PROCEDURA AGGIORNAMENTO LISTE MEDIANTE L'INTERFACCIA WEB

Precondizioni

Per poter eseguire i passi previsti da questa procedura è necessario che:

- l'operatore (di seguito OP) abbia presentato l'istanza presso il Gestore del Registro delle Opposizioni (di seguito GRO) e abbia completato la relativa procedura;
- la persona indicata come responsabile dell'invio delle liste (anche riferito come profilo tecnico) abbia un ***certificato digitale individuale*** emesso da una autorità di certificazione riconosciuta (vedi in Appendice A i certificati riconosciuti) ***contenente le stesse informazioni comunicate nell'istanza (l'indirizzo di casella di posta elettronica, nome e cognome)***;
- la persona indicata come responsabile dell'invio delle liste sia entrata in possesso della password (composta dalle due stringhe di 6 caratteri scambiate tra OP e GRO durante la procedura di presentazione dell'istanza).

Dettaglio della procedura

Passo 1 – Connessione https

OP esegue una connessione HTTPS all'area riservata di OP sul sito web del GRO (url https://operatori.registrodelleopposizioni.it/operatori/area-riservata). La connessione prevede l'autenticazione del client mediante certificato digitale individuale riconosciuto (vedi in Appendice A i certificatori riconosciuti), e del server web mediante certificato digitale rilasciato da Terena SSL CA riconosciuta tramite l'autorità di certificazione Comodo CA dai principali browser in commercio (v. Appendice A per la lista dei browser supportati). Il certificato del server web è acquistato dal Gestore, mentre il certificato per l'autenticazione del client deve essere acquistato da OP. Riservatezza e integrità dei dati scambiati durante questa operazione saranno protette mediante algoritmi crittografici (v. Appendice A per l'indicazione degli algoritmi crittografici) supportati dalle versioni ad oggi disponibili dei suddetti browser web.

Passo 2 - Login

OP Fornisce nome utente (indirizzo di posta elettronica) e password relativi ad un responsabile dell'invio delle liste (responsabile tecnico) e seleziona "tecnico" nel campo "profilo utente"

Passo 3 – Invio elenco

OP invia tramite apposito form web, che realizza il metodo POST del protocollo HTTP, il file elenco da aggiornare secondo un formato da stabilito. Il file inviati (anche interni all'archivio zip) devono avere un nome che inizia con una lettera minuscola, lungo al massimo 100 caratteri comprendenti

l'estensione, e può contenere numeri lettere maiuscole e minuscole e i seguenti simboli: '.', '-', '_'. La violazione di queste regole può comportare l'impossibilità di procedere con il servizio e una comunicazione di errore attraverso messaggio di posta elettronica. Il file inviato deve essere un archivio compresso (mediante l'algoritmo *deflate* (IETF RFC1951)) con all'interno un unico file di testo ASCII contenente sequenze di cifre decimali terminate da sequenze di caratteri corrispondenti al "*carriage return*" e "*line feed*". Il file di testo non deve contenere altri caratteri oltre quelli specificati.

La dimensione minima di un singolo elenco sottoposto a verifica e/o ad aggiornamento è di una numerazione telefonica. La dimensione massima di un singolo elenco sottoposto a verifica e/o ad aggiornamento è di 1.000.000 (un milione) di numerazioni telefoniche (vedi art.3.9 delle Condizioni Generali di Contratto).

Il numero massimo giornaliero di singoli elenchi sottoposti ad aggiornamento da parte di ogni singolo Operatore è pari a 5. È possibile nello stesso giorno richiedere l'aggiornamento di un numero superiore di elenchi, fino a un massimo di 15 richieste, purché ciascuna delle prime 5 richieste contenga non meno di 900.000 numerazioni telefoniche e vi sia la necessità, per il singolo Operatore, di procedere in un unico giorno all'aggiornamento di una quantità complessiva di numerazioni telefoniche superiore a 5.000.000 (cinque milioni) (vedi art. 3.10 delle Condizioni Generali di Contratto).

Passo 4 – Marcatura temporale

GRO marca temporalmente il file ricevuto (auto marcatura temporale). Questa auto marcatura temporale consiste nella firma elettronica da parte di GRO di un file contenente almeno il riferimento temporale e l'impronta digitale (hash) della richiesta. La firma elettronica del GRO sarà in formato PKCS7. Il GRO si riserva la possibilità di utilizzare per la suddetta firma un certificato digitale individuale rilasciato da Trust Italia in caso di problemi nell'utilizzo della firma digitale remota con procedura automatica.

Passo 5 – Presa in carico della richiesta

GRO fornisce risposta di presa in carico via e-mail o PEC (dall'indirizzo e-mail GRO liste.rpo@fub.it o dall'indirizzo PEC registrodelleopposizioni@postecert.it) contenente marcatura temporale come definita al passo 4 (su t0 - riferimento temporale generato dal GRO).

Passo 6 – Elaborazione della richiesta

GRO elabora la richiesta entro le 24 ore.
In caso impossibilità di ottemperare alla richiesta, GRO invia tramite posta elettronica comunicazione a OP.

Passo 7 – Pubblicazione del link a scadenza

GRO mette a disposizione, a scadenza, nell'area privata di OP sul sito web, un archivio compresso mediante l'algoritmo *deflate* (IETF RFC1951,) contenete i seguenti file:

i. Elenco aggiornato nel formato specificato: file di testo ASCII contenente numerazioni telefoniche separate dai codici ASCII "0x0D" e "0x0A".
ii. File di testo contenente almeno
    1. impronta digitale della richiesta
    2. quantità di numerazioni presenti nella richiesta
    3. credito residuo
    4. la marcatura temporale.

Indipendentemente dall'ordine con cui sono fornite nella lista originale, per motivi di efficienza di elaborazione, le stringhe di numerazioni contenute nella lista aggiornata sono elencate in ordine alfabetico crescente,
I numeri contenuti nella lista aggiornata sono contattabili solo se i numeri della lista inviata dall'operatore sono presenti negli elenchi pubblici aggiornati.

Passo 8 – Notifica della pubblicazione del link a scadenza

GRO invia un messaggio email o PEC a OP con i dati di riepilogo dell'avvenuta operazione di aggiornamento della lista sottomessa (data dell'elaborazione, esito dell'operazione, nome del file restituito e impronta digitale del file stesso, credito residuo dopo l'operazione di aggiornamento). Il GRO si riserva la possibilità di firmare le notifiche utilizzando un certificato digitale individuale rilasciato da Trust Italia in caso di problemi nell'utilizzo della firma digitale remota con procedura automatica.

PROCEDURA AGGIORNAMENTO LISTE MEDIANTE PEC E FIRMA DIGITALE

Precondizioni

Per poter eseguire i passi previsti da questa procedura è necessario che:

- OP abbia presentato l'istanza presso il GRO e abbia completato la relativa procedura;
- abbia indicato come responsabile dell'invio delle liste una persona dotata di casella di PEC ed abbia indicato tale casella durante la procedura di presentazione dell'istanza;
- la persona indicata come responsabile dell'invio delle liste disponga della firma digitale con valore legale intestata a se stesso;

Dettaglio della procedura

Passo 1 - Richiesta di aggiornamento elenco

[OP] invia a GRO tramite PEC all'indirizzo registrodelleopposizioni@postecert.it (dall'indirizzo di casella PEC del responsabile dell'invio della lista (responsabile tecnico) comunicata durante la presentazione dell'istanza) la lista da aggiornare (file di testo ASCII contente unicamente stringhe di caratteri numerici separate dalla sequenza di caratteri "0x0D" e "0x0A" corrispondenti al "carriage return" e "line feed") compressa mediante l'algoritmo deflate (IETF RFC1951) e firmata digitalmente in formato PKCS7. I file inviati (anche interni all'archivio zip o PKCS7) devono avere un nome che inizia con una lettera minuscola, lungo al massimo 40 caratteri comprendenti l'estensione e può contenere numeri lettere maiuscole e minuscole e i seguenti simboli: '.', '-', '_'. La violazione di queste regole può comportare l'impossibilità di procedere con il servizio e una comunicazione di errore attraverso messaggio PEC.

Il file firmato digitalmente, allegato al messaggio PEC, deve avere una dimensione inferiore ai 15 MB.
Il certificato di firma digitale utilizzato per firmare il file compresso contenente la lista deve essere valido (non deve essere scaduto o revocato) al momento dell'invio del messaggio PEC.

Ogni messaggio PEC deve contenere solamente una lista da aggiornare. Nel caso in cui siano presenti più archivi di tipo PKCS7 allegati al messaggio PEC, il sistema restituirà un'errore del tipo "Il messaggio PEC contiene piu' di un allegato - impossibile procedere con l'elaborazione". Nel caso in cui oltre all'archivio di tipo PKCS7 contenente la lista siano presenti altri file allegati (ma non di tipo PKCS7) il sistema prenderà in carico ed elaborerà unicamente l'archivio PKCS7 firmato digitalmente.

La dimensione minima di un singolo elenco sottoposto a verifica e/o ad aggiornamento è di una numerazione telefonica. La dimensione massima di un singolo elenco sottoposto a verifica e/o ad

aggiornamento è di 1.000.000 (un milione) di numerazioni telefoniche (vedi art.3.9 delle Condizioni Generali di Contratto).

Il numero massimo giornaliero di singoli elenchi sottoposti ad aggiornamento da parte di ogni singolo Operatore è pari a 5. È possibile nello stesso giorno richiedere l'aggiornamento di un numero superiore di elenchi, fino a un massimo di 15 richieste, purché ciascuna delle prime 5 richieste contenga non meno di 900.000 numerazioni telefoniche e vi sia la necessità, per il singolo Operatore, di procedere in un unico giorno all'aggiornamento di una quantità complessiva di numerazioni telefoniche superiore a 5.000.000 (cinque milioni) (vedi art. 3.10 delle Condizioni Generali di Contratto).

Passo 2 – Elaborazione richiesta

[GRO] elabora la richiesta entro le 24 ore. In caso impossibilità di ottemperare alla richiesta, GRO invia opportuna comunicazione a OP tramite PEC dall'indirizzo registrodelleopposizioni@postecert.it indicante il problema emerso (es. credito esaurito, problema tecnico, casella PEC non abilitata, ecc.).
N.B.: GRO e OP convengono sul fatto che la ricevuta di consegna è equivalente alla ricezione da parte del destinatario.

Passo 3 – Restituzione elenco aggiornato

[GRO] invia a OP tramite PEC dall'indirizzo registrodelleopposizioni@postecert.it la lista aggiornata (file di testo ASCII contente unicamente stringhe di caratteri numerici separate dalla sequenza di caratteri "*0x0D*" e "*0x0A*" corrispondenti al "*carriage return*" e "*line feed*") e un file di testo contenente alcuni dati relativi alla richiesta e il credito residuo, all'interno di un archivio compresso mediante l'algoritmo *deflate* (IETF RFC1951). L'archivio così ottenuto è firmato elettronicamente con il formato PKCS7. Il GRO si riserva la possibilità di firmare le liste aggiornate utilizzando un certificato digitale individuale rilasciato da Trust Italia in caso di problemi nell'utilizzo della firma digitale remota con procedura automatica.
Indipendentemente dall'ordine con cui sono fornite nella lista originale, per motivi di efficienza di elaborazione, le stringhe di numerazioni contenute nella lista aggiornata sono elencate in ordine alfabetico crescente,
I numeri contenuti nella lista aggiornata sono contattabili solo se i numeri della lista inviata dall'operatore sono presenti negli elenchi pubblici aggiornati.

Appendice A

Enti certificatori e certificati riconosciuti per l'autenticazione durante l'accesso all'area riservata.

Trust Italia S.p.A. Certificati individuali di classe 2:

- /C=IT/O=Trust Italia S.p.A./OU=VeriSign Trust Network/OU=Terms of use at https://www.trustitalia.it/rpa (c)10/CN=Trust Italia Class 2 Consumer Individual Subscriber CA - G2

Infocert SpA:

- /C=IT/O=INFOCERT SPA/serialNumber=07945211006/OU=Ente Certificatore/CN=InfoCert Servizi di Certificazione

- /C=IT/O=INFOCERT SPA/OU=Ente Certificatore/serialNumber=07945211006/CN=InfoCert Servizi di Certificazione 2

ArubaPEC S.p.A.

- /C=IT/O=ArubaPEC S.p.A./OU=Certification Authority/CN=ArubaPEC S.p.A. NG CA 1

- /C=IT/O=ArubaPEC S.p.A./OU=Certification AuthorityC/CN=ArubaPEC S.p.A. NG CA 3

- /C=IT/O=ArubaPEC S.p.A./OU=Certification AuthorityB/CN=ArubaPEC S.p.A. NG CA 2

Lista dei Browser supportati

I seguenti browser sono supportati dall'applicazione web:

- Internet Explorer 7+,
- Mozilla Firefox 3.6+,
- Google Chrome 8.0+,
- Safari,
- Opera

Si raccomanda di installare gli aggiornamenti di sicurezza del sistema operativo utilizzato per evitare malfunzionamenti durante l'accesso.

Elenco degli algoritmi crittografici supportati

Il sistema supporta almeno i seguenti algoritmi crittografici:

Nome	Protocollo	Scambio chiavi	Autenticazione	Cifratura	MAC
DES-CBC3-SHA	SSLv3	RSA	RSA	3DES(168)	SHA1
IDEA-CBC-SHA	SSLv3	RSA	RSA	IDEA(128)	SHA1
RC4-SHA	SSLv3	RSA	RSA	RC4(128)	SHA1
RC4-MD5	SSLv3	RSA	RSA	RC4(128)	MD5
EDH-RSA-DES-CBC3-SHA	SSLv3	DH	RSA	3DES(168)	SHA1
EDH-DSS-DES-CBC3-SHA	SSLv3	DH	DSS	3DES(168)	SHA1