ISTRUZIONI PER IL SERVIZIO *SDIFTP*

VERSIONE 4.0

INDICE

STATO DEL DOCUMENTO

Revisione	Data	Note
1.3	13 dicembre 2016	Aggiornamento del file di quadratura per adeguamento alla nuova tipologia di file “Dati fattura” ideata per la trasmissione delle fatture emesse e ricevute”
2.0	3 aprile 2017	Aggiornamento del file di quadratura per la nuova tipologia di file “Liquidazioni IVA”
3.0	1 giugno 2018	Aggiornamento delle tipologie di notifiche attese in seguito a emanazione Provvedimento dell’Agenzia delle Entrate del 30 Aprile 2018 e limitazione dimensionale file contenuti all’interno dei supporti FTP
4.0	1 luglio 2018	Passaggio dal protocollo FTP al protocollo SFTP

Paragrafi interessati dai cambiamenti rispetto alla versione precedente
Modificati i paragrafi 1, 2.1, 2.4, 4.1, 4.2, 7

INTRODUZIONE

Il presente documento descrive le specifiche tecniche relative alla interazione con il Sistema di Interscambio per la Fatturazione Elettronica tramite protocollo SFTP per lo scambio “massivo” di documenti ottimizzando i volumi e riducendo al minimo le connessioni tra sistemi remoti.

L’utilizzo di tale modalità presuppone una struttura a supporto delle attività informatiche, la capacità di gestire sistemi informativi ed un centro di elaborazione dati con caratteristiche di continuità e disponibilità di personale di presidio.

Per le caratteristiche espresse la modalità si adatta a realtà di soggetti intermediari che si configurano come nodi di concentrazione e di smistamento.

1. DEFINIZIONI

Ai fini del presente documento si intende:

- per *SdI*, il Sistema di Interscambio, vale a dire la struttura istituita dal Ministero dell'Economia e delle Finanze attraverso la quale avviene la trasmissione delle fatture elettroniche verso la Pubblica Amministrazione (art.1, comma 211, legge 24 dicembre 2007 n. 244) e soggetti diversi dalla Pubblica Amministrazione;

- per *Nodo*, il sistema remoto del soggetto che trasmette e/o riceve le fatture;

- per *Destinatario*, i soggetti destinatari di fattura;

- per *Flusso*, l'insieme di informazioni scambiate durante una sessione di collegamento tra il SdI ed il Nodo;

- per *Supporto*, il file in formato compresso contenente a sua volta i file che rappresentano le fatture elettroniche o le notifiche;

- per *Esito*, il risultato della trasmissione e della quadratura di ogni singolo supporto ricevuto dal SdI; è rappresentato dal "*file di esito";*

- per *Supporto Operativo,* il servizio di assistenza tecnico-operativa fornito dal SdI e dal Nodo per affrontare le situazioni di errori e malfunzionamenti che si dovessero verificare nel processo di trasferimento.

2. REQUISITI DELLA TRASMISSIONE

L'interazione tra il SdI ed il Nodo prevede:

- la ricezione e la trasmissione delle fatture;
- la ricezione e la trasmissione dei messaggi di notifica e ricevute;
- la trasmissione di file Dati Fattura;
- la trasmissione di file Liquidazioni IVA;
- la diagnostica dei flussi di cui ai punti precedenti per verificare l'esito del trasferimento in ingresso al SdI.

2.1 MODALITÀ DI CONNESSIONE

Il collegamento tra SdI e il Nodo è di tipo *"Secure File Transfer Protocol"* su dorsali pubbliche (Internet e SPC Infranet).

Il colloquio client-server avviene su iniziativa del client SdI (client SFTP) che gestisce i flussi accedendo direttamente al server SFTP del Nodo ed effettuando azioni di "get" e "put".

A questo scopo il Nodo rende noto al SdI:

- indirizzo IP e porte per la connessione al server SFTP;
- credenziali (utente e password) per la connessione.

I flussi sono sempre identificati dal punto di vista del SdI, quindi si distinguono:

- flussi in uscita → dal SdI al Nodo;
- flussi in ingresso → dal Nodo al SdI;

In entrambi i casi, i flussi comprendono fatture e messaggi.

2.2 CONNESSIONE CON IL SERVIZIO IN DISASTER RECOVERY

Grazie ai servizi di Disaster Recovery la continuità operativa rientra nell'offerta che l'Amministrazione Finanziaria ha richiesto a Sogei per il progetto della Fatturazione

Elettronica: a seguito di eventi disastrosi, incidenti gravi o situazioni di emergenza che possono pregiudicare l'operatività del sito primario di Roma, la completa funzionalità dei processi business critical può essere assicurata, nel minor tempo possibile e con la minima perdita di dati, attuando un piano di misure tecniche, logistiche e organizzative, in grado di garantire la continuità dei servizi, grazie alle risorse disponibili nel sito secondario alternativo.

Al momento dell'accreditamento al *Servizio SDIFTP* verranno forniti, oltre agli IP del sito primario, anche quelli per la connessione al sito secondario di Disaster Recovery.

2.3 CALENDARIO DI CONNESSIONE

Lo scambio di flussi avviene sulla base di orari di connessione concordati; è previsto un tempo tecnico, per consentire l'elaborazione della trasmissione da parte del SdI, durante il quale il nodo non deve intervenire sui flussi, siano essi in ingresso o in uscita.

Al fine di ottimizzare le fasi di scambio dei dati, si prevedono diverse finestre temporali di connessione per giornata applicativa, fissate ogni 15 minuti; il tempo tecnico di elaborazione è minore o uguale a un'ora; finestre temporali più ampie possono essere concordate per ogni singolo Nodo.

2.4 TEST D'INTEROPERABILITÀ

Per validare l'accreditamento del proprio canale al Servizio SDIFTP è necessario effettuare dei test di interoperabilità tra il Nodo e il Sistema di Interscambio.

Il test di interoperabilità ha il duplice scopo:

- di testare il colloquio tra sistemi in un'ottica di scambio file via SFTP;
- di testare, attraverso la produzione di supporti e file di esito di prova, il flusso reale prima che esso venga effettuato in ambiente di produzione.

I flussi di test hanno una opportuna nomenclatura e directory di scambio separate.

Il test di interoperabilità viene avviato a partire dalla consegna dei certificati di firma e cifratura presso l'Ente. Quest'ultimo deve, entro 15 giorni, provvedere a fornire conferma della predisposizione dell'ambiente SFTP, comunicando l'allocazione delle cartelle di test e produzione, oltre alla fornitura di utenza e password necessarie allo scambio dati. Dapprima si effettuerà un test di connettività, contestualmente a quello di cifratura/decifratura, attraverso il trasferimento di un file di prova. Se questo test

risulterà positivo si darà inizio ai test relativi al contenuto dei file trasmessi. Tale test avrà una durata massima di 15 giorni e si propone di:

- verificare la corretta ricezione di un supporto in ingresso;
- verificare la corretta predisposizione del supporto in ingresso;
- verificare la corretta trasmissione di un file di esito in uscita;
- verificare la corretta trasmissione di un supporto in uscita.

Per effettuare la trasmissione di flussi di test, dopo aver terminato la fase di test di interoperabilità ovvero dopo il passaggio in produzione dell'Ente, è opportuno un preventivo contatto con il referente tecnico del Sistema di Interscambio.

3. STRUTTURA DELLE INFORMAZIONI

I flussi prevedono lo scambio di *supporti,* fisicamente costituiti da file-archivio in formato ZIP, e di *file esito* in formato xml, sottoposti a firma elettronica e cifratura a garanzia d'integrità e riservatezza durante la trasmissione.

3.1 SUPPORTI

Per "supporto" si intende il file in formato compresso (zip) che costituisce il contenitore oggetto del trasferimento al cui interno si trovano i file fattura, i file messaggio e file Dati Fattura.

3.1.1 CRITERI DI AGGREGAZIONE

I file devono essere inseriti nei supporti secondo le seguenti regole di aggregazione:

- ogni supporto in ingresso al SdI può contenere documenti destinati a soggetti differenti;
- ogni supporto in uscita dal SdI può contenere documenti provenienti da soggetti differenti;
- ogni supporto può contenere le tipologie di file: fattura, Dati Fattura e messaggio.

3.1.2 NUMERO DI SUPPORTI PREDISPOSTI IN CORRISPONDENZA AD OGNI CONNESSIONE

Il numero dei supporti predisposti in corrispondenza a ciascuna connessione è dipendente dalla dimensione totale dei dati da scambiare.

Le regole da rispettare sono le seguenti:

- un documento non può essere distribuito su più supporti;
- il numero massimo di documenti contenuti in un supporto è fissato a circa 20.000; tale valore è comunque indicativo in quanto un lieve superamento di tale soglia, nell'ordine dell' 1%, rientra nella tollerabilità;
- un supporto non può superare il limite massimo di 150 Megabyte. Al suo interno non sono ammessi files più grandi di 5Mb;
- il massimo numero di supporti predisposti in corrispondenza di ogni connessione è 899.

Si ritiene che il rispetto di tali regole sia sufficiente a garantire un'agevole elaborazione dei dati, fermo restando che il dimensionamento massimo dei file e il massimo numero di file può essere rivisto nel caso in cui si rilevi un forte trend di crescita delle informazioni giornaliere scambiate.

3.1.3 ATTIVITÀ PRELIMINARI ALLO SCAMBIO DEI SUPPORTI

Prima di essere messi a disposizione, i supporti sono ulteriormente elaborati al fine di ottimizzare le fasi di trasmissione e rispettare i requisiti di sicurezza espressi dal SdI.

A tale scopo i supporti in chiaro subiscono, nell'ordine, i seguenti processi:

- apposizione della firma elettronica;
- cifratura.

I supporti vengono inseriti in buste conformi allo standard PKCS#7 v.1.5, nelle modalità "signedData" ed "envelopedData".

3.1.4 NOMENCLATURA DEI SUPPORTI

Il nome di ogni supporto è costituito da cinque parti, separate dal carattere punto ".":

- parte fissa identificativa della tipologia di supporto secondo la seguente codifica:

Tipologia di documento	**Valore**
File in ingresso al SdI	FI
File in uscita dal SdI	FO

- parte fissa identificativa del Nodo e corrispondente al codice fiscale del soggetto responsabile del Nodo stesso;
- data di predisposizione del supporto espressa in formato giuliano aaaaggg (e.g. 2016365);
- orario di predisposizione del supporto espresso nel formato hhmm (e.g. 1700);
- tre cifre per il numero sequenziale che, partendo da 001 fino a 899, è incrementato qualora nell'ambito del medesimo orario vengano predisposti più

supporti. I numeri sequenziali da 900 a 999 sono utilizzati esclusivamente per i flussi di test.

A titolo esemplificativo, qualora il 01 gennaio 2013 vengano predisposti 4 supporti (2 FI, 2 FO), alle ore 17.00, gli stessi avranno i seguenti nomi:

- 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 COMPOSIZIONE DEI SUPPORTI

Ogni supporto predisposto contiene un insieme di documenti e, in aggiunta, un file contenente i dati *di quadratura* necessari ai fini di un ulteriore controllo sulla corretta trasmissione. Tale file contiene le informazioni relative a:

- identificativo nodo;
- data di creazione del supporto;
- nome del supporto;
- numero di documenti contenuti nel supporto raggruppati per tipologia (ad esclusione del file di quadratura).

La nomenclatura del file di quadratura corrisponde a quella del supporto ed assume l'estensione .xml.

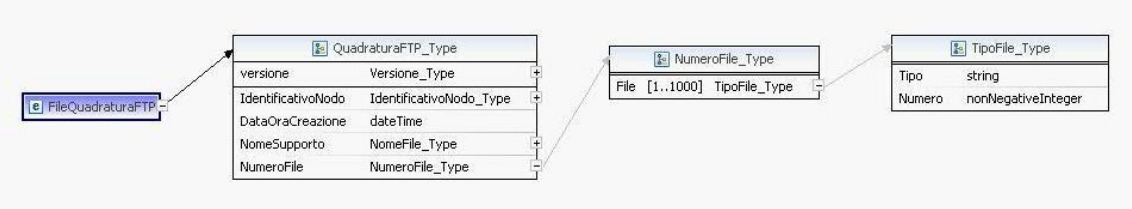
A titolo esemplificativo il supporto denominato:

FI.01234567890.2012001.1700.001.zip

conterrà un file di quadratura denominato:

FI.01234567890.2012001.1700.001.xml.

Il file di quadratura è un file in formato .xml, strutturato secondo lo schema seguente:



I tipi ai quali si fa riferimento sono definiti nel file **FtpTypes_v2.0.xsd**. I valori ammessi per l'elemento `NumeroFile/File/Tipo` sono:

Valore	Descrizione	Ambito
AT	Notifica di attestazione avvenuta trasmissione (riguarda le sole fatture destinate alle PA)	FO
DF	File dati fattura	FI
DT	Notifica di decorrenza termini (riguarda le sole fatture destinate alle PA)	FO
EC	Notifica di esito committente (riguarda le sole fatture destinate alle PA)	FI
ED	Esito Dati Fattura	FO
EL	Esito Liquidazioni IVA	FO
FA	Fattura elettronica PA o B2B	FI, FO
LI	File Liquidazione IVA	FI
MC	Notifica di mancata consegna (per le fatture destinate alle PA) e ricevuta di impossibilità di recapito (per le fatture B2B), ognuna con il proprio schema	FO
MT	File dei metadati invio file, con schema diverso fra fatture destinate alle PA e fatture B2B	FO
NE	Notifica esito cedente (riguarda le sole fatture destinate alle PA)	FO
NS	Notifica di scarto (per le fatture destinate alle PA) e ricevuta di scarto (per le fatture B2B), ognuna con il proprio schema	FO
RC	Notifica ricevuta consegna, con schema diverso fra fatture destinate alle PA e fatture B2B	FO
SE	Notifica scarto esito committente (riguarda le	FO

	sole fatture destinate alle PA)	
DFZ	File dati fattura compresso in formato zip	FI
LIZ	File Liquidazione IVA compresso in formato zip	FI
FL	File dati fattura e Liquidazione IVA compresso in formato zip	FI

Nel file di quadratura, lo stesso valore per l'elemento `NumeroFile/File/Tipo` non può essere presente più volte.

3.1.6 CONTROLLO DEI SUPPORTI

Ogni supporto ricevuto dal SdI (tipologia FI) deve essere controllato prima di generare un file di esito corrispondente. L'esito è dato dal risultato delle seguenti operazioni:

- decifratura e verifica della firma elettronica;
- decompressione del supporto;
- validazione xml del file di quadratura rispetto al formato (allegato);
- verifica che il campo *DataOraCreazione* presente nel file di quadratura non sia successivo all'effettiva data/ora di ricezione;
- verifica che il numero dei file dichiarati nel file di quadratura e raggruppati per tipologia corrisponda al reale contenuto del supporto; il Sistema ammette nei supporti i soli file con estensione .xml e .p7m.

Se tutte le operazioni e le verifiche vanno a buon fine viene generato un file di esito positivo, in caso contrario viene prodotto un file di esito che evidenzia la presenza di errori. Per maggiori dettagli sulla struttura e il contenuto del file di esito si rimanda al successivo paragrafo.

3.2 FILE ESITO

Per ogni supporto ricevuto, a valle delle opportune verifiche sui dati, il SdI produce un file di esito, a conferma della ricezione ovvero per la segnalazione di errori, che sarà scambiato con le medesime modalità seguite per lo scambio dei supporti (paragrafo 4).

3.2.1 NOMENCLATURA DEI FILE DI ESITO

I file di esito hanno una corrispondenza uno ad uno con i supporti ricevuti dal SdI; la loro nomenclatura è identica a quella dei supporti, con la sostituzione dei primi due caratteri (“FI”) con i caratteri “EO”.

A titolo esemplificativo i file di esito corrispondenti ai supporti di tipo “FI” elencati al paragrafo 3.1.4 assumono i seguenti nomi:

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

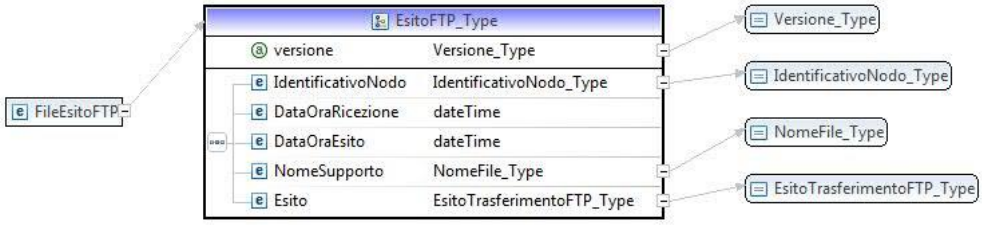
3.2.2 COMPOSIZIONE DEI FILE DI ESITO

Il file di esito è un file in formato .xml contenente le informazioni relative a:

- identificativo nodo;
- data e ora di creazione del file di esito;
- data e ora di ricezione del supporto;
- nome del supporto;
- esito delle verifiche, espresso in termini di ricezione del supporto avvenuta con successo ovvero con la segnalazione di errori secondo la seguente codifica:

Valore	Descrizione
ET01	Ricezione del supporto avvenuta con successo
ET02	Ricezione del supporto avvenuta con errore

Il file di esito è un file in formato *.xml* strutturato secondo lo schema seguente:



I tipi ai quali si fa riferimento sono definiti nel file **FtpTypes_v2.0.xsd** scaricabile nella sezione Documentazione Sistema di Interscambio del sito www.fatturapa.gov.it .

4. DIRECTORY DI SCAMBIO FILE

4.1 FLUSSO REALE

Il server SFTP predisposto dal Nodo dovrà prevedere la raggiungibilità tramite le credenziali fornite al Sistema di Interscambio delle seguenti directory e relative autorizzazioni:

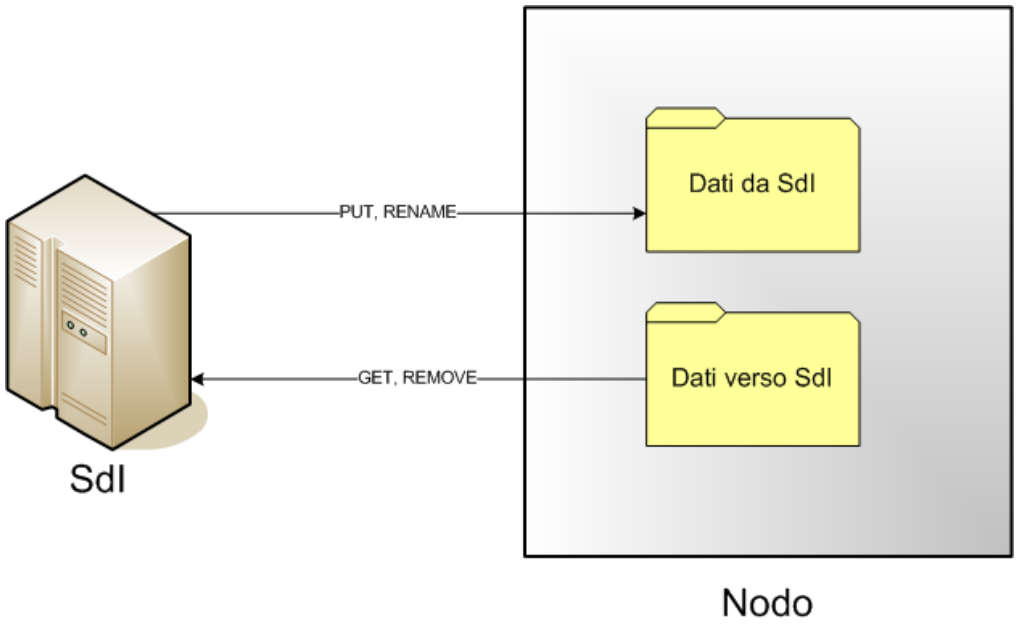
- **DatiVersoSdI** (con permessi di *get* e *delete*): è la directory dove il Nodo colloca i supporti pronti per essere prelevati (tipologia FI).

  Il Nodo deve garantire la presenza sulla directory **DatiVersoSdI** di soli supporti validi, con estensione *.zip*, e non ancora in corso di elaborazione; per ottenere quest'ultima condizione può effettuare l'elaborazione su una directory di appoggio e spostare il file sulla directory **DatiVersoSdI** solo ad elaborazione ultimata, oppure può elaborare il file con un nome diverso rispetto a quello previsto dalle regole di nomenclatura e procedere ad una *rename* al termine dell'elaborazione (si precisa che il non rispetto di queste regole espone al rischio di elaborazione parziale dei file in oggetto). Terminato con successo il trasferimento dei file, lo SdI elimina i file relativi ai supporti dalla directory **DatiVersoSdI**.

- **DatiDaSdI** (con permessi di *put* e *rename*): è la directory che ospita i supporti prodotti da SdI (tipologia FO) e i file di esito relativi ai supporti del flusso in ingresso della connessione precedente (tipologia EO).

  Lo SdI, per evitare che il Nodo acquisisca file non validi in quanto ancora in corso di elaborazione, effettua, una volta terminata la trasmissione e verificato il buon esito, una *rename* dei file trasferiti sulla directory **DatiDaSdI** aggiungendo il suffisso .p7m.enc.

La figura seguente illustra il protocollo di comunicazione tra SdI e Nodo, unitamente alle attività logiche effettuate dalle controparti:



Nelle directory di scambio il Nodo può collocare ulteriori file, se funzionali alle fasi di elaborazione e controllo del processo, a condizione che questi ultimi abbiano un nome in formato diverso da quello concordato per i supporti di fornitura ed i file di esito.

4.2 FLUSSO DI TEST

Per quanto riguarda i flussi di test, lo scambio di file avviene tramite l'uso di due directory separate rispetto ai flussi reali, raggiungibili dal Sistema di Interscambio con le seguenti autorizzazioni:

- **DatiVersoSdITest** (con permessi di *get*, *delete* e *sovrascrittura*): è la directory dove il Nodo colloca i supporti di test pronti per essere prelevati (tipologia FI).
- **DatiDaSdITest** (con permessi di *put* e *rename*): è la directory che ospita i supporti di test prodotti da SdI (tipologia FO) e i file di esito relativi ai supporti del flusso in ingresso della connessione precedente (tipologia EO).

I flussi di test, oltre ad utilizzare la nomenclatura prevista, devono essere concordati con il servizio di Supporto Operativo SdI.

5. ESEMPIO DI FLUSSO

5.1 FLUSSO REALE

5.1.1 FILE DA SDI

Se il SdI produce, alle ore 10:30 del 10 Gennaio 2012, un supporto da inviare al Nodo 12345678901, il flusso prevede i seguenti passaggi:

- al supporto viene attribuito il nome **FO.12345678901.2012010.1030.001.zip**, come previsto dalla nomenclatura;
- SdI applica la firma elettronica e la cifratura sul file prodotto ;
- SdI trasmette il file **FO.12345678901.2012010.1030.001.zip** nella directory **DatiDaSdI** del nodo **12345678901;** al termine della trasmissione (effettuata con successo) rinomina il file in **FO.12345678901.2012010.1030.001.zip.p7m.enc**.

Si precisa che se il supporto contiene file fattura, la data/ora in cui termina con successo la trasmissione del supporto viene riportata nelle Ricevute di Consegna che il Sistema di Interscambio invia relativamente ai file fattura consegnati.

5.1.2 FILE VERSO SDI

Se il Nodo 12345678901 produce, alle ore 12:30 del 15 Gennaio 2012, un supporto da inviare al SdI, il flusso prevede i seguenti passaggi:

- al supporto viene attribuito il nome **FI.12345678901.2012015.1230.001.zip**, come previsto dalla nomenclatura;
- il Nodo applica la firma elettronica e la cifratura sul file prodotto;
- il Nodo sposta (o rinomina) il file **FI.12345678901.2012015.1230.001.zip** nella directory **DatiVersoSdI** ;
- SdI preleva dalla directory **DatiVersoSdI** il supporto **FI.12345678901.2012015.1230.001.zip** e al termine del trasferimento lo rimuove;
- SdI effettua i controlli di quadratura e produce il file di esito **EO.12345678901.2012015.1230.001.xml**.

5.2 FLUSSO DI TEST

I flussi di test devono essere concordati con il servizio di Supporto Operativo di SdI.

5.2.1 FILE DA SDI

Se il SdI produce, alle ore 10:30 del 10 Gennaio 2012, un supporto da inviare al Nodo 12345678901, il flusso prevede i seguenti passaggi:

- al supporto viene attribuito il nome **FO.12345678901.2012010.1030.900.zip**, come previsto dalla nomenclatura;
- SdI applica la firma elettronica e la cifratura sul file prodotto ;
- SdI trasmette il file **FO.12345678901.2012010.1030.900.zip** nella directory **DatiDa SdITest** del nodo **12345678901;** al termine della trasmissione (effettuata con successo) rinomina il file in **FO.12345678901.2012010.1030.900.zip.p7m.enc**.

5.2.2 FILE VERSO SDI

Se il Nodo 12345678901 produce, alle ore 12:30 del 15 Gennaio 2012, un supporto da inviare al SdI, il flusso prevede i seguenti passaggi:

- al supporto viene attribuito il nome **FI.12345678901.2012015.1230.900.zip**, come previsto dalla nomenclatura;
- il Nodo applica la firma elettronica e la cifratura sul file prodotto;
- il Nodo sposta (o rinomina) il file **FI.12345678901.2012015.1230.900.zip** nella directory **DatiVersoSdITest** ;
- SdI preleva dalla directory **DatiVersoSdITest** il supporto **FI.12345678901.2012015.1230.900.zip** e al termine del trasferimento lo rimuove;
- SdI effettua i controlli di quadratura e produce il file di esito **EO.12345678901.2012015.1230.900.xml**.

6. GESTIONE DEGLI ERRORI

6.1 ERRORI DI QUADRATURA

Nel caso in cui il SdI verifichi discordanze tra i dati riportati nel file di quadratura rispetto al contenuto del supporto e/o rispetto alla nomenclatura del supporto stesso, al fine di prevenire possibili situazioni di errore nell'elaborazioni successive, il supporto viene considerato nello stato "sospeso" in attesa di approfondimenti e le incongruenze rilevate vengono comunicate tramite il file di esito. Successivamente l'utente viene contattato per maggiori informazioni.

Le modalità e i tempi di un eventuale recupero dei dati devono essere di volta in volta concordate mediante contatto diretto tra il supporto operativo messo a disposizione dal SdI e dal Nodo.

6.2 MALFUNZIONAMENTI

Sono considerati malfunzionamenti gli errori di tipo tecnico dovuti al mancato rispetto delle specifiche di comunicazione tra Sdi e Nodo (es. errore di decifratura, problemi di connessione, malfunzionamenti dei server). Il referente tecnico dello SdI deve poter contattare l'analogo riferimento del Nodo, e viceversa, in modo da risolvere il problema.

7. SPECIFICHE DI SICUREZZA E CRITTOGRAFIA

I dati trasmessi via SFTP devono essere crittografati e firmati digitalmente allo scopo di assicurarne la provenienza e la riservatezza. I dati saranno prima firmati, con il formato PKCS#7, e quindi cifrati. I formati utilizzati per imbustare i dati firmati e cifrati saranno conformi allo standard PKCS#7 v 1.5, nelle modalità "signedData" ed "envelopedData" (standard misto S/MIME, con busta di firma e cifratura conforme PKCS#7 v.1.5, con codifica in formato DER).

In fase di cifratura i dati sono criptati utilizzando un algoritmo a chiave simmetrica, generata di volta in volta in modo random. La chiave utilizzata è poi inserita nella busta, cifrata con la chiave RSA pubblica del destinatario.

L'algoritmo di cifratura asimmetrica, basato sulla coppia chiave privata-chiave pubblica, è RSA; la lunghezza delle chiavi va da 512 a 4096.

Gli algoritmi di cifratura simmetrica supportati sono: RC2, DES, DES-EDE-3, AES-128, AES-192, AES-256.

Gli algoritmi di hash supportati sono: MD2, MD5, SHA-1, SHA-256, SHA-384, SHA-512.

Sia il Nodo che SdI devono, pertanto, disporre di una coppia di chiavi di cifratura e di una distinta coppia di chiavi di firma.

Il Nodo provvede autonomamente alla generazione delle chiavi e all'invio delle richieste di certificato; SdI emette i certificati che vengono inviati al Nodo; tramite canale sicuro vengono inviati al Nodo anche il certificato di cifra del servizio di Trasmissione Dati e il certificato della Certification Authoriry.

La generazione delle chiavi viene effettuata da SdI; al Nodo vengono forniti su canale sicuro, insieme al certificato di cifra del servizio di Trasmissione Dati e a quello della Certification Authority due file in formato PKCS#12 che contengono rispettivamente la coppia di chiavi e il certificato di firma e la coppia di chiavi e il certificato di cifra. I file PKCS#12 sono protetti da password che vengono comunicate ai responsabili del Nodo.

Per lo sviluppo di procedure che implementino le operazioni di cifratura, decifratura, firma e verifica il Nodo può utilizzare strumenti software diversi, grazie all'uso di formati standard sia per la distribuzione di chiavi e certificati, che per la rappresentazione dei dati firmati e dei dati cifrati.

8. DISPONIBILITÀ DEL SERVIZIO

La "*giornata applicativa SdI*" per la trasmissione e la ricezione dei flussi via FTP va dal Lunedì al Sabato dalle ore 00:00 alle ore 23:00.

La trasmissione dei flussi dei file viene effettuata secondo i tempi descritti nel paragrafo 2.3.

Il servizio di Supporto Operativo del SdI è disponibile dal lunedì al venerdì dalle 8.00 alle 18.00, il Nodo deve garantire una disponibilità del Supporto Operativo che copra le finestre temporali di collegamento.

Per la presa in carico e la risoluzione di tutte le problematiche tecniche inerenti al servizio è reso disponibile dal Nodo un riferimento tecnico, contattabile dal corrispettivo riferimento tecnico SdI dal lunedì al venerdì dalle 8.00 alle 18.00.