INSTRUCTIONS FOR THE *SDIFTP* SERVICE

VERSION 4.1.1

INDEX

DOCUMENT STATUS

Revision	Date	Notes
1.3	13 december 2016	Updating alignment file for new *Invoice Data* file
2.0	3 april 2017	Updating alignment file for new *VAT settlement* file
3.0	1 june 2018	Updating resulting from “Provvedimento Agenzia Entrate”, 30 april 2018, and size limitation of the file contained in FTP support
4.0	1 july 2018	Transition from the FTP protocol to the SFTP protocol
4.1	25 february 2019	Updating of the verifications foreseen during the interoperability test phase and modification of cryptography and signature for EO type supports
4.1.1	27 march 2019	A rejecting file (type ER) for failure of signature and/or decryption checks has been introduced. The outcome file (EO) is no longer signed or encrypted and it’s renamed at the end of transmission (if it ends with success). The description of daily alignment reports about FI-EO and FO supports has been introduced. The section about rules of supports withdrawal has been integrated (par. 3.1.2)

List of main changes from the previous version
Changed paragraphs 5.1.2, 5.2.2. Added paragraphs 3.2.3, 5.5 Changed enumeration of paragraphs 6.1 (modified in 5.3), 6.2 (modified in 5.4), 7 (modified in 6) and 8 (modified in 7)

INTRODUCTION

This document describes the technical specifications relative to the interaction with the Electronic Invoicing Exchange System through SFTP protocol for the bulk exchange of documents, optimising volumes and minimising connections between remote systems.

The use of this method requires a structure to support the computerised activities, the capacity to manage computerised systems and a data processing centre featuring continuity and the availability of personnel to man it.

Due to these characteristics, the method is suitable for systems with intermediary companies which act as concentration and distribution nodes.

1. DEFINITIONS

For the purposes of this document, the following terms are used with the meanings given below:

- *ES*: the Exchange System, i.e. the structure set up by the Ministry of Economy and Finance by which the electronic invoices are transmitted to the Public Administration (Art.1, section 211, of Italian law n° 244 of 24 December 2007) and to subjects other than Public Administration;

- *Node*: the remote system of the subject which transmits and/or receives the invoices;

- *Addressee*: the invoice addressees;

- *Flow:* all the information exchanged during a transmission session between the ES and the Node;

- *Support:* the file in compressed format, containing the files which represent the electronic invoices or the notifications;

- *Outcome:* the result of the transmission and the alignment of every single support received by SdI, which is represented by the "*outcome file";*

- *Operational Support:* the technical-operational assistance service provided by the ES and the Node to deal with errors and malfunctions that may occur during the transfer process.

2. TRANSMISSION REQUISITES

Interaction between the ES and the Node involves:

- the receipt and transmission of the invoices;
- the receipt and transmission of the notification and receipt messages;
- the transmission of *Invoice Data* files;
- the transmission of *VAT settlement* file;
- diagnostics of the flows relative to the preceding point to check the outcome of the transfer in input to SdI.

2.1 CONNECTION METHODS

The connection between the ES and the Node is of the *“Secure File Transfer Protocol”* type on the public network (Internet and SPC Infranet).

The client-server dialogue takes place on the ES client's initiative (SFTP client) which manages the flows by direct access to the Node SFTP server and carrying out “get” and “put” actions.

For this purpose, the Node communicates to the ES:

- IP address and ports for connection to the SFTP server;
- credentials (user ID and password) for the connection.

The flows are always identified from the ES viewpoint, therefore distinguishing:

- outgoing flows →from the ES to the Node
- incoming flows →from the Node to the ES

In both cases, the flows include invoices and messages.

2.2 CONNECTION WITH THE SERVICE DURING DISASTER RECOVERY

Thanks to the Disaster Recovery services, continuity of operations falls within the offer that the Financial Administration has requested from Sogei for the Electronic Invoicing project. Subsequent to disastrous events, grave accidents or emergency situations which could affect operations at the main site in Rome, the complete functioning of business-critical systems is guaranteed, in the shortest possible time and with minimum data loss, by implementing a plan of technical, logistic and organisational measures to deliver service continuity, thanks to the resources available at the alternative secondary site.

At the time the *SDIFTP Service* is registered, in addition to the IPs for the primary site, those for connection to the Disaster Recovery secondary site will also be provided.

2.3 CONNECTION CALENDAR

The exchange of flows takes place on the basis of an agreed connection timetable; technical time is included to allow for the processing of the transmission on the part of the ES, during which the Node must not interfere with the flows, whether incoming or outgoing.

To optimise the data exchange phases, at least several connection time windows are contemplated for every application day, set every 15 minutes. The technical time for processing is less than or equal to one hour; longer time windows can be agreed for each Node.

2.4 INTEROPERABILITY TEST

To validate the registration of a given channel to the SDIFTP Service, it is necessary to carry out an interoperability test between the Node and the Exchange System.

The interoperability test has two purposes:

- to test the communication between the systems for SFTP file exchanges;
- to test the actual flow, through the production of test supports and outcome files, before it is used in a production situation.

The test flows have a special separate nomenclature and exchange directory.

The interoperability test is begun starting from the delivery of the signature and encryption certificates to the Entity. The Entity must, within 15 days, give confirmation that the SFTP environment has been set up, communicating the allocation of test and production files, as well as providing the user names and passwords necessary for the exchange of data. Initially a connectivity test is carried out, at the same time as encryption/decryption, through the transfer of a test file. If this test is successful, then tests regarding the content of the files transmitted are begun. These tests, which envisage a shared calendar, have a maximum duration of 15 days and are intended to:

- verify proper reception of an incoming support
- verify proper preparation of an incoming support
- verify proper transmission of an outgoing outcome file
- verify proper transmission of an outgoing support.

In addition will be provided:

- loading tests related to the data transfer rate for supports of maximum size (150 megabytes)
- contemporary tests of taking charge of the supports by the Node.

To carry out the transmission of test flows after having completed the interoperability test stage, or rather after the passage to production by the Entity, it is appropriate to make preventive contact with the technical reference of the Exchange System.

3. INFORMATION STRUCTURE

The flows contemplate the exchange of *supports,* physically constituted of archive-files in ZIP format, and of *outcome files* in xml format, which must be signed electronically and encrypted to guarantee the intact nature and confidentiality of the files during the transmission.

3.1 SUPPORTS

The term "support" refers to the file in compressed format (zip) which is the container for the transfer, in which the invoice files, message files, *Invoice Data* files and *VAT settlement* files are found.

3.1.1 AGGREGATION CRITERIA

The files must be inserted into the supports according to the following aggregation rules:

- every incoming support to SdI can contain documents addressed to different subjects;
- every outcoming support from SdI can contain documents sent from different subjects;
- every support can contain the types of files: invoice files, *Invoice Data* files, *VAT settlement* files and message files.

3.1.2 NUMBER OF SUPPORTS PREPARED FOR EVERY CONNECTION

The number of supports prepared for each connection depends on the total size of the data to be exchanged.

The rules to be followed are the following:

- one document cannot be distributed over several supports;
- the maximum number of documents contained in a support is fixed at about 20,000; this value is indicative, however, since this threshold can be exceeded slightly, about 1% more falling within the tolerance level;
- a support cannot exceed the maximum limit of 150 Megabytes; the maximum size of each file contained in SFTP support cannot exceed 5 Megabytes;

- for every access to the server (usually every 10 minutes), the presence on the Node of only one support with size smaller than 15 Megabytes is allowed; any additional support must be between 15 and 150 Megabytes in size;

- the maximum number of supports prepared for every connection is 899.

It is maintained that respect for these rules is sufficient to guarantee problem-free processing of the data, the fact that the maximum size of the files and the maximum number of files may be adjusted if there is a strong increase in the amount of information exchanged daily always holding firm.

3.1.3 ACTIVITIES PRELIMINARY TO THE EXCHANGE OF THE SUPPORTS

Before being made available, the supports are further processed in order to optimise the transmission phases and to respect the security requisites laid down by the ES.

For this purpose, the supports are subjected to the following processes, in the order below:

- the electronic signature is applied;

- they are encrypted.

The supports are placed in envelopes conforming to the standard PKCS#7 v.1.5, in "signedData" and "envelopedData" mode.

3.1.4 NAMING OF THE SUPPORTS

The name of every support is composed of five parts, separated by the point ".":

- a fixed part identifying the type of support, according to the following code system:

Type of document	**Value**
Incoming file to the ES	FI
Outgoing file from the ES	FO

- a fixed part identifying the Node and corresponding to the post code of the subject responsible for the said Node;

- support preparation date, expressed in the Julian yyyyddd format (e.g. 2011001);
- support preparation time, expressed in the hhmm format (e.g. 1700);
- three figures for the sequential number which, going from 001 up to 899, increases if several supports are prepared with the same time indication. Sequential numbers from 900 up to 999 are used exclusively for test flows.

For example, if 4 supports (2 FI, 2 FO) are prepared on 1 January 2013 at 17:00, they will have the following names:

- FI.01234567890.2013001.1700.001.zip
- FI.01234567890.2013001.1700.002.zip
- FO.01234567890.2013001.1700.001.zip
- FO.01234567890.2013001.1700.002.zip

3.1.5 COMPOSITION OF THE SUPPORTS

Every support prepared contains several documents and, in addition, a file containing the *alignment* data necessary to carry out a further check on correct transmission. The said file contains the information relative to:

- node identification;
- support creation data;
- support name;
- number of documents contained in the support, grouped according to type (excluding the alignment file).

The name of the alignment file corresponds to that of the support, and has the extension .xml.

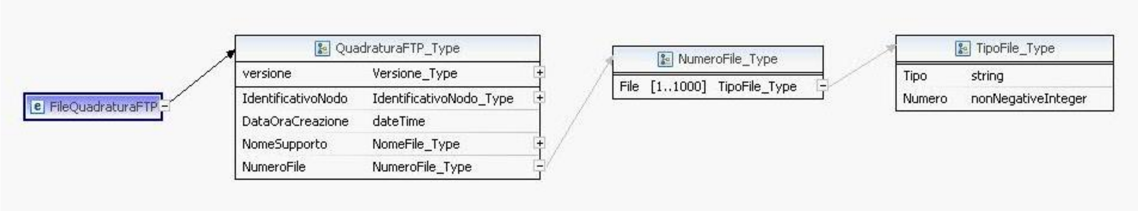
For example, the support named:

FI.01234567890.2012001.1700.001.zip

will contain an alignment file named:

FI.01234567890.2012001.1700.001.xml.

The alignment file is in .xml format, structured according to the following system:



FileQuadraturaFTP
QuadraturaFTP_Type
versione Versione_Type
IdentificativoNodo IdentificativoNodo_Type
DataOraCreazione dateTime
NomeSupporto NomeFile_Type
NumeroFile NumeroFile_Type
NumeroFile_Type
File [1..1000] TipoFile_Type
TipoFile_Type
Tipo string
Numero nonNegativeInteger

The types referred to are defined in the file **FtpTypes_v2.0.xsd.** The allowed values for `NumeroFile/File/Tipo` element are:

Value	Description	Scope of
AT	Proof of invoice transmission with impossibility of delivery (for Invoice PA only)	FO
DF	Invoice Data file	FI
DT	Deadline passed notice (for Invoice PA only)	FO
EC	Client outcome notice (for Invoice PA only)	FI
ED	Invoice Data outcome	FO
EL	VAT settlement outcome	FO
FA	Electronic Invoice PA or B2B	FI, FO
LI	VAT settlement file	FI
MC	Failed delivery notice (for Invoice PA) and Impossibility delivery receipt (for Invoice B2B), each with its own schema	FO
MT	Metadata file, with different schema for Invoice PA and Invoice B2B	FO
NE	Outcome notice (for Invoice PA only)	FO
NS	Rejection notice (for Invoice PA) and Rejection receipt (for Invoice B2B), each with its own schema	FO
RC	Delivery receipt, with different schema for Invoice PA and Invoice B2B	FO
SE	Client outcome rejection notice (for Invoice PA only)	FO
DFZ	Invoice Data file compressed in a zip file	FI
LIZ	VAT settlement file compressed in a zip file	FI

FL	Invoice data file and VAT settlement file compressed in a zip file	FI

In the alignment file, the same value can not be present more than one time per `NumeroFile/File/Tipo` element.

3.1.6 CHECK OF THE SUPPORTS

Every support received by SdI (types FI) must be checked before a corresponding outcome file is generated. The outcome is the result of the following operations:

- decryption and verification of the electronic signature;
- decompression of the support;
- xml validation of the alignment file in respect of the format (attachment);
- check that the *DataOraCreazione* field in the alignment file does not give a value later than the actual date/time of receipt;
- check that the number of the files declared in the alignment file, grouped according to type, corresponds to the actual content of the support; the System admits in the supports only files with .xml and .p7m extensions.

If all the operations and the checks have a positive result, a positive outcome file is generated; otherwise, an outcome file is produced which shows the presence of errors. More details on the structure and content of the outcome file are given in the next paragraph.

3.2 OUTCOME FILE OR REJECTING FILE

For every incoming support, downstream of the opportune checks on the data, the Exchange System produces an outcome file, confirming receipt or to report errors, which will be exchanged in the manner described below for the exchange of the support (paragraph 4).

3.2.1 NAME OF THE OUTCOME FILE

The outcome files correspond one-to-one with the supports received by SdI; their name is identical to that of the support except for the first two characters, which are "EO", in place of the "FI".

For example, the outcome files corresponding to the supports “FI” listed in paragraph 3.1.4 will have the following names:

- EO.01234567890.2012001.1700.001.xml
- EO.01234567890.2012001.1700.002.xml

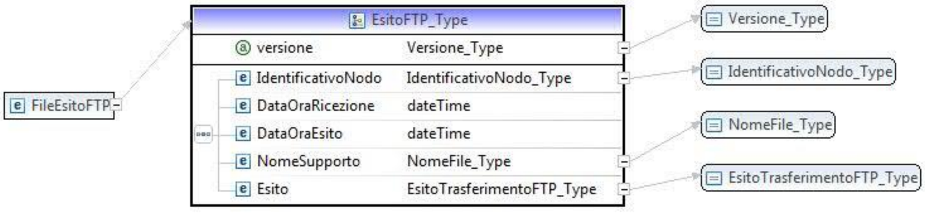
3.2.2 COMPOSITION OF THE OUTCOME FILE

The outcome file is a file in .xml format, and containing the information relative to:

- node identification;
- date and time of the creation of the outcome file;
- date and time of the receipt of the support:
- support name;
- outcome of the checks, expressed in terms of the successful receipt of the support or the report of errors, according to the following code:

Value	**Description**
ET01	Successful receipt of the support
ET02	Support received with error

The outcome file is in *.xml* format, structured according to the following system:



The types referred to are defined in the file **FtpTypes_v2.0.xsd** which can be downloaded from the section Exchange System Documentation of the site www.fatturapa.gov.it .

3.2.3 NAME OF THE REJECTING FILE

The rejecting files correspond one-to-one with the supports received by SdI that have not passed the security checks (signature and encryption); their name is identical to that of the supports except for the first two characters, which are "ER", in place of the "FI".

For example, the rejecting files corresponding to the supports “FI” listed in paragraph 3.1.4 will have the following names:

- ER.01234567890.2012001.1700.001.xml
- ER.01234567890.2012001.1700.002.xml

3.2.4 COMPOSITION OF THE REJECTING FILE

The rejecting file is a file in .csv format, and containing the information relative to:

- name of FI support rejected;
- outcome of the security checks (signature and encryption), with error reports according to the following code:

Value	**Description**
1	Encryption error
2	Signature error

4. FILE-EXCHANGE DIRECTORIES

4.1 REAL FLOW

The Node SFTP server must provide for accessibility through the credential provided to the ES of the following directories and related authorizations:

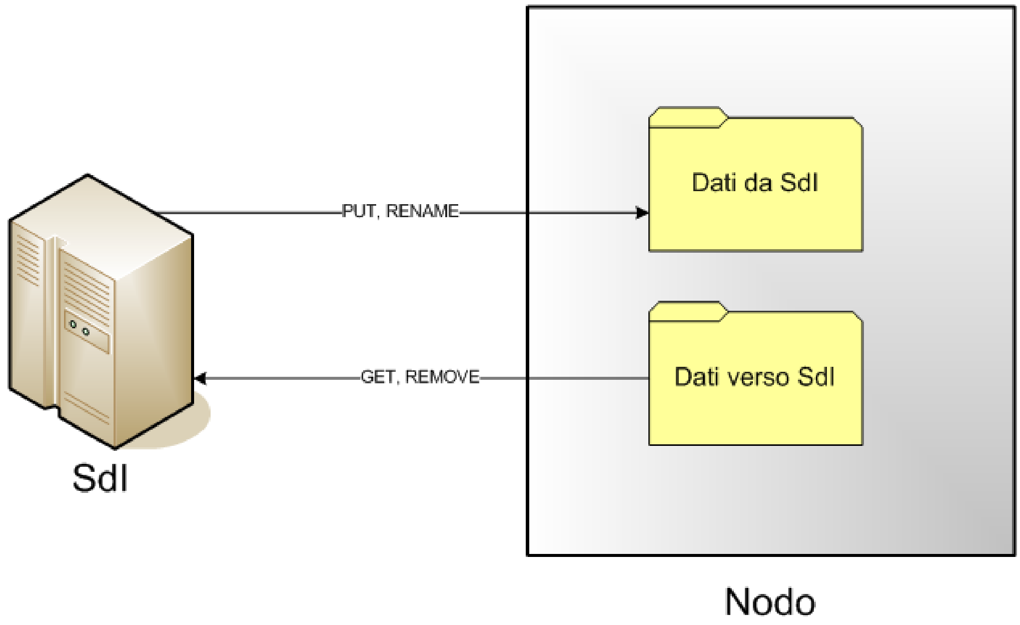
- **DatiVersoSdI** (with *get* and *delete* authorizations): the directory where the Node places the supports ready to be collected (type FI).

  The Node must guarantee that the **DatiVersoSdI** directory contains only valid supports, with .zip extension and not yet being processed; to obtain this latter condition, it can carry out processing on a supplementary directory and then move the file to the **DatiVersoSdI** directory only when processing is finished, or it can process the file with a different name than that contemplated by the naming rules and then rename it again when processing is finished (failure to respect this rule will cause a risk of the partial processing of the file in question). After the successful transfer of the files, the ES eliminates the files relative to the supports from the **DatiVersoSdI** directory.

- **DatiVersoSdI** (with *put* and *rename* authorizations): the directory which contains the supports produced by the ES (type FO) and the outcome files relative to the supports of the incoming flows of the previous connection (type EO).

  To prevent the Node from acquiring files which are invalid since they are still being processed, after the transmission is terminated and the successful outcome is verified, the Node renames the files transferred to the **DatiDaSdI** directory adding the suffix .p7m.enc.

The following figure illustrates the communication protocol between the ES and the Node, together with the logic activities carried out by the counterparts:



The Node may place other files in the exchange directory, if they are functional to the processing and process control phases, providing they have a name in a different format from that agreed for the supply supports and the outcome files.

4.2 TEST FLOW

In regards to the test flows, the exchange of files occurs through the use of two directories separate from real flows, accessible by the ES with the following authorizations:

- **DatiVersoSdITest** (with *get*, *delete* and *overwriting* authorizations): the directory where the Node places the test supports ready to be collected (type FI).
- **DatiVersoSdITest** (with *put* and *rename* authorizations): the directory which contains the test supports produced by the ES (type FO) and the outcome files relative to the supports of the incoming flows of the previous connection (type EO).

The test flows, in addition to using the envisaged nomenclature, must be agreed upon with the ES Operational Support service.

5. FLOW EXAMPLE

5.1 REAL FLOW

5.1.1 FILES FROM THE ES

If at 10:30 on 10 January 2012 the ES produces a support to be sent to the Node 12345678901, the flow contemplate following steps:

– according to the applicable rules, the name will be **FO.12345678901.2012010.1030.001.zip**;

– the ES applies the electronic signature to the file produced and encrypts it;

– the ES transmits the file **FO.12345678901.2012010.1030.001.zip** in the directory **DatidaSdI** of the Node **12345678901;** at the end of the transmission (carried out successfully), it renames the file as **FO.12345678901.2012010.1030.001.zip.p7m.enc.**

If the support contains invoice file, date-time of the end of successfull transmission is mentioned in Delivery Receipe transmitted by ES.

5.1.2 FILES TO THE ES

If at 12:30 on 15 January 2012 the Node 12345678901 produces a support to be sent to the ES, the flow contemplate following steps:

– according to the applicable rules, the name will be **FI.12345678901.2012015.1230.001.zip**;

– the Node applies the electronic signature to the file produced and encrypts it

– the Node moves (or renames) the file **FI.12345678901.2012015.1230.001.zip** in the **DatiVersoSdI** directory

– the ES takes the support **FI.12345678901.2012015.1230.001.zip** from the **DatiVersoSdI** directory and then, at the end of the transfer, removes it.

– the ES carries out the security checks (signature and encryption) on taken file. In case of error, ES produces and transmits the rejecting file **ER.12345678901.2012015.1230.001** neither signed nor encrypted; at the end of transmission of rejecting file (carried out with success) ES renames the file in **ER.12345678901.2012015.1230.001.run.** The file will contain the name of rejecting support and the security phase not correctly ended

- the ES carries out the alignment checks and produces the outcome file **EO.12345678901.2012015.1230.001.xml.** Starting from 8 april 2019 the outcome file is no longer signed or encrypted and at the end of transmission (carried out with success) ES renames the file in **EO.12345678901.2012015.1230.001.xml.run** instead of EO.12345678901.2012015.1230.001.xml.p7m.enc.

5.2 TEST FLOW

5.2.1 FILES FROM THE ES

If at 10:30 on 10 January 2012 the ES produces a support to be sent to the Node 12345678901, the flow contemplate following steps:

- according to the applicable rules, the name will be **FO.12345678901.2012010.1030.900.zip**;
- the ES applies the electronic signature to the file produced and encrypts it;
- the ES transmits the file **FO.12345678901.2012010.1030.900.zip** in the directory **DatidaSdITest** of the Node **12345678901;** at the end of the transmission (carried out successfully), it renames the file as **FO.12345678901.2012010.1030.900.zip.p7m.enc.**

5.2.2 FILES TO THE ES

If at 12:30 on 15 January 2012 the Node 12345678901 produces a support to be sent to the ES, the flow contemplate following steps:

- according to the applicable rules, the name will be **FI.12345678901.2012015.1230.900.zip**;
- the Node applies the electronic signature to the file produced and encrypts it
- the Node moves (or renames) the file **FI.12345678901.2012015.1230.900.zip** in the **DatiVersoSdITest** directory
- the ES takes the support **FI.12345678901.2012015.1230.900.zip** from the **DatiVersoSdITest** directory and then, at the end of the transfer, removes it.
- the ES carries out the security checks (signature and encryption) on taken file. In case of error, ES produces and transmits the rejecting file **ER.12345678901.2012015.1230.900** neither signed nor encrypted; at the end of transmission of rejecting file (carried out with success) ES renames the file in

ER.12345678901.2012015.1230.900.run. The file will contain the name of rejecting support and the security phase not correctly ended

- the ES carries out the alignment checks and produces the outcome file **EO.12345678901.2012015.1230.900.xml.** Starting from 8 april 2019 the outcome file is no longer signed or encrypted and at the end of transmission (carried out with success) ES renames the file in **EO.12345678901.2012015.1230.900.xml.run** instead of EO.12345678901.2012015.1230.900.xml.p7m.enc.

5.3 ALIGNMENT ERRORS

If the ES finds misalignment between the data in the alignment file and the content of the support and/or the name of the support itself, to prevent possible error situations in successive processing, the support is considered "suspended" during investigations and while the inconsistencies found are communicated by means of the outcome file. Then the user is contacted by the mail.

The manner and timing of possible data recovery must be agreed on each occasion by direct contact between the operating support made available by the ES and by the Node.

5.4 MALFUNCTIONING

Technical-type errors due to failure to respect the communication rules between the ES and the Node (e.g. encryption error, connection problems, server malfunctions) are considered as cases of malfunctioning. The technical contact of the ES must be able to contact the corresponding Node contact, and vice versa, in order to resolve the problem.

In particular the following errors are reported by e-mail:

- no connection to the sFTP server of Node, or changes to the consolidated configuration in the test phase;
- errors found in the nomenclature of the files made available by the Node such as:
    - production of non-compliant files with the registered channel;
    - invalid date;
    - nomenclature that does not comply with the environment (Test-Prod);
    - invalid final extension;
    - incorrect file nomenclature length;
    - tax code and Node non-congruent;

- duplication of files made available by the Node;
- files larger than 150Mbytes or empty.

5.5 REPORT

ES produces two daily alignment reports of the transmissions carried out. One for transmission related to EO o ER files and related FI files and one for FO files. These are two “csv” files that will be neither signed nor encrypted and will be named as follows:

1. ST.*VAT number*.FO.date.time

   Containing the list of FO files successfully transmitted to the Node and, for each, the end-date of transmission;

2. ST.*VAT number*.EO.date.time

   Containing the list of FI files successfully retrieved from the Node and, for each of them: the withdrawal date, the corresponding EO or ER file successfully transmitted and the end-date of transmission.

Starting from 8 april 2019, the 2 reports will no longer be sent by e-mail but exclusively via sFTP, similary to the other flows made available by the ES.

6. SECURITY SPECIFICATIONS AND ENCRYPTING

The data transmitted via SFTP must be encrypted and digitally signed in order to ensure its origin and confidentiality. The data will first be signed, with the PKCS#7 format, and then encrypted. The formats used to envelope the signed and encrypted data will comply with the PKCS#7 v 1.5 standard, in the "signedData" and "envelopedData" modes (mixed S/MIME standard, with signature and encrypting envelope compliant with PKCS#7 v 1.5 standard, with encoding in DER format).

In the encryption phase, the data are encrypted using a symmetric key algorithm, randomly generated from time to time. The key used is then inserted into the envelope, encrypted with the public RSA key of the addressee.

The asymmetric encryption algorithm, based on the private-public key pair, is RSA; the length of the keys ranges from 1024 to 4096.

The symmetric encryption algorithms supported are: DES-EDE-3, AES-128, AES-192, AES-256.

The hash algorithm supported are: MD5, SHA-1, SHA-256, SHA-384, SHA-512.

Both the Node and the ES must therefore have a pair of the encrypting keys and a separate pair of the signature keys.

The Node autonomously generates the keys and sends the certificate requests; ES issues the certificates that are sent to the Node; through safe channel, the encrypting certificate and the Certification Authority certificate are sent to the Node.

The generation of the keys is carried out by the ES; together with the encrypting certificate and that of the Certification Authority, two files in PKCS#12 format containing respectively the pair of the keys and the signature certificate and the pair of the keys and the encrypting certificate are communicated to the Node on safe channels. The PKCS#12 files are protected by passwords which are communicated to the Node manager.

For the development of procedures which use encrypting, decrypting, signing and verification operations, the Node may use sundry software tools, because of use of standard formats for the distribution of keys and certificates and for the representation of signed data and encrypted data.

From 4 april 2019, the outcome files (type EO) produced by the ES will no longer be encrypted or signed.

Starting from 8 april 2019:

- the outcome files (EO type) produced by ES are no longer signed or encrypted and will have an **xml.run** extension instead of **xml.p7m.enc**;
- the rejecting files (ER type) produced by ES, neither signed nor encrypted, will have **.run** extension.

7. AVAILABILITY OF THE SERVICE

The transmission of the file flows is carried out according to the timing described in paragraph 2.3.

The Operational Support service of the ES is available from Monday to Friday, from 8.00 to 18.00, and the Node must guarantee availability of the Operational Support which covers the connection time windows.

For acceptance for processing and for resolving all the technical issues inherent to the service, the Node makes a technician available who can be contacted by the relative technicians of the ES from Monday to Friday, from 8.00 to 18.00.