

CERTIFIED EMAIL (PEC)
Operating Manual

Ver. 2.4 of 15/02/2022

Prepared by:	Massimo Barbero Pini *Enterprise Architect*	_____	15/02/2022
Verified by:	Fabrizio Amodio *PEC Service Manager*	_____	15/02/2022
Approved by:	Simone Staffa Guidi *Chair and Chief Executive Officer*	_____	22/02/2022

CONTENTS

1 General information 4
1.1 Purpose of the document..... 4
1.2 Name of the document..... 4
1.3 Responsibility for the Operating Manual 4
1.4 Updating of the Operating Manual 4
1.5 Availability of the Operating Manual 4
1.6 Version of the Operating Manual 5
1.7 Identification data of the Provider 7
1.8 Quality Certification 7
2 Technical and legislative references 8
2.1 Legislative references 8
2.2 Technological standards 10
2.3 Definitions 11
2.4 Technical terms 19
3 General description of the PEC service 22
3.1 Operation of the service 22
3.2 Operation in the event of delivery problems 24
3.3 Operation in the event of viruses 24
3.4 Receipt of ordinary email 25
3.5 Features of the receipts and of the transport envelopes 25
3.5.1 Electronic signature of receipts and transport envelopes 25
3.5.2 Time reference 26
3.5.3 Types of delivery receipts 26
4 Description of the TWT PEC service..... 28
4.1 Types of service 28
4.2 Offer arrangements 29
5 Methods of access to the service 30
5.1 Password 30
5.2 Standard access / Webmail 31
5.3 Protocols 31
5.4 Configuration of the email client. 32
5.4.1 Microsoft Outlook client configuration with POP3S. 33
5.5 Message Logs 42
5.5.1 Request for logs by the holder 42
6 Conditions of supply 44
6.1 Introduction 44
6.2 Obligations and responsibilities 45
6.2.1 Parties to the Service 45
6.2.2 Activities and obligations of the Provider..... 45
6.2.3 Exclusions, Limitation and insurance policy 47

6.2.4 Obligations of the HOLDER 48
7 Service levels 50
7.1 Quality indicators 51
8 Technological systems / infrastructures..... 52
8.1 System 52
8.1.1 Structure 52
8.1.2 Scalability 54
8.1.3 IT Security 54
8.1.4 Reliability and fault-tolerance 54
8.2 System logs 55
8.2.1 Logs on File 56
8.2.2 Logs on Database 56
8.2.3 Archiving 56
8.2.4 Querying 56
8.3 Data security 57
8.3.1 Data backup 57
8.3.2 Data restore 57
8.4 Monitoring 57
8.5 Time Stamping 60
8.6 Interoperability 60
8.7 Description of the data centre 60
9 Operational Aspects 62
9.1 Notes on staff organisation 62
9.2 Organisational Flow 63
9.3 Support Management Procedures 63
9.4 Emergency management 65
10 Protection of personal data (Privacy) 66
10.1 Security measures to protect personal data 68

1 General information

1.1 Purpose of the document

This document is intended to describe the rules and procedures followed by TWT S.p.A. in providing the Certified Email (PEC) service.

The manual is based on the technical provisions of the Ministerial Decree of 2 November 2005 and of CNIPA circular no. 56 of 21 May 2009.

1.2 Name of the document

This document, called the ***Operating Manual***, has been coded internally with the name ***TWT_PEC_Manuale Operativo***.

1.3 Responsibility for the Operating Manual

This document is under the responsibility of Mr Fabrizio Amodio, PEC Service Manager, who can be contacted for any information or clarification regarding this manual on 02-890891 or by email at f.amodio@twt.it.

1.4 Updating of the Operating Manual

In the event of technical, operational or legislative changes, TWT S.p.A. will update this Operating Manual, subject to the approval of the managers of TWT S.p.A. and of the Agency for Digital Italy (AgID).

1.5 Availability of the Operating Manual

This document is available for free consultation and download on the institutional website of TWT S.p.A. at the following address:

https://www.twt.it/pec/manuale/TWT-PEC-MO.pdf

1.6 Version of the Operating Manual

The version and release date of this Operating Manual are shown at the foot of each page.

The following table lists the changes made to this document together with the related dates of validity.

Description of change	Version	Date
First issue	1.0	12/04/2007
Changed URL for Webmail on p. 5 Changed SMTPS port on p. 28 Changed figure 8 on p. 32 Changed figures 11 and 12 on p. 34 Changed figure 13 on p. 35	1.1	21/11/2007
Par. 1.8 Added QUALITY System Certification to UNI EN ISO 9001:2000 Par. 5.4.1 Changed figure 9 Par. 8.2.3 Changed Log archiving Par. 8.3.1 Changed Backup procedure	1.2	23/06/2008
Par. 8.1.3 Changed type of HSM devices	1.3	12/01/2010
Update of the reference legislation throughout the manual	1.4	15/03/2010
Update of the technological platform and legislative references	1.5	23/04/2012
Update of the technological platform and legislative references	1.6	24/01/2014
Par. 3.4 Added description of the PEO blocking, forwarding and PEO AntiSpam filter functions	1.7	21/05/2014
Par. 4.1 Alignment with the AgID circular on the reassignment of PEC mailboxes Par. 6.2.4 Retention of data on termination of the PEC service	1.8	07/08/2015
Par. 7 Increase in the maximum size of email messages	1.9	12/05/2016

Par. 1.7 Provider identification data Chapter 8 General Revision	2.0	01/04/2017
Par. 1.7 Provider identification data Par. 1.8 Quality Certifications Par. 5.1 Standard Access / Webmail Par. 5.2 Protocols Par. 5.3.1 Microsoft Outlook client configuration General Revision	2.1	19/12/2019
Par. 6.2.2 Activities and obligations of the Provider; Par. 6.2.3 Exclusions, Limitation and insurance policy	2.2	09/01/2020
Par. 5.4.1 Microsoft Outlook client configuration with POP3S and correction of typos Par. 5.5.1 Clarification of the quotation mechanism for requests for log information Par. 10 Protection of personal data (Privacy) Par. 10.1 Security measures to protect personal data	2.3	04/06/2021
Par. 7 Service levels	2.4	15/02/2022

1.7 Identification data of the Provider

The Certified Email service is provided by the organisation entered in the public list of providers pursuant to Art. 14 of Presidential Decree no. 68 of 11 February 2005 and identified as follows:

Company name:	TWT S.p.A.
Registered office address:	Via Sangiorgio, 12 – 20145 Milano
Operating office address:	Viale Jenner, 33 – 20159 Milano
Legal representative:	Simone Staffa Guidi (Chair of the Board of Directors)
Milan Companies Register registration no.:	11422580156
VAT no.:	11422580156
Telephone no. (switchboard):	+39 02 890891
Support telephone no.:	800 192 800
Support email:	support@twtcert.it
General website:	http://www.twt.it
PEC webmail website:	https://webmail.twtcert.it
Email (information):	info@twtcert.it
PEC email:	twt@pec.twt.it

1.8 Quality Certification

TWT has brought the certification of its Quality Management System into line with the UNI EN ISO 9001:2015 standard. The scope of certification is: "*Design, provision and support of national and international Telecommunications services to customers and resellers. Provision of the Certified Email (P.E.C.) service*".
TWT obtained certification in accordance with the ISO 27001 standard on 22 July 2019.

2 Technical and legislative references

2.1 Legislative references

General Data Protection Regulation [GDPR]
Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) of 27 April 2016

DPCM 13/01/2004 [DPCM]
Decree of the President of the Council of Ministers of 13 January 2004 – "Technical rules for the creation, transmission, storage, duplication, reproduction and validation, including time validation, of electronic documents" (published in Official Gazette no. 98 of 27 April 2004), as amended and supplemented.

DPR 68/2005 [DPR]
Presidential Decree no. 68 of 11 February 2005 "Regulation laying down provisions for the use of certified email, pursuant to Article 27 of Law no. 3 of 16 January 2003" (published in Official Gazette no. 97 of 28 March 2005).

DM 02/11/2005 [DM]
Ministerial Decree of 2 November 2005 of the Presidency of the Council of Ministers, Department for Innovation and Technologies, "Technical rules for the creation, transmission and validation, including time validation, of certified email" (published in Official Gazette no. 266 of 15 November 2005).

Legislative Decree 82 of 7/3/2005 [CAD]
"Digital Administration Code" (published in Official Gazette no. 112 of 16 May 2005, ordinary supplement no. 93), as amended and supplemented (Legislative Decree no. 159 of 4 April 2006, published in Official Gazette no. 99 of 29 April 2006, ordinary supplement no. 105; it was subsequently amended and supplemented first by Legislative Decree no. 179 of 22 August 2016 and then by Legislative Decree no. 217 of 13 December 2017).
The CAD contains the provisions under which the State, the Regions and local authorities ensure the availability, management, access,

transmission, storage and usability of information in digital form by means of information and communication technologies.
In force since 1 January 2006, it repeals, among others, the provisions of DPR 445/2000 on the transmission of electronic documents (Art. 14) and makes the rules governing the certified email service subject to the provisions of DPR 68/2005.

CNIPA Circular 51/2006 [CR/51]
"Performance of supervision and control of the activities carried out by those entered in the list of certified email (PEC) providers referred to in Article 14 of Presidential Decree no. 68 of 11 February 2005" (published in Official Gazette no. 296 of 21 December 2006).

CNIPA Circular 56/2009 [CR/56]
"Procedures for submitting applications for entry in the public list of certified email (PEC) providers referred to in Art. 14 of Presidential Decree no. 68 of 11 February 2005" (published in Official Gazette no. 168 of 22 July 2009).

Hereinafter in this document, the legislative references listed above will be referred to by the abbreviations defined above in square brackets.

2.2 Technological standards

The Certified Email service provided by TWT complies with the technical reference standards whose specifications are set out in the technical annex to the [DM].

RFC 1847	Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted
RFC 1891	SMTP Service Extensions for Delivery Status Notifications
RFC 1912	Common DNS Operational and Configuration Errors
RFC 2045	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
RFC 2049	Multipurpose Internet Mail Extension (MIME) Part Five: Conformance Criteria and Example
RFC 2252	Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
RFC 2315	PKCS#7: Cryptographic Message Syntax Version 1.5
RFC 2633	S/MIME Version 3 Message Specification
RFC 2660	The Secure Hypertext Transfer Protocol
RFC 2821	Simple Mail Transfer Protocol
RFC 2822	Internet Message Format
RFC 2849	The LDAP Data Interchange Format (LDIF) – Technical Specification
RFC 3174	US Secure Hash Algorithm 1 (SHA1)
RFC 3207	SMTP Service Extension for Secure SMTP over Transport Layer Security
RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
ISO/IEC 9594-8:2001	Open System Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks

2.3 Definitions

AgID
Pursuant to Decree-Law no. 83/2012, converted into Law no. 134/2012, the body DigitPA was abolished and the Agency for Digital Italy (AgID) was established. The PEC legislation assigns the following powers to the Agency for Digital Italy:

- the Agency defines the technical rules and updates them in line with technological developments and the experience gained from the use of the system. The Agency publishes the updates in line with the standards specified by the legislation.

- the Agency manages the public list of certified email providers. It receives and assesses the applications submitted by parties applying to become certified email providers, ordering their entry in the relevant list or rejecting the application for lack of requirements. The Agency provides those entered in the list with the certificates for the electronic signature of receipts and for access to and updating of the Index of PEC Providers (IGPEC). Providers must submit to the Agency any changes to their corporate structure, to the features of the service and to the procedures adopted, with particular regard to continuity, operation and security.

- the Agency supervises and controls the activities carried out by the providers entered in the list. To this end, the Agency issues explanatory and guidance circulars, collects information every two months on the number of PEC domains, the number of PEC mailboxes and the number of messages exchanged in order to produce statistics on the spread and use of PEC, periodically carries out interoperability tests on the PEC systems in operation at the providers and may access the providers' premises to carry out checks on the compliance of the PEC system.
- the Agency provides support and promotes knowledge of the PEC system among public administrations and private parties.

Non-delivery notice
The notice, issued by the system, to report the anomaly to the sender of the original message where the certified email provider is unable to deliver the message to the recipient's certified email mailbox.

Non-acceptance notice
The notice, signed with the signature of the sender's certified email provider, which is issued when the sending provider is unable to accept the incoming message, stating the reason why the message cannot be accepted and specifying that the message will not be delivered to the recipient.

Anomaly envelope
The envelope, signed with the signature of the recipient's certified email provider, in which an incorrect message, or a message that is not certified email, is placed and delivered to a holder, in order to highlight this anomaly to the recipient.

Transport envelope
The envelope created by the access point and signed with the signature of the sending certified email provider, in which the original message sent by the certified email user and the related certification data are placed.

Certified Email Mailbox
The email mailbox located within a certified email domain and associated with a function that issues delivery receipts on receipt of certified email messages.

Certifier
The party that provides certification services for electronic signatures or that provides other services connected with them.

Electronic Certificate
The electronic attestation that links the data used to verify the electronic signature to the identity of the holder (the natural person to whom the electronic signature is attributed and who has access to the devices for creating the electronic signature).

Qualified Certificate
The electronic certificate that meets the requirements of Annex I to Directive 1999/93/EC, issued by certifiers that meet the requirements of Annex II to the same directive.

Accredited Certifier
This is the body (public or private party) that issues qualified certificates complying with European and national legislation on the matter, and that

has applied for and obtained, pursuant to Article 29, paragraph 1 of the [CAD], recognition that it meets the requirements of the highest level, in terms of quality and security, through accreditation in the public list of certifiers maintained and made available by AgID.

Private key
The element of the pair of asymmetric keys, used by the holder, by means of which the digital signature is affixed to the electronic document.

Public key
The element of the pair of asymmetric keys intended to be made public, with which the digital signature affixed to the electronic document by the holder of the asymmetric keys is verified.

Asymmetric keys
The pair of keys, the public one and the private one, that is used for creating and verifying the digital signature, and is assigned to a single holder.

Time stamping keys
Asymmetric keys intended for generating and verifying time stamps.

Encryption
The transcription of electronic evidence according to a confidential code that makes it unintelligible to third parties. Encryption and decryption operations are carried out by applying standard algorithms that involve the use of secret keys.

Certification data
The data, such as the date and time of sending, sender, recipient, subject and message identifier, that describe the sending of the original message and are certified by the sender's certified email provider; these data are included in the receipts and are transferred to the recipient holder together with the original message by means of a transport envelope.

Recipient
The user who makes use of the certified email service of the Provider or of another certified email provider to receive documents produced by means of IT tools.

Electronic document
The electronic representation of legally relevant acts, facts or data.

Certified email domain
The set of all and only the certified email mailboxes whose address refers, in its extension, to the same internet domain, defined according to the standards of that network.

Electronic evidence
A sequence of binary symbols (bits) that can be processed by an IT procedure.

Electronic signature
The set of data in electronic form, attached to or logically associated with other electronic data, used as a method of electronic identification.

Qualified electronic signature
An electronic signature obtained through an IT procedure that guarantees its unique link to the signatory, created using means over which the signatory can maintain exclusive control and linked to the data to which it refers in such a way as to allow any subsequent change to those data to be detected, which is based on a qualified certificate and created by means of a secure signature creation device.

Digital signature
A particular type of qualified electronic signature based on a system of cryptographic keys, one public and one private, related to each other, which allows the holder, by means of the private key, and the recipient, by means of the public key, respectively, to make manifest and to verify the origin and integrity of an electronic document or of a set of electronic documents.

Signature of the Certified Email provider
The advanced electronic signature, based on a system of asymmetric keys, that makes it possible to make manifest the origin and to ensure the integrity and authenticity of the messages of the certified email system, generated through an IT procedure that guarantees its unique link to the provider and the provider’s unique identification, and created automatically using means that guarantee the exclusive control of the Provider.

Certified Email Provider
The party that manages one or more certified email domains with the related access, incoming and delivery points, that holds the key used for signing receipts and envelopes and that interfaces with other certified email providers for interoperability with other holders.

Index of Certified Email providers
The system that contains the list of certified email domains and providers, with the related certificates corresponding to the keys used for signing receipts, notices and envelopes, implemented by means of a Lightweight Directory Access Protocol server, hereinafter referred to as LDAP, located in an area that can be reached by the various certified email providers and which also constitutes the technical structure of the public list of certified email providers.

Message LOG
The electronic log, kept by the provider, of the operations relating to the transmissions carried out by means of certified email.

Operating manual
This public document, which defines and describes the procedures applied by the Provider of the PEC service in carrying out its activity as defined by Art. 23 of the [DM]. It is filed with AgID and is made available for consultation and download on the Provider's website.

Quality manual
The manual prepared by the Provider to document its quality system certified to UNI EN ISO 9001:2015, as required by Article 20, paragraph 2 of the [DM].

Time stamp
Electronic evidence that allows time validation.

Certified email message
An electronic document made up of the text of the message, the certification data and any attached electronic documents.

Original message
The message sent by a certified email user before it reaches the access point, delivered to the recipient holder by means of a transport envelope that contains it.

Sender
A user who makes use of the certified email service to transmit documents produced by means of IT tools.

Security Plan
The document, provided for by Article 16 of the [DM], that defines the appropriate measures adopted to guarantee the integrity, security and continuity of the certified email service. It is a confidential document with controlled distribution.

Certified email (PEC)
Any email system in which the sender is provided with electronic documentation certifying the sending and delivery of electronic documents.

Email
An electronic system for the transmission of electronic documents.

Access point
The system that provides the access services for sending and reading certified email messages, as well as the services for identifying the user and granting access, checking for computer viruses within the message, issuing the acceptance receipt and placing the original message in the transport envelope.

Incoming point
The system that receives the message within a certified email domain, checks the origin and correctness of the message and issues the take-charge receipt, places incorrect messages in an anomaly envelope and checks for computer viruses within ordinary email messages and transport envelopes.

Delivery point
The system that delivers the message to the certified email mailbox of the recipient holder, checks the origin and correctness of the message and issues, as the case may be, the delivery receipt or the non-delivery notice.

Short delivery receipt
The receipt that contains the certification data and an extract of the original message.

Full delivery receipt
The receipt that contains the certification data and the original message.

Acceptance receipt
The receipt, signed with the signature of the sender's certified email provider, containing the certification data, issued to the sender by the access point upon the sending of a certified email message.

Delivery receipt
The receipt, signed with the signature of the recipient's certified email provider, issued to the sender by the delivery point when the message is placed in the recipient's certified email mailbox.

Take-charge receipt
The receipt, signed with the signature of the recipient's certified email provider, issued by the incoming point to the sending certified email provider to certify that the message has been taken charge of by the destination certified email system, bearing the certification data so that it can be associated with the message to which it refers.

Summary delivery receipt
The receipt that contains the certification data.

Time reference
The information containing the date and time that is associated with a certified email message.

Holder
The party to whom a certified email mailbox is assigned.

Certified Email User
The natural person, legal person, public administration and any body, association or organisation, as well as any internal organisational units where present, that is the sender or recipient of certified email.

Time validation
The result of the IT procedure by which one or more electronic documents are given a time reference (date and time information) that is valid against third parties.

Computer virus
A computer program whose purpose or effect is to damage a computer or telematic system, the data or programs contained in it or pertaining to it, or to interrupt, in whole or in part, or alter its operation.

2.4 Technical terms

ISO – International Standard Organization
An international standard-setting body, composed of representatives of national bodies, that produces industrial and commercial standards worldwide.

ITU – International Telecommunication Union
International organisation that acts as the regulatory body for standards in telecommunications.

ITU – T
Acronym identifying the Telecommunications Sector of the ITU ("Telecommunication Sector").

LDAP – Lightweight Directory Access Protocol
A standard protocol for querying and modifying directory services, used to manage access to the certificate register and to carry out operations for retrieving certificates and revocation and suspension lists.

DNS – Domain Name System
DNS is a directory service, used mainly to resolve Host names into IP addresses. The service is implemented by means of a distributed database, made up of DNS servers. This function is essential for the usability of the Internet, since human beings prefer to remember text names, while Hosts and routers are reached using IP addresses. DNS names, or "domain names", are one of the most visible features of the Internet.

PIN – Personal Identification Number
Confidential security code that enables the signature functions to be activated.

HTTP – Hypertext Transfer Protocol
Used as the main system for transmitting information on the web. HTTP works on a request/response mechanism: the client makes a request and the server returns the response. In common usage the client is the browser and the server is the website. There are therefore two types of HTTP messages: request messages and response messages.

HTTPS – Secure Hypertext Transfer Protocol
The term HTTPS refers to the HTTP protocol (Hyper Text Transfer Protocol) used in combination with the SSL (Secure Socket Layer) layer; the standard port dedicated to this service is 443/TCP.

ITSEC – Information Technology Security Evaluation Criteria
European criteria for evaluating security in IT systems.

PKCS – Public Key Cryptography Standard
Technical standards for cryptographic applications (developed by RSA Data Security Inc.).

PKI – Public Key Infrastructure
IT infrastructure made up of applications that use asymmetric key cryptographic techniques (public and private). An infrastructure of this type includes services for generating and distributing keys, issuing and publishing certificates, managing the registers of issued certificates and the suspension and revocation lists, as well as other services such as time stamping. Examples of uses based on the infrastructure are: the generation of confidential electronic transactions (cryptography), the management of authorisation, authentication and identification systems (digital signature), subjective attributability and data integrity (digital signature and time stamping).

URL – Uniform Resource Locator
Standard naming system indicating a site, domain or other object (file, newsgroup, etc.) on the Internet. The first part of the URL (http:, ftp:, file:, telnet:, news:) specifies how the object is accessed.

WWW – World Wide Web
The set of resources and users on the Internet that use the HTTP protocol.

MIME – Multipurpose Internet Mail Extensions
Extension of the standard email protocol that allows binary content to be transmitted with specific applications.

S-MIME – Secure/MIME
Secure version of the MIME email protocol.

POP – Point of Presence
Point of access to the Internet.

RFC – Request for Comments
Written definitions of protocols or standards in use on the Internet.

TLS – Transport Layer Security
Standard protocol for managing secure transactions on the Internet, based on the use of public key cryptographic algorithms.

XML
Extensible Mark-up Language. A language developed specifically for distributing documents on the Web.

3 General description of the PEC service

Certified Email (PEC) is an extension of traditional email that provides certain proof, with legal value, of the delivery of the message.

In other words, it gives the electronic transmission process a value equivalent to that of notification by registered post in all cases provided for by law.

With a Certified Email mailbox it is nevertheless possible to send and receive ordinary email messages.

In particular, the PEC service provided by TWT is a service that complies with Italian legislation, with particular reference to the [DPR], the [DM] and its annexes.

The holder of the TWT PEC mailbox who sends an email will have, as better specified in the following paragraphs, the acceptance receipt and the subsequent delivery receipt, which can be used to prove that the message has been sent and which will certify the completion of the sending process.

Should the sender inadvertently delete the receipts of the messages sent, they can rely on the service of the provider TWT, which will keep track of all messages sent and received for a minimum period of 30 months.

The user of a Certified Email mailbox can access the service either through a traditional email client (Eudora, Outlook, etc) or by browsing with an internet browser (Firefox, Chrome, etc.) on TWT's PEC WebMail portal.

3.1 Operation of the service

The following figure shows the operation of the Certified Email service:

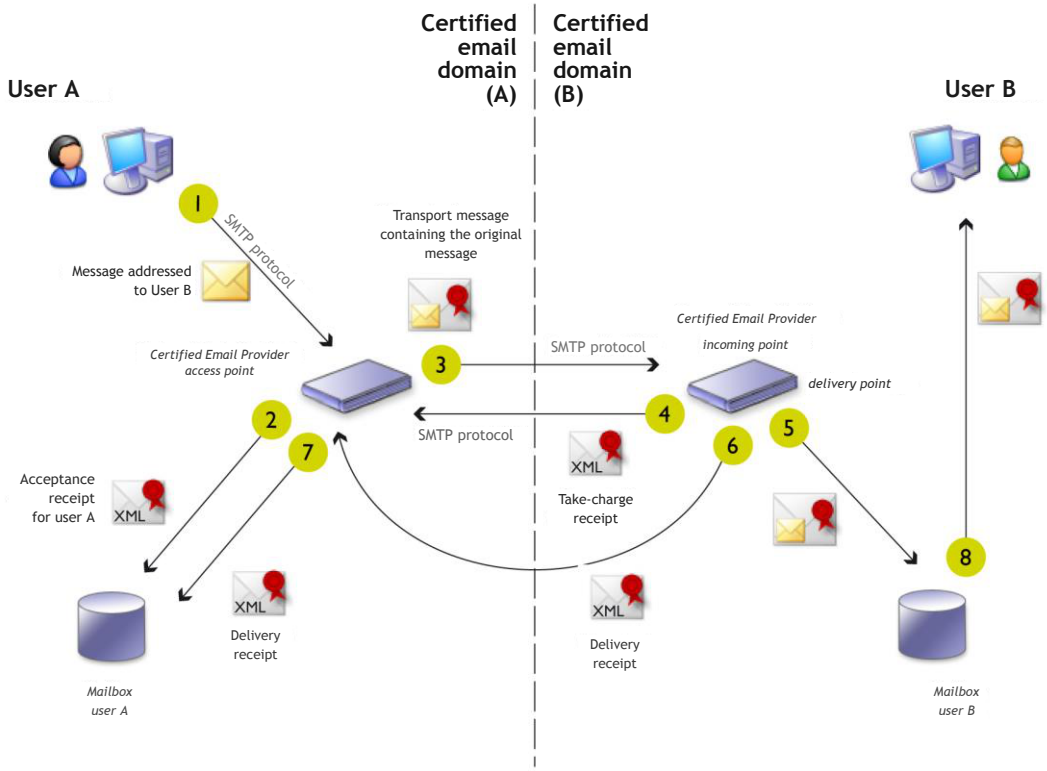


Figure 1: Operation of the service

1. The sender (user A) sends a message to the recipient through the Certified Email server of their provider (access point), after verification of the access credentials.

2. The provider sends to the sender's mailbox (user A) an acceptance or non-acceptance receipt on the basis of the formal checks carried out on the message received. The receipts show the date and time of the event, the subject of the message, the data of the sender and of the recipient and any reason for non-acceptance.

3. The message is then enclosed within another message (called the transport envelope) of the S/MIME type, digitally signed by the provider and sent to the incoming point (recipient's provider).

4. The incoming point checks the signature of the sending provider and verifies the validity of the message; if the outcome is positive, it sends a take-charge receipt for the message to the server of the sending provider and sends the message on to the delivery point.

5. The delivery point makes the message available in the recipient's mailbox (user B); at this point the recipient (user B) is able to read the Certified Email message (point 8, figure 1).

6. The delivery point sends a delivery receipt to the sending provider.

7. The sending provider makes the delivery receipt available in the sender's mailbox (user A).

Where the message is sent at the same time to several Certified Email recipients, the sender will receive a single acceptance receipt and as many delivery receipts, or non-delivery receipts (see next paragraph), one for each recipient.

Where the message is sent to one or more ordinary (non-certified) email recipients, in addition to having no legal value, no delivery receipts will be generated.

3.2 Operation in the event of delivery problems

In compliance with the reference legislation, the operation of the system provides that:

- If, within twelve hours of the message being forwarded, the sender's provider does not receive from the recipient's provider the take-charge receipt or the delivery receipt for the message sent, it informs the sender that the recipient's provider may not be able to deliver the message.

- If, within the following twelve hours, the sender's provider does not receive the delivery receipt for the message sent, it sends the sender a further notice of non-delivery of the message within 24 hours of sending.

3.3 Operation in the event of viruses

The operation of the Certified Email system provides for the following activities to be carried out by the providers where viruses are detected:

- If the sender's provider receives messages containing computer viruses, it is required not to accept them, promptly informing the sender that the transmission cannot proceed. In this case the sender's provider retains the messages received for thirty months in accordance with the procedures defined by the reference legislation;

- If the recipient's provider receives messages containing computer viruses, it is required not to forward them to the recipient, promptly informing the sender's provider so that it can inform the sender that the transmission cannot proceed. In this case the recipient's provider retains the messages received for thirty months in accordance with the procedures defined by the reference legislation.

In all these cases, specific notices stating the reasons for non-delivery are generated and sent to the sender.

3.4 Receipt of ordinary email

Where a certified email (PEC) mailbox receives an ordinary email (PEO) message, the provider encloses it within another message (called the Anomaly Envelope) of the S/MIME type, signed by the provider, to inform the holder that it is not a certified email message.

In the webmail settings, the PEC account can be configured not to accept ordinary email; in this case the PEO message will be rejected by the system and the sender will receive an error indicating that PEO mail is not accepted by this PEC account.

Where PEO is enabled, again in the webmail settings, it is possible to configure forwarding of PEO to another, non-certified mailbox (the PEC mailbox will still receive the anomaly envelope mentioned above, while a copy of the original message will be forwarded to the specified address) and to enable or disable the AntiSPAM filter on incoming PEO.

3.5 Features of the receipts and of the transport envelopes

3.5.1 Electronic signature of receipts and transport envelopes

The receipts and transport envelopes issued by the subscriber are signed by the provider itself by means of an advanced electronic signature,

generated automatically by the email system and based on a pair of asymmetric keys, one public and one private, which makes it possible to make manifest their origin and to ensure their integrity and authenticity.

3.5.2 Time reference

As required by the legislation, a time reference is affixed by the provider to every event relating to the processing of the certified email message.

In order to guarantee the accuracy of the time reference, all the devices that make up the technological infrastructure of TWT S.p.A. are synchronised with several public Time Servers using the standard NTP (Network Time Protocol), including the NTP server of the Istituto Elettronico Nazionale Galileo Ferraris.

3.5.3 Types of delivery receipts

In line with the AgID Technical Rules, the provider can issue three different types of Delivery Receipts, which can meet different user needs and which are summarised below:

- the **Full Receipt** consists of an email message sent to the sender that shows, in readable format, the certification data (sender, recipient, subject, date and time of delivery, message identification code). The same data are included in an XML file attached to the receipt. For deliveries to the primary recipients of the message (who are the direct recipients of the message, as opposed to the recipients in copy), the delivery receipt also contains the original message, text and any attachments.

- the **Short Receipt** is intended to reduce Certified Email transmission flows, especially where the volume of documents and messages exchanged is very large. For this reason, the Short Receipt contains the original message and the cryptographic *hashes* of any attachments. To allow the content transmitted to be verified, the sender must keep the unmodified originals of the attachments included in the original message to which the *hashes* refer.
- the **Summary Receipt** follows the rules for issuing the full receipt, except that the attachment contains only the XML file with the certification data described. The summary receipt is particularly useful for services that include Certified Email as a means of transport

supporting a high degree of automation of communication flows.

4 Description of the TWT PEC service

The TWT certified email service is offered in the form of mailboxes hosted on a domain entered in the relevant index held by AgID.

4.1 Types of service

TWT offers the customer the certified email service in the following types:

1. PEC mailbox on the **TWTCERT.IT** domain
   The certified email mailbox is activated on TWT's certified email domain and is therefore of the type azienda@twtcert.it.

   This type is intended for the category of users for whom it is not particularly important that the domain to which they belong reflects the organisation to which they belong.

2. PEC mailbox on the subdomain chosen by the customer
   The certified email mailbox is activated on a subdomain chosen by the customer but within a certified email domain owned by TWT. In this case the PEC mailbox will be of the type nome@azienda.twtcert.it.

3. Mailboxes hosted on domains owned by the customer
   The certified email mailboxes are activated on a domain owned by the customer, such as nome@azienda.it. Customers are therefore also allowed to use subdomains of the domains they own, such as nome@divisione.azienda.it.

   This type is recommended for companies that wish to register their own certified email domain and activate their mailboxes on it. In this case the customer can administer the mailboxes, i.e. create and delete them, and manage its users independently.

In compliance with the AgID communication of 17.12.2013 with the subject "Requirement on the reassignment of certified email mailboxes", in which "the provider is prohibited, with reference to the PEC addresses it manages, from reassigning the same certified email address to a party other than the original holder",

any “user_name” already used in the past will be automatically rejected.

TWT reserves the right to check the name of the mailbox requested and to refuse activation and/or carry out further checks where the name requested recalls or evokes public, national or EU bodies, or private bodies, insurance companies, banks, credit or financial institutions, or is offensive or defamatory towards other users, groups and social categories, or is excessively long or made up of entirely random alphanumeric sequences.

Regardless of the type chosen, the TWT PEC service provides for configurations that can be customised according to the customer’s needs, such as, by way of example:

- access via web;
- access via secure email protocols;
- access via user name and password;
- access with a digital certificate;
- mailbox administration;
- twt webmail customisations;
- disk space size;

All mailboxes, regardless of the configuration adopted by the customer, meet the functions and features required for certified email by the reference legislation: management of acceptance and delivery receipts, management of transport envelopes, counting of the exact time, antivirus.

4.2 Offer arrangements

TWT certified email is sold both through a direct sales network and through partners: the arrangements may differ depending on the number of mailboxes requested and the type of customer.

For any detailed information, the applicant can write to the email address info@twtcert.it or visit the website www.twt.it.

The commercial offer provides for an activation fee and an annual fee, which varies mainly according to the number of TWT PEC mailboxes purchased by the customer and their size in terms of MB of available

space. TWT may apply discounts of varying amounts to these prices on the basis of various factors.
Activation fees and any annual fees are also provided for optional services, to be quoted according to the specific customisation requested.

By way of example:
- the customisation of some graphic elements in the webmail interface, for all the mailboxes of a domain;
- additional disk space compared with the standard;
- notification of receipt of certified email messages via SMS or via ordinary email.

5 Methods of access to the service

TWT offers its customers access to the service via Mail Client (standard access) and Internet Browser (webmail).

5.1 Password

Access passwords are created directly by the end user during activation and can be changed by the user at any time via the Webmail.

Passwords must be created following a few standard rules: they must be at least 8 characters long and must contain the following three distinguishing elements: at least one upper-case and one lower-case letter, at least one numeric character (from 0 to 9), at least one special character from the following: !$@#%^&*€

Passwords are saved in the TWT databases already encrypted, so no one within the company is able to know them. If the password is lost, the user, by selecting the "reset password" link on the Webmail login page, will receive at their ordinary email address an email containing a link to reset the password.

5.2 Standard access / Webmail

All the components of the TWT solution use standard secure protocols to interact with each other and with external applications.

It follows that the platform is compatible with all mail clients that use the supported standard secure protocols (POP3S, IMAPS) and with browsers that allow the use of TLS v1.2.

The following table shows the clients/browsers and platforms on which the products have been successfully tested.

Operating systems	Minimum supported version (OS)	Browser	Minimum supported version (Browser)	Email client	Minimum supported version (Email client)
Android	4.4.2	All		Mail (native)	5.x
Apple iOS	All versions	All		Mail	11.x
Windows Phone	8.1	Internet Explorer	11		
OSX	10.9	Safari	7.x	Apple Mail	All
		Chrome	34.x	Outlook	2011 (only on OSX from 10.11 to 10.13)
		Firefox	29.x	Thunderbird	45.6
Windows 7	All	Chrome	30.x	Outlook	2010
		Firefox	31.3.0 ESR/45.x		
		Internet Explorer	11	Thunderbird	45.6
		Opera	17.x		
Windows 8	8.0	Chrome	30.x	Outlook	2010
		Firefox	31.3.0 ESR/45.x		
	8.1	Internet Explorer	11	Thunderbird	45.6
		Opera	17.x		
Windows 10	All	All		All	

5.3 Protocols

The protocols used to communicate with the TWT mail server are the following:

- to send email messages with a local client: SMTPS, port 465;
- to receive email messages with a local client via POP3+SSL: POP3S, port 995;
- to receive email messages with a local client via IMAP+SSL: IMAPS, port 993;
- to use an internet browser: HTTPS, port 443.

The minimum version accepted for the secure protocols is TLS v1.2.

5.4 Configuration of the email client.

Using an email client (we will use Microsoft outlook as an example), it is possible to choose how to access the server: via POP3S or via IMAPS.

We will not dwell on the differences between the two systems, other than to say that the main difference is that the IMAPS protocol is based on the concept of processing all mail on a remote, centralised server, so that the whole set of one's messages is available from any machine one connects from, unlike the POP3S protocol, which downloads the messages contained in the mailbox locally, leaving a copy on the server or not.

5.4.1 Microsoft Outlook client configuration with POP3S.

To create the account in Microsoft Outlook, select the **File** menu item (fig. 1).

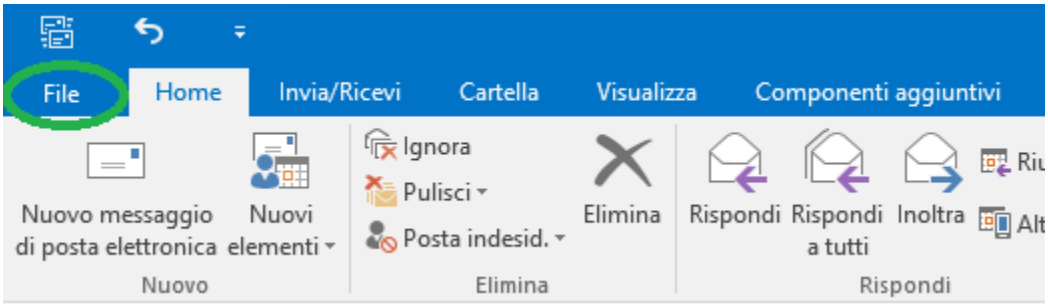


Figure 1: selecting the File menu item

From the **Account Information** tab, click the **Add Account** button (fig. 2).

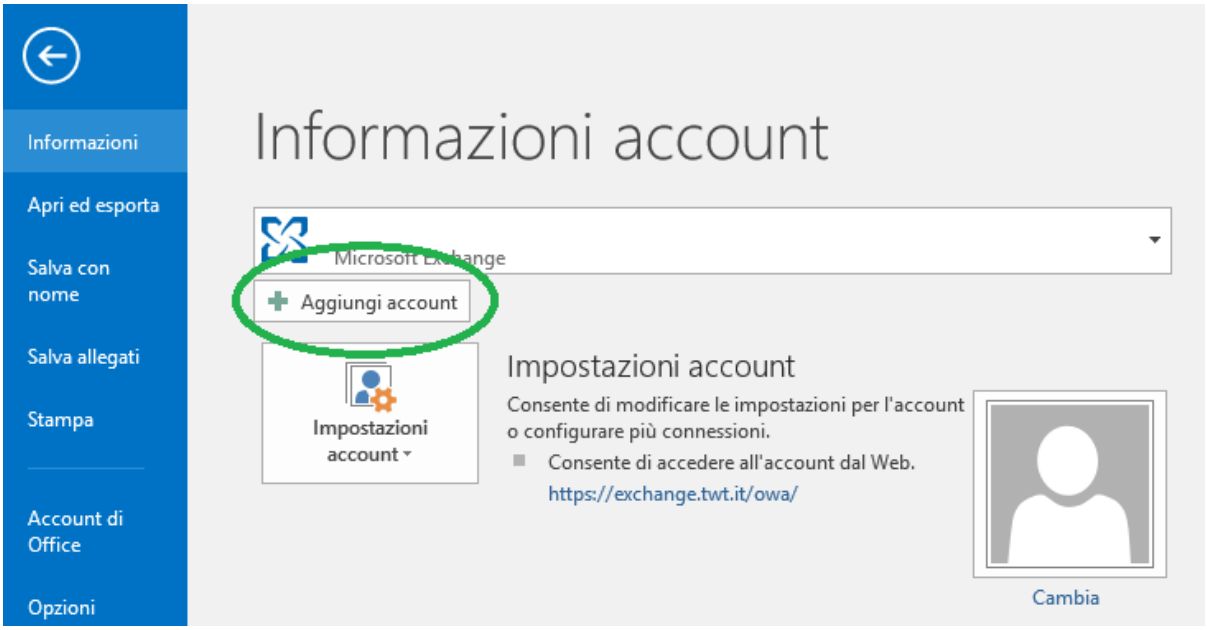


Figure 2: Add Account function

From the **Add Account** window, select the **Manual setup or additional server types** option and then click the ***Next*** button (fig. 3).

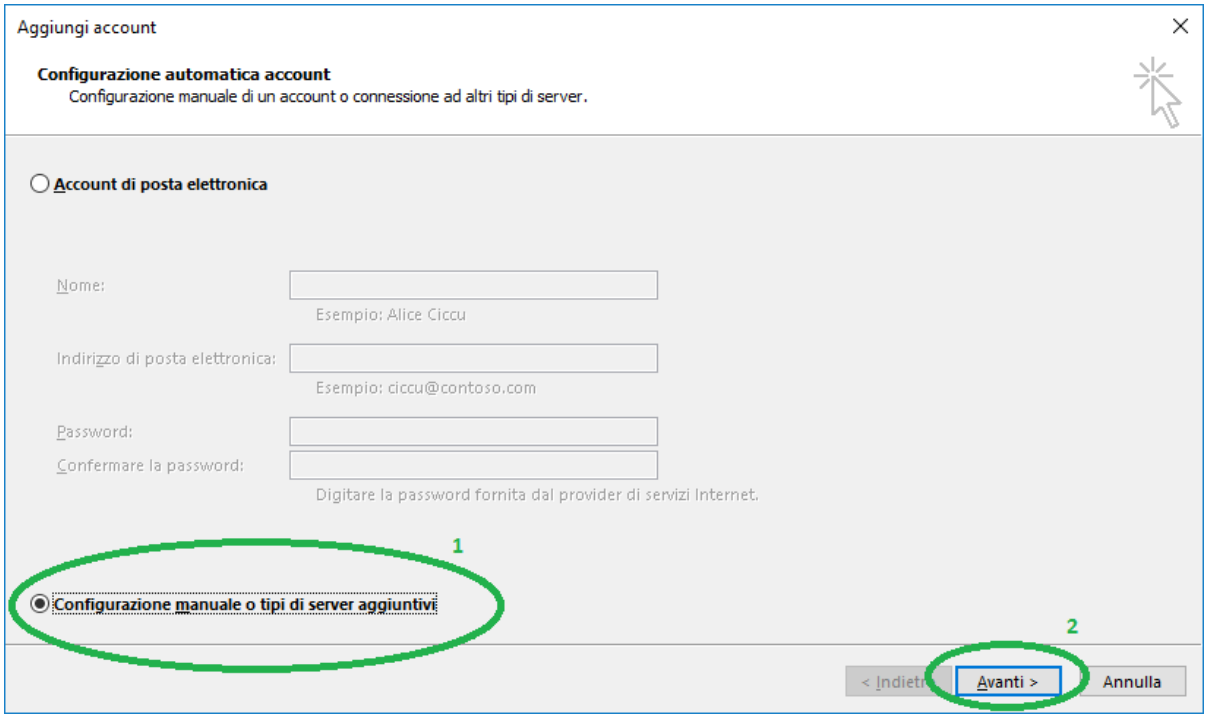


Figure 3: Manual setup or additional server types.

Then choose the **POP or IMAP** option (fig. 4).

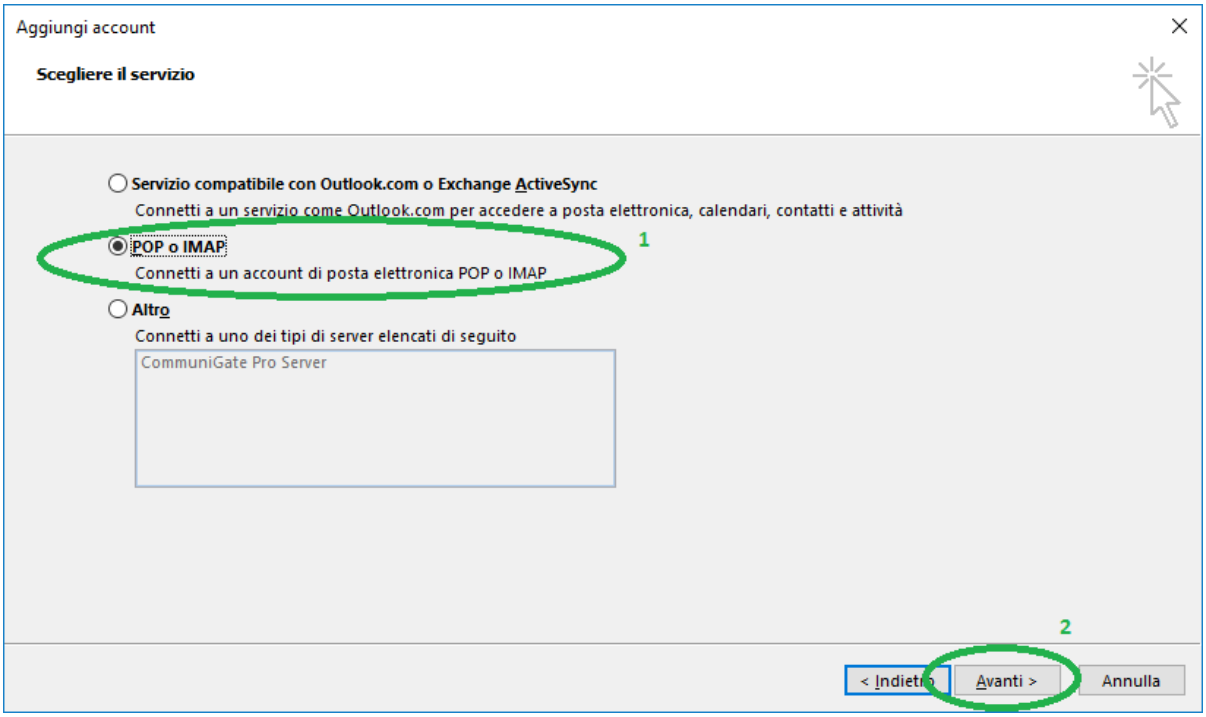


Figure 4: choosing the service

In the **POP and IMAP Account Settings** window, you can enter all the information on the account and on the mail server.

In the **User Information** section:

- enter your name in the **Your Name** field.
- enter the certified email address in the **Email Address** box.

In the **Server Information** section:

- as **Account Type**, select POP3
- in the **Incoming mail server** box, enter *mail.twtcert.it*
- in the **Outgoing mail server (SMTP)** box, enter *smtp.twtcert.it*

In the Logon Information section:

- enter the **User Name** (pre-filled by Microsoft Outlook with the email address)
- enter the **Password** set when configuring the certified email mailbox.

The typical configuration of an account should look similar to the one shown in the figure (fig. 5).

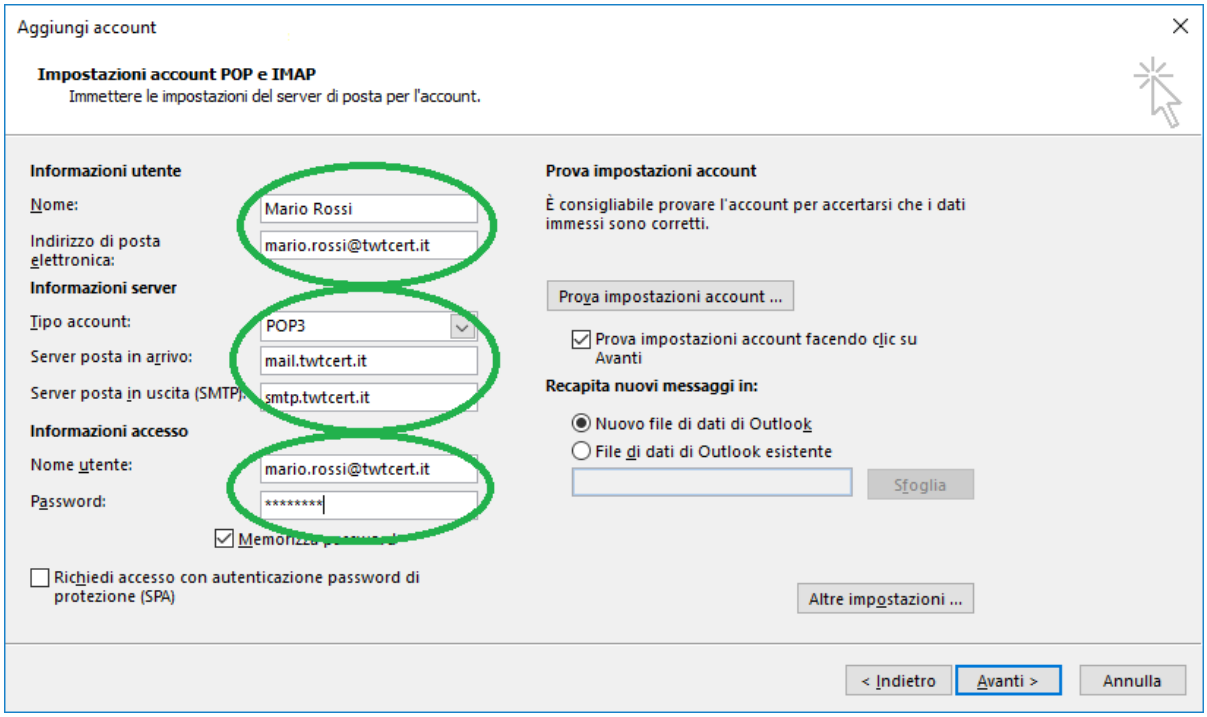


Figure 5: account and server settings

Once the basic information has been completed, click the More Settings button to access the advanced configuration (fig. 6).

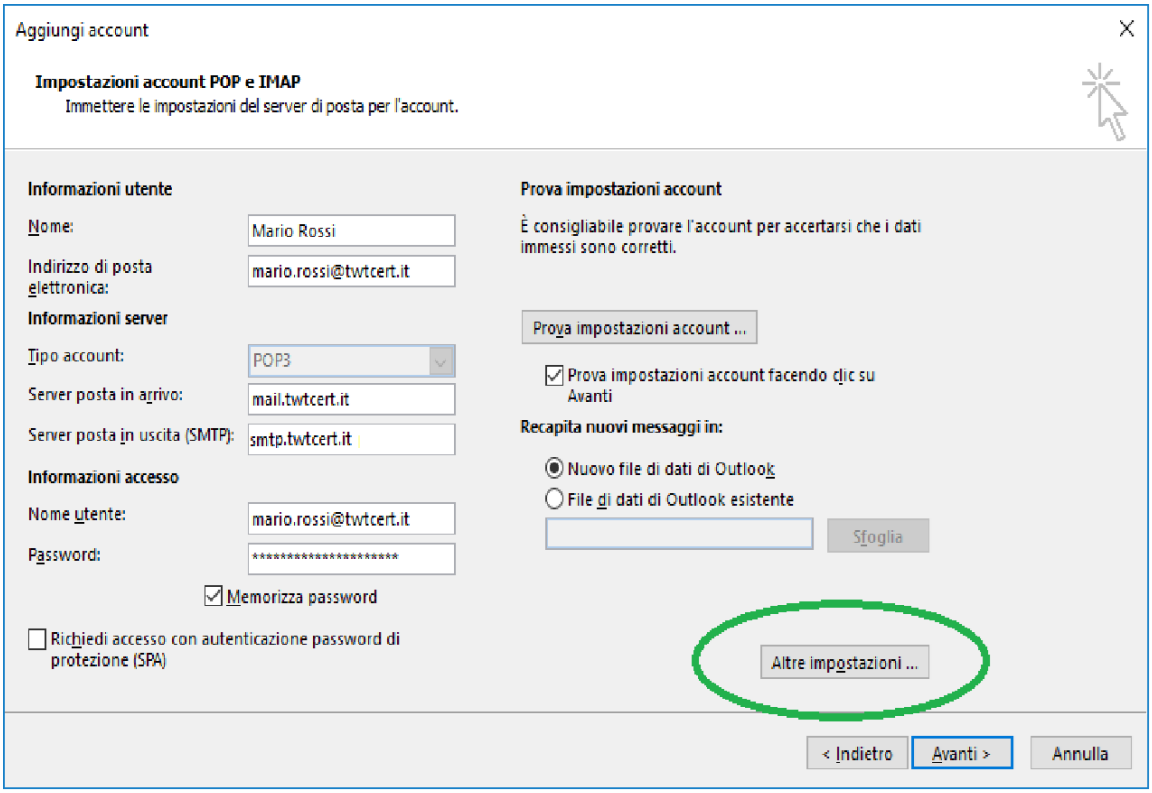


Figure 6: More Settings

Make sure that the correct mail account is shown in the **Internet E-mail Settings** window, on the **General** tab (fig. 7).

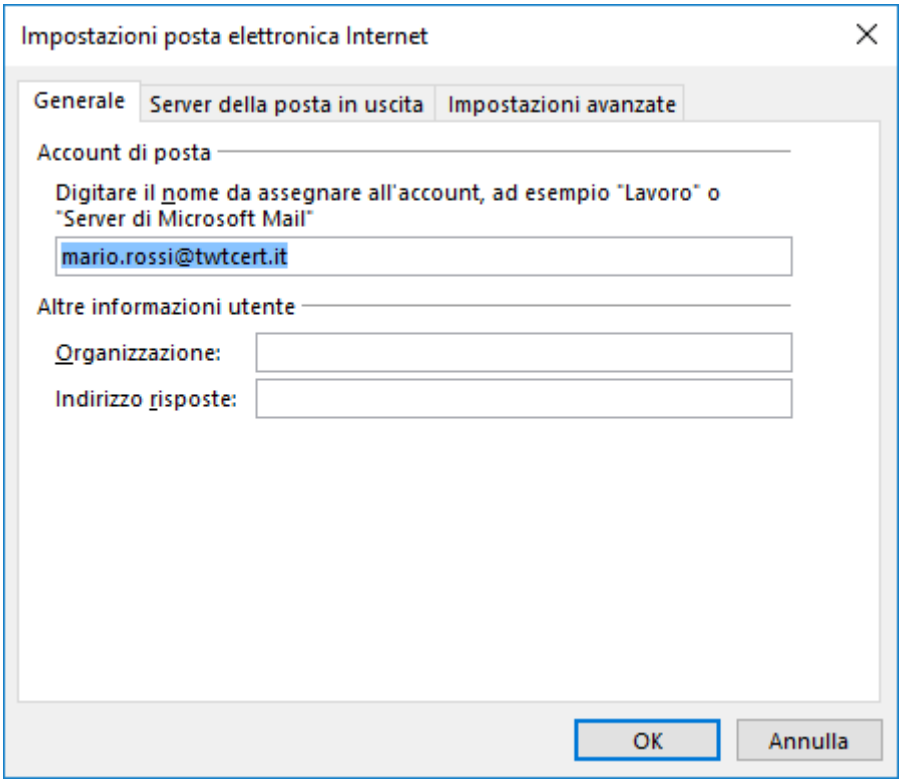


Figure 7: General tab

On the **Outgoing Server** tab, select the **My outgoing server (SMTP) requires authentication** option (fig. 8).

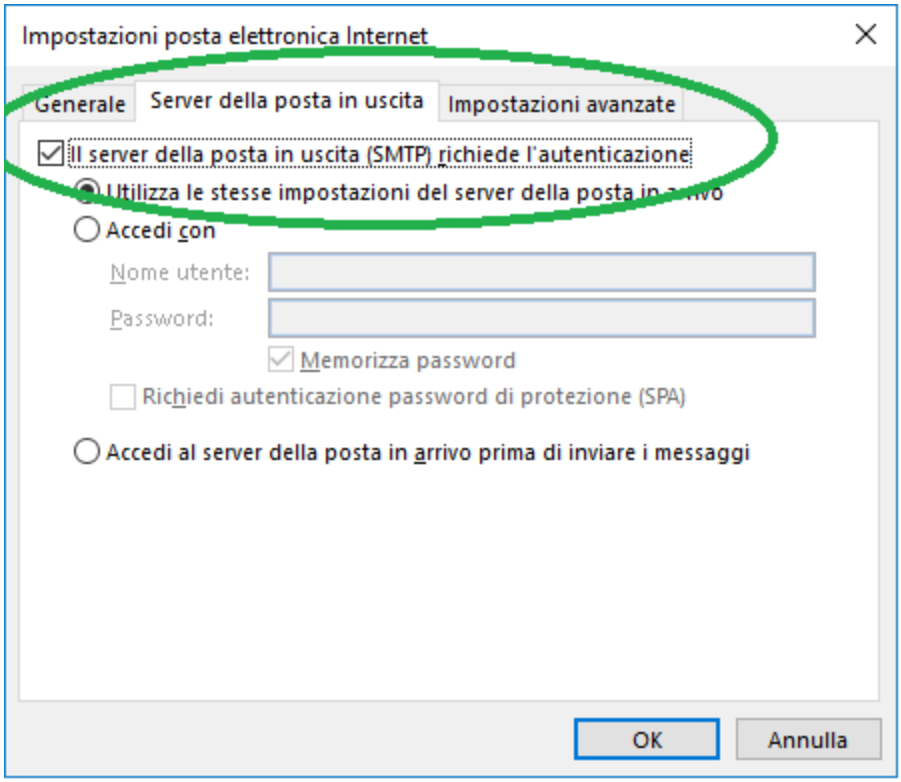


Figure 8: Outgoing Server tab

Finally, on the **Advanced** tab, enter the following parameters:

- **Incoming server (POP3)**: 995
- **This server requires an encrypted connection (SSL)**: yes
- **Outgoing server (SMTP)**: 465
- **Use the following type of encrypted connection**: TLS

The advanced settings tab should look as shown in figure 9:

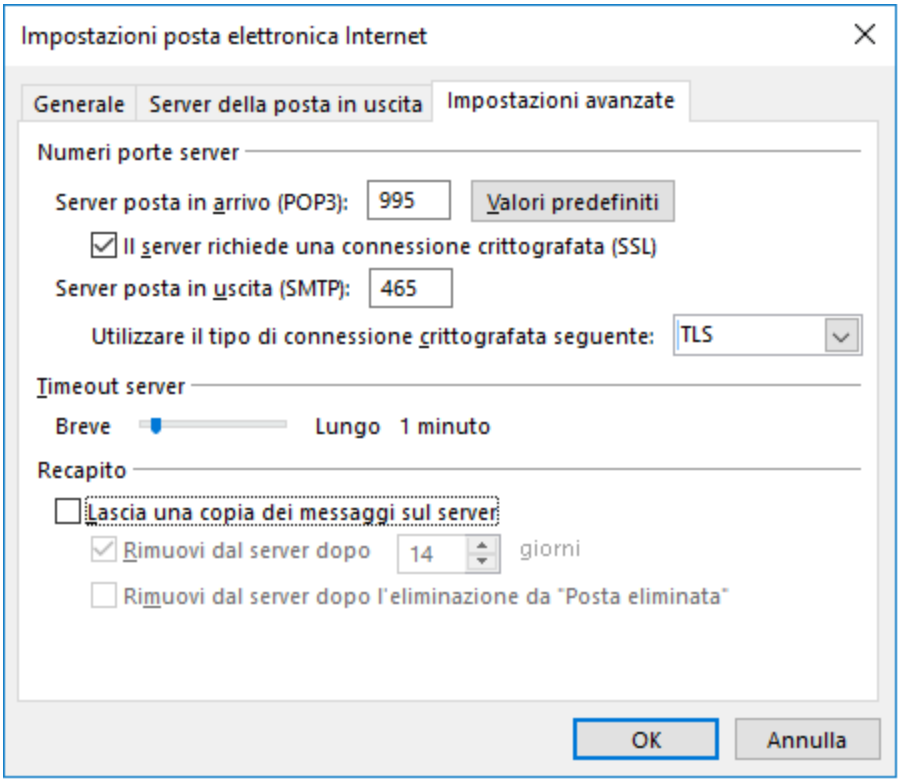


Figure 9: Advanced tab

Then click the OK button to return to the account and server configuration window.

From here you can run an immediate test of the account configuration by clicking the **Test Account Settings** button. Alternatively, you can postpone the test until the configuration is complete by selecting the **Test Account Settings by clicking the Next button** option and then pressing the **Next** button (fig. 10).

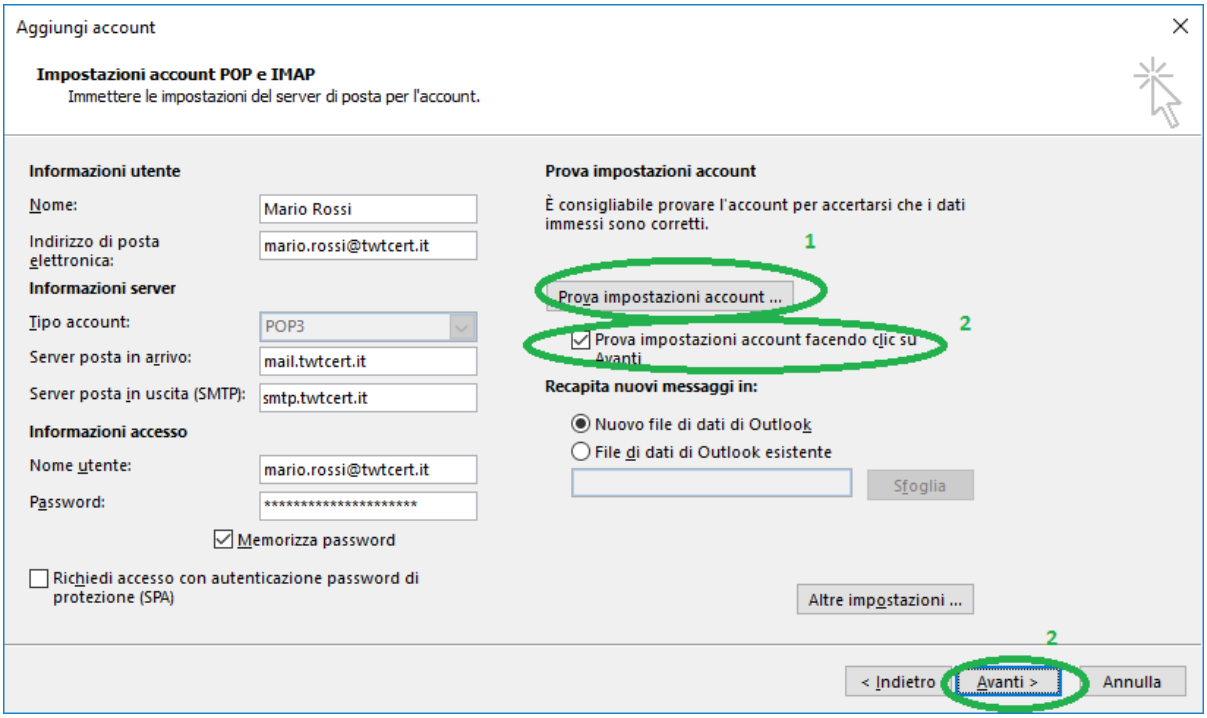


Figure 10: configuration test

The client is now ready to receive and send mail on the newly configured certified email mailbox.

5.5 Message Logs

During the stages of processing of the message at the access, incoming and delivery points (operation explained above in chapter 3), the system that provides TWT's certified email service keeps track of the operations carried out, storing them in an electronic log (LOG).

5.5.1 Request for logs by the holder

As provided for by current legislation, where the holder of the certified email mailbox no longer has the receipts of the certified email messages sent, the information contained in the electronic log stored by the provider is valid against third parties, pursuant to current legislation.

Requests for information on message logs may be submitted only by the holder of the TWT certified email mailbox or by the judicial authorities.

To request information on the message logs, the holder must contact TWT's Customer Care by sending an email from their own certified email mailbox to the certified email mailbox support@twtcert.it.

If it is impossible to access their own pec mailbox, the holder may contact TWT's Customer Care by telephone on the freephone number 800.192.800 to obtain further details on sending the log request by fax.

The request must contain the following data:

- TWT customer code and identifier of the party who signed the TWT PEC contract;
- reference date of the message;
- certified email address of the holder;
- certified email address of the recipient;
- photocopy of an identity document.

Where the request for information and extraction of the logs relates to a single PEC email ("single extraction"), TWT will carry out the activity free of charge. Should the request instead relate to the logs of multiple

PEC emails (“bulk extraction”), TWT will carry out the activity subject to a specific quotation accepted by the Customer.

Once the data have been acquired and, for bulk extraction, the Customer has accepted the quotation, TWT’s Customer Care will forward the request to the head of technical services, who will process it personally or delegate it to an operator of their department.

Once the information to be sent has been retrieved, the head of technical services (or the person delegated by them) will send it to the Holder of the certified email mailbox as agreed during the request stage.

Requests from the judicial authorities will require a formal communication from those authorities to the provider.

6 Conditions of supply

The service is governed and provided in accordance with current legislation and with the provisions of the Contract, which includes:

- the activation request;
- the commercial offer;
- the general conditions of supply;
- the annex containing the Operating Manual;
- the privacy notice;

All the documentation is available on TWT's institutional website at http://www.twt.it.

6.1 Introduction

- There is specific legislation and there are precise technical specifications issued by AgID that govern the provision of the certified email service.

- The PEC service can only be provided by providers entered in the public list of certified email providers kept by AgID (***Public List***).

On these premises, the conditions of supply of the service (***Conditions***) are set out below; they are to be considered essential conditions of the offer, specifically accepted by the ***Holder***, and failure to comply with them gives rise to the application of Art. 1456 of the Italian Civil Code.

6.2 Obligations and responsibilities

6.2.1 Parties to the Service

Within the scope of the ***SERVICE***, the following parties are identified:

PROVIDER	TWT S.p.a., which enters into the contracts for the sale of the ***Service*** with the ***Holders***, and operates as a Certified Email Provider entered in the ***Public List*** of ***AgID*** and that manages the certified email ***Domains*** with the related access, incoming and delivery points defined by current legislation.
HOLDER	the party that purchases the ***Service*** from the ***Provider*** so that it can be used by the persons belonging to its organisation.
USER	The person to whom the ***Holder*** has issued the credentials for accessing the ***Service*** provided by the ***Provider***. Where the ***Service*** is requested by a ***Holder*** for personal use, the ***User*** and the ***Holder*** are the same person.
SENDER	The ***User*** who makes use of the ***Provider***'s ***Service*** to send documents produced by means of IT tools.
RECIPIENT	The ***User*** who makes use of the ***Provider***'s ***Service*** to receive documents produced by means of IT tools.

6.2.2 Activities and obligations of the Provider

The ***Provider*** will provide the ***Service*** in accordance with the provisions of the applicable legislation, in the manner specified in this ***Operating Manual***.

In particular, the ***Provider*** is required to:

- comply with the mandatory technical rules;
- inform the ***Holders*** on how to access the service and on the technical requirements needed to access it;
- implement appropriate technical and organisational measures to ensure a level of security of its systems appropriate to the risk for the personal data processed, in accordance with current privacy legislation;
- guarantee the efficient, timely and secure operation of the ***Service***;

- provide the ***Sender***, belonging to a mail domain it manages, with the acceptance receipt containing the certification data;
- provide the ***Sender***, where the ***Recipient*** belongs to a mail domain it manages, with the delivery receipt containing the certification data;

- when the email message cannot be delivered, inform the ***Sender***, within 24 hours of sending, of the non-delivery;

- sign the receipts and the transport envelope with a digital signature;
- affix the time reference to each message that passes through the system;
- retain, as required by law, the file containing the logs of the messages that passed through the system. The file must be generated daily and contain the logs of the messages generated over a maximum interval of 24 hours. A time stamp must be affixed to each file generated;
- transmit the certified email message from the ***Sender*** to the ***Recipient*** intact in all its parts, enclosing it in the transport envelope;

- keep track, during all stages of transmission of the certified email message, of the operations carried out, in a specific message log;

- retain the log containing the message logs for thirty months;
- adopt appropriate technical and organisational solutions that guarantee the security, integrity and unalterability over time of the information contained in the message log referred to in the previous point;
- Adopt emergency procedures that ensure the completion of the transmission of the message and the issue of the receipts;
- Handle messages containing computer viruses in accordance with current legislation;
- Ensure the minimum service levels required by the attached technical rules;
- Ensure interoperability with the other certified email service providers.

The certified email ***Provider*** is liable for damage caused, through wilful misconduct or negligence, to any natural or legal person as a result of failure to fulfil the contractual obligations and those provided for by current legislation.

The ***Provider*** reserves the right to change the technical specifications for the provision of the ***Service*** in line with legislative and/or technological developments, making them known through the ***Operating Manual*** and subject to AgID approval, where such changes are significant or their publication is required by current legislation.

6.2.3 Exclusions, Limitation and insurance policy

The ***Provider*** will in no way be liable for the following:

- damage of any kind, direct or indirect, or harm suffered by anyone as a result of events arising from acts of the Public Authorities, unforeseeable circumstances, force majeure or other causes not attributable to the ***Provider*** (such as, purely by way of example and not limited to, failure or malfunction of networks, equipment or technical instruments outside the ***Provider***'s control, interruptions in the electricity supply, earthquakes, explosions, fires), except in cases of wilful misconduct or negligence;
- damage of any kind, direct or indirect, or harm suffered by anyone to the extent that such damage
  - arises from the breach of obligations which, under the ***Operating Manual*** or the provisions of current law, are incumbent on the ***User***, the ***Sender***, the ***Recipient***, and those who receive messages transmitted by means of the ***Service;***
  - could have been avoided or limited by knowledge of the provisions contained in the ***Operating Manual*** on the part of the ***Holder***, the ***User***, the ***Sender***, the ***Recipient***, and those who receive messages transmitted by means of the ***Service***
  - arises from the incorrect use of identification codes by the ***Holder*** and the ***User;***
  - arises from the failure to send or deliver messages where caused by anomalies reported, as the case may be, to the ***Sender*** or to the Recipient who have not responded to the anomaly communication sent by the ***Provider;***
  - arises from delays, interruptions, errors or malfunctions of the ***Service*** not attributable to the ***Provider*** or arising from incorrect use of the ***Service*** by the ***Holder*** or the ***User;***
  - arises from the application of the legislative provisions on the handling of messages with malicious content or containing computer viruses;
  - is outside the minimum service levels provided for by current legislation;
  - arises from the use of the ***Service*** outside the current legislative provisions or from the use of email services provided by providers not included in the public list kept by AgID;

Email messages may be subject to delays in their transmission over the Internet; therefore the ***Provider*** accepts no liability, save in the case of wilful misconduct or negligence, for such delays.

The ***Provider*** is released from any power of control, mediation or supervision over the content of the messages sent by the ***Users*** and accepts no liability for their unlawful content or content contrary to morality or public order, as the ***Provider*** has no obligation to delete the content of the messages.

The ***Provider*** assumes no obligation, guarantee or liability beyond those arising from the contract for the supply of the ***Service*** and from current legislation.

The injured party loses the right to compensation for damage attributable to the ***Provider*** if they do not submit a reasoned written complaint to the ***Provider*** within 10 days of the occurrence of the harmful event.

The ***Provider*** has taken out an insurance contract covering the risks of its activity and damage caused to third parties, with these maximum limits:

- **€1,000,000 per single claim**
- **€1,000,000 per year.**

6.2.4 Obligations of the HOLDER

By accepting the provisions of these Conditions of Supply, the ***Holder*** assumes the following obligations:

- consult the ***Operating Manual*** in advance and know its contents;

- provide all the information and documentation requested by the ***Provider*** that is necessary for correct personal identification, guaranteeing, under their own responsibility, its reliability pursuant to current legislation;
- expressly inform the ***Users*** of the obligations they assume with regard to the use of the ***Service;***
- where requested, give consent to the processing of personal data pursuant to current privacy legislation;
- keep, and have the ***Users*** keep, the access codes to the ***Service*** with the utmost confidentiality and diligence;
- immediately inform the ***Provider*** if the confidentiality of the access codes for using the ***Service*** is compromised;

- not use or allow third parties to use the ***Service*** for unlawful purposes or to make communications contrary to the law, morality or public order;
- not use, and not allow the Users to use, the ***Service*** for the purpose of storing, sending, publishing, transmitting and/or sharing applications or electronic documents that conflict with or infringe intellectual property rights, trade secrets, trademarks, patents or other proprietary rights of third parties;
- not allow third parties not authorised by the ***Holder*** to use the ***Service***, for which the ***Holder*** will in any case be responsible

The ***Holder*** acknowledges that on expiry of the contract or in the event of its termination it will no longer be possible to access the ***Service*** and its content, and therefore undertakes to inform the ***Users*** accordingly, releasing the ***Provider*** from any liability arising from the lack of access.
The ***Holder*** also acknowledges that the content of the mailbox on the TWT Infrastructure at the time of termination will be kept for a further 6 months purely as a courtesy, without the ***Provider*** assuming any obligation to do so: any liability of the latter in the event of total or partial loss of or damage to the mailbox itself is therefore excluded. Once this period has elapsed without the ***Service*** being reactivated, the data on that Infrastructure will be permanently deleted and can no longer be recovered. This provision also applies where the "Historical archive" option, as specified in the commercial offer, is active.

7 Service levels

The provider TWT guarantees the users of the service the ability to send certified email messages in accordance with current legislation:

- lists of up to 50 recipients;
- a limit of 100 MB for the product of the number of recipients and the size of the message when using an email client;
- a limit of 50 MB for the product of the number of recipients and the size of the message when using the webmail;
- a technical limit of 1,000 messages sent per hour, in the case of bulk sending, for reasons related to the security of the service.

The certified email service is available 24 hours a day, 7 days a week, with operation equal to 99.8% of the reference period, which is a four-month period.

The maximum duration of each single event of service unavailability does not exceed 50% of the total allowed in the four-month period.

The receipts provided for by the system and intended for the users of the service, during the period of availability of the service, reach the sender within the times provided for by current legislation.

Pursuant to CR/51, TWT has set up an appropriate internal information structure to provide AgID periodically with information on the operation of the certified email service (no. of mailboxes activated, no. of incoming and outgoing messages, viruses detected by the system, service levels provided), and on malfunctions and service disruptions detected.

In order to ensure a high level of transparency towards its customers, TWT has set up an information system that, where the PEC service cannot be used, informs the TWT customer in real time of the time of downtime and uptime of the service. Depending on the degree of malfunction of the Service, the information will be provided by e-mail to the traditional email mailbox provided at the time of activation of the service.

The service level refers to TWT's systems up to the internet connection, thus excluding the internet network, whose service level is the responsibility of the customer's provider.

7.1 Quality indicators

The quality indicators of the certified email service are described below.

DESCRIPTION	THRESHOLD VALUES (OR RANGES OF VALUES)
Availability of access to the certified email service (sending/receiving mail)	7 days a week 24 hours a day
Maximum duration of a single maintenance event involving service downtime	1 hour 20 minutes
Maximum duration of all maintenance events involving service downtime in the reference period (four-month period)	2 hours 40 minutes
Automatic monitoring of the systems (see 8.4)	7 days a week 24 hours a day
Availability of the call centre for customer support	working days from 8.30 to 19.00

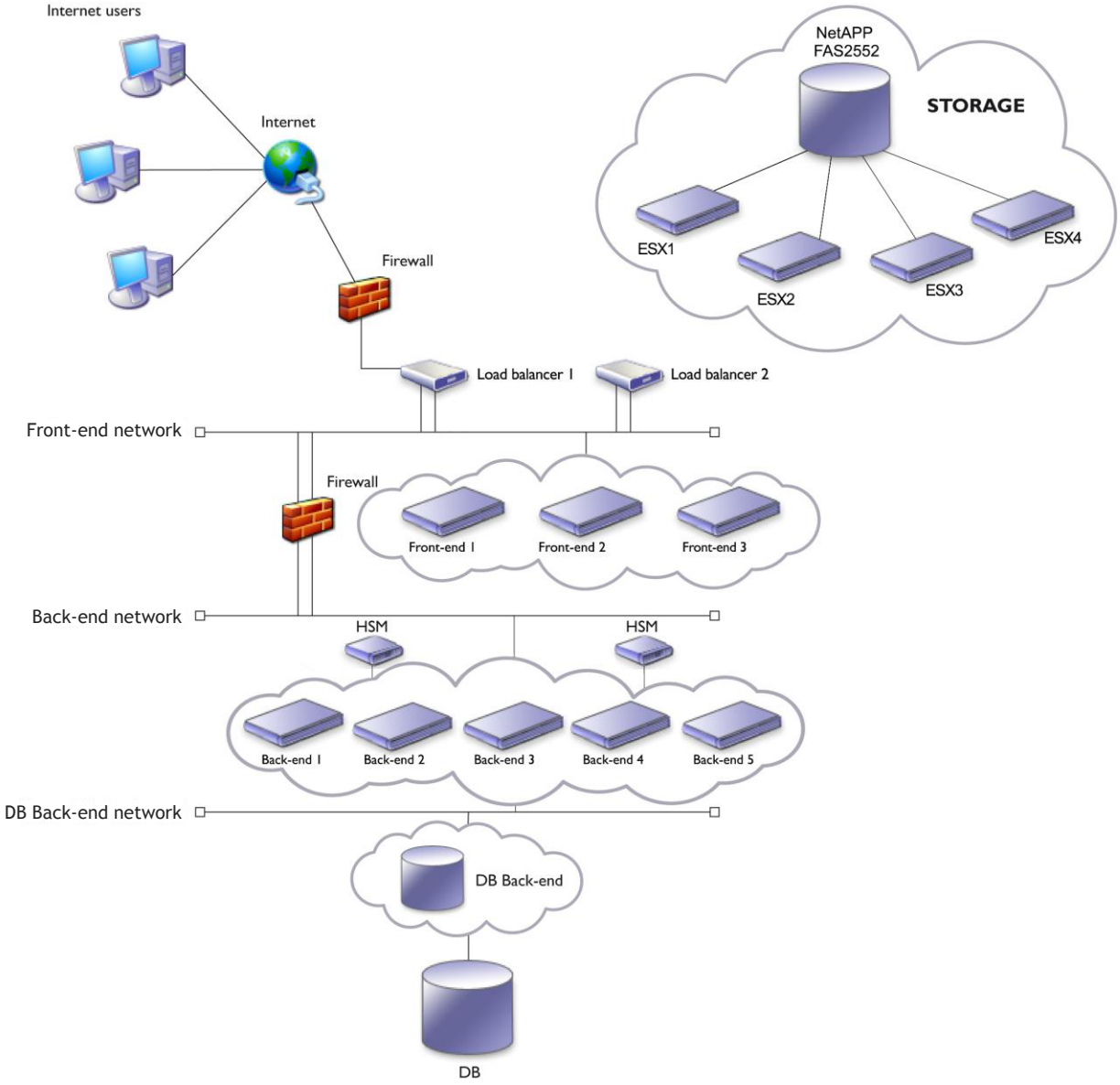
8 Technological systems / infrastructures

8.1 System

In order to guarantee maximum service availability and Fault tolerance, the entire technological system is based on a fully redundant architecture; this architecture is located at TWT's data centre (CED) in Milan.

8.1.1 Structure

The following figure shows the technological structure in use:



The proposed solution provides for a firewall, connected directly to the internet *Core Routers*, which protects the Front-End network from unwanted access. The Firewall is in turn connected to the Load Balancer, which acts as a layer of abstraction between the Internet and the Front-end servers. Users access a Virtual IP address (VIP) on the load balancer, which distributes all requests to the Front-End servers.

These servers accept and validate user requests and forward incoming mail to the mailboxes and outgoing mail to the other mail servers (other certified email providers or other ordinary mail servers).

To access the mail data, the Front-End servers must connect to the Back-End cluster, three or more servers that share the activities in hot-standby mode (if a server has problems or has to be stopped for maintenance, the other members of the cluster take over its activities); to do so they must pass through another firewall, which creates a further layer of abstraction between the Front-End network and the Back-End network.

The servers that make up the back-end cluster in turn need to store the Logs of the transactions they handle in an external SQL Database.

All the servers that make up the PEC infrastructure (front-end, back-end and DB) are virtual servers based on 3 clustered hosts on which the VMWare ESXi Hypervisor is installed.

Both the Back-End cluster and the SQL Database write their information to an external Fiber Channel storage unit equipped with RAID-5 disks, fully redundant in all its parts.

8.1.2 Scalability

The scalability of the entire service, i.e. its ability to adapt to an increase in users and/or performance, is based on the scalability of the individual components.

All the software components in the infrastructure are in fact scalable both vertically (i.e. by increasing the internal system resources to support greater computing power) and horizontally (i.e. by adding new servers alongside the existing ones).

8.1.3 IT Security

As already mentioned, decoupling the logical layer of user access (Front-End) from the logical layer in which the data are actually stored (Back-End) and from the further logical layer in which the logs are actually stored (DB-Back-End) increases the security of the system. Decoupling is achieved by means of Firewall devices.

The system is protected against viruses by integration with the ClamAV antivirus software, supplemented by additional commercial signatures.

For encryption, decryption and digital signature functions, the backend servers use a pair of external HSMs.

All the security certificates used for these functions are stored within the HSMs, which, by means of protection mechanisms, ensure that this information is not misused (copying, alteration, etc.).

8.1.4 Reliability and fault-tolerance

On the Front End, the reliability of the Service is guaranteed by the full redundancy of the individual components of the system and by their balancing through the Load Balancer device.

To guarantee high reliability, the Back End systems use the cluster configuration of the machines and the clustering of the services.

All the servers involved are virtual and high reliability is guaranteed by a cluster of 4 physical VMWare ESXi 6.0 Hosts with Fault Tolerant and High Availability functions.

The data (mailboxes, logs, etc.) are physically stored on an external *Disk Array*, fully redundant (logic, connectivity, power supply, etc.), which stores the data on RAID-5 partitions.

A special feature of high reliability is tolerance to system "faults": if a component of a machine fails, there is always a redundant service that can step in and temporarily replace it, thus avoiding service disruption.

8.2 System logs

All the application components of the certified email service record all the operations carried out in specific Log files, keeping track of the information that makes up each individual event within the system. By way of example, here is some of the information stored:

- system events;
- connections established;
- presence of viruses;
- protocols used;
- synchronisation of systems;
- any anomalies;
- signature checks;
- encoding and decoding of messages.

The data stored may vary from event to event and from component to component.

In addition to the Logs on file (generated by all system components), Logs on Database are also created exclusively for the back-end components, covering all the events that concerned each individual message. By way of example, here is some of the information stored:

- unique original identifier of each message;
- date and time;
- type of event (acceptance, sending, receipt, notices, receipts, etc.);

- sender;
- recipients;
- subject of the message;
- anomalies.

To guarantee the time synchronisation of all the components of the system, the NTP (Network Time Protocol) is used. Synchronisation takes place using several public ***Time Servers*** as the time reference.

8.2.1 Logs on File

All the system components (back-end and front-end) that generate Logs on File close and open a new Log file every day. These Log files do not reside on the Back-end / Front-end servers, but on a fully redundant external storage in ***High Availability (HA)*** configuration.

8.2.2 Logs on Database

The back-end components store, in an external database managed by the physical VMWare cluster, all the events that concerned each individual message handled by the Certified Email system; as in the previous paragraph, these data are also stored on a fully redundant external storage in ***High Availability (HA)*** configuration.

These databases are exported to file every day and are added to the log files already generated in the previous point.

8.2.3 Archiving

Every day all the log files generated are compressed into a single file; this file is time-stamped and retained in accordance with the procedures defined in the "instructions for the retention of message logs and of certified email messages with viruses" published on the AGID website.

8.2.4 Querying

At any time it is possible to retrieve the previously archived files in order to query the logs of an entire day or of a single transaction processed by the PEC system.

8.3 Data security

As already mentioned above, in order to guarantee the highest possible level of service, all important data (mailboxes, event logs, etc.) events are stored on an external Fiber Channel Disk Array, equipped with disks in RAID-5 configuration, redundant in all its parts.

8.3.1 Data backup

The storage system in use for the PEC system uses "Snapshot" logic to periodically take a picture of all the data. These pictures are taken every 2 hours for the current day and once a day for the following days, up to 30 days. The storage is also replicated every 15 minutes to twin equipment located at a remote site; TWT operators are responsible, in accordance with internal policies, for:

- checking daily that the storage systems are working properly and the status of the replicas;
- carrying out ordinary and extraordinary maintenance of the equipment.

8.3.2 Data restore

Where it becomes necessary to restore data, due to accidental loss or incidents, it is possible to restore anything from a single message log up to the entire system.
The restore procedure is the responsibility of the TWT technical department, using suitably trained staff.

8.4 Monitoring

TWT S.p.A. has developed a suite of proprietary software for the monitoring and auditing of all the hardware and software components that make up the technological infrastructure.

This software is developed using the most widespread standard protocols (syslog, snmp, etc.), ensuring integration with the majority of the

systems on the market. Should it become necessary to monitor a *non-standard* system, TWT develops a specific integration in-house.

The components that the system can monitor include:

- PING Check
  Checks that an IP address can be reached; it is therefore possible to check that any device connected to the network is physically operational (pc, server, router, switch, etc. Etc.);

- TCP/UDP Port Check
  Checks that one or more TCP/UDP ports can be reached on a given IP address; in this way it is possible to check that a particular service is active on that device;

- Service Check
  Checks that a given program is running on the machine being checked;

- Cluster Check
  Checks the operation of all the machines that work in cluster mode;

- Disk Space Check
  Checks the space available on the disk of a given server, setting alarm thresholds;

- HTTP Query
  Checks the operation of an HTTP server, checking not only that the server can be reached but also interpreting its response and acting accordingly;

- SNMP Query
  Of all the components that can be monitored, this is considered the broadest in terms of possibilities: the SNMP protocol (acronym of Simple Network Management Protocol) is a standard whereby all the components that use it (both hw and sw) make available a logical and standard structure for accessing the information of the component being queried. The information made available varies from component to component, from status information to statistical information.
  Purely by way of example and not limited to, here are some examples:

- *Server*
  - *Temperatures (Fan, CPU, Power, Ambient, ...);*
  - *Operation of boards (Lan, SCSI, Fiber, ...);*
  - *Memory status;*
  - *Active processes;*

- *Router*
  - *Temperatures;*
  - *Memory;*
  - *Workload;*
  - *Peering status;*

Therefore, by means of this component, it is possible to monitor in all its parts any hw or sw that uses this standard.

When the monitoring system detects an anomaly, on the basis of the rules configured, it can take a series of informative and/or corrective actions:

- send emails to all the addresses predefined for the specific rule, reporting the anomaly detected;
- send SMS messages to all the mobile numbers predefined for the specific rule, reporting the anomaly detected
- if provided for, run external software, passing as parameters those configured on the rule;
- if provided for, carry out specific operations (restarting equipment, resetting software, restarting applications, etc.), informing the staff in charge by email and/or sms of the result of the operation carried out;

- if and when the problem is solved (automatically or following human intervention), the system informs (by email and/or sms) all those concerned of the change of status.

TWT S.p.A. staff are adequately and appropriately trained to interpret, manage and resolve the various anomalies that arise, intervening remotely where possible (via VPN access) or locally at the data centre.

8.5 Time Stamping

Time stamping is like a digitally signed message that securely binds an electronic document (file) to a certain date and time that is valid against third parties.

All transmission logs, when they are archived daily or also when they reach a certain defined size, are time-stamped by affixing a time reference (stamp) that is valid against third parties under the legislation. The Time Stamping service is understood to be provided by an authority (Certification Authority, CA) entered in the relevant list drawn up by AgID of Time Stamping Authorities.

8.6 Interoperability

In compliance with current legislation, TWT S.p.A. undertakes to guarantee interoperability with the other providers in accordance with the Certified Email rules.

TWT also carries out periodic interoperability checks by sending and receiving test messages to and from the other accredited PEC providers.

8.7 Description of the data centre

TWT S.p.A. has a data centre of approximately 600 m² which houses all the company's technological infrastructure.

The building has a 23,000-volt medium-voltage electrical substation, with 2 transformers of 1,000 KVA; the whole circuit is fully redundant. The electrical substation is connected to 2 separate generator sets, redundant to each other in warm/standby mode, Perkins brand, 1,000 KVA each, equipped with remote control and alerts to those responsible for the plant in the event of anomalies.

All the equipment in the data centre is protected by 2 UPS units of 160 KVA each.

The data centre has a Schneider Electric chilled water air-conditioning system made up of 3 chiller units with 2

compressors each, equipped with the free-cooling function and controlled by a proprietary microprocessor; the system is equipped with remote control for sending alarms to the maintenance company and to the TWT managers in the event of problems/faults.

Each cabinet (rack) in the data centre has 2 power supplies of 16A or 32A from separate lines; this allows equipment with redundant power supplies to be connected to two separate electrical lines.

In order to guarantee a sufficient level of security of the data centre and ensure that activities are carried out in accordance with the required requirements, the following security measures have been put in place:

Physical access to the premises is controlled by electronic systems that allow entry only to authorised staff; all persons accessing the data centre are identified by means of a personal badge, which can prevent access by unauthorised staff; the system is also able to carry out *auditing* of staff entering/leaving the data centre.

Logical access to the IT systems takes place through the use of a personal user name and password that can securely identify the staff accessing them.

The number of people authorised for physical/logical access is kept to a minimum in order to guarantee greater security.

A video surveillance system with continuous recording on Hard Disk (KDVR) operates on the premises, connected to the internal network and accessible only to the staff responsible for security with personal user names/passwords.

There is also an Anti-theft/Anti-intrusion system with motion sensors in the rooms and continuity contacts on doors and windows.

This system is equipped with:

- sirens/flashing lights that activate in the event of an alarm;
- 2 telephone diallers (1 analogue and 1 GSM mobile) that call TWT managers in the event of an alarm;
- IP connection to the internal network for management and monitoring of the whole system;

9 Operational Aspects

9.1 Notes on staff organisation

The staff responsible for providing and controlling the certified email service are organised in accordance with Art. 21 of the [DM].

In particular, the following organisational roles are defined:

- Head of holder registration;
- Head of technical services;
- Head of checks and inspections (auditing);
- Head of security;
- Head of message log security;
- Head of the time reference system.

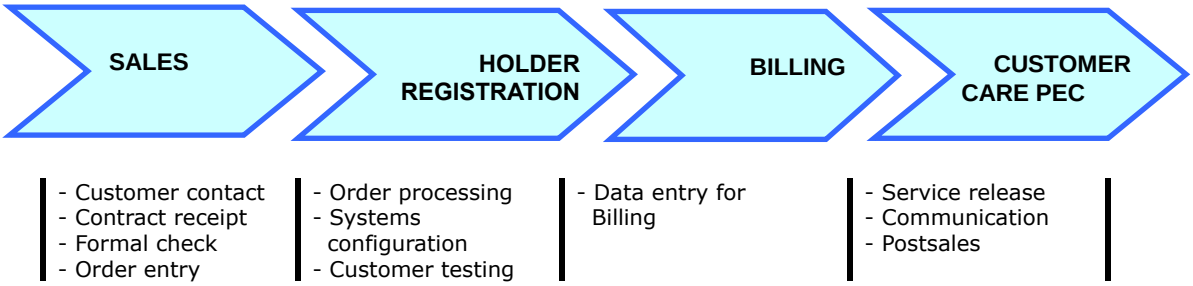
Some professional roles may perform several mutually compatible functions. In particular, the head of security is also responsible for the security of the message logs and of the time reference system.

In performing the functions for which they are responsible, the roles listed above may make use of their own staff, who will operate in accordance with the conduct specifications defined by the head.

All the professional roles involved in the management/supervision of the Certified Email system are appropriately trained through training courses held internally or externally.

9.2 Organisational Flow

The activation process of the TWT PEC service provides for the following operational flow, which involves various company areas and functions from the first contact with the customer up to the release of the service.



This flow is governed and controlled by the managers described in the previous paragraph.

The customer's initial contact is handled by the internal sales structure, which, once it has received the registration request, manages the activities for initiating the order entry process in the TWT management system.

In general, each customer is assigned a sales account manager, who will be their preferred point of contact with TWT.

The operational management of the service and the related contact are instead entrusted to TWT's Customer Care, which, among its main post-sales tasks, is in charge of managing support for PEC customers.

9.3 Support Management Procedures

The support management procedure for the Certified Email service defines and describes the criteria and methods for providing the support requested.

The support service is expressly provided for in the contract and is provided to users registered with the TWT certified email service and to the administrator of certified email mailboxes hosted on a domain owned by the customer.

The service provided by TWT Customer Care is available from 8.30 to 19.00, Monday to Friday excluding public holidays, and can be reached:

- on the freephone number 800.192.800
- by email at support@twtcert.it

The user can request support for the following reasons:

- support during the configuration of the certified email mailbox;

- inability to access the Mail Server;
- support in using the web client;
- support during the configuration of electronic certificates in email clients;
- request for information on certified email (legal validity, features, etc.);

- request for information on interoperability with the other certified email operators;
- loss of the user-id for accessing the service;
- support in the event of loss of the password: TWT will send a reset email containing the instructions needed to set a new one;

- request for message logs;
- requests relating to user support material (for example availability of the user manual or updates);
- compatibility of the email client with the service provided by TWT;
- other information relevant to being able to use the service.

The administrator of certified email mailboxes hosted on a domain owned by the customer may, on the other hand, request support for the following reasons:

- request for assistance when creating a certified email mailbox in their own domain;
- inability to access the service;
- request for information on the service;
- request for assistance in changing user details;
- request for assistance in resetting a user password;
- request to restore receipts;
- requests relating to administrator support material;
- request for support in registering users;
- other information relevant to being able to use the service.

9.4 Emergency management

In order to guarantee the continuity of the service, the automatic monitoring systems (paragraph 8.4) promptly inform TWT's on-call staff of the anomalies detected, and they intervene by analysing the problem and, if possible, solving it or, if necessary, escalating the problem to the required level of technical expertise or responsibility.

When the problem occurs, the person on call carries out these activities:

- Informs their direct manager of the anomaly detected.
- Opens an Internal Trouble Ticket to keep track of the problem.
- For any report from customers, another Trouble Ticket is opened and linked to the Internal Trouble Ticket opened previously.

- If unable to solve the problem independently, involves other internal specialist technicians.
- If necessary, contacts any suppliers who can help solve the problem.

- If the problem persists, informs, if not already aware of it, the PEC Service Manager, with whom the most appropriate activities needed to solve the problem will be agreed.
- Inform, in the manner provided for by the contracts, all PEC customers of the anomaly in progress.
- Inform AgID, in the manner and within the times set by [CR/51].

Once the problem has been solved, the Internal Trouble Ticket and all the related Trouble Tickets are closed, and the customers who experienced the problem are contacted to inform them that it has been resolved.

10 Protection of personal data (Privacy)

The data controller is TWT S.p.A., with registered office in Milan, Via Abbondio Sangiorgio n. 12, 20145, and Operating Office in Milan, Viale E. Jenner n. 33, 20159.
TWT has appointed its own Data Protection Officer, who can be contacted at the email address dpo@twt.it.

The personal data processed are:

- the data provided at registration by the mailbox holder;
- the data on the copy of the identity document of the mailbox holder;
- the data arising from the performance of the services requested (sending and receiving pec messages)
- any personal data contained in pec messages and in the related attachments.

The data are processed for the provision of the service. They may be disclosed to anyone who, having a lawful and proven interest, including outside the European Union, requests to ascertain the ownership of the email mailbox assigned to the data subject or to obtain an account of the messages exchanged and/or their content.

Providing the personal data requested at registration is mandatory, and any refusal makes it impossible to provide the service.

With the consent of the data subject, the data provided by the data subject at registration may be used for the purposes of direct sale of its own products or services, for marketing purposes, for the promotion of activities and for the presentation of TWT's initiatives.

The data retention period is set by law.

The data may also be disclosed or made accessible to companies controlled by and/or associated with TWT, to other Companies that maintain the IT systems and to the parties that handle specific stages of the processing, as processors on behalf of TWT, whose names are available to data subjects on request.

The data subject has the right to ask the data controller for access to and rectification or erasure of the personal data and restriction of processing. They also have the right to object to the processing of their personal

data and the right to data portability. They can exercise their rights by writing to dpo@twt.it.
Finally, the data subject has the right to lodge a complaint with the Italian Data Protection Authority.

10.1 - Security measures to protect personal data

The provider processes personal data in compliance with the applicable personal data legislation, adopting the technical and organisational measures necessary to guarantee a level of security of its systems appropriate to the risk relating to the personal data processed.

With reference to the registration DB, it should be noted that:

- the registration DB and the related management application reside on a dedicated computer, located in a technical room with controlled access;

- to access the application, operators identify themselves by means of unique, personal credentials;
- the application keeps an accurate record, in a specific audit log, of every operation carried out;
- a backup copy of the database and of other information essential for restoring the system in the event of computer failure or accidental loss of data is produced periodically.

With reference to certified email messages, it should be noted that communication between the user's web interface and TWT's PEC system takes place through secure protocols and connections (SMTP+SSL, IMAP+SSL, POP3+SSL, HTTPS), and that only accredited users who have passed the security checks can access their own TWT certified email mailboxes.

This document is an English translation of the original Italian document and is provided for ease of reference. The translation may contain errors, omissions or inaccuracies. In the event of any discrepancy or inconsistency between this translation and the Italian original, the Italian original shall prevail to the extent permitted by applicable law.