PROCEDURE FOR UPDATING LISTS THROUGH WEB INTERFACE

Prerequisites

In order to be able to follow the steps of the present procedure:

- the Operator (hereafter OP) must have presented the application to the Administrator of Registro Pubblico delle Opposizioni (hereafter ARPO) and must have completed the relevant procedure
- the person in charge of submission of telephone number lists for verification (also referred to as technical profile) must have a ***personal digital certificate*** issued by a recognised certification authority (see Appendix A for recognised certificates) ***stating the same information recorded in the application (email address, name and surname)***
- the person in charge of submission of telephone number lists must be in possession of the password (formed by the two password portions transmitted by the OP and the ARPO during the application submission procedure – each password portion is 6 characters long).

Procedure

Step 1 – Https connection

The OP runs an HTTPS connection to the restricted area on the ARPO website (URL https://operatori.registrodelleopposizioni.it/operatori/area-riservata**).** When connecting to the system, a client authentication process is actuated using a recognised certificate (see Appendix A for recognised certificates). At the same time a web server authentication process is actuated using a digital certificate issued by Terena SSL CA, that is recognized under the certificate authority Comodo CA by the main browsers on the market (see Addendum A for the list of supported browsers). The web server certificate is provided by the ARPO, whereas the certificate for the client authentication must be purchased by the OP.
The integrity and privacy of the data exchanged during this procedure will be ensured through cryptographic algorithms (see Addendum A for the list of cryptographic algorithms) supported by the currently available versions of the above-mentioned browsers.

Step 2 – Login

After selecting "technical" in the field "user profile", the OP enters email address and password of the person in charge of the lists transmission.

Step 3 – Lists transmission

The OP sends the file of the list to be updated (fixed format) through web form, the POST method of the HTTP protocol is employed. File name of transmitted files (including zipped files) can be 100 characters long as a maximum (including the extension), must start with a lowercase letter and can include numbers, uppercase letters, lowercase letters and the following special characters '.', '-', '_'. Not

complying with these conditions can result in a failure of the procedure and in an error notification by email. The transmitted file must be a compressed archive (through the *deflate* algorithm (IETF RFC1951)) formed by a single ASCII-only text file containing sequences of decimal numbers separated by sequences of characters corresponding to the "carriage return" and the "line feed". The text file must not contain any other character apart from the required ones.

A single list to be verified and/or updated must contain at least one telephone number and no more than 1,000,000 (a million) telephone numbers (see art.3.9 of General terms and conditions).

Each Operator can submit up to a maximum of 5 lists to be updated every day. It is possible to request a greater number of lists to be updated in the same day, as long as each of the first 5 requests contains not less than 900,000 telephone numbers and it is necessity for the operator to process more than 5,000.000 (five million) telephone numbers in a single day (see art.3.9 of General terms and conditions).

Step 4 – Timestamp

The ARPO records the timestamp of the file received (automatic timestamp). This auto timestamp consists of the ARPO's electronic signature of a file containing at least the time and fingerprint (hash function) of the request. The GRO electronic signature will be in the PKCS7 format. The ARPO may sign using a digital individual certificate issued by Trust Italia in case of problems in using the remote digital signature with automatic procedure.

Step 5 – Confirmation of request review

The ARPO confirms by email or certified email that the request has been reviewed (notification comes from the ARPO email address liste.rpo@fub.it or from the certified email address registrodelleopposizioni@postecert.it). Notification contains timestamp as per step 4 (with t0 – timestamp generated by the ARPO.

Step 6 – Request processing

The ARPO processes the request within 24 hours.
If the request cannot be fulfilled, the ARPO sends a notification by electronic mail to the OP.

Step 7 – Temporary link release

The ARPO releases in the OP's restricted area on the website, a temporary archive compressed through the *deflate* algorithm (IETF RFC1951), containing the following files:

- Updated list in the specified format: ASCII-only text file containing telephone numbers separated by the ASCII codes "0x0D" and "0x0A".
- Text file containing at least
  - request fingerprint
  - quantity of telephone numbers in the request
  - credit balance
  - timestamp

Regardless of the order in which they are provided in the original list, the number strings contained in the updated list are listed in ascending alphabetical order for processing efficiency reasons.
The telephone numbers contained in the updated list can be used only if present in the latest public telephone directories.

Step 8 – Notification of the temporary link release

The ARPO sends a digitally signed email or certified email message to the OP containing summary data regarding the update operation of the submitted list (date and time of processing, result of the operation, the name of the returned file and the fingerprint of the file itself, remaining credit after the update operation). The ARPO may sign notifications using a digital individual certificate issued by Trust Italia in case of problems in using the remote digital signature with automatic procedure..

PROCEDURE FOR THE LISTS UPDATE THROUGH CERTIFIED EMAIL AND DIGITAL SIGNATURE

Prerequisites

In order to be able to follow the steps of the present procedure:

- The OP must have presented the application to the ARPO and must have completed the relevant procedure;
- The person in charge of the lists transmission must be provided with a certified email address and this certified email address must have been recorded at the time of the application submission;
- The person in charge of the lists transmission must also be provided with a personal digital signature with legal validity;

Procedure

Step 1 – List update request

The OP sends to the ARPO the file of the list to be updated (from the certified email of the technical manager in charge of the lists transmission recorded at the time of registration to registrodelleopposizioni@postecert.it). The transmitted file must be a compressed archive (through the *deflate* algorithm (IETF RFC1951)) formed by an ASCII text file containing strings of numbers separated by the characters sequences "0x0D" and "0x0A" corresponding to the "carriage return" and the "line feed" and digitally signed through the PKCS7 format. File name of transmitted files (including zipped ones or PKCS7 files) can be 40 characters long as a maximum (including the extension), must start with a lowercase letter and can include numbers, uppercase letters, lowercase letters and the following special characters '.', '-', '_'. Not complying with conditions can result in a failure of the procedure and in an error notification by PEC message.

The PKCS7 file, attached to the PEC message, must have a size of less than 15 MB.

The digital certificate used to sign the compressed file containing the list must be valid (it must not be expired or revoked) at the moment when the certified e-mail message is sent.

Each certified email message (PEC) must contain only one list to update. If there are more PKCS7 files attached to the PEC message, the system will generate an error message such as "the PEC message contains more than one attachment – impossible to process". If other files are attached, in addition to the PKCS7 file containing the list (but not PKCS7 files) the system will process only the digitally signed PKCS7 file.

A single list to be verified and/or updated must contain at least one telephone number and no more than 1,000,000 (a million) telephone numbers (see art.3.9 of General terms and conditions).

Each Operator can submit up to a maximum of 5 lists to be updated every day. It is possible to request a greater number of lists to be updated in the same day, as long as each of the first 5 requests contains not less than 900,000 telephone numbers and it is necessity for the operator to process more than 5,000.000 (five million) telephone numbers in a single day (see art.3.9 of General terms and conditions).

Step 2 – Request processing

The ARPO processes the request within 24 hours.
If the request cannot be fulfilled, the ARPO sends a certified email notification (from registrodelleopposizioni@postecert.it) to the OP, stating the detected problem (e.g. the OP has run out of credit, there is a technical problem, the certified email has not been enabled, etc.)
N.B.: The ARPO and the OP both agree that the proof of delivery corresponds to all intents and purposes to the receipt by the addressee.

Step 3 – Updated list return

The OP receives by certified email (from registrodelleopposizioni@postecert.it) the updated list (ASCII text file containing strings of numbers separated by the characters sequences "0x0D" and "0x0A" corresponding to the "carriage return" and the "line feed") plus a text file containing some of the details of the request and the indication of the credit balance inside an archive compressed through the *deflate* algorithm (IETF RFC1951). The above-mentioned archive is electronically signed through the PKCS7 format. The ARPO may sign notifications using a digital individual certificate issued by Trust Italia in case of problems in using the remote digital signature with automatic procedure.
Regardless of the order in which they are provided in the original list, the number strings contained in the updated list are listed in ascending alphabetical order for processing efficiency reasons.
The telephone numbers contained in the updated list can be used only if present in the latest public telephone directories.

Addendum A

Certifying bodies and recognised certificates of authentication during access to the secure area

Trust Italia S.p.A. Class 2 individual certificates:

- /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

List of supported Browsers

The following browsers are supported by the web application:

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

Please install the latest security updates for the operating system in use in order to avoid malfunctions when logging in.

List of supported cryptographic algorithms

The system supports at least the following cryptographic algorithms:

Name	Protocol	Key exchange	Authentication	Cypher	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

The original of this document, written in Italian, is the only official version. Any translations are provided solely for the convenience of the user / operator and have no legal significance