DEFINITION OF COMMUNICATION METHODS

OP_EMAIL_RRR Method

In order to employ this method, the Operator [OP] must communicate with the Administrator of the "Registro Pubblico delle Opposizioni" [ARPO] by:

- personal email
  N.B. the OP must accept and underwrite the responsibility to be the only person to access this electronic mailbox
- traditional mail
- physical mail with return receipt requested (Raccomandata R.R.)

OP_CERTIFIED EMAIL_ESIG Method

In order to employ this method, the OP must:

- communicate with the ARPO by certified email
  N.B. the OP must accept and underwrite the responsibility to be the only person to access this certified electronic mailbox (not necessarily the certified email used for the communication of the lists)
- undersign electronic documents with a personal digital signature with legal validity

WEB-BASED PASSWORD CHANGE PROCEDURE

Step 1 – Login to restricted area

At the URL https://operatori.registrodelleopposizioni.it/operatori/area-riservata the OP can login to the restricted area and then change the password by clicking on the relevant link on the main page. If the OP has more than one profile, the above-mentioned procedure will modify only the password of the profile in use at the moment. When connecting to this URL, a 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 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 – Password change

The OP enters current password, new password and confirms new password . New password must be 12 characters long and must include at least 2 uppercase letters, at least 2 lowercase letters and at least 3 numbers.

Step 3 – Log out

At the end of the operations, the OP must log out clicking on the relevant text box (or link).

NEW PASSWORD REQUEST PROCEDURE BY OP_EMAIL_RRR METHOD

Step 1 – First portion of password request

The OP sends a password change request – undersigned with handwritten signature by the legal representative or by a person with power of attorney – by physical mail with return receipt requested to the address

GESTORE DEL REGISTRO PUBBLICO DELLE OPPOSIZIONI – OPERATORI
UFFICIO ROMA NOMENTANO
CASELLA POSTALE 7210
00162 ROMA RM

The request must be submitted through the relevant form, published on the web site of the ARPO, that the OP must compile entering the first 6 characters of the new password.

Step 2 – Second portion of password transmission

The ARPO contacts the OP by phone call (using the provided contacts) and provides the OP with the second portion of the password (last 6 characters).

NEW PASSWORD REQUEST PROCEDURE BY OP_CERTIFIED EMAIL_ESIG METHOD

Step 1 – First portion of password request

The OP sends a password change request – with digital signature with legal validity by the legal representative or by a person with power of attorney – from the certified electronic mailbox used to administrate the application to istanza.rpo@postecert.it. The request must be submitted through the relevant PDF form published on the web site of the ARPO, that the OP must compile entering the first 6 characters of the new password.

Step 2 – Second portion of password transmission

The ARPO contacts the OP by phone call (using the provided contacts) and provides the OP with the second portion of the password (last 6 characters).

ADDENDUM A

Certifying bodies and recognised authentication certificates to access to the restricted area

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

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

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

Password strength requirements

The password cannot be a dictionary word and must be at least 6 characters long and include
- at least 1 lowercase letter
- at least 1 uppercase letter
- at least 1 number
- it is possible to use the following special characters:
    o ! (exclamative mark)
    o $ (dollar sign)
    o ? (question mark)
    o - (minus sign)
    o _ (underscore)
    o @ (at sign)
- Please avoid the use of: capital "I" and "O", lowercase "L", numbers "1" and "0" as they could create ambiguity when entering the password