



TRANSACTION REPORTING UNDER MiFIR: CNMV OPERATIONAL GUIDE

23 February 2018

Index

GLOSARY	3
1. General Overview	4
1.1. Introduction. Applicable Legislation	4
1.2. Users of the Guideline	4
2. Operational Guide	5
2.1. Content	5
2.2. CNMV Transaction Reporting system	5
3. Communication channels	6
3.1. Entities reporting through their own means	6
3.2. Entities reporting through other channels	8
4. Reporting files to CNMV	10
4.1. Naming convention	10
4.2. General rules regarding file Exchange	11
4.3. Special Transaction reporting files REQ	13
4.4. File Exchange flow	14
5. File validation	16
5.1. Validation at the level of file and entity	16
5.2. Content Validations	17
6. Annexes	20
6.1. ESMA / CNMV documentation	20
6.2. Sequence and Version mechanism in SCORE files	21
6.3. Description of "Transaction Status" field	25

GLOSSARY

CNMV	Spanish national competent authority
COM	Electronic procedure for transaction reporting under MiFIR
EEA	European Economic Area
ESMA	European Securities and Markets Authority
FDB	Daily feedback files for transaction reporting “TRA” files
FIRDS	Financial Instrument Reference Data System (ESMA)
FNMT	Spanish certification authority
FRQ	Feedback files for special “REQ” files
FTPS	File Transfer Protocol / Secure Sockets Layer
SI	Systematic Internalizer
ISIN	International Securities Identification Number
LMV	Spanish Securities and Markets Act (Act. 24/1988)
MIC	Market Identifier Code (ISO 10383)
MiFID II	Markets in Financial Instruments Directive 2014/65/EU
MiFIR	Markets in Financial Instruments Regulation No. 600/2014
RM	Regulated Markets
REQ	Special transaction reporting files (under requirement)
PENDING	Transaction status where an instrument is not yet in the FIRDS system
SCORE	System for Collecting Operations Reported by Entities (CNMV)
MTF	Multilateral Trading Facility
OTF	Organized Trading Facility
ARM	Approved Reporting Mechanism
TRA	Daily files for transaction reporting
XML	Extended Marked-Up Language
XSD	XML Schema Definition

1 GENERAL OVERVIEW

1.1 INTRODUCTION. APPLICABLE LEGISLATION.

As of 3 January, 2018, the obligation to report transactions executed on financial instruments provided for in Article 26 of the MiFIR (Regulation 600/2014¹) applies, which provides that investment firms that carry out transactions on financial instruments must report the complete and accurate data of such transactions to the competent authority as soon as possible, and no later than the end of the next business day.

This MIFIR article is supplemented by the [Commission Delegated Regulation \(EU\) 2017/590](#) of 28 July 2016 supplementing Regulation (EU) No. 600/2014 of the European Parliament and of the Council with regard to regulatory technical standards for the reporting of transactions to competent authorities.

In turn, ESMA has published the *MiFIR transaction reporting instructions* that include the XML schemas for reporting as well as the validations applicable to these reports (*validation rules*). This aims to facilitate the development and implementation of reporting systems as well as reporting procedures with CNMV. The annexes at the end of this Guide refer to the documents published by ESMA and CNMV.

1.2 USERS OF THE GUIDELINE

This Guideline is mainly directed to IT Units, as well as Regulatory Compliance and other areas involved in transaction reporting responsible for ensuring that an entity complies with this daily obligation in a thorough, timely and correct manner. It is therefore recommended that entities take all necessary measures to ensure compliance and testing.

Furthermore it is recommended to appoint a responsible person in transaction reporting using both internally and towards CNMV in order to properly coordinate the different areas that might be potentially involved inside the organization.

In order to facilitate this task, CNMV has also enabled the following email addresses: ComunicacionOperaciones@cnmv.es, focused on solving business doubts about regulation, reporting instructions and other business issues, TRMU@cnmv.es mainly focused on IT doubts concerning the daily file exchange, and the helpdesk service of the Electronic Office (sedecnmv@cnmv.es and phone: 902 180 772), to resolve any queries on the COM procedure with CNMV.

¹ Reglamento (UE) n° 600/2014 del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativo a los mercados de instrumentos financieros y por el que se modifica el Reglamento (UE) n° 648/2012.

2 OPERATIONAL GUIDE

2.1 CONTENT

The Operational Guide for Transaction Reporting under MiFIR Art. 26 aims to help guide both entities obliged to report and reporting entities in everything concerning Transaction Reporting to the Spanish competent authority CNMV. It includes the necessary technical procedures to communicate with CNMV, the correct XML file generation, the file submitting process on a daily basis, the information flow between reporting entities and CNMV, and finally the control and validation processes that need to be executed before transaction data records are uploaded onto CNMV's systems.

The detailed description of the information of each transaction to be reported to CNMV is outside the scope of this Guide since both the XML file format and the transaction data contents to be submitted have been previously defined by ESMA (European Securities and Markets Authority).

The main purpose of this guide is to facilitate the understanding of the transaction reporting system for the competent Spanish authority (CNMV), to know how it operates and resolve any possible doubts or incidents. This operating guide is mainly aimed at those responsible for the areas of Organization and IT, but its audience could also cover the business areas of entities obliged to report.

Throughout this Guide is a description of the different communication channels provided by CNMV, as to reporting transaction data files, the file flow between the entity under the obligation to report and CNMV, the different types of files that will be exchanged (data, feedback, and special files), the naming convention defined by CNMV for every file exchanged, the main and basic rules for reporting, CNMV's monitoring and validation processes, and finally the error handling of the information received from entities obliged to report. In addition to this Guide technical documentation (XML schemas and other files) are provided in detail further in the Annexes.

2.2 CNMV TRANSACTION REPORTING SYSTEM

The Spanish competent authority, CNMV, has recently designed a system for reporting transactions under MiFIR Art. 26 in a quick and easy way, as well as receiving feedback from the files sent in a short timeframe and managing incidents easily, so that the entities obliged to report and/or their reporting entities can be diligent and submit their files in a timely manner. The system's name is SCORE (System for Collecting Operations Reported by Entities).

The system SCORE/CNMV is composed of three main modules: the file reception module (available channels, procedures, etc.), the file processing module (including file validation and database update) and the communication module (information exchanged with the entities obliged to report regarding the overall process). The file reception module is available 24 hours a day except for scheduled cut-offs for maintenance purposes. The remaining two modules will be operational between 12 and 16 hours every working day.

3 COMUNICATION CHANNELS

3.1 ENTITIES REPORTING THROUGH THEIR OWN MEANS

CIFRADOCC/CNMV REGISTERING SERVICE

Entities obliged to report must register in the CIFRADOCC/CNMV service before starting to report transaction data and have a valid legal person electronic certificate in CNMV (FNMT, AC Camerfirma, etc.) CIFRADOCC/CNMV is the service for signing and encrypting documents to be submitted by supervised entities through CNMV's Electronic Office.

Additionally, the natural person signing the file must have been previously authorized to access the electronic procedure “COM” (Transaction Reporting under MiFIR) available through the CIFRADOCC/CNMV service.

For entities not yet registered in the CIFRADOCC/CNMV service, the procedure detailed in <https://sede.cnmv.gob.es/sedecnmv/documentos/solicitudPJ.pdf> will serve as a guide.

For entities that have already been registered in the CIFRADOCC/CNMV service but the natural person signing the file has not yet been authorized to access the electronic procedure “COM”, this person must ask CNMV's Electronic Office for this authorization attaching the corresponding power of attorney for this specific electronic procedure.

Taking into account that transaction reporting is a daily obligation, it is recommended that entities have more than one legal person electronic certificate, and more than one natural person authorized to sign and submit files, so the entity will be compliant with the deadlines set for daily reporting.

Taking into account that the CIFRADOCC/CNMV registering process may not be immediate, it is recommended that entities ask for their certificates in advance so they can comply with their obligation regarding the timeframe set for reporting transactions (T+1). Incidences that might happen to an entity² are not a reason to stop reporting.

In the registering process for the electronic procedure COM, the entity will provide CNMV with the responsible contact persons both at business and at technical level, through the registration form at their disposal. In case any incident occurs, CNMV will contact the right person without delay.

REPORTING THROUGH CNMV'S ELECTRONIC OFFICE

Once the entity has generated the XML file and compressed it, the resulting ZIP file must be signed and submitted to CNMV through its Virtual Office using the CIFRADOCC/CNMV service and the electronic procedure “COM”.

The steps to be followed for signing and submitting files to CNMV are:

- Access CNMV's website and click on Electronic Office / Online Register, using the

² Incidents like staff holidays, sick leave, expired certificates, transfer of personnel authorized to sign, etc.

legal person electronic certificate or the username and password provided during the registration process.

- Select the electronic procedure named: Transaction Reporting under MiFIR (COM).
- Following the steps shown on the screen, select the ZIP file and click on the “Sign and Submit” button, which uses @firma platform promoted by the Spanish government, based on open source software and open standards.
- Upon receipt of the file by CNMV, an acknowledgement of receipt of the file in PDF format will be sent to the email address specified in the signing form. This acknowledgement only indicates that the file has been received and registered at CNMV’s systems, it doesn’t mean anything concerning the validity of the information inside which will be checked in a later step.
- The “acknowledgement of receipt” PDF file includes the date and time the original file arrived, and the entry register number if the submission process succeeded. Additionally it will include a CSV code (Secure Verification Code) which can be used to check the authenticity of the acknowledgement PDF itself.
- Should any error occur during the submission, reception or initial validation processes, an email will be sent to the same address with information on the error and the process will not continue.
- Once the content validation process implemented by CNMV has finished, an email will be sent to the addresses previously provided by the entity obliged to report including an XML feedback file with the entire outcome of the validation process. There will be detailed information regardless whether the file passed the content validations or not, in order to facilitate the correction process and proceed to send the corrections.

CNMV FTPS REGISTERING SERVICE

In case of using the FTPS server it will be necessary to have previously requested access to this registering service through the Customer Service of CNMV’s Electronic Office by email. The legal person’s electronic certificate is required for registering. CNMV’s Electronic Office user service will provide you with the registration form asking for some identity and contact details. The entity asking for the service will fill it in and send it back by email. Finally, CNMV’s Electronic Office will provide the entity with all the necessary information (technical documents, validity timeframe, attributes and parameters) to successfully connect with the FTPS server. For any questions or doubts, please contact CNMV’s Electronic Office by phone: 902180772 or email: sedecnmv@cnmv.es

REPORTING THROUGH CNMV’S FTPS SERVICE

Once the entity has generated the XML file and compressed it, the resulting ZIP file must be signed electronically following the signature characteristics and sent to CNMV through its own means. The signature must be generated with the legal person certificate of the CIFRADO/CNMV service. The signature’s characteristics are the following:

- ❖ Format: CAdES-BES
- ❖ Signature algorithm: SHA-512
- ❖ Extension: .SIGN

To submit files follow the steps set out below:

- Sign the file SUBMENT_EXECENT_FILETYPE_SEQUENCE-VERSION_YEAR.ZIP as described above. The file name will have the same name and its extension will then be .ZIP.SIGN.
- Access CNMV's FTPS server ftpserver.cnmv.es using the parameters provided by CNMV's Electronic Office helpdesk, upon requesting this service, and upload the file into the \Inbox folder.
- Upon receipt of the file by CNMV, an acknowledgement of receipt in PDF format will be sent to the email address specified in the signing form. This acknowledgement only indicates that the file has been received and registered in CNMV's systems and in no case means that the information contained is valid, which will be verified in a later step.
- Should any error occur during the submission, reception or initial validation processes, an email will be sent to the same address and the process will not continue.
- Once the content validation process implemented by CNMV has finished, an email will be sent to the email addresses previously provided by the entity under obligation to report including an XML feedback file with the entire outcome of the validation process. Detailed information will be available in case the file does not pass the content validations, in order to facilitate the correction process and former reporting. In addition, a copy of the feedback XML file will be delivered to the sender through the FTPS server in the \Outbox folder.

3.2 ENTITIES THAT COMMUNICATE THROUGH OTHER CHANNELS

Submitting Transaction Reporting data to CNMV is available as well for Trading Venues (RM-Regulated Markets, MTF-Multilateral Trading Facilities and OTF-Organized Trading Facilities) and ARM-Approved Reporting Mechanisms by any competent authority belonging to the EEA. In order to allow the communication and reporting to any of them, CNMV has designed the necessary procedure to facilitate the reporting on behalf of other executing entities.

The Spanish competent authority, CNMV, through its Electronic Office will provide the Trading Venues or ARMs with a simple registration form asking for identification and contact details. CNMV can request for some additional documentation to guarantee the authenticity and legitimacy during the submitting process. After checking that, CNMV will send back the registration form including all the technical details necessary to connect to the FTPS server. For any questions or doubts, please contact CNMV's Electronic Office by phone: 902180772 or email: sedecnmv@cnmv.es

The main features of this procedure are the following:

- ❖ These reporting entities RM/MTF/OTF/ARM will use the FTPS service, so they will have to register by contacting CNMV's Electronic Office by email beforehand.
- ❖ RM, MTF, OTF or ARM will generate every working day at least one XML file per executing entity they are reporting to on their behalf (structure and schemas according to ESMA specifications). The file will be compressed and will have the extension .ZIP (see naming convention in chapter 4).

- ❖ After reaching the FTPS server using the credentials provided by CNMV, the rest of the steps will be the same as described in chapter 3.1.
- ❖ Depending on different circumstances, CNMV could agree with every TV, ARM or SI the most adequate and reasonable timeframe to access, upload, download and process their daily files.

4 REPORTING FILES TO CNMV

4.1 NAMING CONVENTION

NAMES OF FILES SUBMITTED TO CNMV

The file including transaction data to be submitted to CNMV must be XML and validate the corresponding XSD schema provided by ESMA. The file naming convention must be the following naming convention: **SubmEnt_ExecEnt_FileType_Sequence-Version_Year.XML**, whereby:

- ❖ **SubmEnt** (20 characters): must be a valid LEI code for the submitting entity, according to the technical reporting instructions and validation rules provided by ESMA.
- ❖ **ExecEnt** (20 characters): must be a valid LEI code for the executing entity, according to the technical reporting instructions and validation rules provided by ESMA.
- ❖ **FileType** (3 characters): file type submitted to CNMV, valid values are “TRA” for daily reporting or “REQ” for special required reporting.
- ❖ **Sequence**: it is a six-digit-sequence number starting in “000001” and filled with zeros to the left, for each *file submitted* by a reporting entity and admitted to be processed by SCORE/CNMV.
- ❖ **Version**: It is a two-digit-sequence number starting in “00” and filled with zeros to the left, it is the version of the file for a given sequence number. If a file is rejected (e.g. incorrect schema, extension, naming convention error, etc.), it shall be resubmitted by the reporting entity with the same sequence number and an increased version number (previous version number + 1).
- ❖ **Year**: It is a two-digit number. It is the year when the file was submitted. It facilitates filing.

Once the XML file has been generated it must be compressed and keep the same name and extension .ZIP. In the event that the reporting entity communicates transactions through its own means, the ZIP file must be signed according to the specifications previously detailed and its extension must be .ZIP.SIGN.

XML FILE HEADER

The XML file defined by ESMA under standard ISO 20022 includes the BAH (Business Application Header) message definition, which is mandatory and gathers information about the message according to the technical reporting instructions published by ESMA.

The element “Business Message Identifier” must follow the rules specified by each NCA. Files submitted to (and reported back from) CNMV must populate this element using part of the file naming convention: “**ExecEnt_FileType_Sequence-Version**”, (34 characters long) so that it clearly identifies the Business Message for the Messaging-Endpoint that created the Business Message.

NAMES OF FILES REPORTED BACK FROM CNMV

Once an XML file has been successfully sent to CNMV (regardless of the reporting channel), the SCORE/CNMV system starts processing its content, which includes a first set of validations at file level and, if no errors occur, there is a second set of validations, at content level, for each transaction report included in the file. At the end of the process an XML feedback file is generated by the system and sent back to the reporting entity or RM/MTF/OTF/ARM, either by email or through the FTPS server in the “\Outbox” folder.

The XML feedback file from CNMV will keep the same naming convention rules except for the following:

- ❖ **FileType**, the only valid values are “FDB” or “FRQ”, depending on the FileType of the file reported by the entity “TRA” or “REQ” respectively.
- ❖ Exceptionally the **Version** field included in a feedback file could have the values “X1”, “X2”..., “X9”. This singularity will happen when the SCORE/CNMV system needs to send back a feedback file to a reporting entity that has not sent the corresponding transaction report data file. For instance, if a transaction report is “Pending” and after three days it must be accepted (or rejected after seven days) and the reporting entity has no transaction data to report during this period, the Spanish competent authority (CNMV) will send a feedback file to report this status change to a “Pending” transaction.

The XML feedback file will be compressed and sent back with ZIP extension and SCORE/CNMV *will suffix it with a TimeStamp*. The ZIP “feedback” file keep the following naming convention:

SubmEnt_ExecEnt_FileType_Sequence-Version_Year_YYYYMMDDHHMMSS.ZIP

XML FEEDBACK FILE CONTENT

XML Feedback files reported back from SCORE/CNMV will include an optional element called “MessageReportIdentifier”. Regarding this element, it will only appear in the <Document> section identifying in each content validation error the source file in which each operation came, and only in cases where more than one source file is referenced. The different cases are detailed in the section “6.5 Business file header” of the “Technical Reporting Instructions” published by ESMA.

Further down in the same XML, in the cases it includes *content validation errors*, there is a mandatory field at record level called “OriginalRecordIdentification”, defined as a unique and clear identification of the original data for which the status is provided. This element will be populated by the SCORE/CNMV system with the concatenation of two elements: “Executing Entity Code (LEI)” and “Transaction Reference Number” so that it will uniquely identify the report and its validation errors, if any.

4.2 GENERAL RULES REGARDING FILE EXCHANGE

The process of file exchange between CNMV and reporting entities will adhere to the following rules:

- ❖ **Daily file.** Every reporting entity will usually send a file per executing entity before the end of “T+1” to CNMV, as long as it has executed transactions in “T” under the MiFIR

regime Art. 26. However, it will be possible to report more than one file per executing entity in order to correct or update those transactions reported back as erroneous by CNMV, or even to complete the daily reporting before the “T+1” deadline.

- ❖ **Deadline T+1.** The timeframe any entity has to send their transaction data is by the end of “T+1” of the next working day. Working days are all weekdays except for Saturdays and Sundays and except for all official national holidays within the member state of the national competent authority to which the transaction report is submitted.
- ❖ **Duplicated transactions.** A transaction report cannot be sent again if it has been previously sent to CNMV in the same file or in a previously sent file, taking into account that a transaction is uniquely identified by field [2] Transaction Reference Number and field [4] Executing Entity Code (LEI). The SCORE/CNMV system will flag this transaction report as duplicated and it will be returned with an error. In order to update, modify or substitute a transaction already reported and accepted, it is necessary to cancel the original transaction and then report a new one with the correct information.
- ❖ **Subsequent reporting.** It must be taken into consideration that concerning daily “TRA” files, a subsequent file submitted in “T+1” -including transactions executed in “T”- does not replace the preceding submitted file, but complements the daily reporting. By way of an example, in the case of a submitted file including 1,000 transactions with no errors at file level for which CNMV returns a feedback file including errors in 3 different transactions, the reporting entity must submit a second file with a different Sequence number as soon as possible and before the end of “T+1”, including these 3 rectified transactions and perhaps some others executed in “T” and not submitted in the first file. But if the reporting entity includes in its second file those 997 already accepted transactions, the SCORE/CNMV system will process them and report them back as duplicated transactions. In another case, even if the 1,000 transactions have been accepted with no errors after processing the first file, the reporting entity is allowed to send other files before the end of “T+1”, including transactions not reported in the first file in order to complete the daily reporting before the deadline.
- ❖ **CIFRADO and FTPS services.** Both CIFRADO/CNMV and FTPS server services are usually operational 24/7, except for scheduled maintenance outages. Accordingly, any submitting entity will be able to report transactions executed on a Friday not only before the end of the following working day but also during the weekend.
- ❖ **XML file validation.** Reporting entities are obliged to validate any XML file against its corresponding XSD schema before compressing and submitting the file to CNMV, since SCORE/CNMV will validate the file as well after decompressing it.
- ❖ **Acknowledgement of receipt file.** The acknowledgement file automatically reported back from SCORE/CNMV either by email or through the FTPS server is just a simple “acknowledgement of receipt” and it only means that the file has been received by CNMV and the entry of the electronically signed file has been registered. The acknowledgement file does not include any information regarding the validity of the file, which will be checked in a later step.
- ❖ **Electronic Office.** Should a reporting entity not receive the acknowledgement file after submitting a transaction data file within a short period of time, it must contact CNMV through its Electronic Office Helpdesk service (Phone No.: 902 180 772 – email: sedecnmv@cnmv.es) to report the issue.
- ❖ **File received and processed by CNMV.** The reporting entity must not consider a submitted file as processed by SCORE/CNMV until it receives not only the acknowledgement file but also the feedback file, including the outcome of the

validation process. Should a reporting entity not receive the feedback file within the next two working days it must contact CNMV through its Electronic Office Helpdesk service.

- ❖ **Feedback files returned by CNMV.** The SCORE/CNMV system will generate a feedback file for each transaction data file received, including the outcome of the validation process, and will report back to the reporting entity as soon as possible. As mentioned in ESMA's "Technical Reporting Instructions", if the submitting entity does not receive feedback for previously submitted transactions, it should continue to report. Lack of feedback files is not a reason to stop reporting.
- ❖ **Maximum number of transactions.** The maximum number of transactions is set to 500.000 records within a file, including both new transactions and cancellations. Should any reporting entity need to report more than the maximum number in a daily file, the report will be split into two or more different files, which will be processed according to their respective sequence numbers.
- ❖ **Data storage obligation.** Reporting entities are obliged to maintain a backup copy of both data reported to and data received from the Spanish competent authority, CNMV. This obligation starts on 3 January, 2018 and in any case for a period of time of five years since the reporting date. CNMV will find this useful for detecting errors or missing transaction data, and requiring the entity to update or complete its reporting.

4.3 SPECIAL TRANSACTION REPORTING FILES "REQ"

CNMV is considering the possibility of exceptional transaction data reporting, always at the request of CNMV to the executing entity. To carry this out, a simple procedure has been implemented to report *special transaction reporting files* to CNMV, both by entities reporting through their own means and entities reporting through a RM/MTF/OTF/ARM.

Special files named "REQ" (Request file) are those which include late or missing transaction reporting, or modified transaction reports previously reported for which CNMV has detected quality errors not included in ESMA validation rules. Anyway this information will always be reported on CNMV's demand to the corresponding executing entity but never on its own initiative. This does not prevent the entity from detecting any problems in its reporting and asking CNMV to authorize special reporting using the necessary "REQ" files.

The procedure is called "Additional Reporting" and it aims to allow entities to catch up with the transaction reporting obligation in an easy way, without interrupting the daily transaction data reporting.

"REQ" REPORTING FILES PRECONDITIONS

1. CNMV, after identifying errors, quality issues or missing transaction reporting will contact the appointed responsible persons in the entity to let them know about the incidents.
2. The entity obliged to report will take the necessary measures to correct the problems in the daily reporting. Once these problems are fixed, the entity will communicate this to CNMV, in order for it to be reviewed.

3. CNMV will check the information reported concerning the problems detected, in order to ensure that daily transaction data is being reported properly. Then, if necessary, CNMV will send the entity a requirement asking for the rectification of transaction reports, including detailed information on the period of time, type of transactions, trading venues affected, etc.
4. The entity obliged to report must gather the necessary information to rectify the transaction reports as well as identify missing information that needs to be reported.

SPECIAL “REQ” FILES CREATION AND SUBMISSION TO CNMV

The “Additional Reporting” procedure is focused on reporting or rectifying a certain volume -sometimes huge- of reports, after CNMV’s requirement through its Secondary Markets Department. In order to properly report “REQ” files the following steps must be taken:

- ❖ Generate an XML file with the same structure as the regular daily files, including the “REQ” FileType element in the file name. Compress the XML file keeping the original file name.
- ❖ Entities reporting through their own means must sign the ZIP file (using the @firma platform or signing through their own means if they use the FTPS reporting channel), and then submit the file to CNMV.
- ❖ The same day an Entity is reporting a “REQ” file it will be possible to report a daily “TRA” file from the same executing entity, so the reporting of different types of files in the same day does not penalize the daily “TRA” files reporting.
- ❖ “REQ” files will have the same treatment than “TRA” files from the point of view of reception, acknowledgement, naming convention, schema validation, content validations and feedback files returned by CNMV.
- ❖ Regarding file content, it is reminded that transaction reports must be cancelled before sending the modified transaction reports through an “REQ” file.
- ❖ When the entity must report a huge volume of transaction reports, it must take into account the maximum limit of records within a single file.
- ❖ When the Entity received the “FRQ” feedback file with errors it must follow the same steps as with “TRA” files; as soon as possible the entity must report the corrections concerning the transactions flagged with errors using a new “REQ” file with a new sequence number.
- ❖ Special “REQ” files submitted to CNMV will be checked by the Secondary Markets Department before being rejected by CNMV or processed by SCORE/CNMV. The “REQ” file process will take place in special time-slots depending on their volume, content or other characteristics.
- ❖ Feedback files that CNMV reports back to the entity as an outcome of the process will have “FRQ” as FileType instead of “FDB”, which is used for reporting feedback files for “TRA” files.

4.4 FILE EXCHANGE FLOW

File exchange flow between an entity and CNMV can be described as a simple transaction file flow together with the corresponding feedback files. It has been designed to facilitate communication with CNMV and provide the entity with the necessary information concerning the overall process, so the entity can react to any incident that occurs.

The main principles of this file exchange are the following:

- ❖ **CNMV's acknowledgement of receipt.** Every file submitted by an entity will have as an answer the acknowledgement receipt file either by email or through the FTPS server in the "\Outbox" folder. This will happen almost immediately, within the following minutes after sending the file.
- ❖ **XML feedback file.** Once the file has been submitted and the acknowledgement receipt is received by the entity, the SCORE/CNMV system will process the file and report back the corresponding feedback file to the entity either by email or through the FTPS server in the "\Outbox" folder. The feedback file includes comprehensive information regarding the outcome of the validation process, and detailed information about the errors detected per transaction report, if any. The SCORE/CNMV system will not upload to its databases any transactions flagged with an error.
- ❖ **File naming convention.** Reporting entities must have control over the files they are reporting, especially the "Sequence" since they must increase this number every time they generate and report a new file successfully, regardless of the outcome of the validations. Should an error occur at file level during the validation process, the file will not be processed and the next file to be reported will maintain the same "Sequence" and increase the value of the "Version" (o1, o2...) in its file name.
- ❖ **Files including transactions after the deadline.** In theory, a transaction data file could include transactions executed in different days, although this should not be the usual. A file reported in "T+1" could include a transaction executed in "T" and occasionally transactions executed in "T-1" or even before. Although SCORE/CNMV allows for the gathering all these transactions, the Secondary Markets Department will keep track of the transactions reported by entities regarding the deadlines established by MiFIR.
- ❖ **Exceptional operation.** When an entity cannot report its transaction data files for several working days (due to errors at file-level, missing a lot of reports, internal problems, etc.) the person in charge must contact CNMV through the Electronic Office Helpdesk service or via the email: ComunicacionOperaciones@cnmv.es. Once the problem has been solved the reporting entity must send the missing reports in chronological order, either using "TRA" files or gathering all the information and reporting a "REQ" file if requested by CNMV.

5 FILE VALIDATION

5.1 VALIDATIONS AT THE LEVEL OF FILE AND ENTITY

Files received at the SCORE/CNMV system, regardless of the reception channel through which they were sent, go through different verification phases before uploading the transaction information into the corresponding databases. The first phase deals with the file reception and it is mainly focused on checking the file type, format, structure, extension, naming convention as well as identifying the valid LEI codes both for reporting and executing entities. It also checks previously received files by the reporting entity and both Sequence and Version validation.

All controls carried out in this first phase are incompatible with the process of the content of the file, so should at least one of these controls produce an error, an XML feedback file will be reported to the Entity, according to the format designed and published by ESMA and the validation process will not continue. The reporting entity must submit a new file using the same Sequence and a new Version number.

FILE LEVEL VALIDATIONS SENT TO CNMV

Hereafter you can find the validations carried out by SCORE/CNMV at file level, together with the different error codes these validations returned through the feedback file sent back to the reporting entity:

Error codes related to the file name:

- ❖ ESX-109: The file does not follow CNMV's naming convention.
- ❖ ESX-110: The reporting Entity LEI code is not valid, or is not registered in SCORE.
- ❖ ESX-111: The executing Entity LEI code is not valid, or is not registered in SCORE.
- ❖ ESX-112: The FileType code inside file name is not valid.
- ❖ ESX-113: The Sequence code inside the file name is not valid.
- ❖ ESX-114: The Year code inside the file name is not valid.
- ❖ ESX-115: The Version code inside the file name is not valid.

Error codes related to the reported file:

- ❖ ESX-107: The file with SubmEnt and Sequence codes has already been received at CNMV. Duplicated file.
- ❖ ESX-108: The file with new Version code has already been received at CNMV. Invalid file name.

Error codes at format and file structure level:

- ❖ ESX-101: The file signature is not valid.
- ❖ ESX-102: The ZIP file cannot be decompressed.
- ❖ ESX-103: The ZIP file contains more than one file, or a non XML file.
- ❖ FIL-104: The ISO 20022 Message Identifier in the BAH is not valid.
- ❖ FIL-105: The file structure does not validate the XML schema.
- ❖ ESX-106: The ZIP file name does not match the XML file name (excluding the suffix TimeStamp).
- ❖ ESX-116: The number of transactions in the file exceeds the maximum allowed.

- ❖ ESX-117: Sequence code not expected. Please submit a new file using the pending Sequence with an increased Version number.
- ❖ ESX-118: The field “Business Message Identifier” in the BAH is not valid.

This is a non-exhaustive list and therefore could be completed in the future with some other new Error codes based on new validations.

Error code ESX-101 can only occur in files signed (.ZIP.SIGN) by the reporting entities. Both error codes FIL-104 and FIL-105 come from ESMA’s Technical Reporting Instructions derived from mandatory file-level validations included in these instructions, and concerning the XSD schemas used both for the header file and the content or body of every XML transaction data file. Before any reporting entity submits a file to CNMV, it must validate the XML file against the corresponding XSD schema provided by ESMA.

All errors produced during the validation process will be sent back to the reporting entity through the feedback file either by email or through the FTPS server, with detailed information on the errors detected.

5.2 CONTENT VALIDATIONS

In the second phase of the verification, only the files that have successfully passed the first verification phase will move on to the second phase, regarding the content of every transaction or cancellation included in the file.

The content validations carried out in this second phase are attached to this Guide and detailed in the Annex 1 “ESMA Validation rules”, with all the necessary information for every rule to be implemented in the local systems.

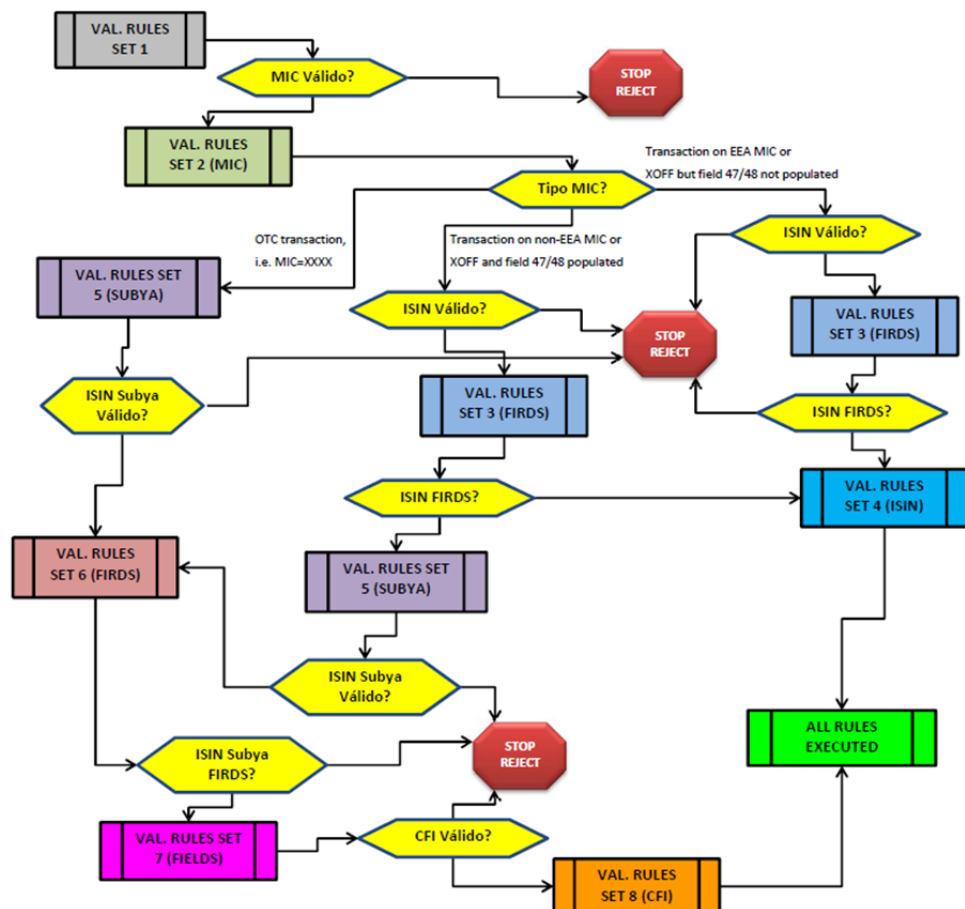


Diagram 1. Validation rules: different sets and execution order.

Since content validation processes implemented in SCORE/CNMV will replicate all validation rules for every transaction, reporting entities are recommended to implement and execute the validation rules procedure the same way in their local systems before submitting the file. The validation rules have been split into eight different sets and must be applied in a specific order.

The content validation process for each transaction can be successful (they go through all the content validations executed for that transaction passed without errors) or can produce one or more errors. The errors of all transactions included in a single file will be detailed in the corresponding feedback file to be sent back to the entity. These errors have an error code and an error description following the format CON-NNN where NNN will be a three-digit number identifying first the field number (01...65) of the field which is being validated in this rule, and then the sequential number of the rule for this field.

The feedback file content is quite complete. Among other data, it includes a “**File Status**” element reporting on the file status after the validation process. The possible values are as follows:

- ❖ ACPT – Accepted, when all transactions included in the file have successfully passed their validation rules and accepted by SCORE/CNMV as valid transactions.
- ❖ PART – Partially Accepted, when there is at least one transaction which produced at least one content error and therefore there is at least one transaction with “Transaction Status” either rejected or pending (pending instrument or underlying validation in the FIRDS system).
- ❖ RJCT – Rejected, when file errors are detected, SCORE/CNMV will not load any records of the file (the whole file is rejected); when no file errors are found but all transactions have been rejected by SCORE/CNMV.

A Feedback file includes a “**Transaction Status**” element for each transaction or cancellation report after the validation process. Possible values for this element are:

- ❖ ACPT – Accepted, when the transaction has successfully passed all its validation rules regarding its Instrument or Underlying Instrument code, and its trading venue code, defined by ESMA according to its ISIN and MIC. The transactions with Transaction Status “Accepted” included in a feedback file will necessarily have to come from the previous status “Pending” (PDNG).
- ❖ PDNG – Pending, this status code is used in case the transaction report cannot be validated due to missing instrument reference data (either instrument or underlying instrument), even if the transactions pass all the remaining validations.
- ❖ RJCT – Rejected, when the transaction report is incorrect and produces one or more content errors.
- ❖ RCVD – Received, when for an operation reported with execution date "T" (Trade Date) the instrument of such operation is not available in ESMA's FIRDS database, which is published regularly in "T + 1", early in the morning, on instruments reported in "T". This will occur for all operations reported on the same day of its execution.

The singularity of the instrument or underlying instrument validation (in the case of OTC transactions or transactions executed in trading venues out of the EEA) consist of checking up if the instrument is included in FIRDS system on the trading date. FIRDS database is updated daily from NCAs, Trading Venues, Systematic Internalizers and Approved Reporting Mechanisms.

The following diagram graphically describes the Transaction Status life cycle of a transaction report, starting with its individual process (received in a file without errors at file level) and the validation rules complied at every moment of its life cycle.

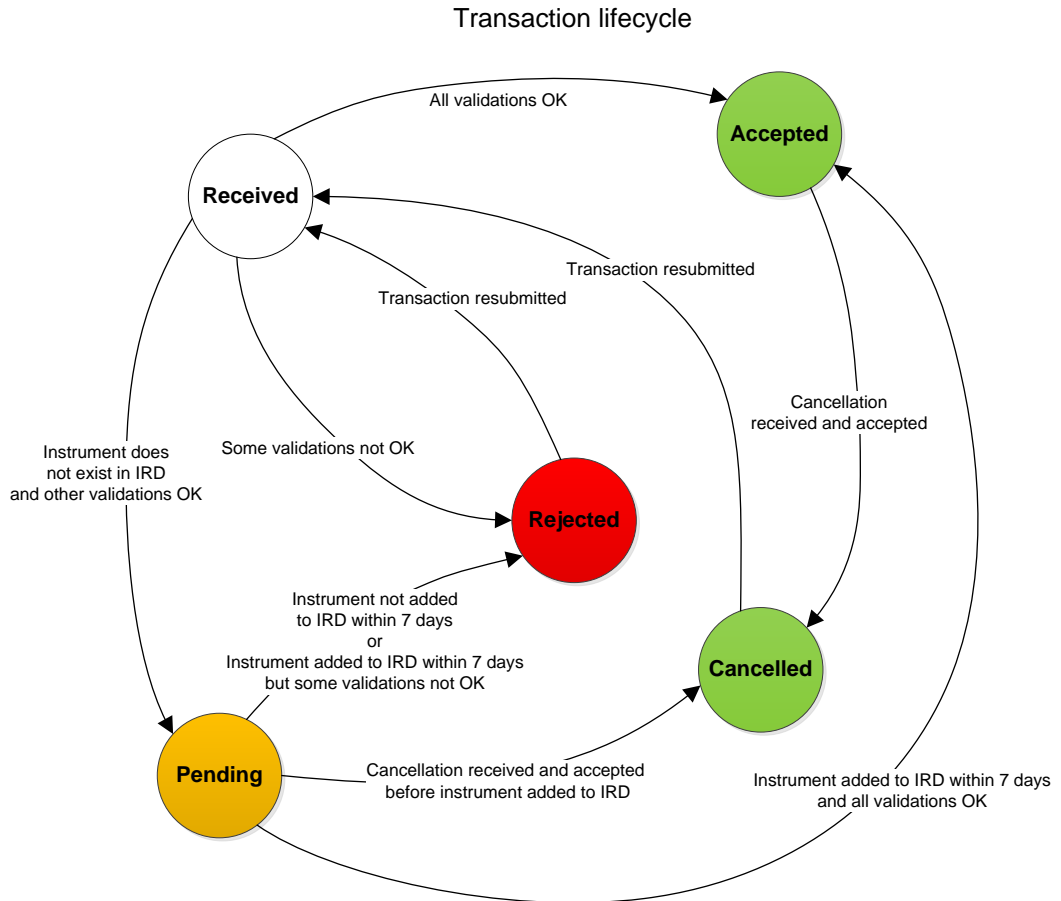


Diagram 2. Transaction Status life cycle according to validation rules.

6 ANNEXES

6.1 ESMA / CNMV DOCUMENTATION

Following the link <https://www.esma.europa.eu/policy-rules/mifid-ii-and-mifir/mifir-reporting-instructions> the MiFIR technical reporting instructions, XML schemas, and validation rules excel file can be downloaded from ESMA's website, this documentation is published and updated on a regular bases.

Together with this Operational Guide you will find different files including documentation within the scope of CNMV.

6.2 SEQUENCE AND VERSION MECHANISM FOR SCORE FILES

As of December 2017 SCORE system has been updated concerning the Sequence number in the way that **Sequence Number will be considered at the level of both Submitting Entity and Executing Entity**. This validation update is going to be ready for MiFID II / MiFIR entry into force.

This annex explains the Sequence-Version mechanism, answers most of the questions recently raised, and is applicable for both Entities submitting through their own means and Entities reporting through other channels like ARMs and TVs reporting on behalf of several clients; in this case the file validation for any file will not have any impact (neither in time nor in schedule) in the daily process of the files belonging to the rest of the ARMs/TVs clients. The SCORE/CNMV naming convention is described in the CNMV Operational Guide as follows: **SubmEnt_ExecEnt_FileType_Sequence-Version_Year.XML** .

PRELIMINARY CONSIDERATIONS

SCORE considers three main concepts inside the XML file:

- ❖ Any **XML File** coming from an Obligated Entity, ARM or TV will be uniquely identified by its SubmEnt, ExecEnt and the rest of the file name.
- ❖ The file **Sequence** is a six-digit-sequence number starting in “000001” and filled with zeros to the left.
- ❖ The Sequence’s **Version** is a two-digit number always starting in “00” and filled with zeros to the left. It is the version of the file for a given Sequence number.

SCORE considers two main dependencies between these three concepts:

- ❖ The Sequence number will always depend on the complete XML file name, the unique pair “SubmEnt” and “ExecEnt” and the outcome of the FILE LEVEL VALIDATIONS (described in Chapter 5.1 of the CNMV Operational Guide) for the *last* XML file with correct “Sequence” and “Version” for this client (same pair “SubmEnt” and “ExecEnt”).
- ❖ The Version number will always depend on the *latest valid* Sequence and Version numbers used (and consequently on the XML file name)

Finally SCORE considers two validation levels, as described in Chapter 5 FILE VALIDATION, and there is a dependency between the first and the second one:

1. **FILE and ENTITY validations:** Check errors in the file name itself, errors related to previously reported files, format errors and file structure errors. In case anyone of these errors appears, the file validation will stop and consequently the file content will not be processed, and SCORE will report a FDB file including ESX/FIL errors. Since it is not possible neither completely validate the file nor process its content, the file itself is considered as not processed by SCORE.
 - If the file passes all file validations the validation process will continue and therefore the XML file will be processed by SCORE.
2. **CONTENT validations:** The file is processed regarding the content of every transaction or cancellation included in the XML file, and SCORE will finally report a FDB file including CON errors if any. Regardless the number of rejected or accepted transactions, the file will be considered as successfully processed by SCORE.

HOW SCORE DEALS WITH FILE NAMES, SEQUENCES AND VERSIONS?

When a file does not successfully complete the first validation level, file is rejected (errors FIL/ESX-XXX), and the following XML file for this pair “SubmEnt” and “ExecEnt” should use the *same Sequence with and increased version number*.

When a file is successfully processed, only content errors (CON-XXX) are included in the FDB file reported back from SCORE. Transactions have been loaded into SCORE database (no matter the status of each one of them). The following XML file for this pair “SubmEnt” and “ExecEnt” should use *the following Sequence number and the initial version number ‘00’*.

In order to ensure that files are processed in the correct order, SCORE/CNMV performs some validations on each file received regarding its file name. Hereafter you can find some of the most common validations and scenarios which will be useful to understand the overall validation process regarding SCORE file naming convention.

VALIDATION – SCENARIO [A]

- ✓ Sequence number should be higher than any other sequence number already received for the pair “SubmEnt” and “ExecEnt”. The only allowed exception for this rule is sending again a file, with the same sequence number than a previously sent file, but with an increased version, to correct previous file validation errors.
- Submitting entity (SUBM*LEI23) submits in the order showed the following files on behalf of several Executing entities (EXEC*LEI01-02-03-04):

File Submitted to SCORE	Outcome after SCORE validation steps	FDB Reported back from SCORE
SUBM*LEI23_EXEC*LEI01_TRA_000001-00_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI02_TRA_000001-00_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI03_TRA_000001-00_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI04_TRA_000001-00_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI01_TRA_000002-00_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI03_TRA_000002-00_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI04_TRA_000002-00_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI02_TRA_000005-00_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI02_TRA_000004-00_18	Invalid sequence (a higher sequence has already been used for that submitting and executing entities).	ESX-113: The sequence code inside the file name is not valid.
SUBM*LEI23_EXEC*LEI01_TRA_000003-00_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI02_TRA_000006-00_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File

VALIDATION – SCENARIO [B]

- ✓ For an XML file created with a new Sequence number for the pair “SubmEnt” and “ExecEnt”, its version should start in ‘00’. In case of starting with the wrong version number, the following XML file should come back to initial version ‘00’.
- Submitting entity (SUBM*LEI23) submits in the order showed the following files on behalf of its Executing entity (EXEC*LEI01):

File Submitted to SCORE	Outcome after SCORE validation steps	FDB Reported back from SCORE
SUBM*LEI23_EXEC*LEI01_TRA_000001-00_18.xml	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI01_TRA_000002-01_18.xml	Valid sequence. Invalid version.	ESX-115: The Version inside the file name is not valid: version number should be 0.
SUBM*LEI23_EXEC*LEI01_TRA_000002-00_18.xml	Valid sequence and version. File with file errors.	FIL-XXX / ESX-XXX errors
SUBM*LEI23_EXEC*LEI01_TRA_000002-01_18.xml	Valid sequence. Invalid version.	ESX-107: File already received. Duplicated file.
SUBM*LEI23_EXEC*LEI01_TRA_000002-02_18.xml	Valid sequence and version. File with file errors.	FIL-XXX / ESX-XXX errors
SUBM*LEI23_EXEC*LEI01_TRA_000002-03_18.xml	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI01_TRA_000003-00_18.xml	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File

VALIDATION – SCENARIO [C]

- ✓ Every XML file rejected by SCORE with file errors (FIL/ESX-XXX) for any pair “SubmEnt” and “ExecEnt” should be corrected before submitting a new Sequence number for the same pair “SubmEnt” and “ExecEnt”.
- Submitting entity (SUBM*LEI23) submits in the order showed the following files on behalf of its three Executing entities (EXEC*LEI01-02-03):

File Submitted to SCORE	Outcome after SCORE validation steps	FDB Reported back from SCORE
SUBM*LEI23_EXEC*LEI01_TRA_000001-00_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI02_TRA_000001-00_18	Valid sequence and version. File with file errors.	FIL-XXX / ESX-XXX errors
SUBM*LEI23_EXEC*LEI01_TRA_000002-00_18	Valid sequence and version. File without any file error. File Processed. Note that File errors in sequence 000001 for a different Executing Entity (EXEC*LEI02) will not impact on files sent by EXEC*LEI01.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI02_TRA_000001-01_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI03_TRA_000001-00_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI01_TRA_000003-00_18	Valid sequence and version. File with file errors.	FIL-XXX / ESX-XXX errors
SUBM*LEI23_EXEC*LEI02_TRA_000002-00_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI03_TRA_000002-00_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File

SUBM*LEI23_EXEC*LEI01_TRA_000004-00_18	Invalid Sequence. Previous Sequence No. 000003 for the same submitting and executing entity should be corrected first.	ESX-117: Sequence code not expected. Please submit a new file using the pending Sequence with an increased Version number: pending sequence = 3
SUBM*LEI23_EXEC*LEI03_TRA_000003-00_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI01_TRA_000003-01_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI01_TRA_000005-00_18	Invalid sequence. Previous Sequence No. 000004 for the same submitting and executing entity should be corrected first.	ESX-117: Sequence code not expected. Please submit a new file using the pending Sequence with an increased Version number: pending sequence = 4
SUBM*LEI23_EXEC*LEI03_TRA_000004-00_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI01_TRA_000004-01_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI01_TRA_000005-01_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI01_TRA_000006-00_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File
SUBM*LEI23_EXEC*LEI02_TRA_000003-00_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File

VALIDATION – SCENARIO [D]

- ✓ For an XML file submitted for the pair “**SubmEnt**” and “**ExecEnt**”, its version number should be higher than any other version previously submitted for the same pair “**SubmEnt**” and “**ExecEnt**” and Sequence number.
- Submitting entity (SUBM*LEI23) submits in the order showed the following files on behalf of its Executing entity (EXEC*LEI01):

File Submitted to SCORE	Outcome after SCORE validation steps	FDB Reported back from SCORE
SUBM*LEI23_EXEC*LEI01_TRA_000001-00_18	Valid sequence and version. File with file errors.	FIL-XXX / ESX-XXX errors
SUBM*LEI23_EXEC*LEI01_TRA_000001-01_18	Valid sequence and version. File with file errors.	FIL-XXX / ESX-XXX errors
SUBM*LEI23_EXEC*LEI01_TRA_000001-04_18	Valid sequence and version. File with file errors.	FIL-XXX / ESX-XXX errors
SUBM*LEI23_EXEC*LEI01_TRA_000001-02_18	Valid sequence, invalid version.	ESX-115: The Version inside the file name is not valid: version number should be higher than 4.
SUBM*LEI23_EXEC*LEI01_TRA_000001-05_18	Valid sequence and version. File without any file error. File Processed.	CON-XXX error(s) or Accepted File

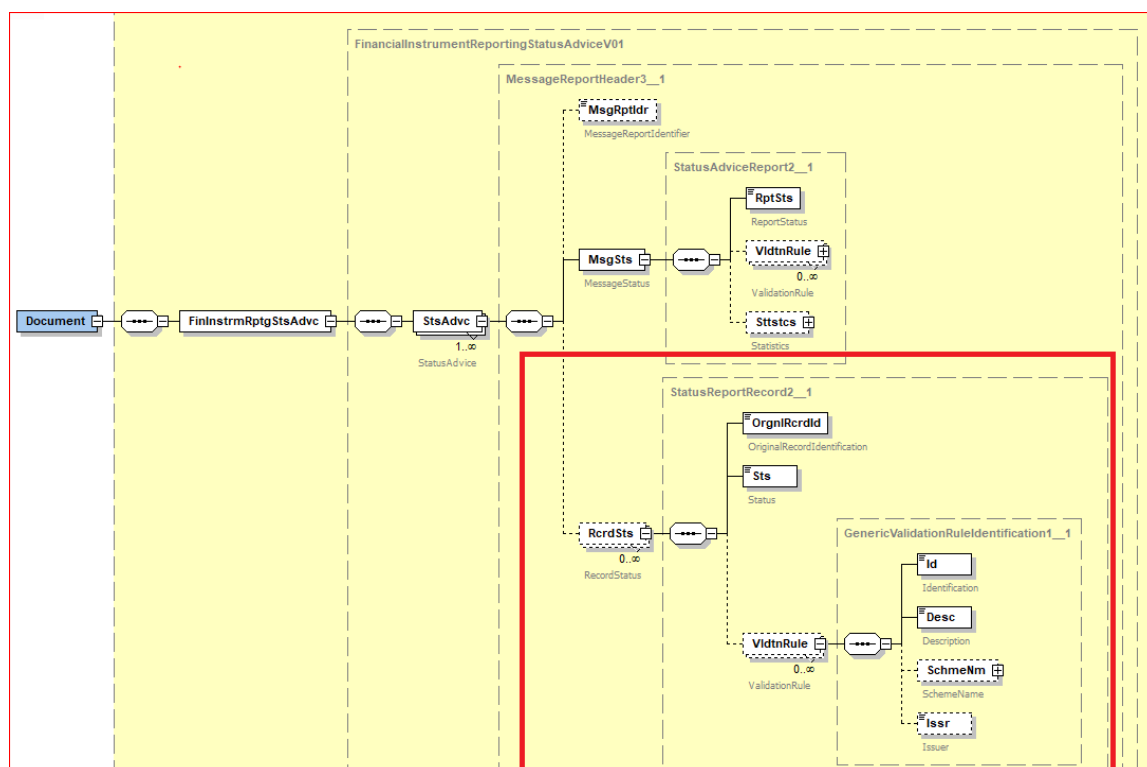
6.3 DESCRIPTION OF “TRANSACTION STATUS” FIELD

This annex explains the different Transaction Status as well as the modifications included in “FDB” feedback files in order to clarify every single transaction status. After the validation process, each transaction report will be flagged with one of these four different status:

- ❖ **ACPT - Accepted**, the transaction report has successfully passed all the validation rules defined by ESMA
- ❖ **RJCT – Rejected**, the transaction report has not passed one or more validation rules and therefore is incorrect and will not be uploaded into the system
- ❖ **PDNG – Pending**, the transaction report passes all validation rules except instrument validation on FIRDS. These reports will not remain pending more than seven days.
- ❖ **RCVD – Received**, the transaction report has been received, but cannot be validated since ESMA’s FIRDS database is not available for the trading date. This will usually happen when transactions are sent the same date of trading, and then these transactions will be validated by the system in the following day.

Transaction reports with status ACPT, PDNG or RCVD can be cancelled. Every transaction report will reach a final status, which will be either ACPT or RJCT.

This picture below shows the part of the XML schema which includes the Transaction Status information for every transaction report:



In order to clarify the tracking of all transaction reports from the point of view of the submitting entity, SCORE/CNMV system has been updated and will include some detailed information inside every “FDB” feedback file.

Any “FDB” feedback file, on its StsAdvc/RcrdSts XML element will include details not only on Rejected or Pending transactions but also on Received transactions, therefore the submitting entity will be able both to distinguish and identify accepted and received transactions. Please note that accepted transactions will not be detailed.

```

<StsAdvc>
  <MsgRptldr>*****_TRA_00001-00</MsgRptldr>
  <MsgSts>
    <RptSts>PART</RptSts>
    <Sttstcs>
      <TtlNbOfRcrds>13</TtlNbOfRcrds>
      <NbOfRcrdsPerSts>
        <DtldNbOfTxs>10</DtldNbOfTxs>
        <DtldSts>ACPT</DtldSts>
      </NbOfRcrdsPerSts>
      <NbOfRcrdsPerSts>
        <DtldNbOfTxs>1</DtldNbOfTxs>
        <DtldSts>PDNG</DtldSts>
      </NbOfRcrdsPerSts>
      <NbOfRcrdsPerSts>
        <DtldNbOfTxs>1</DtldNbOfTxs>
        <DtldSts>RJCT</DtldSts>
      </NbOfRcrdsPerSts>
      <NbOfRcrdsPerSts>
        <DtldNbOfTxs>1</DtldNbOfTxs>
        <DtldSts>RCVD</DtldSts>
      </NbOfRcrdsPerSts>
    </Sttstcs>
  </MsgSts>
  <RcrdSts>
    <OrgnlRcrdId>LEI0000000000000000TRANSACTION12</OrgnlRcrdId>
    <Sts>RJCT</Sts>
    <VldtnRule>
      <Id>CON-XXX</Id>
      <Desc>ERROR DESCRIPTION</Desc>
    </VldtnRule>
  </RcrdSts>
  <RcrdSts>
    <OrgnlRcrdId>LEI0000000000000000TRANSACTION15</OrgnlRcrdId>
    <Sts>PDNG</Sts>
    <VldtnRule>
      <Id>CON-411</Id>
      <Desc>Pending instrument ESXXXXXXXXXX validation</Desc>
    </VldtnRule>
  </RcrdSts>
  <RcrdSts>
    <OrgnlRcrdId>LEI0000000000000000TRANSACTION13</OrgnlRcrdId>
    <Sts>RCVD</Sts>
  </RcrdSts>
</StsAdvc>

```