DAC8 Technical FAQ – version 3.0 – 10/07/2026

Goal of the Technical FAQ

The Technical FAQ is designed to support all Member States by consolidating and sharing Answers to questions raised by individual Member States. By gathering these queries and providing clear, standardized responses, the FAQ ensures that information is disseminated widely and consistently.

This approach helps Member States by:

- **Promoting equal access to knowledge:** Every Member State benefits from Answers, even if only one of them originally asked the question.
- **Building efficiency:** Reduces duplication of effort by addressing recurring issues in one central resource.
- **Ensuring consistency:** Provides harmonized, authoritative guidance so that all Member States are aligned.
- **Strengthening capacity:** Improves understanding and implementation by offering practical, ready-to-use clarifications.
- **Encouraging collaboration:** Signals that concerns raised by one Member State are relevant for all, fostering a sense of shared problem-solving.

TABLE OF CONTENTS

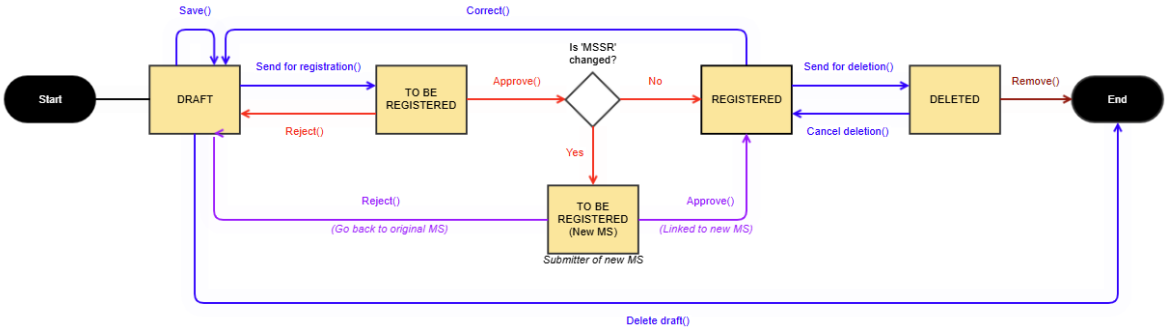
FAQ-1. How does the deletion process work, and how can Member States interact with it to amend data for a CAO?

Answer:

After the 12 months of timelapse since the registration has been deleted, a CAO should be registered anew to be recorded in the Central Register. A new CAO will have to be created, with a new IIN. The reason is that the CAO records will not be stored in the database after the 12 months period. Since all records of the CAO are removed, including the IIN, this IIN is freed. It means that could be reassigned for a new CAO registration (either randomly generated by the system or via the import mechanism).

Please note that this deletion after 12 months occurs only for CAO that have been deleted (i.e. in the "DELETED" status).

CAO in any other statuses will not be deleted after this 12-month period.



A CAO would have been deleted for one of the following reasons:

- **1 - No longer has users**: The Crypto-Asset Operator has notified that it no longer has Reportable Users in the Union;
- **2 - Assume activity as ceased**: There are grounds to assume that the activity of the Crypto-Asset Operator has ceased;
- **3 - No longer meets conditions**: The Crypto-Asset Operator no longer meets the conditions laid down in subparagraph B(2) of Section IV;
- **4 - Revoked registration**: The registration of the Crypto-Asset Operator has been revoked according to subparagraph F(6).

Please also note that the MSSR can cancel this deletion during the 12 months period. After this period, all records of the CAO are deleted from the system.

FAQ-2. How are DAC8 messages submitted and validated within the DAC8 Central Directory, and what is the process for generating and accessing status messages?

Answer:

The National Administrations will be in charge of submitting their DAC8 messages into the DAC8 Central Directory, which can be done either via CCN/CSI or the UI. Once DAC8 messages are submitted, a new entry is added to the table listing all the messages submitted by the National Administration and the DAC8 Central Directory will perform, asynchronously, validations against business and technical rules.

Once the validation will be completed, the Status message will be generated and made available in the related table in the DAC8 Central Directory. In case the DAC8 message was sent using CCN/CSI, the Status message will also be sent over CCN/CSI as a reply to the previous CCN message.

It is worth noting that a specific table listing all the accepted DAC8 messages received by the National Administration.

There is no requirement allowing the NA user to upload a status message in the DAC8 Central Directory, since it is in charge of validating the DAC8 messages (both stateless and stateful rules).

FAQ-3: What types of statistics does the DAC8 system generate, and how are these statistics structured and presented to Member States?

Answer**:**

DAC8 does not require Member States to produce statistics. This is covered in article 8b paragraph 1. Nonetheless, the system will generate 2 kinds of statistics as MS Excel file:

1. **Statistics on messaging:** The statistics will include information from the message headers transmitted to the DAC8 Central Directory. This includes information on the countries involved, the message identifiers, message types and message sizes. One entry in the Statistics Excel file corresponds to one message received by the DAC8 Central Directory (meaning that an initial message followed by a correction will lead to two distinct entries).
2. **Statistics on assets:** The statistics data must include information on Crypto Assets as provided in their latest version (meaning including corrections). This includes information on the countries involved, the crypto-asset types, the transactions and the amounts.

   One entry in the Excel file corresponds to one existing (i.e. having related records in the database) combination of Transmitting country, Receiving country, Crypto asset, Transaction type and Currency. Other elements will be aggregated, based on the latest accepted data (i.e. including corrections, if any). This ensures that the data is anonymised and reflects on the real-world transaction amounts (not counting twice an amount because it was corrected via another message).

FAQ-4: What documentation will be provided to guide Member States in using the DAC8 system, and what is the timeline for the availability of these documents?

Answer:

In order to avoid duplication of work and potential confusion, DG TAXUD will not produce anymore a user guide based on the OECD user guide. (CARF XSD User Guide version 1.5)

Considering that specific EU rules must be supported by DAC8, an ad hoc **document** to **complement the OECD CARF XSD User Guide** is produced and made available on CIRCABC. This document will list all the EU specific rules applying to the OECD CARF XSD and the updated list of business and technical rules applicable to the DAC8 context.

The **External Interface Specifications** is planned to be made available by **February 2026**. This document will contain the needed information for the System-to-System data exchanges.

The **DAC8 User Manual** is planned to be made available by **April 2026**. This document will contain the needed information to use the DAC8 Central Directory.

FAQ-5. What is the scope of the Validation Module to be delivered in April 2026, and how does it differ from the validation process used in the DAC8 Central Directory?

Answer:

The Validation Module to be delivered in April 2026 will implement the same validation process as the one used by the DAC8 Central Directory. This Validation Module will only include the **stateless rules** (i.e. rules which do not require any information external to the XML message to be validated). All stateful rules will be implemented directly in the DAC8 Central Directory and will not be included in the Validation Module that will be provided to the Member States.

FAQ-6. How does the DAC8 Central Register system handle the generation and validation of the Individual Identification Number (IIN) when processing records, and what are the rules for IIN assignment and import scenarios?

Answer**:**

DAC8 CR identifies its records based on their IIN (Individual Identification Number). The IIN is automatically generated by the DAC8 CR for the Member State of Single Registration (MSSR). The IIN in DAC8 is designed to be automatically attributed by the system following the rules defined in section 4.1 of the DAC8 CR Release Product Backlog artefact, shared on CIRCABC on 06/09/2024.

DAC8 Central Register will always generate the IIN when encoding the CAO via the UI.

When importing an XML file into the DAC8 Central Register system, 3 scenarios may occur for a valid file:

1. IIN is missing in the imported file: The system will generate the unique IIN;
2. IIN is provided in the imported file but does not relate to the MS of the user (for a new CAO): The import process fails;
3. IIN is provided in the imported file and relates to the MS of the user: The system checks if that IIN exists in the database:
    a. If it does not exist, the system uses that IIN to create the new 'DRAFT' CAO;
    b. If it already exists, the import process fails.

The structure of the IIN is the following: CCXXXXXXXX

- CC is the ISO Country Code of the Member State where the IIN was generated.
- XXXXXXXX is a unique identifier composed of capital letters (A-Z) and/or numbers (0-9).
- *Regex used:* [A-Z]{2}[A-Z0-9]{8}

Considering the above,

- a Member State may generate its own IINs when uploading a file containing a list of new CAOs to be registered in DAC8-CR. This might be useful for the Member State to share a common reference between its national system and the Central Register.
- when the IIN is missing in a file import, DAC8-CR will always generate the IIN automatically.
- the DAC8-CR UI is always generating the IIN automatically.

FAQ-7. What is the procedure in DAC8 CR when a CAO changes nexus in another Member State of Single Registration (MSSR)?

Answer**:**

DAC8-CR #2 will introduce the possibility to correct information related to CAO when already registered. In this context, a mechanism will allow the transfer of a CAO from a MSSR to another.

The underlying issue is that if a RCASP changes its Member State of Single Registration (MSSR) without notifying it, a new Member State might encode a duplicate record of the RCASP already registered in DAC8-CR under another Member State and with a new IIN. Consequently, this would lead to the same RCASP being registered with several IINs in the

DAC8-CR. To avoid this, a specific transfer of ownership with the possibility of correcting CAO information will be developed.

The process is the following:

- RCASP informs MSSR on change of information leading to the change of MSSR (e.g. tax residence changed which would lead to a change in Member States for the purpose of reporting);
- MSSR triggers the correction of REGISTERED RCASP, where a new field would allow the change to the new MSSR;
    - ✓ The previous MSSR can correct RCASP information and change to the new MSSR;
    - ✓ 4-eyes workflow (currently in place) applies.
- The new MSSR is notified of the transfer via the notification mechanism;
- New MSSR becomes owner of the data and can update it (4-eyes workflow applies for verifying and approving the RCASP);
- The RCASP is identified with the same IIN.

The impacts will be the following:

- Legal/administrative impact
    - The RCASP will notify the MSSR of the change of MSSR to a new one, according to Annex VI, Section V, F(3) of DAC8 and the Regulation.
- IT impact – medium complexity
    - Requires the update of correction mechanism to add a new field, and a warning to inform the user about the consequences of changing the MSSR.
    - The import feature would not be impacted but a new element would be added to the XSD to identify the MSSR in the XML file exported from the application.

FAQ-8. Where can be found the CCN Intranet Services – Programmer's Guide, reference document [R02] in the DAC8 Central Register-External Interface Specifications-v1.00 artefact?

Answer**:**

Newer version 3.00 of the CCN Intranet Services – Programmer's Guide has been uploaded on CIRCABC.

FAQ-9. Who is responsible for each step when changing the MSSR for a CAO with an existing registration and IIN?

Based on the slides of the business presentation in the CR Training Materials, for a CAO registered in IE, it seems we would have someone with the requisite role access the CR and they would trigger a correction for that CAO. This user would provide the new value for that CAO's "Member State of Single Registration" field in the CAO form, and at that point the new MSSR would be able to see a draft record for that CAO which they would then approve or reject for registration. Is this correct?

Answer:
Yes, this is correct. This is how the process works:

- Triggering a Correction: A user with the Encoder role can correct a REGISTERED CAO by accessing its details and clicking the "Correct" button. This action creates a new DRAFT version of the CAO, where the "Member State of Single Registration" (MSSR) field can be updated.
- Updating the MSSR: The Encoder modifies the MSSR field to reflect the new Member State. Once saved, the CAO status changes to "TO BE REGISTERED (New MS)", indicating that the correction involves a change in the MSSR

Approval Workflow:

- Visibility of the Draft: During this process, the CAO remains accessible to users of the original MSSR (in "TO BE REGISTERED (New MS)" status) until the new MS approves or rejects it
- The corrected CAO is first sent to the Submitter of the original MS for approval. If approved, it is then forwarded to the Submitter of the new MS for final approval and registration under the new jurisdiction
- The new MS's Submitter can either approve (changing the status to REGISTERED) or reject (returning it to DRAFT status)

Other important aspects:

- Only the latest registered version of a CAO can be corrected, and corrections are not retained unless saved or sent for registration
- If the CAO is already under correction, further corrections are blocked until the current process completes
- The reason for correction must be provided when sending the CAO for registration.

For full details, refer to sections on "Correct a CAO" of the "DAC8-CR-User Manual-UMN-v2.00".

FAQ-10. What happens when another MS imports a draft CAO with no IIN/their own IIN for a CAO that is currently registered in IE with an existing IIN?

Please see attached a slide from the CR Training Materials that covers some IIN handling cases. It covers the case where another MS tries to import a CAO with an existing IIN, this is disallowed unless the current MSSR is importing the CAO with its existing IIN. However, if we are reading these cases correctly, the import will go through if an MS imports a CAO with a new IIN (provided by them or generated by the CR). Does this leave room for bypassing the correction process and allowing the same CAO to be imported under different IINs?

Answer:

The system creates/corrects/updates CAO(s) by following the subsequent logic:

- If the IIN is missing for the CAO, the system generates it and the CAO is created as a new DRAFT CAO;
- If the IIN is present:
  - If the IIN does not relate to the MS of the user, the system checks if the MS of the user is the MSSR of the CAO:
    - If the MS of the user is not the MSSR, the import process fails;
    - If the MS of the user is the MSSR, the system checks the status of the CAO in the system:
      - If the latest status is DRAFT, the CAO is updated with the uploaded file content;
      - If the latest status is REGISTERED, a DRAFT revision of the CAO is created;
      - If none of the conditions above are met the import process fails.
  - If the IIN relates to the country of the user, the system checks if that IIN exist in the database:
    - If the IIN does not exist yet, the system uses that IIN to create a new DRAFT CAO;
    - If already used, the system checks the status of the CAO in the database:
      - If the latest status is DRAFT, the CAO is updated with the uploaded file content;
      - If the latest status is "REGISTERED", a DRAFT revision of the CAO is created;
      - If none of the conditions above are met, the import process fails.
- If duplicate IINs are imported in the same XML, the import process fails.

Regarding the possibility to bypass, the system only checks IIN conflicts if the IIN is provided and relates to the user's MS. No cross-MS validation occurs for missing/new IINs, meaning the system does not verify whether the operator is already registered elsewhere under a different IIN. This can be avoided from the user who can check in advance if the new CAO's core details (e.g., legal name, tax ID, or other unique identifiers) match an existing REGISTERED CAO in any MS. In this case, the user can stop the procedure as this would be a CAO registered with two different IINs in different MSs.

FAQ-11. What consensus was reached with regards to the handling of Controlling Persons sent to the Central Directory?

Initially a CryptoUser was to be sent to an MS alongside all of its Controlling Persons so long as at least one of its own ResCountryCodes or any of its Controlling Persons' ResCountryCodes aligned with that MS. The CD would then mask the data for Controlling Persons who were not resident in the receiving MS. This clashed with an OECD rule, where a CryptoUser and any of its Controlling Persons should only be sent to an MS if either the CryptoUser or one or more of its Controlling Persons had residence in the receiving MS. This would mean CryptoUser records would need additional splitting logic when generating outbound files. Input was requested on whether MSs wanted to go with the original masking approach or align with the OECD rule, but we cannot see the verdict on CircaBC. Can you please advise of the outcome to this?

Answer: TBD

FAQ-12. We would kindly ask you to present the workflow regarding sending messages to CD. We are unsure on why there is a need for REST API as all the data is transferred via CCN queues (sending and receiving).

Answer:

The workflow for sending messages to the DAC8 Central Directory (CD) relies primarily on CCN queues for asynchronous, high-volume data exchange. However, REST APIs are also used for specific complementary functions.

To submit DAC8 Messages using CCN queues, the queue R-DAC8-<MODE>-QUE.AEOI allows the submission of DAC8 messages into the DAC8 Central Directory.

The workflow to send messages to CD is as follows:

- Queue: R-DAC8-<MODE>-QUE.AEOI
- Purpose: Submit new, corrected, or nil DAC8 messages to the Central Directory.
- Message Types:
    - DAC8-INIT-MSG.AEOI (new data)
    - DAC8-NIL-MSG.AEOI (no data to report)
    - DAC8-CORR-MSG.AEOI (corrections to prior submissions)
- Requirements:
    - Payload must be a GZIP-compressed XML file (max 100 MB compressed/uncompressed).

    - Messages are processed asynchronously (order not guaranteed).

- Response:
    - A status message (DAC8-STATUS-MSG.AEOI) is sent to the default output queue (D-DAC8-<MODE>-QUE.AEOI) or a custom queue (if replyToQueue is specified).

- Possible outcomes:
    - Accepted: Message complies with rules; data is persisted in the CD database. The MessageRefId and all the DocRefIds included in the message persisted and were marked as used in the database. They cannot be reused to identify new data in any subsequent messages submitted to the DAC8 Central Directory.
    - Rejected: Message fails validation; data is not persisted. The MessageRefId and all the DocRefIds included in the message persisted and were marked as used in the database. They cannot be reused to identify new data in any subsequent messages submitted to the DAC8 Central Directory.
    - Failed: An error occurs during processing of the DAC8 message. The RCASPs and Crypto-Asset-Users do not persist in the database. If applicable, the MessageRefId and all the DocRefIds contained in the message are not retained and may be reused for a new message submission.

While CCN queues handle the bulk data exchange, REST APIs are used for lightweight, synchronous interactions that do not require large payloads. Their key purposes include

The following Web services are exposed over REST APIs:

- Retrieve status messages: Allows retrieving the status message to report on the validity (as regards the business and technical rules) of a limited number of DAC8 messages
    - Requesting the validity of DAC8 messages for which the requesting MS is not concerned by the reported information is not allowed and is blocked
- Search messages received: Allows searching for a limited list of received DAC8 messages in order to receive their metadata
    - Searching for DAC8 messages for which the requesting MS has not transmitted the reports is not allowed and is blocked
- For both services, the maximum number of DAC8 messages concerned is configurable (by default, this limit is set to 100 DAC8 messages)

A comparison between the two approaches is given as follows:

Feature	CCN Queues	REST APIs
Data Volume	High (up to 100 MB per message)	Low (metadata/statuses only)
Processing	Asynchronous (no real-time guarantee)	Synchronous (immediate response)

Use Case	Bulk submissions, validations, retrievals	Quick status checks, metadata searches
Complexity	Requires CCN/CSI setup	Simpler HTTP integration
Access Control	Strict (queue-based permissions)	Role-based (e.g., DAC8-CD-MS-USER)

FAQ-13. It is our understanding that the document EIS states/defines three types of error messages: (1) CCN FAILED messages (response with error stack); (2) compressed plain text error in transmitting message (output message error); (3) ErrorResponseMessage as XML on GET queue. Do we understand this correctly? We believe all error messages should be as XML.

Answer:

There are two types of error messages:

1. Error stack messages

- Format:
  - A GZIP-compressed plain-text file containing the error stack trace is sent instead of a status message.
  - This is not XML—it is raw technical error details for debugging.
- Purpose:
  - Intended for support teams to diagnose issues (e.g., system crashes, unhandled exceptions).
  - Not meant for business logic validation (e.g., schema errors or rule violations).

2. Other error messages (status message of an invalid DAC8 message, etc): These apply to all errors except error stack messages.

- Format:
  - A GZIP-compressed XML file compliant with the ErrorResponseMessage schema (defined in received_message.xsd).
- Purpose:
  - Provides structured, machine-readable errors for retrieval failures (e.g., "Message not found").

FAQ-14. In which case will Nexus CARF901-CARF905 be used? Should the Nexus value in the Common Domain be restricted to CARF906/CARF907 only? In which situation could other values be used at the DAC level?

Answer: TBD

FAQ-15. In the CD EIS, the submit process states "Messages sent to the queue are processed asynchronously, which means that the processing order is not guaranteed to match the submission order".

Does this mean that we cannot rely on the Confirmation of Delivery to guarantee that the messages we send are processed in the correct order? As a result, would we need to implement a new system that will handle any submission related to a previously sent message until the reception of the status message related to such message. Is there any alternative solution ? This is a noticeable difference with the current CCN implementation (DAC1/DAC2/DAC4).

Answer:

Such as for the other systems relying on CCN/CSI, the Confirm on Delivery (COD) report is sent to the message sender when the message is consumed from the queue of the recipient, meaning that the message is being processed by the system. The Confirmation of Delivery (CoD) cannot be used to guarantee that messages are processed in the correct order in DAC8 CD. Indeed, CCN does not offer a guarantee that messages will be delivered in order.

DAC8 CD processes the messages following the FIFO principle (first in, first out). Since there is no guarantee that the messages are delivered in the correct order, a wait-and-process mechanism is implemented to increase the chance of having the messages processed in the correct order (a check, based on the RCASP's DocSpec information, is made to know if the initial message has been already processed or not).

If the message has been processed, it will continue the processing or will wait a configured delay before attempting to continue processing again (sleep-and-retry behaviour).

This principle is aligned with the documentation provided for DAC2 (see section named "Correction of a correction message") where the following is mentioned:

"If the RR receives messages that it considers as probably being out of order, it should – as a best practice – wait for some time before discarding the message, in case the previous messages arrive some time later."

Such as for the other systems, a status message is pushed to the dedicated queue (D-DAC8-<MODE>-QUE.AEOI queue) to inform the sender that the message has been completely processed, leading either to the acceptance or rejection of the message.

This status message is actually the source of truth for the complete processing of a message, unlike the COD message which cannot guarantee it.

FAQ-16. In the CD EIS, the submit process states" They cannot be reused to identify new data in any subsequent messages submitted to the DAC8 Central Directory.".

This does not appear to be aligned with the general OECD approach where the DocRefId may be reused when a file has been rejected. Consequently, we would need to implement specific handling for submissions to the Central Directory.

Answer:

When a DAC8 message is sent to CCN queues, there are three possible outcomes:

- Accepted: Message complies with rules; data is persisted in the CD database. The MessageRefId and all the DocRefIds included in the message persisted and were marked as used in the database. They cannot be reused to identify new data in any subsequent messages submitted to the DAC8 Central Directory.
- Rejected: Message fails validation; data is not persisted. The MessageRefId and all the DocRefIds included in the message persisted and were marked as used in the database. They cannot be reused to identify new data in any subsequent messages submitted to the DAC8 Central Directory.
- Failed: An error occurs during processing of the DAC8 message. The RCASPs and Crypto-Asset-Users do not persist in the database. If applicable, the MessageRefId and all the DocRefIds contained in the message are not retained and may be reused for a new message submission.

Therefore, if the outcome is Accepted or Rejected, the MessageRefId and all the DocRefIds cannot be reused anymore.

FAQ-17. Can member states retrieve status messages (with validation results) for the messages intended for another member state?

E.g. member state "a" submits a message to the CD for member state "b" and receives a status message with acceptance of the message, but with some record level errors (e.g. TOW). Can member state "b" retrieve that status message along with the actual message (which holds information on users etc.)

Answer:

Yes, Member State "b" (the receiving country) can retrieve both the status message (with validation results) and the actual DAC8 message submitted by Member State "a", but with the following conditions:

Retrieving the DAC8 Message:

- Member State "b" can retrieve the full content of the message (including user data) only if it is the intended recipient of the message
- This is done via the R-DAC8-GET--QUE.AEOI queue (CCN) or the "Retrieve DAC8 message" REST API
- Only successfully processed and accepted messages can be retrieved this way. Failed or rejected messages must be accessed via the DAC8 Central Directory Web Application

Retrieving the Status Message (Validation Results):

Member State "b" cannot directly retrieve the status message via the "Retrieve DAC8 message" service. This service only returns the original message content, not its validation status

However, Member State "b" can:

- View validation results (including errors) for received messages via the DAC8 Central Directory Web Application (under "Received messages" → "Download validation result")
- Use the "Retrieve status messages" REST API to fetch validation statuses for messages it has received, but this is limited to a configurable number of messages (default: 100)
- If the message was rejected or failed, the validation result file (XML for "Rejected" or plain-text error stack trace for "Failed") can be downloaded from the Web Application

FAQ-18. Ensuring all RCASPs are in scope: Member States rely on public registers and, we expect, some sort of OSINT activities for ensuring all RCASPs are in scope.

Seeing as capacity is scarce and we'd at least partly be doing double work, we would welcome exploring possible solutions or ways of working together. For example by way of publishing a list of identified RCASPs or to share information on identified Crypto-Asset Operators.

Answer:

The DAC8 CR serves as a single EU-wide repository where MS tax authorities can register, update, and share information on CAOs, including those operating across borders. This reduces reliance on individual public registers or OSINT (Open-Source Intelligence) by providing a standardised, verified dataset of CAOs. Access to DAC8 CR is not restricted per MS, all registered CAOs and RCASPs are visible be everyone. In particular, Viewer role users (from any MS) can consult all REGISTERED or DELETED CAOs across the EU, enabling cross-checking and reducing redundant identification efforts. For more details, refer to section 5.2 Activities per Role of the "DAC8-CR-User Manual-UMN-v2.00".

FAQ-19. Definition of Reportable Crypto-Asset.

We anticipate questions from the crypto sector regarding whether specific Crypto-Assets are in scope of reporting. We think it could be useful to consider publishing a list of Crypto-Assets

for which Member States and/or the crypto sector have already established whether they are in scope of reporting or not.

Answer: TBD.

FAQ-20. It would be really helpful to know which error codes mean the rejection of the file and what error codes mean to inform about error but accepting the file therefore the records in the file.

In other AEOI the general approach is that error codes 50XXX and 80XXX cause rejection while the others mean acceptance with errors.

Answer:

The 50XXX errors related with file format and that lead to rejection are as follows:

ID	Description	Details	Error code
TR-MSG-50007a	The referenced file is not a proper XML file.	The message received must be a proper XML file.	50007
TR-MSG-50007b	The referenced file does not comply with the CARF XML Schema.	The message received must comply with the CARF XML Schema.	50007

Other 50XXX error codes related with the message format and that lead to rejection are as follows:

ID	Description	Details	Error code
BR-MH-50008	The structure of the MessageRefID is not in the correct format.	The structure of the MessageRefId must follow the applicable format: • the 2 first characters are equal to the Transmitting Country code of the message; • the 4 characters after the second character are equal to the year of the reporting period; • the 2 characters after the sixth character are equal to the Receiving Country code of the message; • and are followed by a unique identifier.	50008

ID	Description	Details	Error code
		(e.g. FR2026LU123456789).	
BR-MH-50009	MessageRefID has already been used.	The MessageRefId must be unique in space and time.	50009

Finally the following 50XXX error code is related with the correlation mechanism:

ID	Description	Details	Error code
BR-COR-50010	The referenced file contains one or more records with a DocTypeIndic value in the range OECD10-OECD13, indicating test data.	The DocTypeIndic codes relating to testing (OECD10, OECD11, OECD12 and OECD13) cannot be used.	50010

Regarding other 50001-50006 errors, except for 50005 which is implemented by checking the presence of forbidden characters (like in other VMs, these errors are out of scope of DAC8 but must still be implemented at national level when tax administrations exchanges with third-countries through CTS.

The 80XXX error codes that lead to rejection are as follows:

ID	Description	Details	Error code
BR-COR-80000	The DocRefID is already used for another record.	The DocRefId must be unique in space and time.	80000
BR-COR-80001	The structure of the DocRefID is not in the correct format.	The structure of the DocRefId must follow the applicable format: • the 2 first characters are equal to the Transmitting Country code of the message; • the 4 characters after the second character are equal to the year of the reporting period; • and are followed by a unique identifier. (e.g. FR2026123456789).	80001

ID	Description	Details	Error code
BR-COR-80002	The CorrDocRefId refers to an unknown record.	The CorrDocRefId must refer to a known record for the specific MS.	80002
BR-COR-80003	The corrected record is no longer valid (invalidated or outdated by a previous correction message).	The CorrDocRefId must refer to a record that is still valid (cannot be invalidated or outdated by a previous correction message).	80003
BR-COR-80004	New (OECD1) or resent (OECD0) data specifies a CorrDocRefId.	The CorrDocRefId cannot be specified for new or resent data.	80004
BR-COR-80005	Corrected (OECD2) or deleted (OECD3) data does not specify a CorrDocRefId.	The CorrDocRefId must be specified for corrected or deleted data.	80005
BR-COR-80006	The CorrMessageRefId has been provided within a DocSpec element.	The CorrMessageRefId is forbidden within the DocSpec element.	80006
BR-COR-80008	The resend option (OECD0) is used for a CryptoUser element.	The resend option (OECD0) can only be used with respect to the RCASP element.	80008
BR-COR-80009	The RCASP element is deleted (OECD3), while all related CryptoUsers are not deleted.	When deleting (OECD3) a Reportable Crypto-Asset Service Provider, all the related Crypto Users must be deleted.	80009
BR-COR-80010	The message contains DocTypeIndic values that do not match the MessageTypeIndic.	The content of the message does not correspond with a Message Type Indic specifying new information (CARF701): • Only OECD0 or OECD1 must be used for the Doc Type Indic of the Reportable Crypto-Asset Service Provider; • Only OECD1 must be used for the Doc Type Indic of the Crypto User. The content of the message does not correspond with a Message Type Indic specifying corrections or deletions (CARF702):	80010

ID	Description	Details	Error code
		• Only OECD0, OECD2 or OECD3 must be used for the Doc Type Indic of the Reportable Crypto-Asset Service Provider; • Only OECD2 or OECD3 must be used for the Doc Type Indic of the Crypto User.	

FAQ-21. What business rules are "file validations"? Just the 50xxx error codes?

We suggest to use the same taxonomy used in CARF: File Validations, Record Validations for Data Fields, Record Validations for Correction, Record Validations for Domestic, Record Validations for future, Custom Validation and maybe an EU Specific Validations.

Answer:

Please refer to the answer for FAQ-20.

FAQ-22. Some 20XXX validations are set to International Context. However, as these validations are not in the OECD Specifications, these cannot be applied in the exchange with OECD jurisdictions as these do not handle these error codes

Answer:

1. Configure the DAC8 Validation Module to:
   - o Apply 20XXX rules for exchanges between EU Member States.
   - o Disable 20XXX rules for exchanges with non-EU jurisdictions (use OECD CARF rules instead).
2. Document and communicate with non-EU partners about which EU-specific rules are not enforced in messages sent to them.

FAQ-23. It is not straightforward to match the RCASP with the CryptoUser as they have different DocRefIds.

We do not see how to implement the validation. It can be IT resources consuming. Since it is not at OECD either we suggest to remove it.

Answer:

The business rule BR-COR-22020 is validated by the DAC8 Central Directory when a correction or deletion message is received. The validation is performed on the CorrDocRefId of the CryptoUser included in the CARFBody, as these messages must correlate with the initial message in which the CryptoUser was first reported. Then, a correlation of the reporting RCASP is done to check that they are identical (managing any corrections on that RCASP is the same way.

FAQ-24. Regarding error code 50007 in OECD framework, why this validation has been split in two validations with two error codes un DAC8: 50007a and 50007b?

Answer:

The error code is 50007, however there are two scenarios when this error code is verified, the first when the referenced file is not a proper XML file (no XML format) which is the TR-MSG-50007a and the second scenario when the the referenced file does not comply with the CARF XML Schema (the file has an XML format but it does not comply with the CARF XAML Schema) which is the TR-MSG-50007a.

FAQ-25. There is no validation with a number or error threshold in any previous AEOI project. We suggest removing it.

Answer:

The maximum number of errors after which the system stops processing the message can be configured. By default, this limit is set to 5000.

FAQ-26. We ask that in case of file errors, the DocRefId not to be kept in the Central Directory so MS can reuse them. This is to not involve the taxpayer if a file error occurs as file errors are MS responsibility.

Answer:

When a DAC8 message is sent to CCN queues, there are three possible outcomes:

- Accepted: Message complies with rules; data is persisted in the CD database. The MessageRefId and all the DocRefIds included in the message persisted and were marked as used in the database. They cannot be reused to identify new data in any subsequent messages submitted to the DAC8 Central Directory.
- Rejected: Message fails validation; data is not persisted. The MessageRefId and all the DocRefIds included in the message persisted and were marked as used in the

database. They cannot be reused to identify new data in any subsequent messages submitted to the DAC8 Central Directory.

- Failed: An error occurs during processing of the DAC8 message. The RCASPs and Crypto-Asset-Users do not persist in the database. If applicable, the MessageRefId and all the DocRefIds contained in the message are not retained and may be reused for a new message submission.

Therefore, if the outcome is Accepted or Rejected, the MessageRefId and all the DocRefIds cannot be reused anymore.

FAQ-27. In Message Processing, it should be clarified what error codes will cause a Status Message of Rejection.

In other AEOI projects just file errors (50XXX) or Record Errors cause a Status Message of rejection. The rest Error Codes should cause a Status Message of Acceptance with errors so the records can be individually corrected by another record reported by the taxpayer using the correction mechanism. Otherwise the taxpayer will have to report all the records in the file again: those with error and those with no errors.

Answer: TBD

FAQ-28. In Figure 9, Page 21 of the External Interface Specification document, how do these errors match with Status Messages explained in previous section 3.6?

Maybe these errors are at CCN level, and they are in a previous stage to receiving Status Messages.

Answer: TBD

FAQ-29. In CCN MESSAGE PROCESSING ERRORS, how do these errors match with Status Messages explained in previous section 3.6?

We do not see how these CCN errors match with Status Message errors? Some CCN error codes overlap CARF Status Messge error codes. E.g. CARF 50007 and DAC8 DAC8-CCN-XSD-INVALID.

Answer: TBD

FAQ-30. Is the error DAC8-CCN-TECHNICAL-ERROR equivalent to SOAP FAULT?

DAC8-CCN-TECHNICAL-ERROR	**A technical error occurred during the processing of the message.**

Answer: TBD

FAQ-31. Is the error DAC8-CCN-MESSAGE-CONTENT-NOT-GZIP equivalent to 50003

DAC8-CCN-MESSAGE-CONTENT-NOT-GZIP	**The CCN message content is not a valid GZIP archive.**

Answer: TBD

FAQ-32. What does the error DAC8-CCN-XML-PARSING-ERROR mean?

DAC8-CCN-XML-PARSING-ERROR	**An error occurred while parsing the XML extracted from the message content.**

Answer: TBD

FAQ-33. Is the error DAC8-CCN-XSD-INVALID equivalent to 50007?

DAC8-CCN-XSD-INVALID	**The XML extracted from the message content is not XSD valid.**

Answer: TBD

FAQ-34. What is the difference between the error DAC8-CCN-NO-ACCEPTED-MESSAGE-FOUND and the error DAC8-CCN-XSD-INVALID?

In both cases we are looking for a MessageRefId but in this case just the accepted ones.

DAC8-CCN-NO-ACCEPTED-MESSAGE-FOUND	**No accepted message found with the requested MessageRefId.**

Answer: TBD

FAQ-35. In practice, we have difficulties to fully identify which entity can be included in the definition of Crypto-Assets Operators (CAO).

According to our interpretation of DAC8, an operator that is not authorised under MiCA does not fall under the Crypto-Assets Service Provider's definition (CASP). It is then automatically designated as a Crypto-Assets Operator (CAO). However, authorisations appear to be required for any activity in the EU. Therefore, we would be grateful if the EU Commission or some colleagues from Member States could shade some lights on the matter and/or provide concrete examples of situations where a professional will be designated as a CAO (and not a CASP).

Answer:

Essentially, any service provider that does not have an obligation under MiCA to get an autorisation will be defined as a CAO. This could be service providers in the EU or outside. One frequently referred to example is a service provider which provides services exclusively in relation to Non-fungible tokens (NFTs). Such assets are not covered by MiCA. Therefore, no autorisation is required or even possible. These service providers are therefore CAOs and need to follow the steps for separate DAC8 registration

FAQ-36. Compliance of uniqueness of registration in the EU.

According to article 8ad "*Member States shall lay down rules pursuant to which a Crypto-Asset Operator shall register with the competent authority of a single Member State in accordance with the rules laid down in Section V, paragraph F, of Annex VI*" (point 7, paragraph 3). Since we cannot provide for extraterritorial rules to guarantee the uniqueness of registration in the EU, we would like some guidance on how to comply with the DAC8 requirements. We gave some thought to two proposals:

=> Proposal 1: Each Member State shall verify the presence of a previous registration in the central register before registering a CAO in its own jurisdiction.

=> Proposal 2: When a given CAO fulfils the conditions set out in Section I(A), (2), (a), (b), (c), (d) or (B) in more than one Member State, the single Member State of registration shall be the Member State in which the operator will have to report under the nexus hierarchy rule. Each Member State has to actively communication on this issue in a user guide for reporting and registration purposes.

Answer: TBD

FAQ-37. Due diligence obligations related to the self-certification.

In order to confirm the "reasonableness" of a self-certification, we encourage service providers to rely on "supporting documents" listed in a regulatory text (i.e. : documents issued by an authorised public authority, such as a certificate of residence). This approach aims to support

service providers in complying with their due diligence obligations. We would be glad to receive feedback on the matter.

Answer: TBD

FAQ-38. Interpretation of the transaction aggregation rule.

When there are several different "exchange types" (eg: Staking and Crypto Loan) for the same crypto-asset and the same type of exchange transaction (e.g. CryptoToCryptoIn) => the RCASP should not fill in the "ExchangeType" tag for the aggregation. Same reasoning for the "AltValuation" tag. Is that correct?
- When there are several different "transfer types" (eg: Airdrop and Mining income) for the same crypto-asset and the same type of transfer (e.g.: CryptoTransferIn) => the aggregation includes the "TransferType"tag since this tag is mandatory. The tag must be filled in, as many times as necessary.

But can you please indicate if we have to report such "transfer types"(eg: Airdrop and Mining income) in different transaction blocks ?

Or will it be accepted to report them in one single transaction block ? (see illustration bellow)

```
58      <ns1:RelevantTransactions>
59          <ns1:CryptoAsset>DTI-9999</ns1:CryptoAsset>
60          <ns1:CryptoTransferIn>
61              <ns1:TransferType>CARF501</ns1:TransferType>
62              <ns1:NumberofTransactions>10</ns1:NumberofTransactions>
63              <ns1:Amount currCode="USD">50000.00</ns1:Amount>
64              <ns1:NumberofUnits>8000</ns1:NumberofUnits>
65          </ns1:CryptoTransferIn>
66          <ns1:CryptoTransferIn>
67              <ns1:TransferType>CARF507</ns1:TransferType>
68              <ns1:NumberofTransactions>15</ns1:NumberofTransactions>
69              <ns1:Amount currCode="USD">60000.00</ns1:Amount>
70              <ns1:NumberofUnits>15000</ns1:NumberofUnits>
71          </ns1:CryptoTransferIn>
72      </ns1:RelevantTransactions>
```

Answer:

As described in the Ad-hoc document to CARF XSD User Guide, for the rule BR-USR-26020, the Relevant Transactions must be aggregated. A given type of transaction must be reported at most once for a combination of Reporting Period, Reportable Crypto-Asset Service Provider, Crypto-User, Crypto-Asset and, when applicable, the transfer type.

This means that the ExchangeType and AltValuation tags are not taken into account in the combination. If it is needed the ExchangeType and AltValuation tags to be reported then it is allowed only once per combination.

To report transactions with different TransferType it is possible to do so, either in different RelevantTransactions blocks or under the same RelevantTransactions block on condition that they concern the same CryptoAsset. For example, both cases below will be accepted:

Case 1: Same RelevantTransactions block

<carf:RelevantTransactions>

<carf:CryptoAsset>DTI-0001</carf:CryptoAsset>

<carf:CryptoTransferIn>

<carf:TransferType>CARF502</carf:TransferType>

<carf:NumberofTransactions>4</carf:NumberofTransactions>

<carf:Amount currCode="KZT">4110.14</carf:Amount>

<carf:NumberofUnits>1.62217403</carf:NumberofUnits>

</carf:CryptoTransferIn>

<carf:CryptoTransferIn>

<carf:TransferType>CARF501</carf:TransferType>

<carf:NumberofTransactions>4</carf:NumberofTransactions>

<carf:Amount currCode="KZT">4110.14</carf:Amount>

<carf:NumberofUnits>1.62217403</carf:NumberofUnits>

</carf:CryptoTransferIn>

</carf:RelevantTransactions>

Case 2: Different RelevantTransactions blocks

<carf:RelevantTransactions>

<carf:CryptoAsset>DTI-0001</carf:CryptoAsset>

<carf:CryptoTransferIn>

<carf:TransferType>CARF502</carf:TransferType>

<carf:NumberofTransactions>4</carf:NumberofTransactions>

<carf:Amount currCode="KZT">4110.14</carf:Amount>

<carf:NumberofUnits>1.62217403</carf:NumberofUnits>

</carf:CryptoTransferIn>

</carf:RelevantTransactions>

<carf:RelevantTransactions>

<carf:CryptoAsset>DTI-0001</carf:CryptoAsset>

<carf:CryptoTransferIn>

<carf:TransferType>CARF501</carf:TransferType>

<carf:NumberofTransactions>4</carf:NumberofTransactions>

<carf:Amount currCode="KZT">4110.14</carf:Amount>

<carf:NumberofUnits>1.62217403</carf:NumberofUnits>

</carf:CryptoTransferIn>

</carf:RelevantTransactions>----------

FAQ-39. Implementation issues of the article 8ad §3 of the DAC8 on the communication in a single Fiat currency.

We would have an extra legal and practical implementation issue on the implementation of the article 8ad §3 of the DAC8 on the communication in a single Fiat currency.

In the EU business rules and in particular the BR-USR-26030, we understand that the relevant transactions related to one type of crypto-asset must be declared in a single Fiat currency "as per article 8ad paragraph 3".

- However, in the case where there are several transactions of crypto-assets "A-type" and several transactions of crypto-assets "B-type", under this business rule, can a RCASP declare the aggregated amount of transactions under A-type in a single Fiat currency such as dollar? And in parallel in euro with respect to transactions under "B-type"?
- In the case where any transactions irrespective of the type of crypto-assets shall be communicated in a single Fiat currency (*e.g* in euro):
    - Would there be a need to amend the business rule?
    - In addition, from an operational point of view, should the RCAPs declare the amount based on the value of euro on 31 December N? Do the Member States have to implement a conversion rule?

Answer:

According to Article 8ad(3)(c) of Council Directive (EU) 2023/2226 of 17 October 2023 amending Directive 2011/16/EU on administrative cooperation in the field of taxation, it is stated that:

- "(vi) where the amount was paid or received in multiple Fiat Currencies, the amount converted and reported in a single Fiat Currency, converted at the time of each Relevant Transaction in a manner that is consistently applied by the Reporting Crypto-Asset Service Provider;"
- This means that any transaction reported within the EU context must be reported in a single fiat currency; otherwise, business rule BR-USR-26030 will be breached.
- This rule is applied at message level. Therefore, if two or more different DAC8 messages are submitted for the same CryptoUser, the transactions may be reported in different fiat currencies across those messages.

Regarding the conversion rules and the operational aspects, the following holds

Section II of the CARF:

«A. For each relevant calendar year or other appropriate reporting period, and subject to the obligations of Reporting Crypto-Asset Service Providers in Section I and the due diligence procedures in Section III, a Reporting Crypto-Asset Service Provider must report the following information with respect to its Crypto-Asset Users that are Reportable Users or that have Controlling Persons that are Reportable Persons: »

«B.3. for each type of Relevant Crypto-Asset with respect to which it has effectuated Relevant Transactions during the relevant calendar year or other appropriate reporting period:
…
(b) the aggregate gross amount paid, the aggregate number of units and the number of Relevant Transactions in respect of acquisitions against Fiat Currency;
(c) the aggregate gross amount received, the aggregate number of units and the number of Relevant Transactions in respect of disposals against Fiat Currency;

«D. For the purposes of subparagraphs A(3)(b) and (c), the amount paid or received must be reported in the Fiat Currency in which it was paid or received. In case the amounts were paid or received in multiple Fiat Currencies, the amounts must be reported in a single Fiat Currency, converted at the time of each Relevant Transaction in a manner that is consistently applied by the Reporting Crypto-Asset Service Provider.»

FAQ-40. In the deletion process, a CAO which has been deleted, why should it be re-registered after 12 months from the deletion date?

Answer:

A CAO can be deleted for various reasons based on the legislation (ceased operations, no clients, etc). When a CAO is deleted due to a reason, then it may be possible that the same

CAO starts having activity again after some time. In this case, if a period of 12 months has passed from the deletion, it must be re-registered with a new IIN (Individual Identification Number).

FAQ-41. Overwriting of the IIN initially generated by DAC8 CR.

When using the UI, upon registration, in our country we provide an IIN to the registering RCASP. The same IIN is used in the reported messages. When we try to submit these data of the RCASP to the CR, the IIN we provided initially to the RCASP will be overwritten by the one generated by DAC8 CR. How can this problem be solved?

Answer:

The workaround to this problem is not to use the UI, but to send these RCASP for registration only by using the S2S interface.

FAQ-42. Why cannot we use our own IIN in the UI? Why is this only in the S2S mode?

Answer:

Using the UI to encode the RCASP, the IIN will be automatically generated by the system. While if you want to use an existing IIN and import it, you have to import it through the use of the S2S interface.

FAQ-43. Why on some occasions we use the word CAO instead of RCASP? Are these synonyms?

Answer:

RCASP is a more broad term and under the RCASP category there are service providers that should report under the MiCA directives. These RCASPs are not concerned by the CR. In the CR we are concerned only about RCASPs which are not under the MiCA directive and we call these CAOs.

FAQ-44. Regarding the procedure for the registration of the change, which is described for the case of UI, is it the same also in the case of S2S interface?

Answer:

We confirm that the change of MSSR is possible by REST API and can be handled via S2S. However, only the approval of the change of MSSR is covered by REST APIs. The change of MSSR itself cannot be triggered via S2S, only the approval of the new MSSR.

FAQ-45. The change of the MMSR is considered as a sensitive administrative operation. Once the MMSR is transferred, the original MS permanently loses access to the related CAO. Is this operation possible through the REST APIs?

Answer:

Given the impact of this operation, this has been intentionally excluded from the encode and register REST APIs, which are designed for fully automated and repeatable S2S processes. Allowing MMSR changes via REST would introduce a significant risk of unintended or incorrect transfers through automation, without sufficient human validation. For security reasons, MSSR transfers are therefore restricted to the DAC8 CR UI, where the action is performed explicitly with full user awareness.

FAQ-46. Regarding the procedure of change of nexus, if it is the MSSR that identifies the change of nexus, does the procedure remain the same?

Answer:

Yes, the procedure remains the same. The new MSSR is notified of the transfer via the notification mechanism.

FAQ-47. How does the notification mechanism work?

Regarding the process of change of nexus, it is mentioned that the new MSSR is notified of the transfer via the notification mechanism. How should the notification mechanism work when we are not using the S2S interface? Is there a notification by email or any other notification?

Answer:

The solution is the one based on the CCN/CSI communication platform which is widely used for the exchange of information between the MSs.

FAQ-48. Compliance for single registration.

According to the DAC8 directive, each MS will make sure for a single registration of an operator. However, we do not have extraterritorial rules which would give us the possibility to

check that the operator has already another registration in another country and we would like to know how this can be dealt with by the domestic rules? Since it is difficult to translate this into the domestic rules, is the procedure in DAC8 CR compliant with the directive and the domestic rules?

Answer: TBD:

FAQ-49. Regarding the uniqueness scope which is effectively global for the sending jurisdiction/system, does this mean that the DocRefID is unique only for the single MS or for all the MSs?

Answer:

The uniqueness is globally unique because the structure of the of the DocRefID is: Country code of sending jurisdiction + reporting year + unique identifier. This makes it unique for the single country but also unique globally.

FAQ-50. What happens if the message was not delivered for some (technical) reason?

Does it mean that the DocRefID was used even though the receiving state does not have it in its records because it did not receive it?

Answer:

If DAC8 CD did not consume the message due to a delivery issue, then the DocRefIDs are not considered as used.

FAQ-51. Regarding DocRefID logged for audit/debugging, does this mean that if we submit a file with errors, we cannot resubmit the corrected file using the same DocRefID?

Answer:

Yes, the same DocRefID cannot be used anymore.

FAQ-52. Uniqueness of DocRefIDs,

Regarding the uniqueness of DocRefIDs, there have been different interpretations whether the same DocRefID can be used it if has been sent in CCN. Unique in space and time has been

interpreted that if sent to CCN, it has been used and it cannot be reused. In previous DACs, before DAC8, there have been different interpretations on this topic.

Answer:

The implementation in DAC8 is different compared to previous DACs. The already consumed DocRefIDs cannot be used anymore.

FAQ-53. As to the rules that will not lead to rejection: rule TR-MSG-99999 will thus lead to rejection. What comment should be provided to the reporting RCASP as the message reported has already been approved by the MS.

Answer: TBD

FAQ-54. Nexus values clarification.

Concerning the user of Nexus values, all values that are provided in the Nexus_Type_enumtype are meant to be used for all case that apply, even the EU specific CARF906 and CARF907. When submitting to the Central Directory, the RCASP is either a CARF906 or a CARF907. We don't see any scenario where the RCASP can be another value in the range CARF901-CARF905. Can you elaborate and provide examples? We intend to check that an IIN or LEI is provided based on the nexus information and this could not work if other values could be provided.

Answer: TBD

FAQ-55. If a message contains a record affected by an error 90000/90001/90002, will the message and the record be accepted or will the message be accepted except for the record impacted by the error/warning?

Answer:

Yes, the message will be accepted.

FAQ-56. Are 90000, 90001, 90002 rules for exception, therefore no reason for rejection.

Answer:

Yes, this is correct.

FAQ-57. Does the validation rule BR-USR-26030 mean that an error is always generated when a Crypto User has multiple transaction types associated with a single crypto asset and different currencies are specified for those transactions?

Answer: TBD

FAQ-58. What happens when you send split messages?

Answer:

When sending split messages, you should first send the first part and make sure that is has been processed before sending the second part. This is to avoid that the second arrives before the first part has been processed.

FAQ-59. When is the splitting in parts of a message necessary?

Answer:

Splitting is required only if the Message is larger than 100MB.

FAQ-60. Explanations regarding the definition of CAO.

Answer:

Essentially, any service provider that does not have an obligation under MiCA to get an authorisation will be defined as a CAO. This could be service providers in the EU or outside. One frequently referred to example is a service provider which provides services exclusively in relation to non-fungible tokens (NFTs). Such assets are not covered by MiCA. Therefore, no authorisation is required or even possible. These service providers are therefore CAOs and need to follow the steps for separate DAC8 registration.

FAQ-61. What is meant by Data Retention?

Answer:

Data retention refers to the practice of determining how long personal data is stored and what happens to it over time within an organization. It involves keeping data only for a specific purpose and ensuring that it is not stored indefinitely without justification. Once the purpose for which the data was collected has been fulfilled, the organization should either delete the data or anonymize it so that it can no longer be linked to an individual. This approach is closely linked to the General Data Protection Regulation (GDPR), which establishes strict rules on how personal data must be handled within the European Union. One of the key principles under GDPR is the "storage limitation" principle, which requires that personal data be kept only for as long as necessary for the purposes for which it was collected. This means organizations must actively decide and justify retention periods instead of keeping data indefinitely.

FAQ-62. What are the implications of Data Retention for MSs?

Answer:

As explained in Recital 40 of DAC8, the minimum retention period of records of information obtained through the exchange of information between Member States pursuant to Directive 2011/16/EU should not be longer than necessary but, in any event, not shorter than five years. Member States should not retain information longer than necessary to achieve the purposes of this Directive. Regarding implications for MSs, Article 22 of DAC8, defines that Member States shall retain the records of the information received through the automatic exchange of information pursuant to Articles 8 to 8ad for no longer than necessary but in any event not less than five years from its date of receipt to achieve the purposes of this Directive.

Based on the above, DAC8-CD will provide MSs with the flexibility to configure via the user Interface of DAC8 the data retention periods that align with the MSs own data retention policy.

FAQ-63. OECD XSD 1.5 Typos

Answer:

In version v1.5 of the CARF XSD schema, there is a typographical error for the value value="CARF504" in the TransferType EnumType. The label is defined as "Crpyto loan" instead of "Crypto loan". In addition, there is a lock of unified approach to the presentation of values, as the same term currently appears with different capitalisation, namely "Loan" and "loan.

1. FAQ-64. What is meant by uniqueness of DocRefID in space and time?

The OECD CARF XML Schema User Guide states that DocRefID must be globally unique and not just within a file or reporting period, but "in space and time". The definition is:

“MessageRefID and DocRefID must be unique in space and time (i.e. there must be no other message or record in existence that has the same reference identifier).” The guide further explains:

- DocRefID is the unique identifier for a record/document and all its child elements.
- Any correction or deletion must use a new DocRefID.
- CorrDocRefID must point to the latest previously sent DocRefID for that record.

The OECD also gives the expected structure:

- country code of sending jurisdiction
- reporting year
- unique identifier

Example:
CA2023286abc123xyz
Practically, this means:

- It must never be reused a DocRefID, even in later years or later correction cycles.
- A corrected record gets:
  - a new DocRefID
  - a CorrDocRefID referencing the immediately preceding version.
  - The uniqueness scope is effectively global for the sending jurisdiction/system.

FAQ-65. What is the behaviour in DAC8 CD in case of file errors?

Answer:

The DAC8 Central Directory adheres to the OECD’s definitions and implements them as specified in the artefacts validated by the Member States. In the event of a file error, the entire file is rejected, and both the message and associated DocRefIDs are stored in the database. Additionally, users have the option to download rejected messages for debugging purposes.

Designed as a message hub, DAC8 records all incoming messages. However, users should not treat the Central Directory as a trial-and-error system, repeatedly uploading the same message until a successful validation is received. This approach was intentionally restricted to minimise unnecessary data volume in the database, ensuring smoother processing of large datasets. Given that pre-validation of data is a key concern before submission to DAC8, the application provides a dedicated validation service, as detailed in the External Interface Specification (EIS). Message processing may result in one of three outcomes: accepted, rejected, or failed. While no CARF-compliant status message (as per the Status Message XSD) is generated, the system returns a response containing the error stack trace for troubleshooting. In all cases, neither the DocRefIDs nor the MessageRefId are marked as used, meaning they remain available for revalidation or resubmission.

To prevent submission issues, National Administrations are strongly advised to utilise the validation service prior to submitting any messages. For further guidance, please refer to the EIS documentation.

FAQ-66. Error code 26020.

With the error code 26020 - "*The RelevantTransactions elements are not aggregated*.", if we have to report several ExchangeType_EnumTypes (Staking / Crypto Loan / Wrapping / Collateral) for a specific relevant transaction type (e.g. : CryptoFiatOut), how do we aggregate the different amounts? (Same question for transfers)

And same question for the "AltValuation" tag (Book Value / Third-party value / Recent RCASP valuation / Reasonable estimate by RCASP). Can the tag be repeated as the CARF XML allows it?

Answer:

To report multiple ExchangeType_EnumTypes for a given relevant transaction type, this must be done by supplying multiple RelevantTransactions elements.

For example:

The following will break the BR 26020 as the two CryptoToCryptoIn transactions should be aggregated since they are reported under the same RelevantTransactions element even though the ExchangeType is different for these two:

```
<carf:RelevantTransactions>
   <carf:CryptoAsset>DTI-0001</carf:CryptoAsset>
   <carf:CryptoToCryptoIn>
      <carf:ExchangeType>CARF402</carf:ExchangeType>
      <carf:NumberofTransactions>1</carf:NumberofTransactions>
      <carf:Amount currCode="KZT">1027.54</carf:Amount>
      <carf:NumberofUnits>0.41</carf:NumberofUnits>
   </carf:CryptoToCryptoIn>
   <carf:CryptoToCryptoIn>
      <carf:ExchangeType>CARF401</carf:ExchangeType>
      <carf:NumberofTransactions>1</carf:NumberofTransactions>
      <carf:Amount currCode="KZT">1027.54</carf:Amount>
      <carf:NumberofUnits>0.41</carf:NumberofUnits>
   </carf:CryptoToCryptoIn>
</carf:RelevantTransactions>
```

But the following will be accepted, as per each RelevantTransactions element, only one CryptoToCryptoIn is reported with different ExchangeType_EnumTypes:

```
<carf:RelevantTransactions>
   <carf:CryptoAsset>DTI-9999</carf:CryptoAsset>
   <carf:CryptoToCryptoIn>
      <carf:ExchangeType>CARF401</carf:ExchangeType>
      <carf:NumberofTransactions>1</carf:NumberofTransactions>
      <carf:Amount currCode="KZT">1027.54</carf:Amount>
      <carf:NumberofUnits>0.41</carf:NumberofUnits>
   </carf:CryptoToCryptoIn>
</carf:RelevantTransactions>
<carf:RelevantTransactions>
   <carf:CryptoAsset>DTI-9998</carf:CryptoAsset>
   <carf:CryptoToCryptoIn>
      <carf:ExchangeType>CARF402</carf:ExchangeType>
      <carf:NumberofTransactions>1</carf:NumberofTransactions>
      <carf:Amount currCode="KZT">1027.54</carf:Amount>
      <carf:NumberofUnits>0.41</carf:NumberofUnits>
   </carf:CryptoToCryptoIn>
</carf:RelevantTransactions>
```

For the use of 'AltValuation', the previously described method has to be followed by reporting multiple RelevantTransactions elements.

FAQ-67. Reporting and validation of the CryptoAsset element.

Under Article 8ad(3)(c)(i) of DAC8, Reporting Crypto-Asset Service Providers are required to report the full name of each type of Reportable Crypto-Asset. OECD CARF guidance indicates that the Crypto-Asset name should be reported in line with the Digital Token Identifier (DTI) where possible, while also allowing the use of other commonly used names or free text if no DTI is available.

Considering that the use of DTI is not mandatory and that no official, publicly available OECD DTI database currently exists, the questions are:

1. Is the tax authority expected to verify whether the *CryptoAsset* element reported by the RCASP follows DTI naming conventions, beyond basic technical (XML) validation?

2. If such verification is expected, what official and up-to-date source of DTI information should the tax authority use?

Answer:

Regarding the Digital Token Identifier (DTI), OECD CARF guidance indicates that:

- The Crypto-Asset name should be reported in line with the Digital Token Identifier (DTI) where possible.
- The use of other commonly used names or free text is allowed if no DTI is available.

The use of the DTI is not mandatory and there is no official DTI database. In addition, there is no need to validate DTI against any naming conventions. MSs should just proceed with a technical XML validity check.

FAQ-68. With error code 24010 - "The TIN is set to unknown, but no Identification Service was used., how to manage multi-residents that could involve EU residences and extra-EU residences and when should the "unknown" value for a TIN be used?

Answer:

The error code 24010 will be triggered as per Article 8ad paragraph 3(a) and (b). There is no distinction between EU or third-countries TIN. All TINs reported will be validated, either EU or non-EU. In case a non-EU TIN is provided as unknown, but no Identification Service has been used, then the error code 24010 will be thrown away and the whole file will be rejected. To avoid that, the unknown non-EU must not be reported.

There should be no cases where mixture of known and unknown TIN must be reported. The "unknown" TIN is only allowed to comply with the reporting using an Identification Service. Considering a CryptoUser with multiple TINs, all of them must be known and at least one should match the receiving country indicated.

All TINs reported should be known unless an Identification Service has been used. As described in the "Ad-hoc document to CARF XSD User Guide", when an Identification Service is used, the TIN must be marked as unknown as this is the discriminating factor for the Identification Service scenario in the EU context. An Identification Service refers to any direct service provided by a Tax Administration for the purpose of enabling an RCASP to verify the identity and residence of a Reportable Person.

FAQ-69. Interpretations regarding the Error code 24020.

With Error code 24020 - "A jurisdiction is reported for the issuance of the TIN, while the TIN was marked unknown.". As per the explanations provided, the jurisdiction that issued the TIN must always be provided, unless the TIN was marked as unknown. However, it is important to to know precisely what will be verified by the validation module.

Which of the following interpretations holds in this regard?

a) if the TIN is marked unknown, then the Jurisdiction must not be provided (prohibition)

b) if a TIN is provided then the Jurisdiction of issuance must be indicated (mandatory). And in this case, does the VM verify whether each TIN provided is linked to an "IssuedBy" tag ?

Answer:

Since the use of an 'unknown' TIN is permitted only for reporting and Identification Service, the error code should address cases where a known TIN is provided without an associated jurisdiction. Therefore, the second approach (point b) should be applied. The VM will verify all TINs submitted. The VM will verify whether each TIN provided is linked to an "IssuedBy" tag.

The description of error code 24020 will be updated to match applied approach.

FAQ-70. Regarding error code 24040 - "The place of birth is reported, while an Identification Service was used.", which of the following check(s) will be carried out?

a) The place of birth is reported, while an Identification Service was used (prohibition)
b) The place of birth must be provided for an individual Reportable User, unless an Identification Service was used (mandatory).

Answer:

Both checks a) and b) mentioned above will trigger the error code 24040.

Therefore, the error code 24040 must be split into 2 rules:

- BR-PAR-24040a: The place of birth is reported, while an Identification Service was used. In this case, the place of birth must not be provided (prohibition)
- BR-PAR-24040b: The place of birth is missing, while an individual Reportable User was reported. In this case, the place of birth is mandatory to be provided (mandatory)

FAQ-71. Regarding error code 60011 - "The CryptoUser element is missing while no OtherNexus is provided.", should we report data with OtherNexus element in a separate file?

Is it mandatory or optional? Should we report such files, do we report them as CARF701 with no CryptoUsers or CARF703 messages?

Answer:

According to the CARF Schema User Guide, when reporting in another jurisdiction with stronger nexus, the Other Nexus must be provided, and no Crypto User must be reported. Based on the XSD, a DAC8 message may contain multiple CARFBody elements with one RCASP element only, and data does not need to be reported in a separate file. If reported as separate files, they can be reported either as CARF701 or CARF703 but without any CryptoUsers in both cases.

FAQ-72. Regarding error code 10020 - "The referenced file exceeds the maximum allowed size." What is the maximum file size that will be accepted by the validation module?

Answer:

The message size limit is, by default, set to 100MB.

FAQ-73. Regarding Error code 22010 - "The Message only contains resent data (OECD0)", our understanding is that "OECD0" can only be used for RCASP's data. We would like to know exactly what the validation module will verify when it comes to that specific error code.

Does this mean that the VM will only check that no CryptoUser data is sent with an "OECD0" code ? Or does this mean that the VM will also check that no RCASP element is sent with the "OECD0" code , when no crypto user data is to be sent ?

Answer:

The VM will check:

- all DocTypeIndic elements, and;
- if all DocTypeIndic values are set to OECD0.

If some CryptoUsers have the DocTypeIndic set to OECD0, the error code 80008 will be triggered (both error codes might then be reported).

FAQ-74. Regarding error code 20050 -"The TransmittingCountry does not match the user's country code.", do you mean by "user" the CCN user's ISO code? Should we refer to the ACDT n°111 document for the ISO codes?

Answer:

Indeed, we mean the CCN user's country ISO code, e.g. "FR" for France or "IT" for Italy. The DAC territorial scope is determined in Article 2 of the DAC (COUNCIL DIRECTIVE 2011/16/EU):

- "1. This Directive shall apply to all taxes of any kind levied by, or on behalf of, a Member State or the Member State's territorial or administrative subdivisions, including the local authorities."
- "4. This Directive shall apply to the taxes referred to in paragraph 1 levied within the territory to which the Treaties apply by virtue of Article 52 of the treaty of the European Union."

FAQ-75. Terminology of OECD and DAC8.

We noticed that the wording in the "OECD UserGuide" is different from the "DAC8 Ad hoc document to CARF Userguide".

We understand that for DAC8 purposes, the nexuses Authorisation or Remote (and Branch) have to be used:

• CARF906 – Authorisation

[EU specific] This value indicates that the Reporting Crypto-Asset Service Provider is reporting in the EU Member State where it is authorised under Regulation 2023/1114

• CARF907 – Remote Services

[EU specific] This value indicates that the Reporting Crypto-Asset Service Provider that is not authorised under Regulation 2023/1114 is reporting in the EU Member State of single registration.

• CARF905 – Branch

This value indicates that the Entity Reporting Crypto-Asset Service Provider maintains a branch in the jurisdiction in respect of which it is reporting.

Instead, for CARF purposes we would use:

• CARF901 – Tax Residence

This value indicates that the Entity or individual Reporting Crypto-Asset Service Provider is reporting in the jurisdiction where it is resident for tax purposes.

• CARF902 – Incorporation

This value indicates that the Entity Reporting Crypto-Asset Service Provider is reporting in the jurisdiction under the laws of which it is incorporated or organised and either has legal personality in such jurisdiction or has an obligation to file tax returns or tax information returns to the tax authorities in such jurisdiction with respect to the income of the Entity.

• CARF903 – Management

This value indicates that the Entity Reporting Crypto-Asset Service Provider is reporting in the jurisdiction where it is managed from.

• CARF904 – Place of Business

This value indicates that the Entity or individual Reporting Crypto-Asset Service Provider is reporting in the jurisdiction where it has a regular place of business.

• CARF905 – Branch

This value indicates that the Entity Reporting Crypto-Asset Service Provider maintains a branch in the jurisdiction in respect of which it is reporting.

The question about the element “OtherNexus” arose at this point, especially as the wording between EC and CARF differs:

- *OCDE (page 19): This optional element, which jurisdictions may choose to use for domestic reporting purposes or in order to notify the concerned partner jurisdiction, indicates that Reporting Crypto-Asset Service Provider has an **equivalent or stronger nexus** in another jurisdiction, whereby reporting under the CARF will take place in such jurisdiction.*
- *DAC8 Ad hoc document to CARF Userguide (BR-RCASP-60010 page 31) : "The value of OtherNexus must be **equal or inferior** to the value of Nexus or correspond to CARF906.*

For DAC8 purposes, this element should be used in case of “Remote nexus” to indicate whether there is an equal or lower nexus in other Member States. In this case, this element should be repeatable, which is not the case. Only one information can be included (which seams not reflecting the reality). For which purposes/aim does “OtherNexus” should be used in DAC8/What information is expected here?

Moreover, in CARF, this element is used in case reporting is done in a JSD/MS with a lower nexus, e.g. HQ is in the US which is the highest nexus, but reporting was done in Luxembourg as US has not implemented CARF yet.

Can you clarify this issue?

Answer**:**

“Concerning the use of Nexus values, all values that are provided in the Nexus_Type_enumtype are meant to be used for all cases that apply, even the EU specific CARF906 and CARF907.

In DAC8 the use of OtherNexus is meant for cases where the RCASP is reporting in a jurisdiction with a lower nexus because the higher nexus jurisdiction is not yet participating in CARF schema.

According to the rule BR-RCASP-60010 described in the Ad-hoc document to CARF XSD User Guide, the expected value for the OtherNexus is equal to or greater than the Nexus value.

Furthermore, the value CARF907 is not allowed for the OtherNexus as it is the smallest value in the enumeration.

The following examples summarise the cases that are accepted, or not, by DAC8.

{code:xml}

<!--Accepted-->

```
<carf:Nexus>CARF902</carf:Nexus>
   <carf:OtherNexus Nexus="CARF902" ResCountryCode="LU"/>

<!--Accepted-->
<carf:Nexus>CARF905</carf:Nexus>
   <carf:OtherNexus Nexus="CARF902" ResCountryCode="LU"/>

<!--Accepted-->
<carf:Nexus>CARF907</carf:Nexus>
   <carf:OtherNexus Nexus="CARF906" ResCountryCode="LU"/>

<!--Not Accepted-->
<carf:Nexus>CARF906</carf:Nexus>
   <carf:OtherNexus Nexus="CARF907" ResCountryCode="LU"/>

<!--Not Accepted-->
<carf:Nexus>CARF902</carf:Nexus>
   <carf:OtherNexus Nexus="CARF905" ResCountryCode="LU"/>
{code}
```

FAQ-76. Regarding the security aspects for the security logs, the exploitation and analysis of business logs that are requested in the COM Security Polic, is apparently not mandatory, but we would like to be conform to those rules. Is there a document on these aspects?

Answer:

Please be informed that a brand-new Taxation Security Plan will be published shortly (currently in review cycle). This innovative Security Plan is incorporating the most recent NIST and ISO 27001 standards, while providing a self-assessment tool for the identification and implementation of security measures adapted to the needs of each specific administration.

In this context we would suggest to the tax administrations of MS to expect the publication of the new Taxation Security Plan for a more effective application of security measures. Detailed information and guidance will be provided shortly by DG TAXUD.

FAQ-77. Exchange rate and valuation for crypto-asset transfer transactions.

A Reporting Crypto-Asset Service Provider (RCASP) has submitted a question to the national Tax Administration regarding the valuation method for crypto-asset transfer transactions. Specifically, the RCASP seeks clarification on whether using end-of-day rates is permissible under DAC8. The RCASP notes that, given the vast and continuously expanding range of crypto-assets, it is practically impossible to determine an accurate exchange rate at the (exact) time each relevant transaction occurs.

Our preliminary assessment is that using end-of-day valuation rates, consistently applied, is permissible. This view is based on the valuation and currency translation rules for crypto-to-fiat and/or crypto-to-crypto transactions as set out in the OECD CARF Commentary (sections II (D), (E) and (F). Seeing as the valuation methods used across Member States can have quite some impact on the information reported under DAC8-obligations, we would like to seek your confirmation (or rebuttal) of our view.

Answer: TBD