Allegato tecnico per il trasferimento dagli operatori telefonici al gestore del Registro pubblico delle opposizioni dei numeri fissi non presenti negli elenchi telefonici pubblici

Il presente allegato definisce le modalità tramite cui gli Operatori Fornitori comunicano al Gestore del RPO le numerazioni fisse non pubblicate negli elenchi telefonici, al fine della loro iscrizione di default nel RPO qualora non già iscritte, in accordo a quanto previsto dall'art. 7, comma 10, del decreto del Presidente della Repubblica 27 gennaio 2022, n. 26.

1. Definizione processo di trasferimento

Gli Operatori Fornitori devono registrarsi presso il Gestore del RPO al fine di poter inviare le numerazioni fisse non pubblicate negli elenchi telefonici, secondo il processo descritto in Figura 1.

Tale registrazione è distinta da quella effettuata per l'accesso ai servizi messi a disposizione dal Gestore del RPO per la consultazione del suddetto Registro ai fini della verifica dell'esercizio del diritto di opposizione.

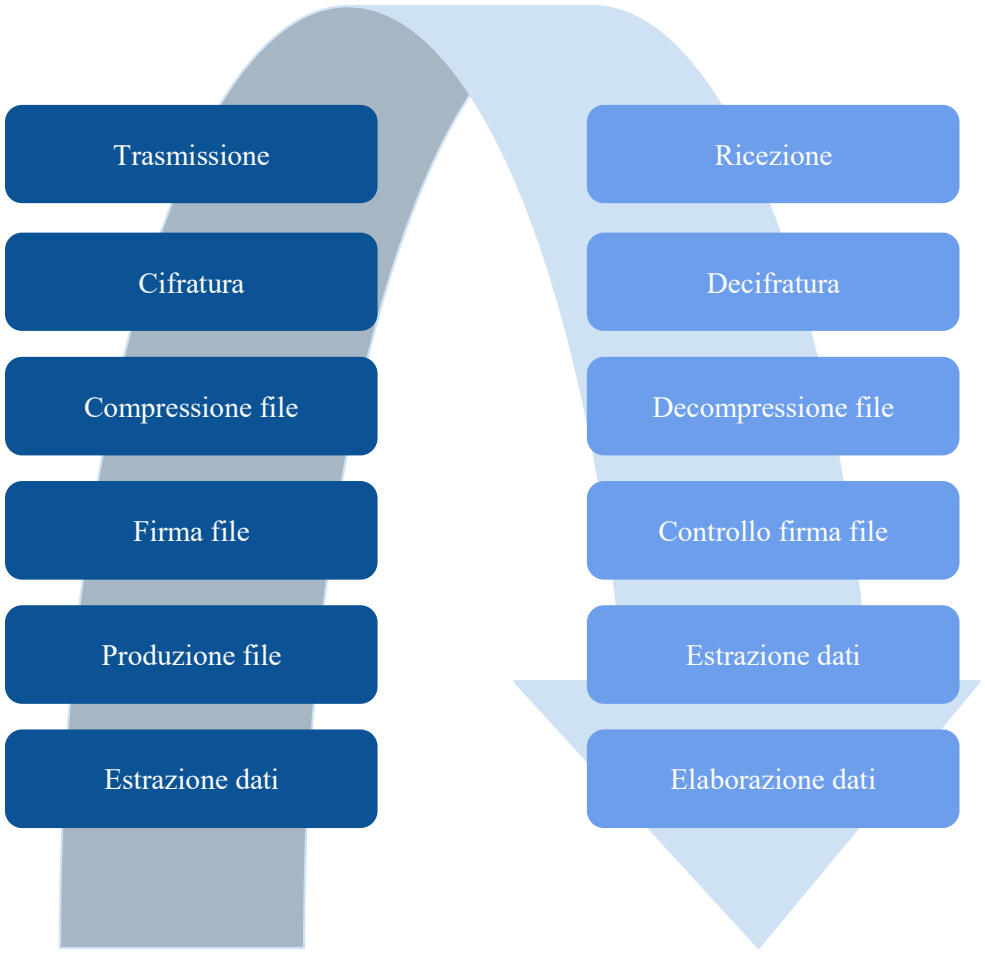

Figura 1 - Processo di produzione ed elaborazione dei file

Nel dettaglio, gli Operatori Fornitori devono svolgere le seguenti operazioni:

1. Estrazione dei dati;
2. Produzione del file di dati;
3. Firma del file di dati;
4. Compressione del file di dati;
5. Cifratura del file di dati;
6. Trasmissione del file di dati su canale cifrato;

7. Archiviazione del file trasmesso;
8. Gestione di eventuali errori.

Il Gestore del RPO, invece, deve svolgere le seguenti operazioni:

1. Realizzazione del web service per la trasmissione dei file di dati;
2. Gestione del web service per la trasmissione dei file di dati;
3. Ricezione del file di dati;
4. Decifratura del file di dati;
5. Decompressione del file di dati;
6. Controllo della firma del file di dati;
7. Estrazione dei dati dal file;
8. Segnalazione di eventuali errori;
9. Elaborazione dei dati;
10. Archiviazione dei dati e dei file.

Ogni Operatore Fornitore è responsabile dell'esattezza, della conformità e dell'integrità dei dati comunicati.

È fatto divieto al Gestore del RPO di modificare e/o cancellare i dati contenuti nei file inviati dagli Operatori Fornitori.

I file ricevuti dal Gestore del RPO sono conservati da quest'ultimo per ventiquattro mesi secondo criteri di completezza, integrità, inalterabilità e verificabilità. Tali file sono protetti dal Gestore del RPO contro l'accesso abusivo, in modo da consentire l'accesso ad essi solo per finalità ispettive da parte dell'Autorità per la protezione dei dati personali o dell'Autorità giudiziaria.

I file firmati inviati dagli Operatori Fornitori tramite il web service sono conservati da questi ultimi per almeno 30 giorni dalla sottomissione.

2. Processo di registrazione

Ogni Operatore Fornitore si registra presso il Gestore del RPO per la trasmissione delle numerazioni fisse non presenti negli elenchi telefonici.

La registrazione avviene mediante compilazione di apposito modulo digitale reso disponibile dal Gestore del RPO, in cui vengono indicati:

- dati societari dell'Operatore Fornitore;
- sigla dell'Operatore Fornitore[1];
- dati personali del riferimento tecnico:
    - nome;
    - cognome;
    - codice fiscale;
    - numero di telefono;
    - email;
- indirizzo di posta elettronica per la notifica di informazioni relative al servizio, compresi gli errori;
- fingerprint (SHA-256) del certificato di firma dei file di numerazioni.

Al termine del processo di registrazione, l'Operatore Fornitore riceverà un link di attivazione del web service per la trasmissione dei dati, nonché le istruzioni per la corretta configurazione dei sistemi e le credenziali RPO di accesso.

L'Operatore Fornitore che intende variare i dati forniti deve compilare apposito modulo digitale reso disponibile dal Gestore del RPO.

[1] Vedi documento *RU tracciato record e controlli (Tabella C)* degli allegati tecnici per la gestione del DBU

3. Soluzione tecnica

La soluzione tecnica prevede i seguenti punti fondamentali:

1. Una comunicazione sincrona (Request-Reply) tra la parte client e quella server;
2. Un protocollo di comunicazione sicuro per la comunicazione, specificamente HTTPS;
3. Un web server presso il Gestore del RPO in grado di accettare la richiesta HTTPS proveniente dai client degli Operatori Fornitori, espletare il servizio richiesto e infine restituire al client l'esito della richiesta;
4. Un web client presso ogni Operatore Fornitore in grado di effettuare le richieste HTTPS al web server del Gestore del RPO;
5. Un data server presso il Gestore del RPO che contiene i file che sono stati inviati al Gestore del RPO;
6. Un data server presso ogni Operatore Fornitore che contiene i file che sono stati inviati al Gestore del RPO.

Di seguito vengono elencati gli step funzionali per la trasmissione delle numerazioni fisse non pubblicate negli elenchi telefonici:

1. Estrazione: composizione da parte dell'Operatore Fornitore del file da inviare;
2. Trasporto: invio da parte dell'Operatore Fornitore del file;
3. Consegna: ricezione da parte del Gestore del RPO del file;
4. Gestione delle notifiche: procedure di gestione delle notifiche e delle anomalie attuate dal Gestore del RPO.

Di seguito vengono dettagliati i passi relativi a ogni punto.

Per quanto riguarda l'**estrazione**, l'Operatore Fornitore deve:

- predisporre, con cadenza predefinita, i dati definiti dal presente regolamento nel formato stabilito.

La dimensione massima del file da inviare per una certa data di competenza è pari a 15 MB. In caso il file eccedesse tale limite, l'Operatore Fornitore deve includere i dati in più file di dimensione minore di 15 MB.

Per quanto riguarda il **trasporto**, dopo aver composto il file di dati, l'Operatore Fornitore deve:

- accedere ad un web server opportunamente predisposto dal Gestore del RPO;

- certificare la sua identità per ogni richiesta HTTPS (tramite un certificato digitale e le credenziali di accesso);
- inviare il file di dati in base alla data di estrazione.

Il Gestore del RPO deve:

- verificare, per ogni richiesta, l'identità del soggetto che accede tramite la sua certificazione e permettere l'accesso al web service tramite HTTPS.

Per quanto riguarda la **consegna**, l'Operatore Fornitore deve:

- verificare che l'intero file sia stato inviato con esito positivo.

Il Gestore del RPO deve:

- tracciare l'operazione di ricezione del file di dati.

Per quanto riguarda la **gestione delle notifiche**, il Gestore del RPO deve:

- verificare la cifratura del file;
- verificare la validità della firma del file;
- verificare la conformità del file con il formato previsto;
- fornire una notifica in merito all'esito dell'invio.

L'Operatore Fornitore deve:

- verificare l'esito dell'invio;
- in caso di errori, predisporre un nuovo invio del file corretto.

I servizi realizzati con web service sono i seguenti:

- invio dei file;
- notifica dell'esito della trasmissione;
- verifica dell'esito della trasmissione di un file;
- elenco dei file trasmessi negli ultimi 3 mesi con relativo esito;
- aggiornamento del fingerprint del certificato di firma dei file di numerazioni, che dovrà essere firmato con il certificato di firma già comunicato.

È previsto un processo che operi secondo due modalità distinte:

- Modalità Automatica;
- Modalità Online (browser).

A seconda della modalità di accesso utilizzata, l'Operatore Fornitore deve disporre degli strumenti di autenticazione riportati in Tabella 1.

Modalità di accesso	Strumento autenticazione	Utilizzo	Specifiche
Automatica	Credenziali RPO	Obbligatorio	- Assegnate al termine del processo di registrazione dell'Operatore Fornitore
	Certificato lato client	Obbligatorio	- Certificato emesso da fornitore riconosciuto (vedi paragrafo *Sicurezza*) - I dati dell'Operatore Fornitore devono essere presenti nel certificato
Online (browser)	Credenziali RPO	Alternativo	- Assegnate al termine del processo di registrazione dell'Operatore Fornitore
	SPID		- L'identità SPID deve essere di tipo personale o professionale - Il codice fiscale contenuto nell'identità SPID deve essere quello del riferimento tecnico
	CIE		- Il codice fiscale contenuto nell'identità CIE deve essere quello del riferimento tecnico
	Certificato lato client	Obbligatorio	- Certificato emesso da fornitore riconosciuto (vedi paragrafo *Sicurezza*) - I dati dell'Operatore Fornitore devono essere presenti nel certificato

Tabella 1 - Strumenti di autenticazione al web service

Si evidenzia che per l'accesso al web service nella Modalità Automatica è necessario utilizzare sia il certificato digitale (che identifica l'Operatore Fornitore) sia le credenziali RPO (che identificano il riferimento tecnico), mentre nella modalità di accesso Online (browser) oltre a tale certificato digitale occorre utilizzare una delle seguenti modalità di autenticazione per il riferimento tecnico: credenziali RPO, SPID oppure CIE.

Di seguito si riportano gli step delle due modalità possibili per l'invio del file.

Modalità Automatica

1. Il client si autentica al web service presentando un opportuno certificato digitale e le credenziali RPO del riferimento tecnico;

2. Il client ottiene in risposta un token di autenticazione e un token di rinnovo;

3. Il client invia un form contenente il file richiesto, fornendo il token di autenticazione nell'header "Authorization" della richiesta HTTPS;

4. Il server risponde con l'esito del caricamento del file, fornendo un codice di errore nel caso il file non corrisponda ai limiti di grandezza e formato oppure un identificativo da utilizzare per verificare lo stato dell'elaborazione della lista inviata;

5. Il Gestore del RPO avvisa l'Operatore Fornitore tramite email circa la disponibilità dell'esito dell'invio;

6. Se necessario, il client rinnova il token di autenticazione oppure si autentica di nuovo al web service presentando un opportuno certificato digitale e le credenziali RPO del riferimento tecnico, ottenendo una nuova coppia di token;

7. Il client invia una richiesta al web service fornendo l'identificativo ottenuto durante il caricamento del file oppure richiedendo informazioni in merito ai file trasmessi negli ultimi 3 mesi per ottenere l'esito dell'operazione.

Modalità Online (browser)

1. Il client si autentica al web server presentando un opportuno certificato digitale e utilizza una tra le seguenti modalità di autenticazione: credenziali RPO, SPID oppure CIE;

2. Il web server risponde con una pagina nella quale presenta al client i servizi che rende disponibili;

3. In base al servizio selezionato dal client, il web server presenta una vista nella quale richiede al client di caricare il file da inviare;

4. A seguito del caricamento del file, il server risponde con l'esito dell'operazione, fornendo un codice di errore nel caso il file non corrisponda ai limiti di grandezza e formato oppure un link da utilizzare per verificare lo stato dell'elaborazione della lista inviata;

5. Il Gestore del RPO avvisa l'Operatore Fornitore tramite email circa la disponibilità dell'esito dell'invio;

6. Se necessario, il client si autentica di nuovo al web server presentando un opportuno certificato digitale e utilizza una tra le seguenti modalità di autenticazione: credenziali RPO, SPID oppure CIE.

7. Il web server risponde con una pagina nella quale presenta al client i servizi che rende disponibile;

8. In base al servizio selezionato dal client, il web server presenta l'esito dell'elaborazione del file inviato oppure un elenco dei file trasmessi negli ultimi 3 mesi con i relativi esiti.

4. Dati da inviare

Gli Operatori Fornitori sono tenuti a inviare al Gestore del RPO le numerazioni fisse attive dei contraenti telefonici con cui hanno un contratto in essere non pubblicate negli elenchi telefonici (non già comunicate in precedenza).

I dati personali diversi dal numero telefonico relativi agli intestatari delle numerazioni fisse non devono essere inviati.

Le numerazioni devono essere comunicate mediante il seguente formato: prefisso distrettuale e numero di telefono, come riportato in Tabella 2.

Dato	Formato
Numerazione completa (prefisso distrettuale e telefono)	Stringa numerica {4,13}

Tabella 2 - Struttura delle numerazioni

Ogni numerazione deve essere comunicata una volta sola all'interno dello stesso file.

Sono previste due modalità di estrazione dei dati:

1. Estrazione massiva (da effettuarsi per il primo invio);
2. Estrazione nuovi inserimenti decadali (da effettuarsi per gli invii successivi al primo).

La prima volta che un Operatore Fornitore effettua la comunicazione al Gestore del RPO deve effettuare un'estrazione massiva, inviando tutte le numerazioni telefoniche fisse attive della propria clientela (aggiornate al mese precedente all'invio) non pubblicate negli elenchi telefonici.

Le volte successive al primo invio il medesimo Operatore Fornitore deve effettuare un'estrazione dei nuovi inserimenti, comunicando al Gestore del RPO solamente le nuove numerazioni fisse attive della propria clientela non pubblicate negli elenchi telefonici alla data di riferimento, rispetto alle precedenti comunicazioni.

Per "*nuovi inserimenti*" si considerano:

- le nuove numerazioni fisse attivate rispetto alla precedente comunicazione che i titolari delle utenze hanno deciso di non pubblicare negli elenchi telefonici;
- le numerazioni fisse attive al momento delle precedenti comunicazioni i cui titolari dell'utenza hanno successivamente deciso di non pubblicare più negli elenchi telefonici;
- le numerazioni fisse attive non pubblicate negli elenchi telefonici che non sono state comunicate in precedenza.

In caso di portabilità di un numero, qualora necessario l'Operatore Fornitore che ha acquisito tale numerazione è tenuto a comunicarla al Gestore del RPO dopo aver completato l'eventuale scambio di informazioni previsto dal DBU con l'Operatore Fornitore cedente, in merito alla pubblicazione o meno di tale numerazione nel DBU stesso.

I giorni attesi di pubblicazione delle estrazioni decadali sono i primi tre giorni lavorativi a partire dai giorni 1, 11, 21 di ogni mese.

Ogni Operatore Fornitore deve garantire l'invio di un solo file logico per decade.

I file inviati possono avere dimensione massima pari a 15 MB. Se le numerazioni contenute nell'estrazione superano tale valore massimo, dovranno essere prodotti più file.

In caso di disservizio dei propri sistemi o di assenza di nuovi inserimenti, l'Operatore Fornitore deve inviare un insieme di numerazioni vuoto.

In casi straordinari, ad esempio di disservizio o per la verifica delle informazioni conservate, il Gestore del RPO può chiedere all'Operatore Fornitore l'estrazione massiva anche dopo il primo invio.

Al momento dell'invio del file l'Operatore Fornitore deve fornire i seguenti parametri relativi al file inviato:

- per le estrazioni massive
    - mese di competenza dell'estrazione massiva;
    - anno di competenza dell'estrazione massiva;
    - numero di file componenti l'estrazione massiva;
    - progressivo parziale dei file componenti l'estrazione massiva;
- per le estrazioni decadali
    - decade di riferimento (I, II, III);
    - mese di competenza dell'estrazione decadale;
    - anno di competenza dell'estrazione decadale;
    - numero di file decadali pubblicati per la giornata [in caso di file vuoto assumerà il valore 0];
    - cardinalità del file nell'insieme di quelli trasmessi nella giornata [In caso di file vuoto, il valore indicherà la causale per cui il file pubblicato è vuoto: il valore 0 indicherà che il file è vuoto per mancanza di variazioni nella giornata, il valore 1 espliciterà l'indisponibilità dell'Operatore Fornitore a fornire il file corretto].

5. Formato file

Le numerazioni fisse non pubblicate negli elenchi telefonici devono essere inserite in un file di testo ASCII (in formato TXT) rispettando le seguenti specifiche:

1. Ogni riga deve essere separata dalla sequenza di caratteri “0x0D” e “0x0A” (corrispondenti al “carriage return” e “line feed”);
2. La prima riga deve contenere la sola stringa “`----- BEGIN LIST -----`”;
3. L’ultima riga deve contenere la sola stringa “`----- END LIST -----`”;
4. Le numerazioni devono essere inserite, ognuna su una riga separata, all’interno dei separatori di cui ai punti 2 e 3;
5. Nel caso non ci siano numeri da inviare, il file conterrà solo la prima e ultima riga di cui ai punti 2 e 3;
6. I numeri devono contenere unicamente stringhe di caratteri numerici;
7. Il file deve essere firmato digitalmente in formato PKCS7 e successivamente compresso mediante l’algoritmo deflate[2] (IETF RFC1951).

La violazione di queste regole può comportare l’impossibilità di procedere correttamente con il servizio e una comunicazione di errore.

In analogia a quanto avviene per la gestione del DBU, il file di dati inviato dall’Operatore Fornitore viene salvato dal Gestore del RPO sui propri server, in funzione dei parametri di configurazione forniti, con la seguente struttura del nome:

- ***EstrazioneRPO***_*codOperatoreFornitore_AAAAMM_AAAAMMGG_T_L****.txt*** (primo invio);
- ***EstrazioneRPO***_*codOperatoreFornitore_AAAAMMX****DEC***_*AAAAMMGG_N_K****.txt*** (invii successivi al primo).

Le parti variabili del nome del file sono dettagliate in Tabella 3.

Codice	Descrizione
codOperatoreFornitore	Sigla dell’Operatore Fornitore[3].
AAAAMM	Anno e mese di competenza dell’estrazione massiva.
AAAAMMGG	Anno, mese e giorno di trasmissione dell’estrazione.

[2] Deflate64 non sarà supportato.
[3] Vedi documento *RU tracciato record e controlli (Tabella C)* degli allegati tecnici per la gestione del DBU.

AAAAMMX	Anno e mese di competenza dell'estrazione decadale. La X indica la decade di riferimento (I, II, III).
T	Totale di file componenti l'estrazione massiva.
L	Progressivo parziale dei file componenti l'estrazione massiva.
N	Totale di file decadali pubblicati per la giornata. In caso di file vuoto assume il valore 0.
K	Cardinalità del file nell'insieme di quelli trasmessi nella giornata. In caso di file vuoto, il valore di K indica la causale per cui il file pubblicato è vuoto: il valore 0 indica che il file è vuoto per mancanza di variazioni nella giornata, il valore 1 esplicita l'indisponibilità dell'Operatore Fornitore a fornire il file corretto.

Tabella 3 - Convenzione del nome del file salvato dal Gestore del RPO

6. Sicurezza

Al fine di garantire un elevato livello di sicurezza, i file inviati dagli Operatori Fornitori al Gestore del RPO tramite il web service devono utilizzare sistemi crittografici basati su certificati digitali.

Tramite tali certificati sono garantiti sia la riservatezza del canale di comunicazione tra client e server sia l'autenticazione di entrambe le parti.

Il certificato del web server documenta in modo inalterabile e verificabile l'associazione tra una chiave pubblica e l'identità del titolare che possiede la corrispondente chiave privata. La correttezza dei dati è garantita da parte dell'entità di certificazione che lo emette (Certification Authority).

Il server del web service fornisce il proprio certificato al client, in modo da dare garanzia di connessione all'applicazione del Gestore del RPO.

Il server del web service richiede al client oltre al suo certificato anche le credenziali RPO di accesso al servizio, nel caso di Modalità Automatica di accesso, oppure le credenziali RPO, SPID o CIE del riferimento tecnico, se si utilizza la Modalità Online (browser).

Nel caso di mutua autenticazione effettuata con successo può avvenire la trasmissione dei dati.

In Figura 2 sono riportate le operazioni da effettuare sul file prima dell'invio e al momento della ricezione.

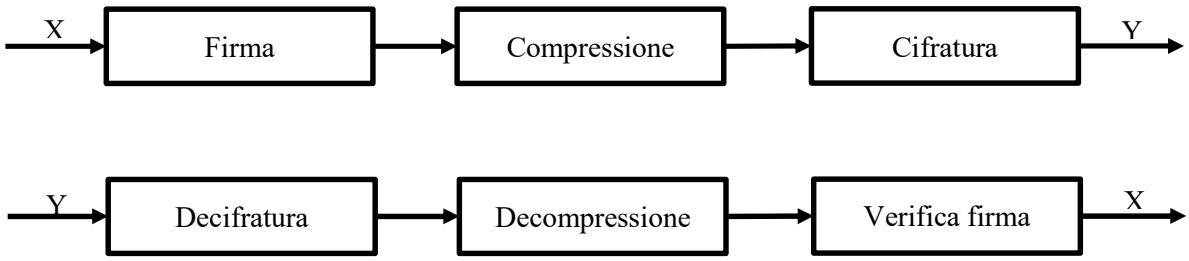

Figura 2 - Schema di riferimento delle misure di sicurezza

Per quanto riguarda la firma del file, ogni Operatore Fornitore deve essere dotato di certificato di firma adeguato, mentre il Gestore del RPO deve disporre del fingerprint del certificato per verificare la firma di ogni Operatore Fornitore.

Con riferimento alla compressione deve essere applicato l'algoritmo deflate[4] (IETF RFC 1951).

Con riferimento alla cifratura del canale, ogni Operatore Fornitore deve disporre della chiave pubblica del Gestore del RPO.

Ogni Operatore Fornitore deve acquistare un certificato X.509 necessario per l'autenticazione client verso il server del web service.

Il certificato X.509 (lato client) ha le seguenti caratteristiche:

1. Il certificato ha validità di un anno;
2. Il "Subject" del certificato è sempre il nome dell'Operatore Fornitore in qualità di organizzazione richiedente il certificato (non una persona fisica);
3. Le procedure di identificazione del richiedente e rilascio del certificato devono garantire l'identità dell'organizzazione richiedente (Operatore Fornitore), opzionalmente è consigliabile utilizzare certificati con Extended Validation;
4. In nessun caso sono utilizzabili i certificati che le CA rilasciano verificando l'esistenza del solo dominio senza effettuare controlli sull'organizzazione richiedente;
5. La lunghezza minima della coppia di chiavi RSA dovrà essere di 2048 bit;
6. L'algoritmo di cifratura dovrà essere di tipo SHA-256.

I file inviati dagli Operatori Fornitori al Gestore del RPO devono essere firmati digitalmente, compressi, cifrati e trasmessi mediante un canale cifrato, in modo da garantire autenticità, integrità, inalterabilità e riservatezza.

[4] Deflate64 non sarà supportato.

Per soddisfare il requisito della riservatezza e mutua autenticazione si dovrà:

- utilizzare il protocollo HTTPS con gli algoritmi di cifratura restituiti dalla versione di OpenSSL 1.1.1n con il comando: *openssl ciphers -V 'HIGH:!aNULL:!MD5'*;
- garantire, tramite l'utilizzo di una coppia di chiavi asimmetriche, l'operazione di mutua autenticazione, che dovrà avvenire in modo automatico a livello di macchine, tramite protocollo SSL del tipo TLS 1.0, TLS 1.1 o TLS 1.2.

Gli algoritmi di cifratura del canale potranno essere aggiornati dal Gestore del RPO.

L'Operatore Fornitore è tenuto a conservare il file firmato inviato tramite il web service per almeno 30 giorni dalla sottomissione.

Per la firma del file il Gestore del RPO deciderà se richiedere certificati qualificati emessi da una CA accreditata presso l'AgID. Alternativamente, in analogia a quanto avviene per la gestione del DBU, il Gestore del RPO e gli Operatori Fornitori potrebbero stabilire in un accordo per iscritto che la firma digitale con certificati acquisiti presso una CA pubblica garantisce l'integrità e il non ripudio del file inviato/ricevuto, riconoscendone la validità legale ai fini di un eventuale contenzioso.

Il certificato di firma digitale utilizzato per firmare il file contenente la lista deve essere valido (non deve essere scaduto o revocato) al momento dell'invio del file.

Il certificato per la firma digitale deve essere generato con chiavi RSA di lunghezza pari a 2048 bit e hash di tipo SHA-256. La firma deve essere generata con l'algoritmo di tipo SHA-256.

Il formato cui far riferimento per "l'imbustamento" dell'informazione che gli Operatori Fornitori dovranno inviare al Gestore del RPO sarà CMS come descritto nella RFC 3369 – "Cryptographic Message Syntax (CMS)".

Per quanto non specificato nel presente regolamento in merito al formato della firma, compressione e cifratura si fa riferimento alla documentazione tecnica inerente alla gestione del DBU e in particolare l'allegato 3.7 – DBU Specifiche funzionali.

7. Gestione dei file

Il Gestore del RPO preleva i file che sono stati inviati dagli Operatori Fornitori, effettuando le seguenti operazioni:

- decifratura;
- decompressione;
- verifica della firma;
- controllo di conformità del formato del file;
- estrazione dei dati contenuti nel file.

Se i controlli danno esito positivo e il file è formalmente corretto, il Gestore del RPO memorizza le informazioni, in vista della successiva elaborazione, e rende disponibile all'Operatore Fornitore titolare dei dati una notifica circa l'esito positivo della trasmissione.

Nel caso in cui i controlli di conformità sul file diano esito negativo, il Gestore non prende in carico l'inserimento delle numerazioni nel RPO Telefonico e rende disponibile all'Operatore Fornitore titolare dei dati una notifica circa l'esito negativo della trasmissione, riportando il problema riscontrato (vedi paragrafo *Gestione delle notifiche*).

Il Gestore del RPO rende disponibile all'Operatore Fornitore la notifica circa l'esito della trasmissione entro dieci giorni solari dalla ricezione del file.

L'Operatore Fornitore che riceve una notifica di errore provvede a ritrasmettere al Gestore del RPO il file corretto nel periodo di pubblicazione della decade successiva.

Sono considerate errore una serie di problematiche sul file che non consentono la fruizione in sicurezza delle informazioni ivi contenute. A titolo esemplificativo e non esaustivo, gli errori possono essere relativi alla cifratura, compressione, alla firma, al formato del file o dei dati.

Il Gestore del RPO deve memorizzare sia il file contenente l'eventuale errore sia il conseguente file corretto, mantenendo evidenza di quanto avvenuto nell'ambito della trasmissione delle numerazioni fisse non pubblicate negli elenchi telefonici.

In caso di ricezione di file inviati da parte dello stesso Operatore Fornitore con gli stessi parametri, il Gestore del RPO prenderà in carico le informazioni contenute nel file più recente, qualora il precedente file con i medesimi parametri non sia stato ancora elaborato.

8. Elaborazione dei dati

Il Gestore del RPO estrae dai file inviati in modo formalmente corretto dagli Operatori Fornitori le numerazioni telefoniche fisse.

Il Gestore del RPO iscrive di default nel RPO Telefonico le numerazioni telefoniche comunicate dagli Operatori Fornitori qualora non già iscritte.

Per tali numerazioni non viene inserita (caso di numeri mai iscritti) né modificata (caso di numeri precedentemente iscritti ma non allo stato attuale) la data di iscrizione nel RPO Telefonico, in modo da non annullare i consensi precedentemente rilasciati dal contraente telefonico.

Il Gestore del RPO è tenuto a inserire nel RPO Telefonico tutte le numerazioni contenute nei file inviati dagli Operatori Fornitori in modo formalmente corretto (qualora non già iscritte), anche nel caso in cui tali numerazioni risultino al Gestore del RPO presenti nel DBU.

I numeri comunicati dagli Operatori Fornitori sono iscritti nel RPO entro 30 giorni dalla data di ricezione del file.

Nel caso in cui l'Operatore Fornitore si renda conto di errori nei dati inviati lo deve comunicare prontamente al Gestore del RPO, il quale nel caso non avesse ancora inserito le numerazioni interessate dall'errore nel RPO Telefonico scarta il file contenente l'errore in attesa della nuova comunicazione da parte dell'Operatore Fornitore. Nel caso le numerazioni telefoniche interessate dall'errore fossero già state inserite nel RPO Telefonico, l'Operatore Fornitore informa i contraenti telefonici interessati riguardo all'errore e le numerazioni rimangono iscritte.

9. Gestione delle notifiche

Il Gestore del RPO fornisce all'Operatore Fornitore l'esito del caricamento del file in maniera sincrona (risposta HTTPS), mentre l'esito della completa trasmissione del file (con specifica dell'eventuale errore) viene comunicata tramite una richiesta successiva al web service.

Inoltre, il Gestore del RPO invia notifiche tramite email in merito alla disponibilità dell'esito della trasmissione dei file inviati, nonché sul funzionamento del web service.

Se si rende necessario un nuovo invio del file sottomesso dall'Operatore Fornitore, il Gestore del RPO invia apposita notifica all'Operatore interessato indicando il motivo della richiesta.

In seguito alla ricezione di una notifica di errore l'Operatore Fornitore è tenuto a verificare il problema, correggerlo e inviare nuovamente il file nel periodo di pubblicazione della decade successiva.

Gli Operatori Fornitori devono conservare i file inviati al Gestore del RPO per almeno 30 giorni dalla data di trasmissione.

Con riferimento all'indisponibilità del web service nonché a eventuali aggiornamenti il Gestore del RPO notifica a tutti gli Operatori Fornitori registrati le informazioni necessarie mediante l'apposito indirizzo di posta elettronica fornito.

Nel caso siano in programma modifiche tecniche e/o procedurali del web service, queste saranno notificate dal Gestore del RPO agli Operatori Fornitori interessati, con almeno trenta giorni solari di anticipo, mediante l'apposito indirizzo di posta elettronica fornito.

In caso di disservizio programmato del web service, il Gestore del RPO informa gli Operatori Fornitori tramite l'indirizzo di posta elettronica fornito almeno 3 giorni prima dell'inizio del disservizio. Al termine del periodo di disservizio, il Gestore del RPO notifica l'operatività del web service.

Se un Operatore Fornitore rileva un disservizio sul web service, informa prontamente il Gestore del RPO, che, qualora necessario, notifica l'indisponibilità temporanea del servizio a tutti gli Operatori Fornitori. Al termine del periodo di disservizio, il Gestore del RPO notifica l'operatività del web service.

Nel caso di disservizio da parte del web service e di mancata trasmissione del file, l'Operatore Fornitore invia, a sua discrezione, il file al Gestore del RPO nella decade successiva contenente i nuovi inserimenti rispetto alle precedenti comunicazioni.

Nel caso di disservizio da parte dell'Operatore Fornitore e di mancata estrazione, l'Operatore Fornitore deve inviare al Gestore del RPO un file vuoto nei giorni previsti per l'invio delle numerazioni. In questo caso l'Operatore Fornitore deve rendere disponibili i dati con l'invio del file nella decade successiva contenente i nuovi inserimenti rispetto alle precedenti comunicazioni.

Ogni Operatore Fornitore deve essere dotato di un indirizzo di posta elettronica, per le seguenti finalità:

- notifica della disponibilità dell'esito della trasmissione;
- notifica di informazioni relative al servizio.

Il Gestore del RPO rende disponibile agli Operatori Fornitori un indirizzo di posta elettronica al fine di supportarli nel corretto invio dei file.

Di seguito sono riportati gli errori.

Casistica	Codice	Descrizione
Formato del file non conforme	001	Il file non segue il formato specificato
Presenza di un record duplicato	002	Record duplicato
Separatore numeri non conforme	003	I numeri devono essere separate dalla sequenza di caratteri "0x0D" e "0x0A" (corrispondenti al "carriage return" e "line feed")
Errore del parsing di un singolo record	004	Record (riga) non leggibile
Uno o più numeri contengono caratteri non consentiti	005	Carattere non ammesso
Numero troppo corto	006	La lunghezza di un numero è più corta della lunghezza minima specificata
Numero troppo lungo	007	La lunghezza di un numero è più grande della lunghezza massima specificata
Un numero (riga) non è popolato	008	Campo vuoto
Un numero non è fisso	009	Il numero non è una numerazione fissa
File corrotto (errore trasmissivo o comunque file non integro)	901	File corrotto
Firma non valida	902	La verifica della firma è fallita
Cifratura del file non valida	903	Le decifratura del file è fallita
Certificato della firma non valido	904	Il certificato della firma non è stato trovato o non può essere validato
Il file non è leggibile (errore del parser TXT)	905	File illeggibile

Tabella 4 - Codici errore

10.Frequenza invio dati

A seguito dell'estrazione massiva, gli Operatori Fornitori sono tenuti a inviare al Gestore del RPO le numerazioni fisse non pubblicate negli elenchi telefonici con frequenza decadale.

La trasmissione delle estrazioni decadali avviene entro il terzo giorno lavorativo a partire dai giorni 1, 11, 21 di ogni mese. Ciò implica che qualora i giorni 1, 11 e 21 del mese fossero non lavorativi si considera il primo giorno lavorativo successivo per l'inizio dell'invio dei file.

Sono considerate tre decadi per mese indicate con I-II-III decade, dove nella:

1. I decade, i nuovi inserimenti (rispetto agli invii precedenti) di numerazioni telefoniche fisse non pubblicate negli elenchi telefonici occorse nei giorni 1-10 del mese x di riferimento sono trasmesse entro il terzo giorno lavorativo a partire dal giorno 11 del mese x (giorni attesi di pubblicazione);

2. II decade, i nuovi inserimenti (rispetto agli invii precedenti) occorsi nei giorni 11-20 del mese x di riferimento sono trasmesse entro il terzo giorno lavorativo a partire dal giorno 21 del mese x (giorni attesi di pubblicazione);

3. III decade: i nuovi inserimenti (rispetto agli invii precedenti) occorsi nei giorni 21-ultimo giorno del mese x di riferimento sono trasmesse entro il terzo giorno lavorativo a partire dal giorno 1 del mese x+1 (giorni attesi di pubblicazione).

La trasmissione delle estrazioni decadali deve avvenire (a meno di disservizi) entro il giorno stabilito.

I giorni non lavorativi sono sabato, domenica e le festività nazionali.

11.Reportistica

Il Gestore del RPO produce annualmente un report relativo all'invio delle numerazioni fisse da parte degli Operatori Fornitori, indicando eventuali errori, omissioni e numero di invii vuoti per disservizio del fornitore.

Il rapporto prodotto viene condiviso con il MiSE, l'AGCOM e l'Autorità Garante per la protezione dei dati personali.