DDRL DOCUMENT DETAILING ENGAGEMENT BETWEEN DDRL AND TRACE AND NON-TRACE AUTHORITIES UNDER SFTR

July 2020

Contents

OVERVIEW AND REGULATORY SCOPE

The Securities Financing Transaction Regulation ('SFTR') is part of the European Union ('EU') legislative framework seeking to regulate securities financing transactions and provide increased transparency with the aim of monitoring systemic risk factors. SFTR is born out of a global financial stability board ('FSB') agreement to monitor financing markets and illuminate shadow banking, in a similar way to G20 commitments to monitor systemic risk in derivatives through premier regulations such as European Market Infrastructure Regulation ('EMIR') in Europe, and Dodd-Frank Act in the United States of America ('USA'). The European Securities and Market Authority ('ESMA') is the European overarching regulator that has been mandated to implement the rules and technical standards for SFTR.

The DTCC Derivatives Repository Plc ('DDRL') intends to register its business for SFTR Trade Repository services and once authorized will provide regulatory reporting under the rules and requirements of the SFTR regime. The purpose of this document is to provide an overview of DDRL's engagement with TRACE and Non-TRACE authorities for the purposes of regulatory reporting under the rules and requirements of the SFTR regime.

First, it presents the legislative framework that has prompted a new relationship eco-system with supranational and national authorities within the EU and wider European Economic Area ('EEA') and DDRL's position at the heart of the SFTR product offering.

Secondly, it describes how the regulatory authorities are set up and are enabled to access SFTR data captured and stored within DDRL.

Thirdly, it describes how authorities connect; how authorities send data queries; what are the naming conventions for data queries; how authorities send feedback messages; how authorities send data response file back and lastly, information around service level agreements ('SLAs').

Fourthly, this document presents an overview of how recurrent and ad-hoc data queries are processed via TRACE and outside the TRACE environment (i.e. Non-TRACE) for SFTR authorities.

Last, both types of queries, for TRACE as well for Non-TRACE are presented with their service level agreements ('SLAs').

DDRL follows the same data query execution model for TRACE and Non-TRACE authorities, in line with regulatory specifications in the commission delegated regulation (EU) 2019/357 of 13 December 2018 and TRACE schema. There is, nevertheless, one major distinction at the 'Inbound/Outbound' stage of query processing, which will be explained throughout this document.

LEGISLATIVE FRAMEWORK

One of DDRL's key regulatory requirements under the SFTR regime is to offer transfer and data availability to all authorities listed in the EU regulation No 2015/2365 of the European Parliament and of the Council of 25 November 2015 on transparency of securities financing transactions and of reuse ('SFTR'). article 16 (1) of SFTR stipulates that a trade repository shall make the necessary information available to the following regulatory entities, enabling them to fulfill their respective responsibilities and mandates.

For DDRL to meet its requirements for transparency and data availability, it must ensure that the regulatory authorities enumerated in the EU regulation No 2015/2365 ('SFTR'), article 32, receive direct and immediate access to the details of SFT Reports in a timely manner, allowing those entities to fulfil their respective regulatory mandates.

Authorities listed in the EU regulation No 2015/2365 of the European Parliament and of the Council of 25 November 2015 on transparency of securities financing transactions and of reuse ('SFTR')
ESMA
EBA
EIOPA
ESRB
The competent authority supervising the trading venues of the reported transactions
The relevant members of the ESCB, including the European Central Bank (ECB) in carrying out its tasks within a single supervisory mechanism under Council Regulations (EU) No 1024/2013
The relevant authorities of a third country in respect of which an implementing act pursuant to Article 19(1) has been adopted
Supervisory authorities designated under Article 4 of Directive 2004/25/EC of the European Parliament and of the Council
The relevant Union securities and market authorities whose respective supervisory responsibilities and mandates cover transactions, markets, participants and assets which fall within the scope of this Regulation]
The Agency for the Cooperation of Energy Regulators established by Regulation (EC) No 713/2009 of the European Parliament and of the Council
The resolution authorities designated under Article 3 of Directive 2014/59/EU of the European Parliament and the Council
The Single Resolution Board established by Regulation (EU) No 806/2014 of the European Parliament and of the Council
Under EU regulation No 2015/2365, Article 16(1). For the purpose of this Regulation, competent authorities shall comprise the following: For **financial counterparties**, competent authorities or national competent authorities within the meaning of Regulations (EU) No 648/2012, (EU) No 1024/2013 and (EU) No 909/2014 and of Directives 2003/41/EC, 2009/65/EC, 2011/61/EU, 2013/36/EU and 2014/65/EU, and the supervisory authorities within the meaning of Directive 2009/138/EC For **non-financial counterparties**, the competent authorities designated in accordance with Article 10(5) of Regulation (EU) No 648/2012
For the purpose of Articles 13 and 14 of this Regulation, concerning UCITS management companies and UCITS investment companies, the competent authorities designated in accordance with Article 97 of Directive 2009/65/EC

For the purpose of Articles 13 and 14 of this Regulation, concerning AIFMs, the competent authorities designated in accordance with Article 44 of Directive 2011/61/EC.

The financial counterparties classified under SFTR lists a wider range of corporation sectors than the EMIR list of financial counterparties, and they are defined as per European System of Accounts 2010.

The list of Financial Counterparties, classified under SFTR as fit and apt to withhold the responsibility of full reporting for both sides of an SFTR trade report
Credit institutions ('CDTI')
Investment firms ('INVF')
Insurance undertakings ('INUN')
Alternative fund managers managed by AIFMs ('AIFD')
Institution for occupational retirement provisions ('ORPI')
Central counterparties ('CCPS')
Reinsurance undertakings ('REIN')
Central securities depositories ('CSDS')
UCITs and its management companies ('UCIT')

The list of Non - Financial Counterparties, categorized as per the main sections of Statistical classification of economic activities in the European Community('NACE')
'Agriculture, forestry and fishing'
'Mining and quarrying'
'Manufacturing'
'electricity, gas, steam and air conditioning supply'
'Water supply, sewerage, waste management and remediation activities'
'Construction'
'Wholesale and retail trade, repair of motor vehicles and motorcycles'
'Transportation and storage'
'Accommodation and food service activities'

'Information and communication'
'Financial and insurance activities'
'Real estate activities'
'Professional, scientific and technical activities'
'Administrative and support service activities'
'Public administration and defense; compulsory social security'
'Education'
'Human health and social work activities'
'Arts, entertainment and recreation'
'Other service activities'
'Activities of households as employers; undifferentiated goods – and services – producing activities of households for own use',
'Activities of extraterritorial organizations and bodies.

TRACE AUTHORITY SET-UP

TRACE is the system provided by ESMA to authorities to enable access to SFTR data held within trade repositories. An authority can only be set for TRACE via ESMA. Designated users within competent authorities will be able to connect to TRACE and submit data requests via the ESMA Hub. For new requests, ESMA will email ddrltrace@dtcc.com requesting TRACE set up for the authority.

The Regulatory Reporting team provide authorities with the necessary information and support to get registered with the trade repository from the initial contact to the final stage by verifying the account has been set up and that the first reports are received by the authorities. The requesting authority must complete the DDRL SFTR onboarding form and sign it off before it is passed on to DDRL Compliance for final diligent checks and approval. Once this first stage of the workflow is completed, the onboarding process will progress.

The Onboarding team will be approached in order to set up the requesting authority for TRACE. The same team will confirm via email once the set-up for TRACE for the requested authorities is complete.

The Common Data Transfer Service (CDTS) team will check and confirm that encryption certificates are available for Prod / PSE for the authorities, and that they have been downloaded in preparation to process any data queries received. Certificates will be loaded at a weekend, as part of the Change Management process. Once CDTS have confirmed that the certificates are available, and the

internal support team have confirmed that the account is set up correctly for Production / PSE, the EU Regulatory Reporting team will contact the authority to confirm that the account set-up is complete, and that they can now start to submit data queries in Production / PSE.

If CDTS confirm any issues with downloading certificates (for example certificates aren't available or they have expired), the EU Regulatory Reporting team will contact ESMA (support@esma.europa.eu) to confirm the issue and ask when the correct certificate will be available. More granular details on the TRACE authority set-up process flow are to be followed as part of the adjacent DDRL regulator on-boarding procedure.

The EU Regulator Reporting team will verify the regulator reports are produced and email the authority to confirm they have been able to access the reports in the portal and that they understand the contents of each report. Should the authority be unable to access the reports in the portal, the EU Regulatory Reporting team will investigate and include any other relevant support teams until the issue is resolved.

Once the onboarding of the TRACE authority is completed, the respective authority will be assigned with a 'NCA Code' (see below example) and the onboarding data will be captured and stored internally.

AUTHORITY	COUNTRY	NCA TRACE CODE
Bundesbank	Germany	'CABUN'

If the requesting authority is a Supranational Authority (i.e. 'ESMA', 'EBA', 'EIOPA', 'ESRB) the authority will be entitled to access all SFTs (subject to self-declared restrictions based on the Corporate Sector of the Reporting Counterparty or Product Type).

If the requesting authority is a Member State Authority, they must clearly identify their mandates and defined responsibilities. There may be one or multiple mandates based on their underlying objectives and responsibilities and this prerequisite will drive the jurisdiction and type of static data captured under each Member State authority profile. This static data will be used to filter reports to only include SFTR data that authorities are entitled to access, when generating the data response reports.

NON -TRACE AUTHORITY SET-UP

Any authority which has not subscribed to ESMA Hub for common and centralized access to SFTs is considered a Non -Trace Authority, for the purpose of a clear distinction between TRACE and Non-TRACE authorities. Many of these authorities have different mandates and needs and as a result, their onboarding process and account set-up are tailored as per their specific regulatory profile. However, to avoid unnecessary administrative burden, DDRL will offer a single connectivity per each authority profile, irrespective of the number and nature of mandates, also in line with the regulatory basis (article 2 of the Commission Delegated Regulation (EU) 2019/357 of 13 December 2018 supplementing Regulation (EU) 2015/2365).

The EU Regulatory Reporting team represents the designated DDRL Hub responsible for the regulatory liaison with the authorities. The team is also responsible for the publication of instructions on the DDRL website that the SFTR mandated entities are to follow in order to access SFTs reports. The EU Regulatory Reporting team provides authorities with the necessary information and support to get registered with the trade repository from the initial email contact to the final regulatory onboarding stage.

The Regulatory Reporting team verifies the completeness and accuracy of the regulatory onboarding forms, as per article 4 of the Commission Delegated Regulation (EU) 2019/357, as well as the successful authority profile set-up and the timely and successful receipt of first SFTR reports. The requesting authority must complete the DDRL SFTR onboarding form and sign it off before it is passed on to DDRL Compliance for final diligent checks and approval. Once this first stage of the workflow is completed, the onboarding process will progress.

The onboarding team will set up the regulatory authority profile and confirm the internal account set up. The same team will ensure that the regulator reports will generate from the next reporting date and be available for download from the EU Portal.

DDRL has implemented the necessary technical arrangements to enable the SFTR mandated authorities to connect using the SSH File Transfer Protocol and standardized XML messages as per ISO methodology. The latest ISO20022 XML schemas for SFTR Reporting may be found on ESMA's official website under "XML SFTR Reporting Schemas. Each Non-TRACE authority will be assigned a unique OCODE which be used by the authority when making data requests to DDRL.

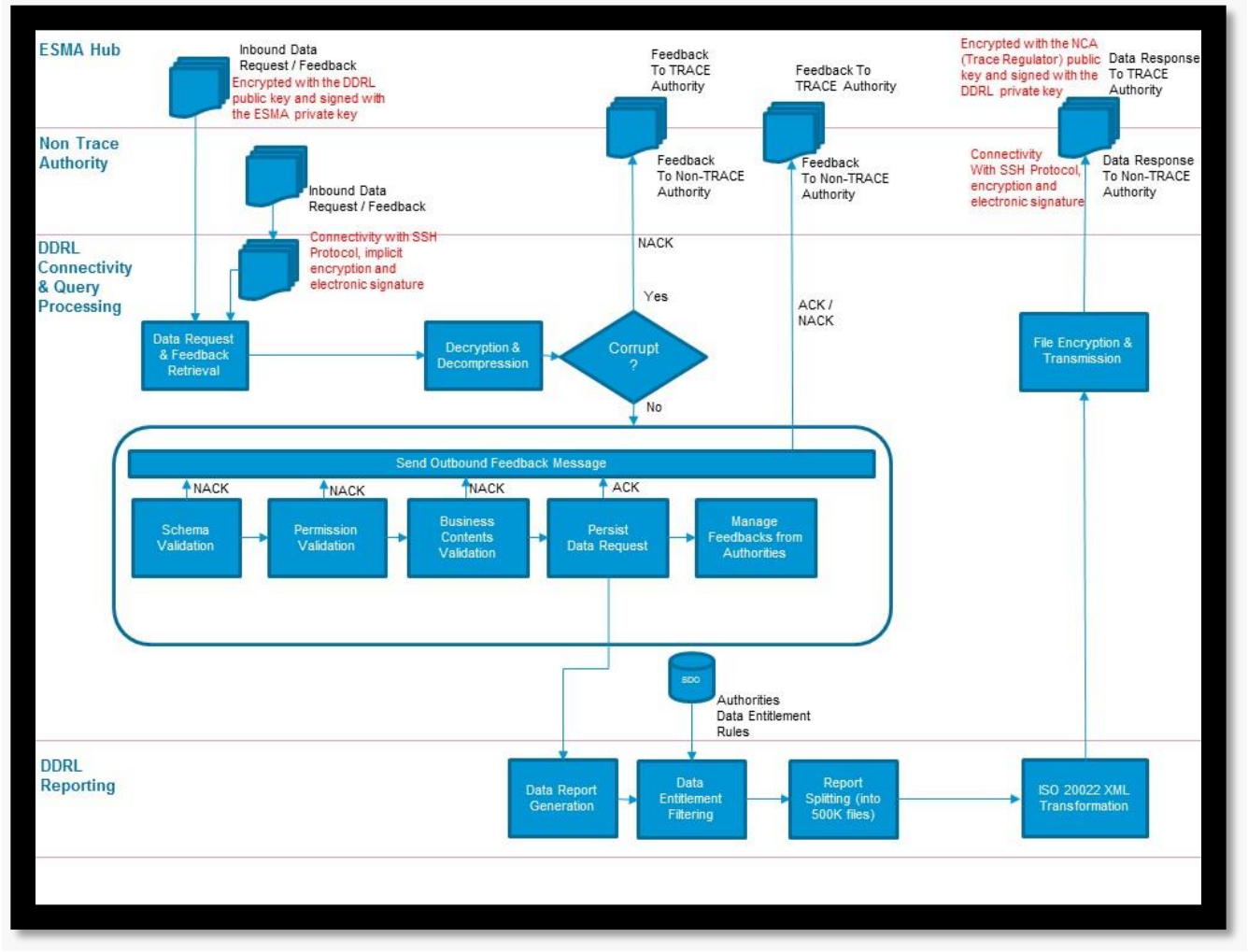
Once onboarded the GTR Regulator Reporting team will verify that the regulator reports are produced in XML format and will email the authority to confirm whether they have been able to access the reports. Should the authority be unable to access the reports, the EU Regulatory Reporting team will investigate and reach out to any other relevant support teams for the successful and complete resolution of the regulatory profile set-up.

Should an authority advise the EU Regulatory Reporting team of a change in its mandate or a change to its Super Access Administrators, the EU Regulatory Reporting team should present the authority with the DDRL SFTR Onboarding form and/or the Super Access Coordinator form. If the authority is only requesting the addition of a Super Access Coordinator form, they should be advised that the opt-in/opt-out facility is to be performed by any of the existing two super user administrators.

Alternatively, if any of the two super user administrators is no longer with the organization, then a new Super Access Administrator should be sent to set up in order to set up a new Super Access Administrator. The EU Onboarding team will follow the same set-up steps as for a new regulatory account/profile set-up.

All the above stages of the Non-Trace authority account set-up are followed in conformity with the DDRL regulator onboarding procedure. Once Non-Trace authorities are onboarded, the connectivity process will be initiated by the EU Regulatory Reporting team.

OVERVIEW OF DATA EXCHANGE BETWEEN DDRL & AUTHORITIES



DDRL will provide direct and immediate access to all SFTs, Margin and Reuse data to onboarded authorities so that they can fulfil the objectives of their mandates and responsibilities. Access will be made available to authorities through one of two channels:

1. Access via TRACE / ESMA Hub
2. Direct Access

The diagram provides an overview of how authorities will engage with DDRL when accessing SFTR data.

1. Authorities will submit data requests for recurrent or ad-hoc reports to DDRL.
2. DDRL will validate the data requests and send a feedback message back to the authorities within 60 minutes of receiving the data request.
3. If the data request is valid an Accepted status will be provided in the feedback message.
4. If the data request is not valid a Rejected status will be provided in the feedback message.
5. Accepted data requests will be scheduled as reports.

6. DDRL will generate reports ensuring the data reported is restricted based on the requesting authority's data entitlements.
7. The reports will be split into multiple smaller report files and transformed into ISO 20022 XML format.
8. The transformed reports will be transmitted to the authorities by the specified SLA.
9. Recurrent reports will be generated daily, transformed and transmitted to authorities within the specified SLA.

DDRL will provide access to the following reports:

- The reports of SFTs reported including the latest trade states of SFTs that have not matured or which have not been the subject of reports with action types "Error", "Termination/Early termination", or "Position component".
- The relevant details of SFT reports rejected by the trade repository, including any SFT reports rejected during the previous working day and the reasons for their rejection.
- The reconciliation status of all reported SFTs for which the trade repository has carried out the reconciliation process, except those SFTs that have expired or for which SFT reports with action types "Error", "Termination/Early termination" or "Position component" were received more than a month before the date on which the reconciliation process takes place.

The access to the details of SFTs shall be provided in accordance with the following deadlines, in line with Commission Delegated Regulation (EU) 2019/357, article 5, paragraph 4:

- Where access is requested to details of outstanding SFTs, or of SFTs which have either matured or for which reports with action types "Error", "Termination/Early termination", or "Position component" were made not more than one year before the date on which the request was submitted then the details will be provided no later than 12:00 Universal Coordinated Time on the first calendar day following the day on which the request to access is submitted.

- Where access is requested to SFT details which have either matured or for which reports with action types "Error", "Termination/Early termination", or "Position component" were made more than one year before the date on which the request was submitted then the details will be provided no later than three working days after the request to access has been submitted.

- Where access is requested to SFT details falling under both points (a) and (b) then the details will be provided no later than three working days after the request to access is submitted

TRACE AUTHORITIES (CONNECTIVITY AND PROCESSING OF FILES)

DDRL will connect to ESMA Hub (as Authorities will direct their queries to DDRL via ESMA HUB) and download any files in the DDRL incoming folder multiple times every hour.

DDRL will verify if the downloaded ESMA Hub file is a:

- Data Request (Query) File or
- Feedback File (feedback message) File

DDRL will accept both recurrent and ad-hoc data requests from ESMA Hub.
Both the Data Request files and feedback files must be provided to DDRL in ISO 20022 XML format.

Encryption of Data Request Files

The exchange of data between authorities, ESMA and DDRL is shielded under confidentiality by way of encryption via public/private keys and electronic signature. Each TRACE authority user will have a unique pair of private/public encryption keys, irrespective of one or multiple flows of data requests launched. All public keys are published on the ESMA Hub and are known by all system users (authorities) during Hub exchanges. Any system user private key is private and known only by the responsible user.

Data request files received by DDRL from ESMA Hub must be received as encrypted and compressed files. Feedback files received by DDRL from ESMA Hub must be received as compressed files.

Once the data request or feedback files have been downloaded by DDRL, ESMA Hub will move the downloaded files to Incoming Archive Folder.

Data Request Validations

When data request files are downloaded, DDRL will decrypt and decompress the data request files (decrypt with DDRL private key and signed with ESMA public key). DDRL will then perform the following validation on the incoming data queries and will respond to ESMA Hub within 60 minutes with a Feedback message:

1. Schema validation of the data query to ensure the data query is compliant with the ISO 20022 XML format
2. Permission validation to ensure the requesting authority is onboarded with DDRL
3. Content validation to ensure that the data query is valid from a business logic perspective.

If the data query is valid then a feedback message will be sent back to ESMA Hub indicating that the data query is Accepted and will be scheduled.

If the data query is not valid then a feedback message will be sent back to ESMA Hub indicating that the data query is Rejected and will not be scheduled.

DDRL generated ACK/NACK feedbacks will be uploaded by DDRL onto the ESMA HUB Outgoing folder. These feedback messages will be in ISO 20022 XML format.

TRACE Data Request Filenames

In order to manage the flow of files, ESMA Hub routing rules are based only on a file naming convention. This means that file names must strictly follow the naming convention defined.

When the ESMA Hub routes a file, it suffixes it with a timestamp in YYYYMMDDHHMMSS format. The name of a data request file which is routed by the ESMA Hub to DDRL will have the format below:

SenderCode_FileType_ReceiverCode_GenericCode1_GenericCode2_Timestamp.zip

- SenderCode will be TRACE
- FileType will be SFTQRY
- ReceiverCode will be TRDDR

GenericCode1 is the first code used to identify files according to the specific context of each system. For TRACE system this field should be 6 or 13 digits long. The first digit should be an indication of the type of message (e.g. A – ad-hoc, R – Recurring, etc.) followed by a 5 characters unique sequence number in hexadecimal notation. This sequence number does not depend on the file type, recipient or any other characteristic and it is related to the Query id number. (It can start again at 00000 after 99999). For an ad-hoc query with current state, this would reflect the date of the query submission. In all other query types, this date will be the day before the execution date of the request, or day of execution date if query is executed the same day it was received. This date will be in the following format: YYMMDD. The hyphen-minus character will be used to separate the query id from the date.

GenericCode2 is the second code used to identify files according to the specific context of each system For TRACE system it should be made up of two parts. First part the number of total files, second part the sequence of the file (E.g. 005001 meaning there are 5 files in total and this file is file 1 in the sequence). Due to the potential large size of response files, in several cases the file will have to be split. Specifically, for the SFTTRA, SFTTRS, SFTPOS, SFTREC, SFTREJ and STFSTA file types a separate digit will be added after the two parts (separated by the hyphen-minus character). This digit will represent the version of the file (i.e. for the first file submission it should always be 0, for every next resubmission of the same file it should raise by 1)

File extension: each file generated by ESMA Hub will be first given an .xml extension. Subsequently, the file will be signed and encrypted or compressed (other file types) and the extension is converted to .zip.

Filename example of an incoming data query from ESMA Hub: TRACE_SFTQRY_TRDDR_A11132-190321_001001-0_20190321090033.zip

TRACE Feedback Filenames

When the ESMA Hub routes a feedback file, it suffixes it with a timestamp in YYYYMMDDHHMMSS format. The name of a feedback file which is routed by the ESMA Hub to DDRL will have the format below:

SenderCode_FileType_ReceiverCode_GenericCode1_GenericCode2_Timestamp.zip

- **SenderCode** will be TRACE
- **FileType** will be SFTFBE (feedback from ESMA) or SFTFBC (feedback message from a competent authority
- **ReceiverCode** will be TRDDR

GenericCode1 is the first code used to identify files according to the specific context of each system. For TRACE system this field should be 6 or 13 digits long. The first digit should be an indication of the type of message (e.g. A – ad-hoc, R – Recurring, etc.) followed by a 5 characters unique sequence number in hexadecimal notation. This sequence number does not depend on the file type, recipient or any other characteristic and it is related to the Query id number. (It can start again at 00000 after 99999). Moreover, in the feedback messages (SFTFBC, SFTFBT, EMRFBC, STFSTA, STFFBE), the as of date in the file should indicate the report date for which the feedback is provided. This date will be in the following format: YYMMDD. The hyphen-minus character will be used to separate the query id from the date.

GenericCode2 is the second code used to identify files according to the specific context of each system. For TRACE system it should be made up of two parts. First part the number of total files, second part the sequence of the file (E.g. 005001 meaning there are 5 files in total and this file is file 1 in the sequence). Specifically, for the SFTTRA, SFTTRS, SFTPOS, SFTREC, SFTREJ and STFSTA file types a separate digit will be added after the two parts (separated by the hyphen-minus character). This digit will represent the version of the file (i.e. for the first file submission it should always be 0, for every next resubmission of the same file it should raise by 1)

File extension: each TRACE feedback file generated will be first given an .xml extension. Subsequently, the file will be compressed, and the extension is converted to .zip.

Filename example of an incoming ESMA Feedback message: TRACE_SFTFBE_TRDDR_A00034-191216_001001-0_20191216022422.zip

Filename example of an incoming Authority Feedback message: CAHNB_SFTFBC_TRDDR_A00034-191216_001001-0_20191216022422.

DDRL Generated Feedback Filenames

DDRL will generate feedback messages for each incoming TRACE Data Request files. The naming convention for these feedback files is provided below:

SenderCode_FileType_ReceiverCode_GenericCode1_GenericCode2_Timestamp.zip

- **SenderCode** will be TRDDR
- **FileType** will be SFTFBT
- **ReceiverCode** will be ESMAS or a National Competent Authority

GenericCode1 is the first code used to identify files according to the specific context of each system. For TRACE system this field should be 6 or 13 digits long. The first digit should be an indication of the type of message (e.g. A – ad-hoc, R – Recurring, etc.) followed by a 5 characters unique sequence number in hexadecimal notation. This sequence number does not depend on the file type, recipient or any other characteristic and it is related to the Query id number. (It can start again at 00000 after 99999). Moreover, in the feedback messages (SFTFBC, SFTFBT, EMRFBC, STFSTA, STFFBE), the as of date in the file should indicate the report date for which the feedback is provided. This date will be in the following format: YYMMDD. The hyphen-minus character will be used to separate the query id from the date.

GenericCode2 is the second code used to identify files according to the specific context of each system. For TRACE system it should be made up of two parts. First part the number of total files, second part the sequence of the file (E.g. 005001 meaning there are 5 files in total and this file is file 1 in the sequence). Specifically, for the SFTTRA, SFTTRS, SFTPOS, SFTREC, SFTREJ and STFSTA file types a separate digit will be added after the two parts (separated by the hyphen-minus character). This digit will represent the version of the file (i.e. for the first file submission it should always be 0, for every next resubmission of the same file it should raise by 1)

File extension: each DDRL feedback file generated will be first given an .xml extension. Subsequently, the file will be compressed, and the extension is converted to .zip.

Filename example of an outgoing DDRL Feedback Message: TRDDR_SFTFBT_CAAMF_R45632-190421_001001-0_20190422090533.zip

NON-TRACE AUTHORITIES (CONNECTIVITY AND PROCESSING OF FILES)

Connectivity for Non-TRACE Authorities

Non-TRACE Authorities will be expected to push their data queries and feedback files to DTCC via the Distributed CDTS and DataPower using a designated Product IDs. The Distributed CDTS uses DataPower which is technology that provides electronic signature and encryption.

SFTP (SSH) - DTCC Distributed EU (Netherlands)				
SFTP (SSH) Inbound (to DTCC)		**DTCC Destination IP Address**	**DTCC Destination DNS Name**	**DTCC Port #**
SFTP (SSH) Production (Distributed EU)		167.188.80.52	sftp.eu.dtcc.com	22
SFTP (SSH) PSE / UAT (Distributed EU)		167.188.80.55	sftppse.eu.dtcc.com	22

Non-TRACE Authorities will need to connect to the SFTP servers. Server details are provided above.

The Product IDs for Data Queries and Feedback files are provided below:

Environment	Data Query Files	Feedback Files
Production	60921	60920
PSE	60921	60920

The Non-TRACE data request files and feedback files will be uploaded to the below SFTP file path by the Requesting Authorities:

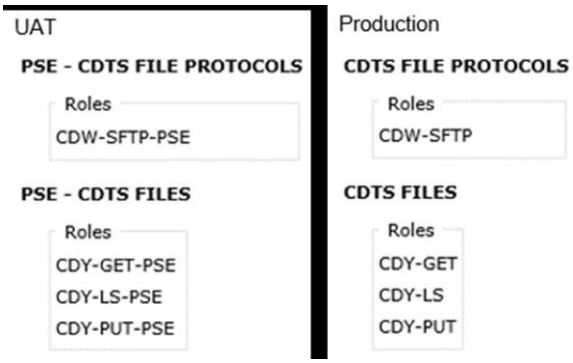
/apps/cdts/sftr/data_in_datapower/put

Configuring Global User IDs

For SFTP access to submit Non-TRACE data requests (or feedback messages), a Global User ID that has CDTS Products enabled will be required.

Super Access Coordinators and Global User ID's are managed on the DTCC Customer Registration System (access and information to the DTCC Customer Registration System will be provided at the time of onboarding).

Super Access Coordinator (SAC) accounts require the 'CDTS' Products (see below) to be enabled before these SACs can create and enable a Global User ID with the same Products. SACs with CDTS Products enabled will create Global User IDs and pass on the CDTS Products to these Global User ID's.



DDRL will need to be informed which Global User IDs, Product IDs and OCODE will be used to connect and submit SFTR files (and retrieve reports) by the Non-TRACE Authority (via SFTP).

Authorities will follow the same naming convention as described for ESMA Hub files but will include an OCODE as the SenderCode and will add the Product ID at the end of the filename (see filename descriptions below).

DDRL will verify if a file sent by a Non-TRACE authority is a:

1. Data Request (Query) File or
2. Feedback File (feedback message) File

Data Request Validation

DDRL will accept both recurrent and ad-hoc data requests from Non-TRACE authorities.

All incoming data request files and feedback files will be in ISO 20022 XML format and compressed.

- DDRL will decompress the data request files and the feedback files before processing the files.
- DDRL will perform the following validations on the incoming data requests and will respond to requesting authority within 60 minutes with a feedback message:
    a. Schema validation of the data query to ensure the data query is compliant with the ISO 20022 XML format
    b. Permission validation to ensure the requesting authority is onboarded with DDRL
    c. Content validation to ensure that the data query is valid from a business logic perspective

- If the data query is valid then a feedback message will be sent back to requesting authority indicating that the data query is Accepted and will be scheduled.

- If the data query is not valid then a feedback message will be sent back to requesting authority indicating that the data query is Rejected and will not be scheduled.

DDRL generated ACK/NACK feedbacks will be sent to the Authority's requested destination and folder. The destination and file path will be configured as per the Authority's subscription by GTR Connectivity at onboarding. These feedback messages will be in ISO 20022 XML format.

Non-TRACE Data Request Filenames

When the Non-TRACE Authority routes a file, it suffixes it with a timestamp in YYYYMMDDHHMMSS format. The name of a data request file which is routed by the Non-TRACE Authority will have the format below:

ReceiverCode_FileType_ProductID_SenderCode_GenericCode1_GenericCode2_Timestamp.zip

SenderCode will be OCODE of the Non-TRACE Authority
FileType will be SFTQRY
ReceiverCode will be TRDDR
ProductID will be 60921

GenericCode1 is the first code used to identify files according to the specific context of each system. This field should be 6 or 13 digits long. The first digit should be an indication of the type of message (e.g. A – ad-hoc, R – Recurring, etc.) followed by a 5 characters unique sequence number in hexadecimal notation. This sequence number does not depend on the file type, recipient or any other characteristic and it is related to the Query id number. (It can start again at 00000 after 99999). For an ad-hoc query with current state, this would reflect the date of the query submission. In all other query types, this date will be the day before the execution date of the request, or day of execution date if query is executed the same day it was received. This date will be in the following format: YYMMDD. The hyphen-minus character will be used to separate the query id from the date.

GenericCode2 is the second code used to identify files according to the specific context of each system. This should be made up of two parts. First part the number of total files, second part the sequence of the file (E.g. 005001 meaning there are 5 files in total and this file is file 1 in the sequence). Due to the potential large size of response files, in several cases the file will have to be split. Specifically, for the SFTTRA, SFTTRS, SFTPOS, SFTREC, SFTREJ and STFSTA file types a separate digit will be added after the two parts (separated by the hyphen-minus character). This digit will represent the version of the file (i.e. for the first file submission it should always be 0, for every next resubmission of the same file it should raise by 1)

File extension: each file generated by ESMA Hub will be first given an .xml extension. Subsequently, the file will be compressed (other file types) and the extension is converted to .zip.

Filename example of an incoming data query from a non-TRACE Authority:

- TRDDR_SFTQRY_60921_9R22_R00175-200318_001001-0_20200318090533.xml
- 9R22 is a sample (i.e. not real) OCODE being used for demonstration purposes.

Non-TRACE Authority Feedback Filenames

When the Non-TRACE Authority routes a file, it suffixes it with a timestamp in YYYYMMDDHHMMSS format. The name of a feedback file which is routed by the Non-TRACE Authority will have the format below:

ReceiverCode_FileType_ProductID_SenderCode_GenericCode1_GenericCode2_Timestamp.zip

SenderCode will be OCODE of the Non-TRACE Authority
FileType will be DRCTTR
ReceiverCode will be TRDDR
ProductID will be 60920

GenericCode1 is the first code used to identify files according to the specific context of each system. This field should be 6 or 13 digits long. The first digit should be an indication of the type of message (e.g. A – ad-hoc, R – Recurring, etc.) followed by a 5 characters unique sequence number in hexadecimal notation. This sequence number does not depend on the file type, recipient or any other characteristic and it is related to the Query id number. (It can start again at 00000 after 99999). Moreover, in the feedback messages (SFTFBC, SFTFBT, EMRFBC, STFSTA, STFFBE), the as of date in the file should indicate the report date for which the feedback is provided. This date will be in the following format: YYMMDD. The hyphen-minus character will be used to separate the query id from the date.

GenericCode2 is the second code used to identify files according to the specific context of each system. This should be made up of two parts. First part the number of total files, second part the sequence of the file (E.g. 005001 meaning there are 5 files in total and this file is file 1 in the sequence). Specifically, for the SFTTRA, SFTTRS, SFTPOS, SFTREC, SFTREJ and STFSTA file types a separate digit will be added after the two parts (separated by the hyphen-minus character). This digit will represent the version of the file (i.e. for the first file submission it should always be 0, for every next resubmission of the same file it should raise by 1)

File extension: each Non-TRACE feedback file generated will be first given an .xml extension. Subsequently, the file will be compressed, and the extension is converted to .zip.

Filename example of an incoming feedback file from a non-TRACE Authority:

- TRDDR_DRCTTR_60920_9R22_R00175-200318_001001-0_20200318090533.xml

DDRL Generated Feedback Filenames

DDRL will generate feedback messages for each incoming Non-TRACE Data Request files. The naming convention for these feedback files is provided below:

SenderCode_FileType_ReceiverCode_GenericCode1_GenericCode2_Timestamp.zip

SenderCode will be TRDDR
FileType will be SFTFBT
ReceiverCode will be ESMAS or a National Competent Authority

GenericCode1 is the first code used to identify files according to the specific context of each system. This field should be 6 or 13 digits long. The first digit should be an indication of the type of message (e.g. A – ad-hoc, R – Recurring, etc.) followed by a 5 characters unique sequence number in hexadecimal notation. This sequence number does not depend on the file type, recipient or any other characteristic and it is related to the Query id number. (It can start again at 00000 after 99999). Moreover, in the feedback messages (SFTFBC, SFTFBT, EMRFBC, STFSTA, STFFBE), the as of date in the file should indicate the report date for which the feedback is provided. This date will be in the following format: YYMMDD. The hyphen-minus character will be used to separate the query id from the date.

GenericCode2 is the second code used to identify files according to the specific context of each system. This should be made up of two parts. First part the number of total files, second part the sequence of the file (E.g. 005001 meaning there are 5 files in total and this file is file 1 in the sequence). Specifically, for the SFTTRA, SFTTRS, SFTPOS, SFTREC, SFTREJ and STFSTA file types a separate digit will be added after the two parts (separated by the hyphen-minus character). This digit will represent the version of the file (i.e. for the first file submission it should always be 0, for every next resubmission of the same file it should raise by 1)

File extension: each DDRL feedback file generated will be first given an .xml extension. Subsequently, the file will be compressed, and the extension is converted to .zip.

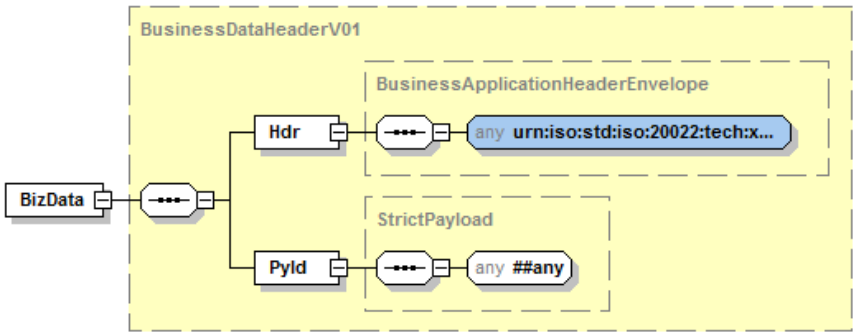
Filename example of an outgoing DDRL Feedback Message:
TRDDR_SFTFBT_9R22_R45632-190421_001001-0_20190422090533.zip

DATA EXCHANGE MESSAGE STRUCTURES

All data exchange between ESMA Hub, Non-TRACE Authorities and DDRL will be ISO200 22 XML compliant. This means that data request, feedback messages and the data response reports that will be sent between ESMA Hub and DDRL (for TRACE reporting) and between the requesting authority and DDRL (for Non-TRACE reporting) must be in XML format based on the latest published ESMA SFTR XSDs. The latest XSDs may be found on ESMA's official website under "XML SFTR Reporting Schemas".

Business Data Header (Envelope)

Each ISO 20022 business message (payload) will be sent together with the Business Application Header (BAH) message. These are separate messages and should be packaged within the additional structure ('envelope') in order to constitute a single XML file. The messaging will be based on a Business Data Header <Head003> which will act as an XML envelope:



Business Application Header

Application Header <Head001>: this will be the message header which will include a unique Business Message Identifier for the message and will indicate what type of submissions are captured in the message's payload.

The Business Application Header (BAH) is a header that has been defined by the ISO 20022 community that can form part of an ISO 20022 business message. Specifically, the BAH is an ISO20022 message definition (head.001.001.01) which can be combined with any other ISO20022 message definition to form a business message. It gathers together, in one place, data about the message, such as which organization has sent the business message, which organization should be receiving it, the identity of the message itself, a reference for the message and so on. The purpose of the BAH is to provide a consistent and predictable way for this data to be conveyed with the message, regardless of implementation factors such as the choice of network.

The use of the BAH is mandatory in all messages sent through the TRACE system or directly to DDRL. The below table presents the list of mandatory elements of the BAH that must be included in all messages and how they should be populated:

Element	Description	Usage by System Users
From	The sender of the message	CA user/OCODE/TR identification
To	The recipient of the message	CA user/OCODE/TR identification
Business Message Identifier	Unique identification of the message	The same as the file sequence number
Message Definition Identifier	Identification of the type of the message (ISO 20022 message identifier).	The identifier of relevant ISO 20022 message
Business Service	Specifies the business context of the use of the message.	Specific version of the XML schema.
Creation Date	Date and time when this Business Message was created	Date and time in ISO 8601 format.
Related	Specifies the Business Application Header of the Business Message to which this Business Message relates.	Should be left empty.

XML Message Payload

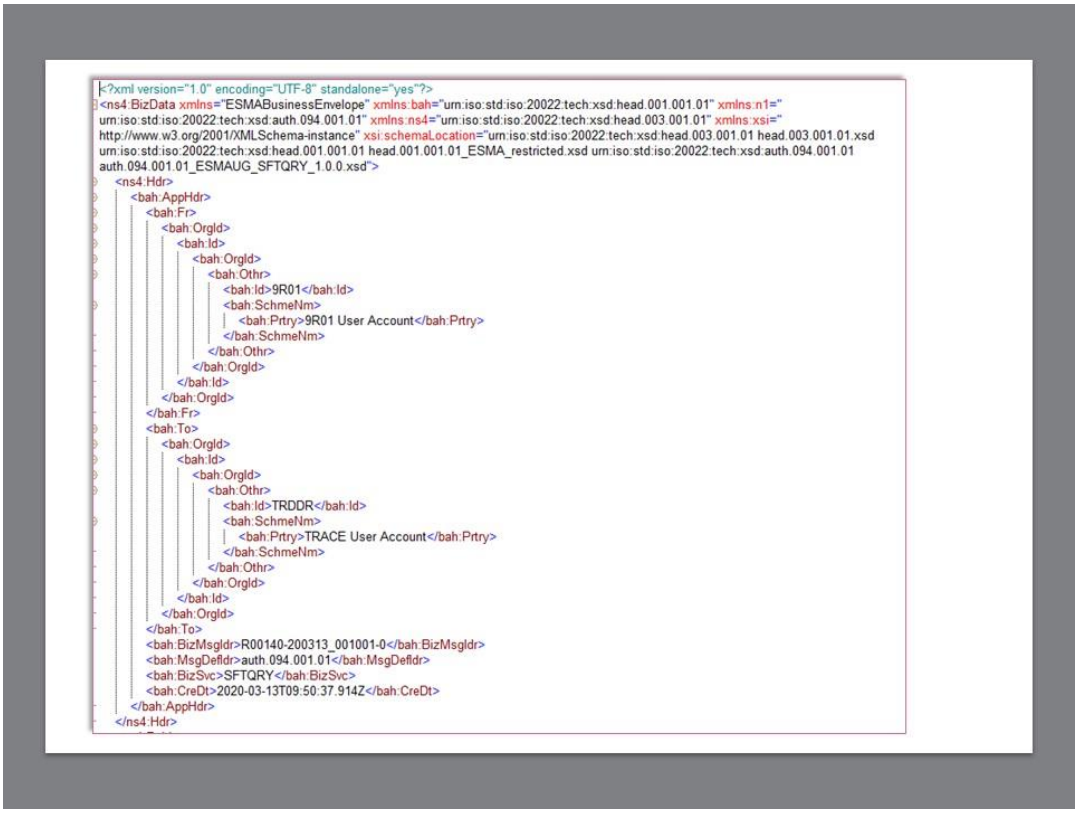
Pay Load: this will be the body of the message. The body may include any one of the following document types depending on the filetype and reporting data. The body of the message will contain the actual submissions:

- **Filetype SFTQRY**: SFTR Data Request <auth094>
- **Filetype SFTFBT**: DDRL feedback <auth31>
- **Filetype SFTFBE**: ESMA (TRACE) feedback <auth31>
- **Filetype SFTFBC**: NCA (TRACE) feedback <auth31>
- **Filetype DRTCTR**: Non-TRACE authority feedback <auth31>
- **Filetype SFTTRA**: SFT Transactions <auth052>
- **Filetype SFTTRA**: Margin Transactions <auth070>
- **Filetype SFTTRA**: Collateral Reuse Transactions <auth071>
- **Filetype SFTTRS**: SFT Transaction State <auth079>
- **Filetype SFTTRS**: Margin Transaction State <auth085>
- **Filetype SFTTRS**: Collateral Reuse Transaction State <auth086>

- **Filetype SFTREC**: Reconciliation Status <auth080>
- **Filetype SFTREJ**: Rejection Status <auth084>
- **Filetype STFSTA**: Statistics file on a quarterly basis – STFSTA <auth084>

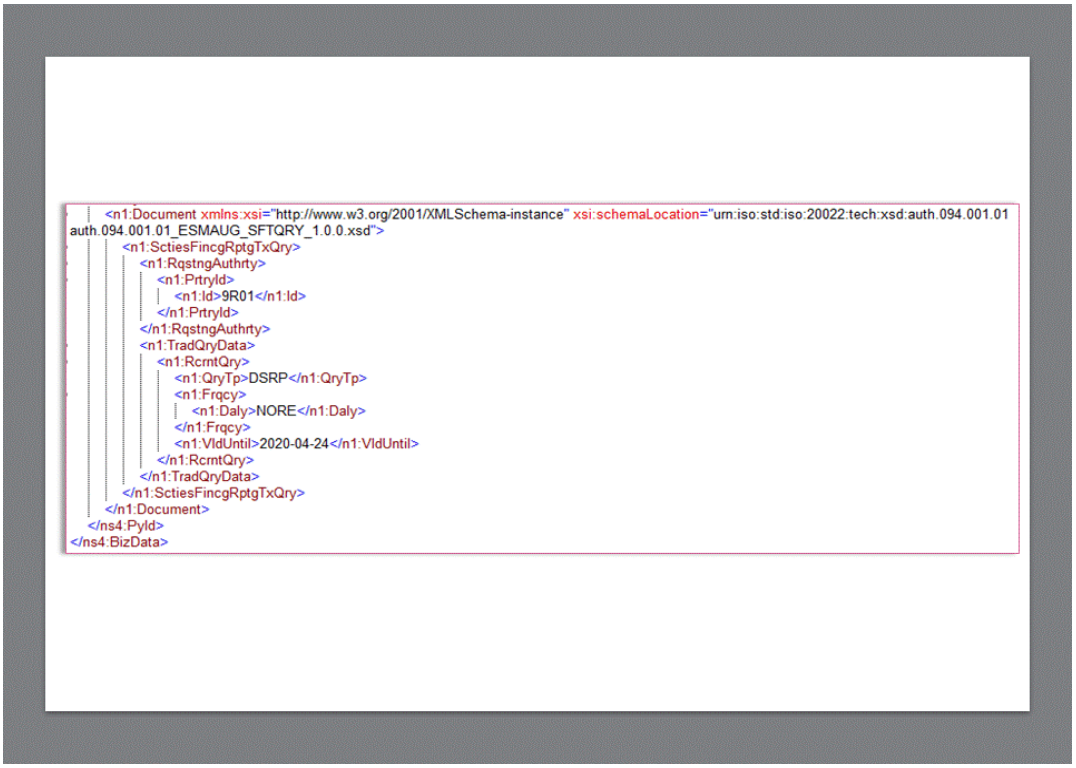
Sample Data Request

A sample data query that will be submitted by a requesting authority to DDRL is provided below. This section shows a Business Data Header (head.003 envelope) encapsulating a Business Application Header (head.001).



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns4:BizData xmlns="ESMABusinessEnvelope" xmlns:bah="urn:iso:std:iso:20022:tech:xsd:head.001.001.01" xmlns:n1="
urn:iso:std:iso:20022:tech:xsd:auth.094.001.01" xmlns:ns4="urn:iso:std:iso:20022:tech:xsd:head.003.001.01" xmlns:xsi="
http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:iso:std:iso:20022:tech:xsd:head.003.001.01 head.003.001.01.xsd
urn:iso:std:iso:20022:tech:xsd:head.001.001.01 head.001.001.01_ESMA_restricted.xsd urn:iso:std:iso:20022:tech:xsd:auth.094.001.01
auth.094.001.01_ESMAUG_SFTQRY_1.0.0.xsd">
  <ns4:Hdr>
    <bah:AppHdr>
      <bah:Fr>
        <bah:OrgId>
          <bah:Id>
            <bah:OrgId>
              <bah:Othr>
                <bah:Id>9R01</bah:Id>
                <bah:SchmeNm>
                  <bah:Prtry>9R01 User Account</bah:Prtry>
                </bah:SchmeNm>
              </bah:Othr>
            </bah:OrgId>
          </bah:Id>
        </bah:OrgId>
      </bah:Fr>
      <bah:To>
        <bah:OrgId>
          <bah:Id>
            <bah:OrgId>
              <bah:Othr>
                <bah:Id>TRDDR</bah:Id>
                <bah:SchmeNm>
                  <bah:Prtry>TRACE User Account</bah:Prtry>
                </bah:SchmeNm>
              </bah:Othr>
            </bah:OrgId>
          </bah:Id>
        </bah:OrgId>
      </bah:To>
      <bah:BizMsgIdr>R00140-200313_001001-0</bah:BizMsgIdr>
      <bah:MsgDefIdr>auth.094.001.01</bah:MsgDefIdr>
      <bah:BizSvc>SFTQRY</bah:BizSvc>
      <bah:CreDt>2020-03-13T09:50:37.914Z</bah:CreDt>
    </bah:AppHdr>
  </ns4:Hdr>
```

This section shows the payload which is also encapsulated within the Business Data Header (head.003 envelope). The payload is based on the schema auth.094 which is a data request message. This sample Data request is for a recurrent rejected status report.



FEEDBACK MESSAGES AND ERROR CODES

File related errors

Data request files will be validated to ensure that the file sent by the TRACE or Non-TRACE requesting authority can be processed. This includes whether the file was transmitted properly, conforms to expected XSD schema and common file identifiers are valid.

Similarly, data response report files will be validated to ensure that the file sent by DDRL can be processed by the TRACE or Non-TRACE requesting authority

1. A feedback file from DDRL to the requesting authority will be provided with a Status "**CRPT**" and with one of the below error codes if a data request file fails the file level validations.
2. A feedback file from the requesting authority to DDRL will be provided with a Status "**CRPT**" and with one of the below error codes if a data response report file fails the file level validations.

Error code	Error Message	Control
FIL-001	The file cannot be decompressed or decrypted	Data request files will be compressed in zip format and encrypted. This error will be returned by the system if the file cannot be decompressed or decrypted.
FIL-006	The XML schema cannot be located: Incorrect name space	The XML schema must be located (receiver must be able to find the XML schema name within the file).

FIL-007	The XML schema name (*.xsd) is incorrect. It must refer to a correct existing XML schema file in its name space.	The XML schema name and version must refer to a correct existing XML schema
FIL-008	The file structure does not correspond to the XML schema: [result of XML validation]	Validate that the file sent fits to the corresponding XML schema. For information purposes, if there is an error in the validation, the error message produced by the XML parser is displayed in place of [result of XML validation].
FIL-015	Dataset incomplete	Not all files are received from the total submitted files (Reminder)
FIL-020	Response to query is missing	A response to query has not yet been submitted (Reminder)

Query execution errors

The below error codes shall be provided in the feedback file to the requesting authority if there are is an execution error. A feedback file from DDRL to the requesting authority will be provided with a Status "**RJCT**" and with one of the below error codes if a data request file fails the execution level validations.

Error code	Error Message	Control
EXE-001	Authority not onboarded.	The authority submitting the query has not yet onboarded to DDRL for Regulatory Reporting.

Query fields content validation error messages

Below validations shall be implemented on the level of the TRACE system to ensure proper and schema compliant queries are generated and sent out to the trade repositories. DDRL is expected to implement the below validation rules for Non-TRACE Authorities. A feedback file from DDRL to the requesting authority will be provided with a Status "**RJCT**" and with one of the below error messages if a data request file fails the business contents level validations.

Error Message	Control
Reporting Counterparty ID is invalid	Reporting Counterparty ID does not comply with any of the supported formats
Type of ID does not relate to Reporting Counterparty ID	Reporting Counterparty ID doesn't match the selected type of ID
Other Counterparty ID is invalid	Other Counterparty ID does not comply with any of the supported formats
Type of ID does not relate to Other Counterparty ID	Other Counterparty ID doesn't match the selected type of ID

Broker ID is invalid	Broker ID does not comply with any of the supported formats
Type of ID does not relate to Broker ID	Broker ID doesn't match the selected type of ID
Report submitting entity ID is invalid	Report submitting entity ID does not comply with any of the supported formats
Type of ID does not relate to Broker ID	Report submitting entity ID doesn't match the selected type of ID
Beneficiary ID is invalid	Beneficiary ID does not comply with any of the supported formats
Type of ID does not relate to Beneficiary ID	Beneficiary ID doesn't match the selected type of ID
CCP ID is invalid	CCP ID does not comply with any of the supported formats
Type of ID does not relate to CCP ID	CCP ID doesn't match the selected type of ID
Reporting Counterparty Branch ID is invalid	Reporting Counterparty Branch ID does not comply with any of the supported formats
Type of ID does not relate to Reporting Counterparty Branch ID	Reporting Counterparty Branch ID doesn't match the selected type of ID
Other Counterparty Branch ID is invalid	Other Counterparty Branch ID does not comply with any of the supported formats
Type of ID does not relate to Other Counterparty Branch ID	Other Counterparty Branch ID doesn't match the selected type of ID
The Maturity Date is invalid.	The dates should be within sensible range (e.g. not earlier than "1900-01-01")
The Termination Date is invalid.	The dates should be within sensible range (e.g. not earlier than "1900-01-01")
The Execution Date is invalid.	The dates should be within sensible range (e.g. not earlier than "1900-01-01")
The Reporting date is invalid.	The dates should be within sensible range (e.g. not earlier than "1900-01-01")
Maturity Date: TO date should be greater or equal than FROM date	Dates are wrongly selected
Termination Date: TO date should be greater or equal than FROM date	Dates are wrongly selected
Execution Date: TO date should be greater or equal than FROM date	Dates are wrongly selected

Reporting Date: TO date should be greater or equal than FROM date	Dates are wrongly selected
Execution date must be equal or prior to Termination date	Execution date after termination date
"Valid until" date is in the past	User inputs a validity date for recurrent query in the past
Corporate Sector does not match Nature of Counterparty.	Corporate Sector of Counterparty value is not included in the list of values of selected Nature of Counterparty field
Type of SFT does not match the list of predefined values	Type of SFT value is not included in the list of predefined values
Type of collateral component does not match the list of predefined values	Type of collateral component is not included in the list of predefined values
Only one identifier can be provided when OR is selected	OR operator is used between the 'parties' or 'additional party' fields and user has provided more than one identifier
Recurrent query already defined by user XXX	User tries to define a new query with a template that is already used by the authority in another active query (e.g. defined by another user from this authority)
All trades and current status not allowed	User selecting inappropriate combination of values in Current state and All trades fields
Query ID is not unique	A query with the same ID has been already received by TR. It does not apply to recurrent query where the valid until date was updated
Execution Date: TO date should be less or equal than current date	TO Date is in the future
Reporting Date: TO date should be less or equal than current date	TO Date is in the future
The mandatory fields are missing	Query field is mandatory in Recurrent queries screen
The mandatory fields are missing	Execution frequency field is mandatory in Recurrent queries screen
The mandatory fields are missing	Valid until date field is mandatory in Recurrent queries screen
The mandatory fields are missing	Trade Repository field is mandatory in Recurrent queries screen
The mandatory fields are missing	Trade Repository field is mandatory in Ad-hoc queries screen

At least one field should be populated in Ad-hoc queries screen	At least one field should be populated
Reporting timestamp: The user has completed only one of the from/To fields	For date fields, both the "FROM" and "TO" values must be provided
Execution timestamp: The user has completed only one of the from/To fields:	For date fields, both the "FROM" and "TO" values must be provided
Maturity date: The user has completed only one of the from/To fields:	For date fields, both the "FROM" and "TO" values must be provided
Termination date: The user has completed only one of the from/To fields	For date fields, both the "FROM" and "TO" values must be provided

Feedback Files received by DDRL (from TRACE or Non-TRACE Authorities) will be validated to ensure conformance to the expected XSD schema and common file identifiers.

If these feedback files fail this validation, then DDRL will:

1. Open a ticket with ESMA Support for TRACE feedback files failing this validation
2. Raise a support ticket with the Non-TRACE authority if their feedback file fails this validation

RECURRENT DATA REQUESTS AND REPORTS

Recurrent Data Requests

TRACE and Non-TRACE authorities may request recurrent data reports by submitting recurrent data requests (queries) to DDRL. TRACE authorities may submit recurrent data requests (queries) to DDRL via the TRACE system. Non-TRACE authorities may submit recurrent data requests directly to DDRL. These recurrent data requests must conform to the ISO 20022 XML format (data query XSD). The XML schema for data requests is provided in the following XSD:

- **SecuritiesFinancingReportingTransactionQueryV01 (auth.094.001.01_ESMAUG_SFTQRY_1.0.0.xsd)**

A recurrent data request will result in the output file for such data query to be generated automatically and repeatedly according to the frequency defined by the user (e.g. daily, weekly, monthly). It should be noted that initially all SFTR recurrent reports will be offered as daily reports only.

The recurrent data requests submitted to DDRL will be validated, and a feedback message will be provided by DDRL to the requesting authorities within 60 minutes of receiving the data request. The feedback message will indicate whether the request was accepted or rejected. If rejected an error message will be provided to inform the requesting authority of the validation failure. If the recurrent data request is accepted, then the recurrent data report will be scheduled and will be delivered in line with the regulatory SLA.

If a recurrent data request is received by DDRL with a query id that has not been previously sent, then the recurrent report will be scheduled as a new request and will be generated every day until the valid until date expires.

If a recurrent data request is received by DDRL with a query id that has been previously sent, and:

1. If the valid until date of the recurrent data request is in the future, then the existing scheduled recurrent report will have its valid until date updated and will continue to be generated every day until the new valid until date expires.
2. If the valid until date of the recurrent data request is the current date, then the existing scheduled recurrent report will not be generated from the next reporting cycle onwards.
3. If the valid until date of the recurrent data request is in the past, then recurrent data request will be rejected.

For SFTR, there will be 5 recurrent reports available and these will be identified through the Query Type:

4. **ASPD** (All SFT Reports Submitted on Previous)
5. **AOPD** (All Outstanding Trades at Close of Previous Working Day)
6. **DSRP** (Details of SFT Reports Rejected on Previous Working Day)
7. **RSST** (Reconciliation Status of SFT Reports Subject to Reconciliation)
8. **POSR** (Position Report) – this report is deferred and will be delivered at a later date.

The Frequency of the report <Frqcy> will be Daily

The Valid Until Date <VldUntil> will be a date in ISO 8601 Date format and must represent a current date or date in the future.

The Query ID will be found in the Business Message ID (head.001.001.01) and in the filename within the GenericCode1 and must be unique unless it is being submitted for an existing recurrent data query where the Valid Until date <VldUntil> is being changed.

Outbound recurrent TRACE data response reports will be generated on a daily basis and provided to TRACE authorities via ESMA Hub and the TRACE system.

Outbound recurrent Non-TRACE data response reports will be generated on a daily basis and provided to the Non-TRACE authorities directly via SFTP.

ESMA SFTR Recurrent Reports

All SFT reports submitted on the previous working day	All trades (message 'T') where 'Reporting Timestamp' = 'T – 1'. Example: Query sent on 03 June 2019 - > processed on 04 June 2019 = result outcome contains all trades reported on 03 June 2019.	Query (ASPD) Files Response: **'SFTTRA'** – all SFT Submissions

All outstanding SFT reports as of end of previous working day	Latest state (for each field) of all trades where the 'Maturity Date' = blank, and where the Action Type is different from ''POSC', ETREM', 'ERROR', as of close of previous day. Example: Query sent on 03 June 2019 -> processed on 04 June 2019 = result outcome contains all outstanding trades as of close of business of 03 June 2019.	Query (AOPD) Files Response: '**SFTTRS' –** Latest state of the outstanding trades
All SFT rejections reports on the previous working day	All rejected SFT trades within the reference period which were submitted to DDRL but did not pass data validations. The report should also contain the rejections reasons.	Query (DSRP) Files Response '**SFTREJ'** – SFT rejection status responses
SFTs Reconciliation Report	All reconciled SFT reports at the end of the reference period which are included in the reconciliation process. Example: Outstanding SFTs [not matured or terminated] not more than 30 days before the initiation of the reconciliation process.	Query (RSST) Files Response: **'SFTREC'** – SFT Reconciliation Status Responses
SFT Positions Report	Aggregate positions calculated for the last day of the selected frequency. [Still to be defined].	Query (POSR) Files Response: **'SFTPOS'** – SFT Position – level data response.

SFT Transaction Reports

It should be noted that for recurrent reports the transaction reports (i.e. Query Type is ASPD and filetype will be SFTTRA) will include the following transactions data. Each type of transaction data will be in separated report files and in the XSD structures listed below:

For all SFTR transactions (applicable ISO 20022 messages provided):

- **SFT Transactions**: SecuritiesFinancingReportingTransactionReportV01 (auth.052.001.01_ESMAUG_SFTTRA_1.0.0.xsd)
- **Margin Transactions**: SecuritiesFinancingReportingTransactionMarginDataReportV01 (auth.070.001.01_ESMAUG_SFTTRA_1.0.0.xsd)
- **Reuse Transactions:** SecuritiesFinancingReportingTransactionReusedCollateralDataReportV01 (auth.071.001.01_ESMAUG_SFTTRA_1.0.0.xsd)

SFT Transaction State Reports

It should be noted that for recurrent reports the transaction state reports (i.e. Query Type is AOPD and filetype will be SFTTRS) will include the following transaction state data. Each type of transaction state data will be in separated report files and in the XSD structures listed below:

For all SFTR transaction states (applicable ISO 20022 messages provided):

a. **SFT Transaction States**: SecuritiesFinancingReportingTransactionStateReportV01 (auth.079.001.01_ESMAUG_SFTTRS_1.0.0.xsd)
b. **Margin Transaction States:** SecuritiesFinancingReportingMarginDataTransactionStateReportV01 (auth.085.001.01_ESMAUG_SFTTRS_1.0.0.xsd)
c. **Reuse Transaction States:** SecuritiesFinancingReportingReusedCollateralDataTransactionStateReportV01 (auth.086.001.01_ESMAUG_SFTTRS_1.0.0.xsd)

SFT Reconciliation Status Reports

Recurrent reports for reconciliation status of the SFTs and the reasons for lack of reconciliation (i.e. Query Type is RSST and filetype will be SFTREC) will be sent by DDRL in a separated report file (applicable ISO 20022 messages provided):

- **SFT Reconciliation Status**: SecuritiesFinancingReportingReconciliationStatusAdviceV01 (auth.080.001.01_ESMAUG_SFTREC_1.0.0.xsd)

Rejection data message

Recurrent reports for rejection data messages that contain details on rejected SFTs and the reasons for rejection (i.e. Query Type is DSRP and filetype will be SFTREJ) will be sent by DDRL (applicable ISO 20022 messages provided):

- **SFT Rejection Status:** SecuritiesFinancingReportingTransactionStatusAdviceV01 (auth.084.001.01_ESMAUG_SFTREJ_1.0.0.xsd)

AD-HOC DATA REQUESTS AND REPORTS

Ad-hoc Data Requests

TRACE and Non-TRACE authorities may request ad-hoc data reports by submitting ad-hoc data requests (queries) to DDRL. TRACE authorities may submit ad-hoc data requests (queries) to DDRL via the TRACE system. Non-TRACE authorities may submit ad-hoc data requests directly to DDRL. These ad-hoc data requests must conform to the ISO 20022 XML format (data query XSD). The XML schema for data requests is provided in the following XSD:

SecuritiesFinancingReportingTransactionQueryV01
(auth.094.001.01_ESMAUG_SFTQRY_1.0.0.xsd)

Queryable Fields

The ad-hoc data request will result in either an SFT transaction report or a SFT transaction state report. Margin and Reuse reports will not be supported for ad-hoc data reports. The requesting authority will be able to use the data request message to provide filtering logic for ad-hoc reports. The queryable fields that can be specified in an ad-hoc data query are provided in the below table:

No	Field name	Reference to SFTR RTS	Type of filter	Additional comments
Parties (with OR/AND query operators)				
1	Reporting Counterparty ID	Item 1.3	Equal to (=), multiple values	• ISO 17442 Legal Entity Identifier (LEI) 20 alphanumerical character code. Multiple counterparty identifiers separated by comma can be input in that filter. As a result all trades concluded by any of the counterparties specified should be provided.
2	ID of the other counterparty	Item 1.11	Equal to (=), multiple values	• ISO 17442 Legal Entity Identifier (LEI) 20 alphanumerical character code. • CLC (up to 50 alphanumerical digits) Multiple counterparty identifiers separated by comma can be input in that filter.
3	Broker ID	Item 1.15	Equal to (=), multiple values	• ISO 17442 Legal Entity Identifier (LEI) 20 alphanumerical character code. Multiple broker identifiers separated by comma can be input in that filter.
4	Report submitting entity ID	Item 1.2	Equal to (=), multiple values	• ISO 17442 Legal Entity Identifier (LEI) 20 alphanumerical character code. Multiple report submitting entity identifiers separated by comma can be input in that filter.
5	Beneficiary ID	Item 1.13	Equal to (=), multiple values	• ISO 17442 Legal Entity Identifier (LEI) 20 alphanumerical character code. • CLC (up to 50 alphanumerical digits) Multiple beneficiary identifiers separated by comma can be input in that filter.
6	CCP	Item 2. 7	Equal to (=), multiple values	• ISO 17442 Legal Entity Identifier (LEI) 20 alphanumerical character code. Multiple values separated by comma can be input in that filter. The field can be queried for 'blank' values.
7	Branch of the reporting counterparty	Item 1.7	Equal to (=), multiple values	• ISO 3166, Alpha-2 country code.

				Multiple branch identifiers separated by comma can be input in that filter.
8	Branch of the other counterparty	Item 1.8	Equal to (=), multiple values	• ISO 3166, Alpha-2 country code. Multiple branch identifiers separated by comma can be input in that filter.
Types (with OR/AND query operators)				
9	Type of SFT	Item 2.4	Equal to (=), multiple values	Possible values: 'SLEB', 'SBSC', 'REPO', MGLD'. Multiple values separated by comma can be input in that filter. As a result all trades with any of the specified values should be provided.
10	Type of collateral component	Item 2.75	Equal to (=), multiple values	Possible values: 'SECU', 'COMM', 'CASH'. Multiple values separated by comma can be input in that filter. As a result all trades with any of the specified values should be provided.
Dates				
11	Reporting timestamp	Item 1.1	Range (=>,<=)	ISO 8601 Date and full hour. TO date should be greater or equal than FROM date.
12	Execution timestamp	Item 2.12	Range (=>,<=)	ISO 8601 Date and full hour. TO date should be greater or equal than FROM date.TO date should be greater or equal than FROM date.
13	Maturity date	Item 2.14	Range (=>,<=)	ISO 8601 Date. TO date should be greater or equal than FROM date. The field can be queried for 'blank' values.
14	Termination date	Item 2.15	Range (=>,<=)	ISO 8601 Date. TO date should be greater or equal than FROM date. The field can be queried for 'blank' values.
Additional filters				
15	Trading venue	Item 2.8	Equal to (=), multiple values	Valid MIC code (including 'XXXX' or 'XOFF'). Multiple execution venues separated by comma can be input in that filter.
16	Action type	Item 2.98	Selection, multiple values allowed	The following values are possible: 'NEWT' – New; 'MODI' – Modify; 'VALU' – Valuation update; 'COLU' – Collateral update; 'EROR' – Error;

				'CORR' – Correction; 'ETRM' – Early Termination; 'POSC' – Position component. 'All' – all records are returned (default). This field is only applicable when the full trade history is requested.
17	Sector of the reporting counterparty	Item 1.5	Equal to (=), multiple values	Possible values: 'CDTI', ' INVF', 'INUN', 'AIFD', 'ORPI', 'CCPS', 'REIN', 'CSDS', 'UCIT', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T' and 'U'. Multiple values separated by comma can be input in that filter. As a result all trades with any of the specified values should be provided.
18	Nature of the reporting counterparty	Item 1.4	Equal to (=)	Possible values: 'F', 'N'
Technical fields				
19	Report type	Not applicable	Selection	Possible values: 'Trade activity' – all reports submitted by counterparties for a given trade (i.e. the first report as well as all the following updates of the trade) are provided as separate records; 'Trade state' – only the current trade state as of the day of data query submission is returned (i.e. one record per trade containing only the most up-to-date values reported in each field). Default value: 'Trade state'.
20	Scope of trades	Not applicable	Selection	Possible values: 'Outstanding trades' – only outstanding trades are returned in the output file; 'All trades' – all trades are returned in the output file. Default value: 'Outstanding trades'. If 'All trades' is selected the response can include only the trade lifecycle history. No trade state information will be provided for those trades that are not outstanding.
21	Send query to	Not applicable	Selection (multiple	The user can select 'All' or indicate any specific TRs which the query should be sent to.

			values allowed)	Default value: 'All'.

When using the Trade Party Criteria to specify an ad-hoc data query, for Reporting Counterparty one or more LEIs may be provided and the TR will need to filter the data response to include trades for these reporting counterparties. However, one of the enumerators for Reporting Counterparty is NotRptd. NotRptd will not apply to Reporting Counterparty, Other Counterparty or Report Submitting Entity as these are mandatory for all submissions and trade states. NotRptd may only be provided for Trade Party Criteria fields that are optional when trade submissions are ingested.

Determining the Type of Ad-hoc Report to Generate

There are 2 critical report type attributes for ad-hoc data queries which exist in the data request XML schema. These together indicate what type of data response is expected by the requesting authority.

Trade Lifecycle History <TradLifeCyclHstry**>**

The Trade Lifecycle History will indicate if the data response for the query will be trade activities or trade states.

Possible values for this tag are:

- 'Trade activity' – all reports submitted by counterparties for a given trade (i.e. the first report as well as all the following updates of the trade) are provided as separate records; In this scenario the TradLifeCyclHstry will be set to TRUE in the incoming data query.

- 'Trade state' – only the current trade state as of the day of data query submission is returned (i.e. one record per trade containing only the most up-to-date values reported in each field). In this scenario the TradLifeCyclHstry will be set to FALSE in the incoming data query.

Default value if not provided in the data query is 'Trade state'.

Outstanding Trade Indicator < OutsdngTradInd>

The Outstanding Trade Indicator will indicate if the data response for the query will be for outstanding trades (i.e. trades that have not expired or cancelled) for all trade.
Possible values for this tag are:

- 'Outstanding trades' – only outstanding trades are returned in the output file; In this scenario OutsdngTradInd will be set to TRUE in the incoming data query.
- 'All trades' – all trades are returned in the output file. In this scenario OutsdngTradInd will be set to FALSE in the incoming data query.

Default value: 'Outstanding trades.

If 'All trades' is selected the response can include only the trade lifecycle history. No trade state information will be provided for those trades that are not outstanding. This means data queries that include TradLifeCyclHstry = FALSE and OutsdngTradInd = FALSE will be rejected on ingestion with the Error Message "All trades and current status not allowed".

The table below illustrates the different combinations of TradLifeCyclHstry and OutsdngTradInd and the interpretation that needs to be applied.

TradLifeCyclHstry	OutstandingInd	Data Response
TRUE	TRUE	Trade Activities for outstanding trades only (i.e. will not include expired or cancelled trades)
TRUE	FALSE	Trade Activities for outstanding, expired or cancelled trades.
FALSE	TRUE	Trade States for all outstanding trades only.
FALSE	FALSE	NACK (Not allowed)

For ad-hoc SFT transactions (applicable ISO 20022 messages provided) the report will be delivered in the format:

- **SFT Transactions**: SecuritiesFinancingReportingTransactionReportV01 (auth.052.001.01_ESMAUG_SFTTRA_1.0.0.xsd)
    - For ad-hoc SFT transaction states (applicable ISO 20022 messages provided) the report will be delivered in the format:
- **SFT Transaction States**: SecuritiesFinancingReportingTransactionStateReportV01 (auth.079.001.01_ESMAUG_SFTTRS_1.0.0.xsd)

DATA ENTITLEMENTS FOR AUTHORITIES

Authorities will be able to submit data requests to DDRL and DDRL will respond with the requested data. However, entitlement filters will determine if an authority is entitled to receive data that is returned from the execution of a data request query. The model will be to filter out all data which the requesting authority is not entitled to, by applying entitlement filtering rules to the data extracted for a given query.

Main authorities will have access to all SFT, Margin and Reuse data. However, all other authorities will have restricted access to the data. Authorities that are not main authorities will be given access to data that falls under their mandates and responsibilities. This will be achieved by assigning authorities with Sub Authority Types during the onboarding process, and these Sub Authority Types will represent the mandates and responsibilities of the authorities. The Sub Authority Types assigned to a given requesting authority will activate filters on data that is returned for a given data request from that requesting authority.

Authorities may be assigned multiple Sub Authority Types based on their mandates and responsibilities. In such cases, at least one of the entitlement criteria must be met for the authority to get access to the requested data.

TRACE AND NON-TRACE DATA RESPONSE REPORT FILENAMES

The naming convention of the outbound data response reports will be the same for both the TRACE and Non-TRACE Authorities.

SenderCode_FileType_ReceiverCode_GenericCode1_GenericCode2_Timestamp.zip

SenderCode is a code that identifies the sending partner. For data response reports this will be TRDDR.

Filetype is a 6-character field previously defined. This field identifies what type of data is in the data response report file:

a. **SFTTRA** – for all SFT submissions;
b. **SFTTRS** – for latest state of the outstanding trades;
c. **SFTPOS** – for SFT position-level data responses; [DEFERRED]
d. **SFTREC** – for SFT reconciliation status responses;
e. **SFTREJ** – for SFT rejection status responses.

ReceiverCode is a code that identifies the receiving partner:

- National Competent Authority (CA user): 'CA' should be used for the first 2 characters plus a 3-characters short name for TRACE authorities.
- ESMA (CA user): 'ESMA' should be used plus 1 more character to describe the specific ESMA user. (for TRACE reporting)
- OCODE: for Non-TRACE authorities

GenericCode1 is the first code used to identify files according to the specific context of each system. This field should be 6 or 13 digits long. The first digit should be an indication of the type of message (e.g. A – ad-hoc, R – Recurring, etc.) followed by a 5 characters unique sequence number (Query ID) in hexadecimal notation. This sequence number does not depend on the file type, recipient or any other characteristic and it is related to the Query id number. (It can start again at 00000 after 99999). In the case of SFTTRA, SFTTRS, SFTPOS, SFTREC and SFTREJ files, this code will also include the date for which the query is executed, and data is included in the file. The hyphen-minus character will be used to separate the query id from the date.

GenericCode2 is the second code used to identify files according to the specific context of each system. This should be made up of two parts. First part the number of total files, second part the sequence of the file (E.g. 005001 meaning there are 5 files in total and this file is file 1 in the sequence). Due to the potential large size of response files, in several cases the file will have to be split. Specifically, for the SFTTRA, SFTTRS, SFTPOS, SFTREC, SFTREJ file types a separate digit will be added after the two parts (separated by the hyphen-minus character). This digit will represent the version of the file (i.e. for the first file submission it should always be 0, for every next resubmission of the same file it should raise by 1).

File extension: each file generated is first given an .xml extension. Subsequently, the file is signed and encrypted (SFTTRA, SFTTRS, SFTPOS, SFTREC and SFTREJ files) specifically for TRACE reporting and compressed (other file types) and the extension is converted to .zip.

Example:
TRDDR_SFTTRA_9R01_A11132-190321_003001-0_20190321090033.zip
TRDDR_SFTTRA_9R01_A11132-190321_003002-0_20190321090033.zip
TRDDR_SFTTRA_9R01_A11132-190321_003003-0_20190321090033.zip

DATA RESPONSE REPORT DELIVERY MECHANISM

TRACE Authorities

TRACE data response reports and DDRL feedback messages will be uploaded to ESMA Hub and will be made available to the requesting authorities via ESMA Hub / TRACE infrastructure. These data response reports and DDRL feedback messages will have a Receiver Code in the filename which will indicate the NCA Code of the recipient so that ESMA Hub is able to route the files to the requesting authority.

Non-TRACE Authorities

The data response reports and feedback messages will be made available via Distributed CDTS and sent through DataPower.

Non-TRACE data response reports and DDRL feedback messages will be made available to the requesting authorities directly. Non-TRACE Authorities will be expected to either pull their reports from a local DTCC SFTP folder or they may require DDRL to push their reports to a remote server and SFTP folder.

Each report and OCODE for the Non-TRACE Authorities will be associated to a subscription and this subscription will point to either a local SFTP folder (for Authorities pulling data reports) or to a remote IP address and folder (for Authorities requiring DDRL to Push data reports). These subscriptions will be configured for the Non-TRACE Authority as part of the connectivity process (which will happen once onboarding of the authority has been completed).

The data response reports and DDRL feedback messages will have a Receiver Code in the filename which will indicate the OCODE of the recipient.

SERVICE LEVEL AGREEMENTS

The service level agreements are designed in line with the Commission Delegated Regulation (EU) 2019/357.

Parameter	Service level requirements
The minimum number of recurrent queries that DDRL will process on a particular day from all authorities. **Execution of queries exceeding this limit may be delayed.**	180 TRACE daily queries related to transaction data and position, reconciliation and rejection data; 180 Non-TRACE daily queries related to transaction data and position, reconciliation and rejection data; The above estimates are made with an assumption that all queries, submitted by each NCA, are requested on a daily basis.
The minimu number of ad-hoc queries that DDRL process on a particular day from all authorities. **Execution of queries exceeding this limit may be delayed.**	150 TRACE queries 150 Non-TRACE queries
Minimum length of time window for ad-hoc queries that should be supported by all TRs.	Unlimited
Size limit for the responses to data queries. **Queries exceeding this limit may be delayed.** **This restriction can override the limits for the length of the time window (see above), i.e. if the query complies with the time window limits but the size of the output file still exceeds the limit, the query may be delayed.**	Equal to 150% of the average number of reports received daily by the given TR within the previous calendar year. If the the 150% threshold is exceeded by any query then the report will be made available in 3 working days.
Maximum time for validation of data queries by TRs and sending feedback message to the ESMA System (TRACE Authority) or directly to the Non TRACE Authority.	1 hour
Maximum time for delivering the data requested in an ad-hoc query.	
For queries related exclusively to outstanding trades or trades terminated within last year.	By 12:00 (noon) UTC on the next day after the data query submission (including non-working days)

	For queries related to trades that terminated more than one year ago (trades that are not outstanding and there was no report on these trades within the last year).	3 working days
Time for delivery of response for recurrent data queries.		
	For queries related to transaction-level data.	By 12:00 (noon) UTC on the day of data query execution (including non-working days)
	For queries related to position-level reports.	By 12:00 (noon) UTC on the day of data query execution (including non-working days)

Recurrent data responses will be provided by 12:00 (noon) UTC on the day of data query execution (including non-working days). If the recurrent data response is not delivered by 12:00 PM UTC, then the requesting authority may send DDRL a feedback message with a status "RMDR".

For Recurrent queries, if a recurrent template is requested then DDRL will provide the data response reports as follows:

1. Tuesday EOD on Wednesday by 12:00 PM UTC
2. Wednesday EOD on Thursday by 12:00 PM UTC
3. Thursday EOD on Friday by 12:00 PM UTC
4. Friday EOD on Saturday by 12:00 PM UTC
5. Saturday, Sunday and Monday EOD on Tuesday by 12:00 PM UTC