Banca d'Italia

Money Market Statistical Reporting

Versione 2.1

Aprile 2021

Storia del documento

Versione	Data	Descrizione modifiche
1.0	Agosto 2019	Stesura documentazione dedicata alla rilevazione MMSR
2.0	Gennaio 2021	Inserimento istruzioni relative alla modalità di invio dei messaggi tramite canale alternativo (*contingency*), definizione di un periodo di *retention* per il download delle comunicazioni
2.1	Aprile 2021	Precisazioni su nomenclatura del file

Sommario

1. Accesso interfaccia A2A Banca d'Italia per segnalazioni MMSR

Per accedere al servizio di invio dei messaggi MMSR è previsto l'accreditamento verso la Banca d'Italia da parte degli intermediari segnalanti. Gli intermediari già coinvolti nel progetto di nuova interfaccia applicativa (A2A) per lo scambio via internet dei flussi di Anagrafe soggetti (AS), Centrale Rischi (CR) [1] ed AnaCredit [2], possono utilizzare le stesse utenze (e quindi certificati digitali) sia in ambiente di collaudo che di produzione valide per le segnalazioni CR ed AnaCredit sulla nuova interfaccia A2A via Internet. Tutti gli intermediari sprovvisti della sopra citata utenza potranno accreditarsi tramite la procedura descritta nel "Manuale di accreditamento e di gestione delle credenziali" disponibile sul sito della Banca d'Italia[3]. In questo caso la procedura, sia per l'ambiente di produzione che di collaudo, richiede di dotarsi di una specifica credenziale applicativa. Per completare l'accreditamento andrà poi inviato l'apposito modulo all'indirizzo di posta elettronica certificata res@pec.bancaditalia.it.

Le caratteristiche generali del sistema sono le seguenti:

- lo scambio di messaggi tra Bankit e segnalanti avviene su canale HTTPS con mutua autenticazione mediante certificati X.509;
- il client deve essere in grado di instaurare una connessione sicura con il server, in particolare deve supportare il protocollo TLSv1.2 e la client authentication;
- l'interfaccia applicativa è di tipo REST ed utilizza un formato dati JSON;
- i messaggi MMSR inviati dal segnalante dovranno essere sottoposti nell'ordine a:

  - ✓ compressione per contenere le dimensioni del payload da trasferire in rete;
  - ✓ cifratura con l'uso di chiave asimmetrica per garantirne la riservatezza;
  - ✓ firma elettronica per assicurare l'integrità;

- analogamente a quanto avviene per i flussi in ingresso, anche i flussi in uscita contenenti informazioni relative alle transazioni MMSR (in particolare rilievi) saranno sottoposti a compressione e cifratura.

L'interfaccia applicativa espone agli utenti una struttura ad albero simile a quella dei filesystem tradizionali. In particolare, ad ogni credenziale applicativa verrà associato uno spazio riservato contenente due cartelle: *upload* e *download*, destinate rispettivamente all'invio ed alla ricezione dei flussi. Su entrambe le folder saranno presenti sotto-cartelle con nome delle survey per cui vengono effettuate le segnalazioni MMSR (MMNS, MMSE, MMOS, MMFX).
L'endpoint HTTPS esposto agli intermediari varierà per ambiente (produzione o collaudo). In particolare valgono i seguenti puntamenti per ambiente:

AMBIENTE ELABORATIVO	Indirizzo Internet (URL)
PRODUZIONE	https://mft.bancaditalia.it/a2a/

[1] https://www.bancaditalia.it/statistiche/raccolta-dati/centrale-rischi/doc-tecnica-cr/modalita_di_scambio_VER_8.5.pdf

[2] https://www.bancaditalia.it/statistiche/raccolta-dati/segnalazioni/rilevazione-dati-granulari/comunicazioni-produzione-segnalazioni/manuale_per_segnalanti_AnaCredit_ver_1_7.pdf

[3] Il manuale è disponibile alla pagina Accreditamento nella sezione Statistiche, Centrale dei Rischi, e raggiungibile al seguente link: https://www.bancaditalia.it/statistiche/raccolta-dati/centrale-rischi/accreditamento-cr/index.html

COLLAUDO	https://certmft.bancaditalia.it/a2a/

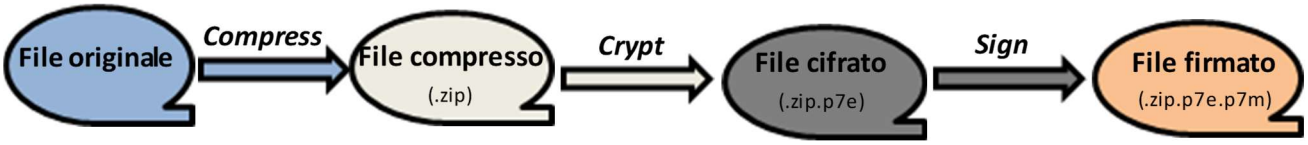
Nel prosieguo del documento gli esempi contengono l'endpoint dell'ambiente di Produzione Banca d'Italia, ma le stesse URL sono da ritenere valide per l'ambiente di Collaudo, fatta salva la sostituzione di mft.bancaditalia.it con certmft.bancaditalia.it nelle URL.

Si suggerisce, prima di avviare il colloquio, di **verificare la corretta configurazione** della credenziale mediante un test di canale. A tale scopo è possibile utilizzare la funzionalità di "Consultazione lista file" (cfr. paragrafo A capitolo 3 e paragrafo omonimo in capitolo 6.)

2. Invio Messaggi

Il file contenente la segnalazione deve essere opportunamente "imbustato", quindi inviato assieme ad alcuni metadati descrittivi. Le operazioni da effettuare sono descritte di seguito.
Prima dell'invio, i messaggi MMSR devono essere compressi, cifrati e firmati elettronicamente:

1) La prima operazione da effettuare è la compressione zip del file.
2) Il *file* dev'essere quindi cifrato con il certificato associato alla credenziale applicativa.
3) La firma elettronica deve essere applicata al *file* compresso e cifrato.



Il *file* deve essere caricato nella cartella *upload*, mediante una richiesta *http* così caratterizzata:

- indirizzo: ad esempio *https://mft.bancaditalia.it/**upload/filename**.zip.p7e.p7m*
- metodo: PUT
- content type: *application/octet-stream*
- il nome del *file* sul server sarà ricavato dall'indirizzo (la parte che segue */upload/*)

Il nome del *file* inviato deve rispettare i seguenti vincoli:

- l'estensione deve essere coerente con le operazioni di imbustamento descritte sopra, occorre utilizzare l'estensione ".zip.p7e.p7m" sempre in minuscolo;

- univocità: l'invio di un file con lo stesso nome di uno già presente sul server provocherà la sovrascrittura del file stesso. L'intermediario dovrà aver cura di garantire l'univocità del nome, ad es. aggiungendo un timestamp come suffisso. Non devono essere presenti spazi vuoti.

- Il file con estensione ".zip.p7e.p7m" deve avere la stessa nomenclatura del suo contenuto, fatto salvo la possibilità di poter apporre eventuali suffissi al nome del file. Il file "plain" contenuto all'interno dell'archivio zip deve seguire la naming-convention adottata per MMSR, che prevede il seguente formato:

<MARKET SEGMENT IDENTIFIER>.<LEI>.<DATE>.<INCREMENTAL TRANSMISSION NUMBER>

Campo	Descrizione
<MARKET SEGMENT IDENTIFIER>	Lunghezza: 15 Il segment di mercato a cui si riferisce il file, che può essere: • "***auth.012.001.02***" per mercati secured • "***auth.013.001.02***" per mercati unsecured • "***auth.014.001.02***" per foreign exchange swaps • "***auth.015.001.02***" per overnight index swaps
<LEI>	Lunghezza: 20 Legal Entity Identifier (LEI) del Reporting Agent
<DATE>	Lunghezza: 8 Reporting Date Nel formato: YYYYMMDD
<INCREMENTAL TRANSMISSION NUMBER>	Lunghezza: 4 Valore numerico incrementale su 4 posizioni: il primo file trasmesso da un segnalante per segmento e data parte da "0001".

Ad esempio, il messaggio di tipo SEND del segmento FX, inviato da MPS per la data 01/07/2019 (a cui si riferisce la trade date delle transazioni contenute nel file) a partire dalle ore 18.00 del giorno 01/07/2019, deve avere il seguente pattern:

auth.014.001.02.J4CP7MHCXR8DAQMKIL78.20190701.0001

Dopo aver inviato il file, attraverso una seconda invocazione (di tipo POST) verso l'endpoint https esposto al segnalante autenticato, è necessario specificare alcune informazioni aggiuntive necessarie per l'elaborazione del messaggio come ad esempio survey, codice partner dell'ente segnalante, tipo messaggio, data di riferimento, ecc... Le informazioni devono essere codificate in formato JSON ed inviate tramite POST. La correlazione tra il file ed i rispettivi metadati avviene tramite il path della richiesta, che rappresenta la risorsa su cui si sta operando.

Formato richiesta:

- indirizzo: *https://mft.bancaditalia.it/**upload/filename**.zip.p7e.p7m*
- metodo: PUT
- formato payload: *Content-Type: application/JSON;*

Metadati da inviare in formato JSON:

- "***Flow_userVars.Partner***": codice *partner* (cioè il codice ABI dell'ente segnalante seguito dal codice di controllo):

Segnalante	Codice partner [4]	Codice LEI
MPS	10306	J4CP7MHCXR8DAQMKIL78
Unicredit	20081	549300TRUWO2CD2G5692
ISP	30692	2W8N8UU78PMDQKZENC08
IMI	32490	QV4Q8OGJ7OA6PA8SCM14
BPM	50344	815600E4E6DCD2D25E30
CDP	76026	81560029E2CE4D14F425

- "***Flow_userVars.Survey***": codice della rilevazione in base al segmento a cui si riferiscono i dati (per MMSR: MMSE, MMNS, MMFX o MMOS);

- "***Flow_userVars.MessageType***": tipo di messaggio (SEND se il primo messaggio per la data/segmento oppure ADJUSTMENT per messaggi successivi nella stessa data/segmento);

- "***Flow_userVars.ReportingDate***": data di riferimento della segnalazione;

- "***newFilePath***": percorso di destinazione del *file*, specifico per le rilevazioni MMSR, es. */upload/MMFX/auth.014.001.02.J4CP7MHCXR8DAQMKIL78.20190701.0001.zip.p7e.p7m.* In generale si richiede di valorizzare questo parametro con il path "/upload/<Survey>/<filename>.zip.p7e.p7m", in quanto sotto la folder /upload, a disposizione del segnalante tramite accesso con utenza A2A, saranno disponibili le sotto-directory relative alle quattro survey (MMSE, MMNS, MMFX e MMOS).

- "***Flow_userVars.Community***": valore della community statistica, per MMSR valorizzare con BANKITALIA;

- "***Flow_userVars.MessageScope***": scope del messaggio inviato, per diagnostici valorizzare con DIAGNOSTIC altrimenti PRODUCTION;

- "***Flow_userVars.DataFragmentName***": nome del file in chiaro (comprensivo di eventuali estensioni) che rappresenta il messaggio MMSR, contenuto nell'archivio zip. Vale la sintassi esposta in precedenza sul filename: <MARKET SEGMENT IDENTIFIER>.<LEI>.<DATE>.<INCREMENTAL TRANSMISSION NUMBER>;

- "***Flow_userVars.DataFragmentPath***": path relativo (comprensivo di nome file e sua estensione) del file in chiaro all'interno dell'archivio zip.

Valorizzazione dei parametri:

[4] Va inserito ABI e il codice di controllo.

- il codice da inserire nel campo *Partner* è costituito dal codice ABI che identifica l'ente segnalante seguito dal codice CIN, in formato numerico (non sono ammessi punti, trattini ed altri caratteri di separazione, con dimensione massima di 7 posizioni);

- i campi Partner e Survey devono essere valorizzati in modo coerente con il messaggio MMSR inviato;

- Il campo ReportingDate deve essere valorizzato con la data di inizio della segnalazione: nel caso MMSR tale data rappresenta, almeno nel messaggio di SEND, la "*trade date*", quindi nel caso di SEND essa dovrà essere uguale alla data precedente rispetto a quella corrente di invio del messaggio;

- il campo MessageType deve essere coerente con i messaggi inviati in precedenza per la stessa data e segmento: in particolare il primo messaggio riferito alla Trade Date deve essere di tipo SEND mentre i successivi riferiti alla medesima data e segmento devono essere di tipo ADJUSTMENT.

  I parametri **Flow_userVars.DataFragmentName** e **Flow_userVars.DataFragmentPath** devono essere coerenti con il contenuto dell'archivio zip. In particolare deve essere presente per l'invio MMSR un unico file in chiaro avente un nome uguale al valore di **Flow_userVars.DataFragmentName** ed esso deve essere presente nel path relativo dichiarato in **Flow_userVars.DataFragmentPath** una volta aperto l'archivio zip. Il caso più semplice, e pertanto quello consigliabile ai segnalanti, è quello di disporre il file in chiaro direttamente sotto la root dell'archivio. Ad esempio, nel caso del file *auth.014.001.02.J4CP7MHCXR8DAQMKIL78.20190701.0001.zip.p7e.p7m*, che a valle delle operazioni di "sbustamento" (verifica firma e decrittografia) presenta l'archivio *auth.014.001.02.J4CP7MHCXR8DAQMKIL78.20190701.0001.zip*, che a sua volta contiene il solo file in chiaro denominato "*auth.014.001.02.J4CP7MHCXR8DAQMKIL78.20190701.0001*", la valorizzazione del JSON per i metadati del file deve essere la seguente:

```
{
"newFilePath": "/upload/MMFX/auth.014.001.02.J4CP7MHCXR8DAQMKIL78.20190701.0001.zip.p7e.p7m",
"Flow_userVars.Partner": "10306",
"Flow_userVars.Survey": "MMFX",
"Flow_userVars.ReportingDate": "2019-07-01",
"Flow_userVars.MessageType": "SEND",
"Flow_userVars.Community": "BANKITALIA",
"Flow_userVars.MessageScope": "PRODUCTION",
"Flow_userVars.DataFragmentName": "auth.014.001.02.J4CP7MHCXR8DAQMKIL78.20190701.0001",
"Flow_userVars.DataFragmentPath": "auth.014.001.02.J4CP7MHCXR8DAQMKIL78.20190701.0001",
```

}

Per le segnalazioni MMSR si consiglia l'utilizzo di un path che preveda il file in chiaro sotto la root dell'archivio, ottenendo così l'uguaglianza nella valorizzazione dei parametri ***Flow_userVars.DataFragmentName*** e ***Flow_userVars.DataFragmentPath***, entrambi uguali al nome del file in chiaro contenuto nell'archivio.

Al termine della chiamata POST che invia i metadati di imbustamento, il *file* non sarà più visibile nella cartella *upload* ma rimarrà nel percorso di destinazione *(/upload/MMxx*) definito nel parametro **newFilePath** fino a quando non verrà preso in carico dal sistema per l'innesco del processo di acquisizione.

Attenzione: Se il file caricato non rispetta il formato richiesto o i metadati sono incompleti o mancanti la segnalazione non verrà acquisita.

3. Ricezione delle comunicazioni

Viene messo a disposizione dei segnalanti un servizio di consultazione che fornisce l'elenco dei file presenti nella cartella *download*. I file di interesse possono essere scaricati con un'apposita chiamata.
Analogamente a quanto avviene per i flussi in ingresso, i file sono sottoposti a compressione, cifratura e firma[5]. Il segnalante dovrà quindi decifrarli utilizzando la chiave privata di cifratura corrispondente alla propria credenziale applicativa. Il segnalante è tenuto a scaricare i messaggi e si consiglia di salvarli in locale per una consultazione futura[6]. Si consiglia altresì di effettuare l'eliminazione dei file già scaricati.

Le comunicazioni che la cartella download potrà contenere saranno:

- Rilievi a seguito dell'invio messaggi
- Scarti a seguito dell'invio messaggi
- Notifiche di protocollo a seguito dell'invio messaggi
- Solleciti di invio messaggio

Le notifiche saranno in formato XML.
Di seguito si elencano i file relativi alle strutture xsd dei messaggi che costituiscono le comunicazioni e alcuni file di esempio dei file xml riportati nel file "strutturexsd-esempi-comunicazioni.zip".

[5] L'apposizione della firma elettronica potrebbe non essere necessaria su alcuni flussi, in funzione del livello di riservatezza delle informazioni in essi riportate.
[6] Per le comunicazioni si applica un periodo di retention dei dati pari a 30 giorni. Dopo tale periodo le comunicazioni potrebbero non essere più disponibili per il download.

Schema xsd messaggi	message.xsd
Schema xsd rilievi	remark.xsd
Esempio file xml scarto messaggio	503235_2019062010 2727810_DISCARD.x
Esempio file xml rilievi	503235_2019080818 0226807_REMARK.xr
Esempio file xml notifica di protocollo	503235_2019022512 0115234_PROTOCOL
Esempio file xml sollecito invio	503235_2019080818 1918067_REMINDER

In particolare per quanto riguarda i rilievi, sono possibili diverse tipologie, tra cui le principali:

- *CONVERSION*
- *LOADING*
- *FORMAL*
- *DETERMINISTIC*

Essi sono identificati dall'attributo *uniqueId* nel tag *remarkItem*.

Di seguito le funzionalità esposte tramite interfaccia A2A, utili alla gestione delle comunicazioni ricevute dai segnalanti.

A) Consultazione lista file

L'elenco dei file scaricabili può essere ottenuto mediante una richiesta così strutturata:

- indirizzo: *https://mft.bancaditalia.it/**download**/MMSE*
- indirizzo: *https://mft.bancaditalia.it/**download**/MMNS*
- indirizzo: *https://mft.bancaditalia.it/**download**/MMFX*
- indirizzo: *https://mft.bancaditalia.it/**download**/MMOS*
- metodo: GET

L'output sarà codificato in formato JSON – nella proprietà "***files***" – e conterrà un *array* di oggetti contenenti almeno le seguenti proprietà:

- "*fileName*": il nome del *file;*
- "*lastModifiedTime*": *timestamp* di ultima modifica (formato *Unix time*);
- "*size*": la dimensione del *file.*

Un esempio di invocazione con relativo output è disponibile al capitolo 5.

B) Scaricamento di un file

Richiesta di *download* di un file:

- indirizzo: *https://mft.bancaditalia.it/MMxx/**download/fileName*** dove il valore di "fileName" è ricavato dall'output fornito dal servizio di consultazione descritto sopra
- metodo: GET

Il *file* verrà fornito nel *body* della *response*.
Un esempio di invocazione è disponibile al capitolo 5.
Dopo aver scaricato un *file*, è possibile cancellarlo dal *server* utilizzando lo stesso indirizzo usato per il download ed il metodo DELETE.

> **Attenzione**: Tutti i flussi devono essere scaricati quanto prima e comunque entro trenta giorni dalla data in cui sono resi disponibili per il *download*. Oltre questo limite temporale i flussi potrebbero essere cancellati e non essere più disponibili.

C) Estrazione della comunicazione (sbustamento)

Per ottenere il contenuto in chiaro del file scaricato, il segnalante dovrà effettuare una sequenza di operazioni inversa rispetto a quella utilizzata per l'invio:

- estrazione del *file* cifrato dalla busta *p7m* (se il *file* è firmato)
- decifratura mediante la chiave privata associata al certificato di cifratura caricato in fase di auto-registrazione (vedi manuale "Manuale di accreditamento e di gestione delle credenziali")
- decompressione (*unzip*)

4. Certificati e standard crittografici

Autenticazione

L'autenticazione al servizio avverrà mediante mutua autenticazione (scambio di certificati tra *client* e *server*) con utilizzo del protocollo TLSv1.2.
Per supportare questo meccanismo di autenticazione, ai segnalanti è richiesto di dotarsi di un certificato applicativo con *extended key usage* "*TLS WWW Client Authentication*", rilasciato da certificatori riconosciuti dai principali *browser web* di mercato[7].

[7] Cfr. https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.3.3.pdf.

Crittografia

Per garantire la riservatezza dei dati inviati alla Banca d'Italia, il segnalante dovrà utilizzare il certificato di chiave pubblica di cifratura che l'Istituto metterà a disposizione sul proprio sito.
L'operazione di cifratura del file dovrà avvenire in conformità a [R08], con le seguenti specifiche:

- modalità "*Enveloped Data Type*";
- algoritmo di cifratura simmetrica AES con lunghezza di chiave pari a 256 bit;
- chiave pubblica di cifratura della chiave simmetrica con cui viene cifrato il dato, RSA a 2048 bit;
- certificato di chiave pubblica di cifratura nel formato X.509 Binario codificato DER.

I dati inviati dalla piattaforma per la raccolta delle segnalazioni MMSR di Banca d'Italia ai segnalanti saranno cifrati mediante la chiave pubblica di cifratura del destinatario. Ai segnalanti è richiesto di acquisire certificati di cifratura con l'attributo "*key usage*" impostato a *"key encipherment"*.

Firma

Per la firma sarà necessario utilizzare certificati rilasciati da certificatori accreditati AGID per la firma digitale (https://applicazioni.cnipa.gov.it/TSL/IT_TSL_signed.xml).
Saranno accettate firme in formato CADES [R02].

Riepilogo certificati digitali in uso

Obiettivo	Certificato richiesto
Autenticazione	Certificato applicativo di autenticazione rilasciato da certificatore appartenente alla lista dei certificatori riconosciuta dai *browser* più comuni
Firma dei dati in ingresso a Banca d'Italia	Certificato rilasciato da certificatore accreditato AGID per il rilascio di certificati per utilizzo con dispositivo sicuro per l'apposizione della firma digitale
Cifratura dati in ingresso a Banca d'Italia	Certificato di chiave pubblica di Banca d'Italia, emesso da CA Banca d'Italia e messo a disposizione sul sito internet della Banca d'Italia
Firma dei dati in uscita da Banca d'Italia	Firma non qualificata mediante certificati emessi da CA Banca d'Italia
Cifratura dati in uscita da Banca d'Italia	Certificato di chiave pubblica di cifratura della controparte

Standard di riferimento

Rif.	Requisito	Standard di riferimento	Ver.	Data
R01	Firma digitale	XAdES Specifications – ETSI TS 101 903	1.4.2	12/2010
R02		CAdES Specifications – ETSI TS 101 733	2.2.1	04/2013
R03		Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile – IETF RFC 5280	N/A	05/2008
R04		OCSP – IETF RFC 6960	N/A	06/2013
R05		Electronic Signatures and Infrastructures; Signature verification procedures and policies – ETSI TS 102 853	1.1.1	07/2012
R06		XAdES Baseline profiles – ETSI TS 103 171	2.1.1	03/2012
R07		CAdES Baseline profiles – ETSI TS 103 173	2.2.1	04/2013
R08	Cifratura	Cryptographic Message Syntax (CMS) – IETF RFC 3852		07/2004

5. Problemi e soluzioni

Impossibile stabilire una connessione con il server

Per stabilire una connessione, è necessario che il client supporti il protocollo TLSv1.2, che client e server riescano ad autenticarsi reciprocamente e che riescano a negoziare un algoritmo di cifratura. Durante questa fase possono verificarsi vari tipi di problemi, alcuni tra i più comuni vengono riportati di seguito.
In ogni caso, è utile verificare che non sussistano problemi di connettività o blocchi dovuti alla configurazione della rete aziendale ed attivare le funzionalità di log rese disponibili dall'ambiente utilizzato. A titolo di esempio: in java è possibile impostare la proprietà di sistema **javax.net.debug** al valore "ssl" oppure "all", sotto curl è disponibile l'opzione "**-v**" e così via.

Problema nella verifica del certificato del server

L'applicazione client sta cercando di verificare la validità del certificato presentato del server ma non ci riesce. Probabilmente ciò è dovuto al fatto che il certificato della CA che lo ha emesso non è stato aggiunto all'elenco dei certificati attendibili. La procedura da utilizzare per aggiungere una CA all'elenco di quelle attendibili (detto anche CA bundle o trust store) varia a seconda dello strumento usato per la realizzazione del client, si rimanda quindi alla documentazione specifica.

Impossibile individuare un certificato client

Il problema è simile al precedente, in questo caso però il problema risiede nella scelta del certificato da inviare al server. È necessario che l'applicazione client possa accedere all'archivio che contiene il proprio certificato di autenticazione e la chiave privata corrispondente. Anche in questo caso, le modalità d'accesso a questo archivio (a volte chiamato key store) variano da caso a caso.

Errore "Referer header doesn't match the white-list"

Problema: in fase di upload si ottiene uno status code 400 (Bad Request) ed il contenuto della risposta del server è simile a questo:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<message>
        <msg>Referer header doesn't match the white-list.</msg>
</message>
```

Soluzione: aggiungere alla richiesta un *header* "*Referer:"*. Per valorizzarlo si consiglia di utilizzare l'endopoint del servizio (*https://free.ep/*).

Errore "Error occurred while getting file size and type"

Problema: si ottiene uno status code 404 (Not Found) ed il contenuto della risposta del server è simile a questa:

```
{
  "message" : "Error validating request",
  "validationErrors" : [ "Error occurred while getting file size and type." ]
}
```

Soluzione: controllare il path della richiesta, probabilmente fa riferimento ad un file o cartella inesistente. Utilizzando il servizio di consultazione file sulla cartella padre (es. upload o download) è possibile controllare che il nome utilizzato sia presente come "fileName" tra i risultati.

Errore "Unable to rename filePath: <XXX> to newFilePath: <YYY>"

Problema: si ottiene uno status code 403 (Forbidden) ed il contenuto della risposta del server è simile a questa:

```
{
  "message" : "Error validating request",
  "validationErrors" : [ " Unable to rename filePath: \"/upload/xxx\" to newFilePath: \"/upload/yyy\"" ]
}
```

Soluzione: controllare che il parametro filePath identifichi correttamente il percorso di un file precedentemente caricato, utilizzando il servizio di consultazione file. Controllare inoltre che il

parametro newFilePath faccia riferimento ad una cartella di destinazione esistente (ad es. /upload/CR).
È possibile che questo errore venga restituito anche quando i parametri sono corretti, se l'invocazione avviene immediatamente dopo l'upload del file. In questo caso è sufficiente attendere alcuni secondi e ripetere la chiamata.

6. Esempi di invocazione con sintassi cURL

Di seguito vengono proposti alcuni esempi di colloquio con la nuova interfaccia applicativa realizzati mediante il tool open source *curl*.
Tale strumento, assieme alla libreria associata *libcurl*, è disponibile per una varietà di piattaforme hardware e sistemi operativi ed è scaricabile gratuitamente dal sito del progetto cURL[8].
Gli esempi non costituiscono in alcun modo un invito all'utilizzo di questo strumento in ambienti di produzione, essi vengono forniti al solo scopo di fornire una descrizione delle funzionalità in un "linguaggio" ampiamente noto in ambiente tecnico e ben documentato.
Prima di passare agli esempi, si segnalano alcune opzioni di utilità generale. Per ulteriori informazioni si rimanda comunque alla documentazione del progetto cURL.

Opzione	Effetto
-v	modalità "verbose", vengono visualizzate in output informazioni dettagliate sulle operazioni in corso, può essere utile per diagnosticare problemi durante l'handshake TLS
--noproxy "host"	disabilita l'utilizzo del proxy per le connessioni al server "host"
--cacert e --capath	consentono di specificare il certificato della CA da utilizzare per verificare il certificato del server, in alternativa è possibile disabilitare la verifica con l'opzione **–k** (usata per semplicità negli esempi)

In tutti gli esempi si ipotizza che il certificato di autenticazione del client, assieme alla sua chiave privata, si trovi in un file denominato "auth_cert.pem" nella cartella di lavoro.
Viene esemplificata inoltre la predisposizione del file per l'invio, mediante i tool *zip* e *openssl*. Anche in questo caso lo scopo è puramente illustrativo.

Caricamento file

Caricamento del file "*auth.013.001.02.J4CP7MHCXR8DAQMKIL78.20190607.0001.zip.p7e.p7m*".

```
$ curl -k -E auth_cert.pem --upload-file auth.013.001.02.J4CP7MHCXR8DAQMKIL78.20190607.0001.zip.p7e.p7m
"https://mft.bancaditalia.it/upload/auth.013.001.02.J4CP7MHCXR8DAQMKIL78.20190607.0001.zip.p7e.p7m"
```

[8] L'homepage del progetto si trova all'indirizzo https://curl.haxx.se/.

NOTE:

- l'opzione "-X PUT" non è necessaria in quanto implicata da "--upload-file"
- la cartella di upload ed il nome del file vengono indicati mediante la porzione di URL che segue l'endpoint

Invio metadati

Esempio di invio metadati per una segnalazione di MMNS, messaggio di tipo SEND e consegna ufficiale, per il partner con codice ABI "10306" e data di riferimento 20190607.

```
$ curl -k -E auth_cert.pem -X POST -H "Content-type: application/json" -d '{
"newFilePath": "/upload/MMNS/auth.013.001.02.J4CP7MHCXR8DAQMKIL78.20190607.0001.zip.p7e.p7m",
"Flow_userVars.Partner": "10306",
"Flow_userVars.MessageType": "SEND",
"Flow_userVars.MessageScope": "PRODUCTION",
"Flow_userVars.ReportingDate":"2019-06-07",
"Flow_userVars.Community": "BANKITALIA",
"Flow_userVars.Survey": "MMNS",
"Flow_userVars.DataFragmentName": "auth.013.001.02.J4CP7MHCXR8DAQMKIL78.20190607.0001",
"Flow_userVars.DataFragmentPath": "auth.013.001.02.J4CP7MHCXR8DAQMKIL78.20190607.0001"}'
"https://mft.bancaditalia.it/upload/auth.013.001.02.J4CP7MHCXR8DAQMKIL78.20190607.0001.zip.p7e.p7m "
```

Esempio di invio metadati per una segnalazione MMSE, messaggio di tipo rettifiche (ADJUSTMENT) di consegna ufficiale, per il partner con codice ABI "30692" e data di riferimento 20190701.

auth.012.001.02. 2W8N8UU78PMDQKZENC08.20190701.0002

```
$ curl -k -E auth_cert.pem -X POST -H "Content-type: application/json" -d '{
"newFilePath": "/upload/CR/auth.012.001.02.2W8N8UU78PMDQKZENC08.20190701.0002.zip.p7e.p7m”,
"Flow_userVars.Partner": "30692",
"Flow_userVars.MessageType": "ADJUSTMENT",
"Flow_userVars.MessageScope": "PRODUCTION",
"Flow_userVars.ReportingDate":"2019-07-01",
"Flow_userVars.Community": "BANKITALIA",
"Flow_userVars.Survey": "MMSE",
"Flow_userVars.DataFragmentName": "auth.012.001.02.2W8N8UU78PMDQKZENC08.20190701.0002",
"Flow_userVars.DataFragmentPath": "auth.012.001.02.2W8N8UU78PMDQKZENC08.20190701.0002"}'
"https://mft.bancaditalia.it/upload/auth.012.001.02.2W8N8UU78PMDQKZENC08.20190701.0002.zip.p7e.p7m "
```

Consultazione lista file

Elenco file da scaricare per segmento MMSE:

```
$ curl -k -E auth_cert.pem "https://mft.bancaditalia.it/download/MMSE"
```

Elenco file da scaricare per segmento MMNS:

```
$ curl -k -E auth_cert.pem "https://mft.bancaditalia.it/download/MMNS"
```

Elenco file da scaricare per segmento MMFX:

```
$ curl -k -E auth_cert.pem "https://mft.bancaditalia.it/download/MMFX"
```

Elenco file da scaricare per segmento MMOS:

```
$ curl -k -E auth_cert.pem "https://mft.bancaditalia.it/download/MMOS"
```

Esempio di output dei comandi precedenti:

```
{
  "files" : [ {
    "fileName" : “20081_20190611171949396_REMARK.xml.zip.p7e.p7m”
    "lastModifiedTime" : 1480080720000,
    "size" : 87613,
    "isDirectory" : false,
    "isRegularFile" : true,
    "isSymbolicLink" : false,
    "isOther" : false,
    "permissions" : "644"
  }, {
fileName" : "20081_20190603095849546_PROTOCOL_NOTIFICATION.xml.zip.p7e.p7m"
 "lastModifiedTime" : 1480331460000,
    "size" : 91444,
    "isDirectory" : false,
    "isRegularFile" : true,
    "isSymbolicLink" : false,
    "isOther" : false,
    "permissions" : "644"
  } ]
}
```

Scaricamento di un file

Scaricamento del file di comunicazione di esempio (notifica protocollo):

"128270852_20190401101212885_PROTOCOL_NOTIFICATION.xml.zip.p7e.p7m"

(nome da lista di output del paragrafo precedente):

```
curl -k -E auth_cert.pem –o 20081_20190401101212885_PROTOCOL_NOTIFICATION.xml.zip.p7e.p7m"
“https://mft.bancaditalia.it/download/MMSE/20081_20190401101212885_PROTOCOL_NOTIFICATION.xml.zip.p7e.p7m"
```

L'opzione "-o" evita che il contenuto del file, in formato binario, venga scritto sullo standard output.

Per eliminare il file dopo averlo scaricato:

```
$ curl -k -E auth_cert.pem –X DELETE
“https://mft.bancaditalia.it/download/MMSE/20081_20190401101212885_PROTOCOL_NOTIFICATION.xml.zip.p7e.p7m”
```

Predisposizione del file

Esempio di "imbustamento" per un file denominato:

“auth.013.001.02.J4CP7MHCXR8DAQMKIL78.20190204.0001”

```
$ # compressione
$ zip auth.013.001.02.J4CP7MHCXR8DAQMKIL78.20190204.0001
$ # cifratura
$ openssl cms -encrypt -binary -aes256 -in auth.013.001.02.J4CP7MHCXR8DAQMKIL78.20190204.0001.zip -outform DER -out
auth.013.001.02.J4CP7MHCXR8DAQMKIL78.20190204.0001.zip.p7e certificato_bdi.pem
$ # firma
$ openssl smime -sign -binary -in msg002_999999_201612071513.zip.p7e -out
auth.013.001.02.J4CP7MHCXR8DAQMKIL78.20190204.0001.zip.p7e.p7m -nodetach -outform DER -signer
certificato_di_firma.pem
```

7. Segmento Unsecured: invio messaggi tramite canale alternativo (*contingency*)

Nei casi in cui il canale primario di comunicazione per l’invio dei messaggi sia indisponibile è prevista l’attivazione di una modalità di invio alternativa (c.d. *contingency*) con riferimento al segmento del mercato monetario non garantito (*unsecured*). Non è prevista una modalità di invio alternativa per gli altri segmenti del mercato.

La modalità di invio prevede che il file opportunamente crittografato e firmato digitalmente sia inviato tramite posta elettronica alla casella funzionale dedicata contingency_mmsr@bancaditalia.it. Le caratteristiche del file sono le medesime descritte nella sezione 2 e si ribadiscono di seguito per correntezza:

- il file deve essere crittografato e firmato;
- Il nome del file crittografato e firmato, con estensione “.zip.p7e.p7m”, deve seguire la stessa naming convention utilizzata per il file “plain” in esso contenuto, ovvero quella adottata per MMSR;
- eventuali file trasmessi che non rispettano tali caratteristiche non saranno utilizzati.

L’invio di file relativi a segmenti diversi da quello del segmento *unsecured* sarà ignorato.

L’oggetto della mail e/o il testo della stessa dovrà indicare il nome ovvero il codice ABI dell’ente segnalante e la data contabile a cui si riferiscono le transazioni; il segnalante non riceverà un feedback a seguito dell’invio in modalità *contingency*.

L’attivazione della modalità di invio descritta nel presente paragrafo è prevista al verificarsi di almeno una delle seguenti condizioni:

- almeno 5 tentativi di invocazione del canale A2A sono falliti (i tentativi di invocazione dovrebbero essere effettuati almeno con un intervallo di 10 minuti);
- non è stata ricevuta la notifica di protocollo.

A seguito dell’attivazione della modalità di *contingency*, il segnalante è invitato a ripetere il tentativo di invio ad intervalli regolari; infatti l’attivazione della misura di *contingency* non esonera i segnalanti dall’obbligo di inviare i dati appena possibile tramite il canale ordinario, anche al fine di ricevere eventuali comunicazioni di rilievo.