The "S2S Keys Manager" will then be able to handle the related keys to authenticate S2S calls.



On top of the "S2S Keys manager" role, the LE manager needs to assign one of the following roles to the person issuing the S2S keys. The following table lists the ECHA Submission portal relevant roles that should be considered.

Table 25: Roles required per S2S service (endpoint)

Submission type	Role	S2S service				
		submit	report	events	sbr ²	disable
PCN/SCIP	Submission Portal Manager	√	√	√	√	√
PCN/SCIP	Submission Portal Reader		√	√		

² It refers to SSN

Submission type	Role	S2S service				
		submit	report	events	sbr ²	disable
PCN/SCIP	Submission Portal Manager Restricted	√	√ ³	√	√	√ ³
C&L/PCN	REACH Manager	√	√	√		√
C&L/PCN	REACH Reader		√	√		

The following sub-steps need to be followed:

- Go to <https://idp.echa.europa.eu/ui/login>
- Log in using the LE manager credentials
- Click on 'Legal Entity' on the left side menu
- Navigate to the 'Users' tab
- Click on the username of the user you want to assign the 'S2S Keys Manager' role to
- Click on 'Edit' on the right side of the screen
- Add the role 'S2S Keys Manager' and the relevant role described in Table 25
- Click on 'Save'

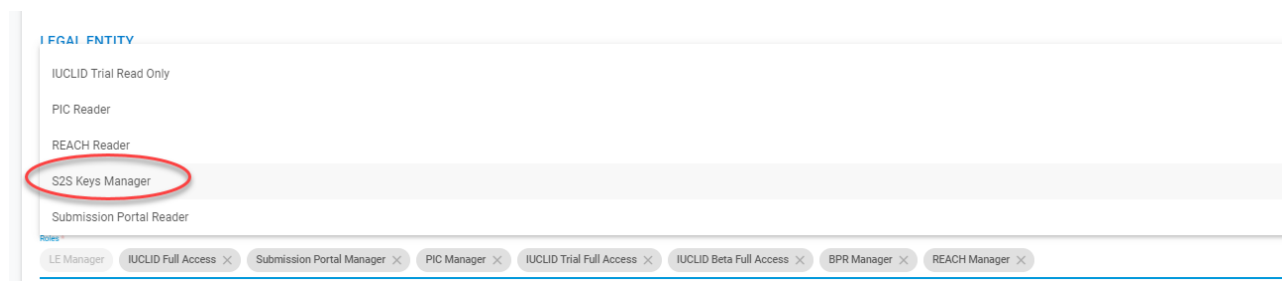


Figure 13 - ECHA Account S2S access right

For further reference on how to assign a user role, please see the [ECHA accounts manual](#).

E.3 Step 3 – Create S2S keys

Once the role has been assigned, the S2S Key manager can proceed to the keys management page of ECHA accounts page:

³ Users can only get the submission report or disable the submissions they have performed, not submissions performed by other users on behalf of the same company.

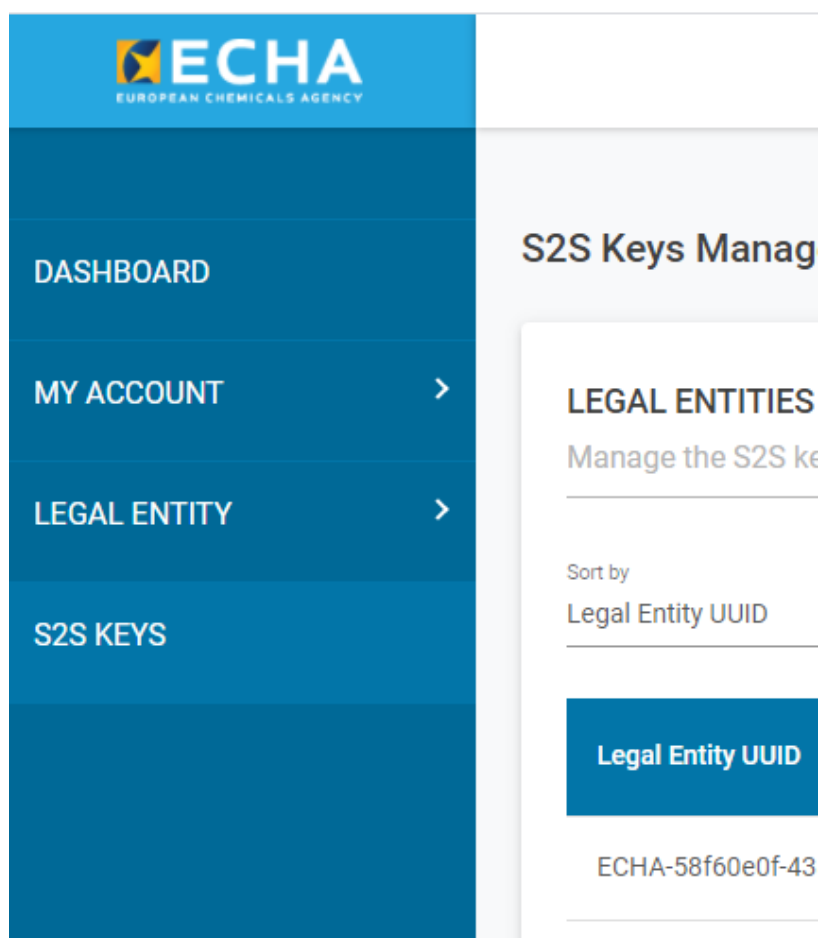


Figure 14 - S2S Key management in ECHA accounts page

Each user can generate one key per LE in which the user has been assigned the S2S Keys Manager role by following the steps below:

- Go to <https://idp.echa.europa.eu/ui/login>
- Login using any account which has the S2S Keys Manager role
- Click on 'S2S keys' on the left side
- The first time the user accesses the S2S keys management page, Terms and Conditions will be presented and need to be accepted. Click on 'Accept and Continue' after reading the document and acknowledging that you read the terms and conditions.

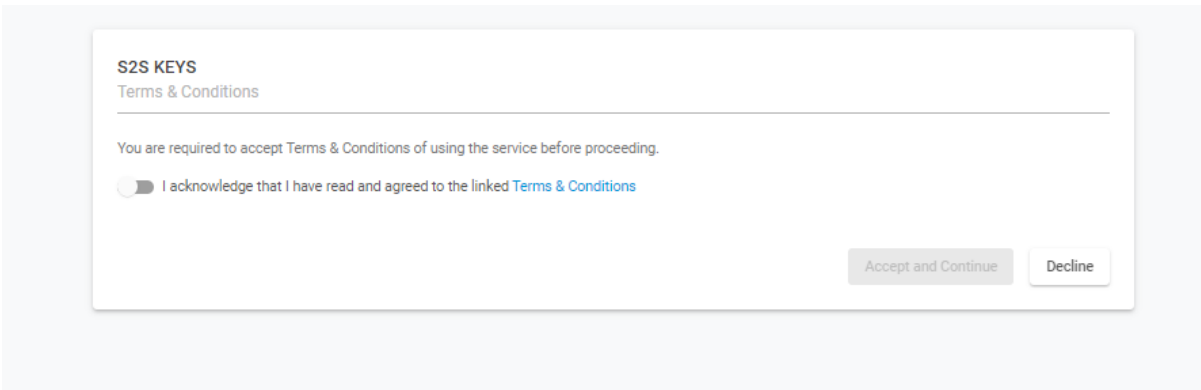



Figure 15 - Accepting T&Cs

- In the S2S keys page, click on  to generate a new key:
- A pop up window will show you the S2S key for the user generating it:

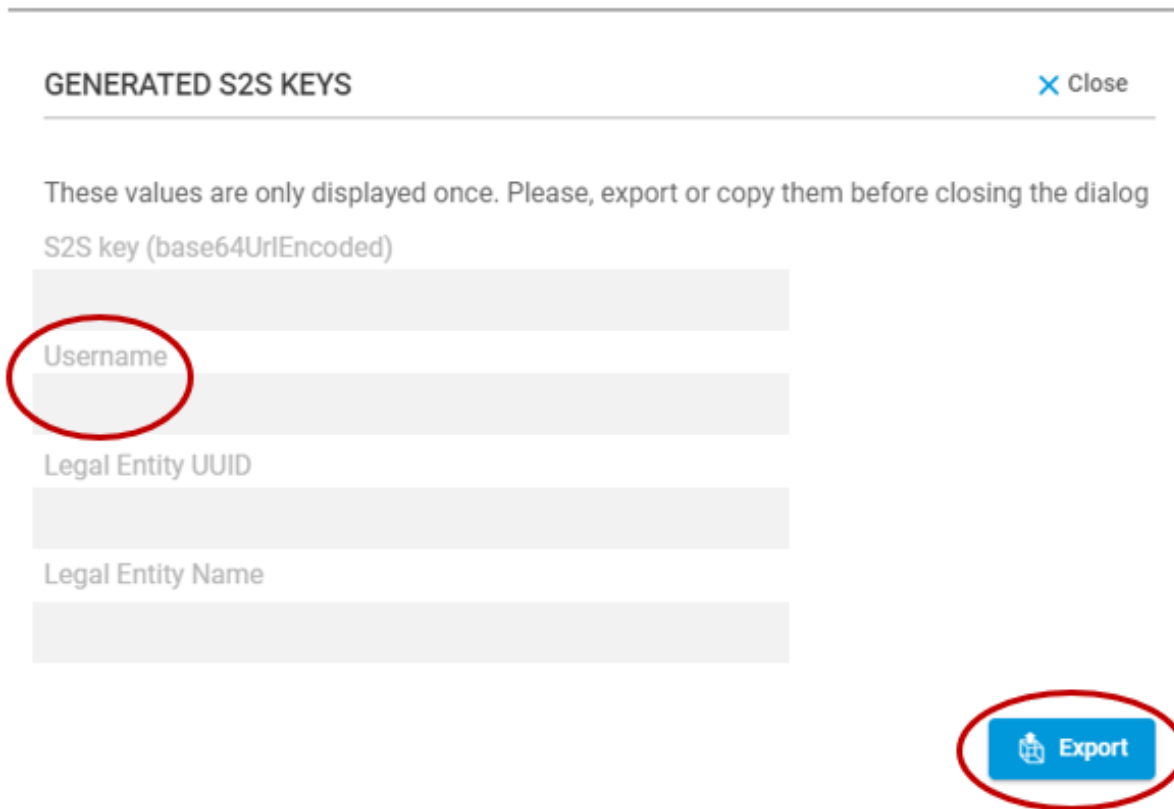


Figure 16 - Key creation pop up window

- Please note that when you log in with a different user, who has also the S2S key manager role, you can generate a different key for the same legal entity.
- Please note that you need to additionally include the username in the token creation: it is not enough to include the S2S key. For additional information, see [3.2_HMAC-Signed JWT](#).

Save the key in a secure manner so that it can be included in the client system configuration. For that, the user can copy the key or export it as a comma separated file. Once the window is closed, it will not be possible to retrieve the key anymore. If the key is lost, the user must re-generate a new one.

E.4 Step 4 – Test the implemented setup



Test the System-to-System configuration before submitting notifications in production mode.

Please see [chapter 4. Testing instructions and switch to production mode] for information on how to use the TEST mode in the API requests. For any problems during the testing phase, please contact ECHA service desk via the contact form:

http://comments.echa.europa.eu/comments_cms/Contact_S2S.aspx

Once you successfully tested the implementation you may switch to production mode.

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