POSTA ELETTRONICA CERTIFICATA
Manuale Operativo

Ver. 2.4 del 15/02/2022

Redatto da:	Massimo Barbero Pini *Enterprise Architect*	_____	15/02/2022
Verificato da:	Fabrizio Amodio *Responsabile del Servizio PEC*	_____	15/02/2022
Approvato da:	Simone Staffa Guidi *Presidente e Amministratore Delegato*	_____	22/02/2022

INDICE

1 Generalità

1.1 Scopo del documento

Questo documento vuole descrivere le regole e le procedure seguite da TWT S.p.A. nell'erogazione del servizio Posta Elettronica Certificata.

Il manuale si basa sulle disposizioni tecniche ai sensi del DM 2 novembre 2005 e alla circolare CNIPA del 21 maggio 2009, n. 56.

1.2 Denominazione del documento

Il presente documento chiamato ***Manuale Operativo*** è stato internamente codificato con il nome di ***TWT_PEC_Manuale Operativo***.

1.3 Responsabilità del Manuale Operativo

Il presente documento è sotto la responsabilità del sig. Fabrizio Amodio, Responsabile del Servizio PEC, che è contattabile per qualsiasi informazione o chiarimento riguardante il presente manuale al numero 02-890891 oppure via Email all'indirizzo f.amodio@twt.it.

1.4 Aggiornamento del Manuale Operativo

In caso di variazioni tecniche, operative o legislative, TWT S.p.A. aggiornerà, previa approvazione dei responsabili di TWT S.p.A. e dell'Agenzia per l'Italia Digitale, il presente Manuale Operativo.

1.5 Reperibilità del Manuale Operativo

Il presente documento è disponibile per la libera consultazione ed il download sul sito istituzionale di TWT S.p.A. al seguente indirizzo:

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

1.6 Versione del Manuale Operativo

La versione e la data di rilascio del presente Manuale Operativo sono indicati in calce ad ogni pagina.

Nella seguente tabella sono elencate le modifiche apportate al presente documento unitamente alle relative date di validità.

Descrizione Modifica	Versione	Data
Prima emissione	1.0	12/04/2007
Modificato URL per Webmail a pag. 5 Modificata porta SMTPS a pag.28 Modificata figura 8 a pag. 32 Modificate figura 11 e 12 a pag. 34 Modificata figura 13 a pag. 35	1.1	21/11/2007
Par. 1.8 Inserita Certificazione Sistema QUALITA' norma UNI EN ISO 9001:2000 Par. 5.4.1 Modificata figura 9 Par. 8.2.3 Modificata l'archiviazione Log Par. 8.3.1 Modifica procedura di Backup	1.2	23/06/2008
Par. 8.1.3 Modificata tipologia apparati HSM	1.3	12/01/2010
Aggiornamento normativa di riferimento su tutto il manuale	1.4	15/03/2010
Aggiornamento piattaforma tecnologica e riferimenti normativi	1.5	23/04/2012
Aggiornamento piattaforma tecnologica e riferimenti normativi	1.6	24/01/2014
Par. 3.4 Aggiunta descrizione funzionalità di blocco posta PEO, inoltro e filtro AntiSpam PEO	1.7	21/05/2014
Par. 4.1 Adeguamento alla circolare AgID sulla riassegnazione delle caselle di posta PEC Par. 6.2.4 conservazione dei dati in caso di cessazione del servizio PEC	1.8	07/08/2015
Par. 7 Ampliamento dimensione massima dei messaggi di posta	1.9	12/05/2016

Par. 1.7 Dati identificativi del gestore Capitolo 8 Revisione Generale	2.0	01/04/2017
Par. 1.7 Dati identificativi del gestore Par. 1.8 Certificazioni Qualità Par. 5.1 Accesso Standard / Webmail Par. 5.2 Protocolli Par. 5.3.1 Configurazione client Microsoft Outlook Revisione Generale	2.1	19/12/2019
Par. 6.2.2 Attività e obblighi del Gestore Par. 6.2.3 Esclusioni, Limitazione e polizza assicurativa	2.2	09/01/2020
Par. 5.4.1 Configurazione client Microsoft Outlook con POP3S e correzione refusi Par. 5.5.1 Esplicitazione del meccanismo di quotazione per richiesta informazioni su log Par. 10 Protezione dei dati personali (Privacy) Par. 10.1 Misure di sicurezza a protezione dei dati personali	2.3	04/06/2021
Par. 7 Livelli di servizio	2.4	15/02/2022

1.7 Dati identificativi del Gestore

Il servizio di Posta Elettronica Certificata è erogato dall'organizzazione iscritta nell'elenco pubblico dei gestori ai sensi dell'Art. 14 del DPR 11 febbraio 2005, n. 68 e identificata come segue:

Denominazione sociale:	TWT S.p.A.
Indirizzo sede legale:	Via Sangiorgio, 12 – 20145 Milano
Indirizzo sede operativa:	Viale Jenner, 33 – 20159 Milano
Legale rappresentante:	Simone Staffa Guidi (Presidente del Consiglio di Amministrazione)
N° di iscrizione Registro Imprese Milano:	11422580156
N° di Partita IVA:	11422580156
N° di telefono (centralino):	+39 02 890891
N° di telefono assistenza:	800 192 800
E-mail assistenza:	support@twtcert.it
Sito web generale:	http://www.twt.it
Sito webmail PEC:	https://webmail.twtcert.it
E-mail (informativo):	info@twtcert.it
E-mail PEC:	twt@pec.twt.it

1.8 Certificazione Qualità

TWT ha adeguato la certificazione del Sistema di Gestione per la Qualità in conformità alla norma UNI EN ISO 9001:2015. Lo scopo di certificazione è: "*Progettazione, erogazione ed assistenza di servizi di Telecomunicazione nazionali ed internazionali ai clienti ed ai reseller. Erogazione del servizio di Posta Elettronica Certificata (P.E.C.)*".
TWT ha ottenuto la certificazione in conformità alla norma ISO 27001 il 22 luglio 2019.

2 Riferimenti tecnici e legislativi

2.1 Riferimenti normativi

General Data Protection Regulation [GDPR]
Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati) del 27 aprile 2016

DPCM 13/01/2004 [DPCM]
Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 – "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici" (pubblicato sulla Gazzetta Ufficiale n. 98 del 27 aprile 2004) e successive modifiche ed integrazioni.

DPR 68/2005 [DPR]
Decreto del Presidente della Repubblica 11 febbraio 2005 n. 68 "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata a norma dell'articolo 27 del 16 gennaio 2003, n. 3" (pubblicato sulla Gazzetta Ufficiale n. 97 del 28 marzo 2005).

DM 02/11/2005 [DM]
Decreto ministeriale 2 novembre 2005 della Presidenza del Consiglio dei Ministri Dipartimento per l'Innovazione e le Tecnologie, "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata" (pubblicato sulla Gazzetta Ufficiale n. 266 del 15 novembre 2005).

Decreto Legislativo 82 del 7/3/2005 [CAD]
"Codice dell'amministrazione digitale" (pubblicato sulla Gazzetta Ufficiale n. 112 del 16 maggio 2005, supplemento ordinario n. 93) e sue successive modifiche ed integrazioni (Decreto Legislativo 4 aprile 2006 n. 159, pubblicato sulla Gazzetta Ufficiale n. 99 del 29 aprile 2006, supplemento ordinario n. 105 è stato successivamente modificato e integrato prima con il decreto legislativo 22 agosto 2016 n. 179 e poi con il decreto legislativo 13 dicembre 2017 n.217).
Il CAD reca le disposizioni in base alle quali lo Stato, le Regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la

trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale mediante le tecnologie dell'informazione e della comunicazione.
In vigore dal 1° gennaio 2006, esso abroga tra le altre le disposizioni del DPR 445/2000 relative alla trasmissione del documento informatico (art. 14) e sottopone la disciplina del servizio di posta elettronica certificata alle disposizioni contenute nel DPR 68/2005.

Circolare CNIPA 51/2006 [CR/51]
"Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell'elenco dei gestori di posta elettronica certificata (PEC) di cui all'articolo 14 del Decreto del Presidente della Repubblica 11Febbraio 2005 n. 68" (pubblicata sulla Gazzetta Ufficiale n. 296 del 21 dicembre 2006).

Circolare CNIPA 56/2009 [CR/56]
"Modalità per la presentazione delle domande di iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata (PEC) di cui all'art. 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68" (pubblicata sulla Gazzetta Ufficiale n. 168 del 22 luglio 2009).

D'ora in poi nel presente documento i riferimenti normativi esposti verranno nominati con le abbreviazioni sopra definite in parentesi quadra.

2.2 Standard tecnologici

Il servizio di Posta Elettronica Certificata erogato da TWT è conforme agli standard di riferimento tecnico le cui specifiche sono riportate nell'allegato tecnico al [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 Definizioni

AgID
Ai sensi del decreto legge n. 83/2012, convertito in legge n. 134/2012, l'ente DigitPA è stato soppresso ed è stata istituita l'Agenzia per l'Italia digitale (AgID). La normativa PEC attribuisce all'Agenzia per l'Italia digitale le seguenti competenze:

- l'Agenzia definisce le regole tecniche e provvede al loro aggiornamento in funzione dell'evoluzione tecnologica e dell'esperienza derivante dall'utilizzo del sistema. L'Agenzia pubblica gli aggiornamenti in coerenza con gli standard specificati dalla normativa.
- l'Agenzia gestisce l'elenco pubblico dei gestori di posta elettronica certificata. Accoglie e valuta le domande presentate dai soggetti che si candidano al ruolo di gestori di posta elettronica certificata, decretandone l'iscrizione nell'apposito elenco o respingendone la domanda per carenza di requisiti. L'Agenzia fornisce agli iscritti i certificati per la firma elettronica delle ricevute e per l'accesso e l'aggiornamento dell'Indice dei Gestori PEC (IGPEC). I gestori devono presentare all'Agenzia eventuali modifiche dell'assetto societario, delle caratteristiche del servizio e delle procedure adottate, con particolare riguardo agli aspetti di continuità, funzionamento e sicurezza.
- l'Agenzia vigila e controlla le attività esercitate dai gestori iscritti nell'elenco. A tal fine, l'Agenzia emette circolari esplicative e di indirizzo, acquisisce bimestralmente informazioni relative al numero di domini PEC, al numero di caselle PEC e al numero di messaggi scambiati al fine di produrre statistiche relative alla diffusione e all'utilizzo della PEC, esegue periodicamente test di interoperabilità sui sistemi di PEC in esercizio presso i gestori e può accedere presso le sedi dei gestori per effettuare attività di verifica circa la conformità del sistema PEC.
- l'Agenzia fornisce supporto e diffonde la conoscenza del sistema PEC presso le amministrazioni e i privati.

Avviso di mancata consegna
L'avviso, emesso dal sistema, per indicare l'anomalia al mittente del messaggio originale nel caso in cui il gestore di posta elettronica certificata sia impossibilitato a consegnare il messaggio nella casella di posta elettronica certificata del destinatario.

Avviso di non accettazione
L'avviso, sottoscritto con la firma del gestore di posta elettronica certificata del mittente, che viene emesso quando il gestore mittente è impossibilitato ad accettare il messaggio in ingresso, recante la motivazione per cui non è possibile accettare il messaggio e l'esplicitazione che il messaggio non potrà essere consegnato al destinatario.

Busta di anomalia
La busta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, nella quale è inserito un messaggio errato ovvero non di posta elettronica certificata e consegnata ad un titolare, per evidenziare al destinatario detta anomalia.

Busta di trasporto
La busta creata dal punto di accesso e sottoscritta con la firma del gestore di posta elettronica certificata mittente, all'interno della quale sono inseriti il messaggio originale inviato dall'utente di posta elettronica certificata ed i relativi dati di certificazione.

Casella di Posta Elettronica Certificata
La casella di posta elettronica posta all'interno di un dominio di posta elettronica certificata ed alla quale è associata una funzione che rilascia ricevute di avvenuta consegna al ricevimento di messaggi di posta elettronica certificata.

Certificatore
Il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime.

Certificato Elettronico
L'attestato elettronico che collega all'identità del titolare (persona fisica cui è attribuita la firma elettronica ed ha accesso ai dispositivi per la creazione della firma elettronica) i dati utilizzati per verificare la firma elettronica.

Certificato Qualificato
Il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciato da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva.

Certificatore Accreditato
È tale l'organismo (soggetto pubblico o privato) che emette certificati qualificati conformi alla normativa europea e nazionale in materia, il quale

ha richiesto ed ottenuto, ai sensi dell'art. 29 comma 1 del [CAD], il riconoscimento del possesso dei requisiti del livello più alto, in termini di qualità e sicurezza, con l'accreditamento nell'elenco pubblico dei certificatori mantenuto e reso disponibile presso AgID.

Chiave privata
L'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico.

Chiave pubblica
L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche.

Chiavi asimmetriche
L'insieme della coppia di chiavi, quella pubblica e quella privata, che viene utilizzata per la creazione e la verifica della firma digitale, e attribuita ad un solo titolare.

Chiavi di marcatura temporale
Chiavi asimmetriche destinate alla generazione e verifica delle marche temporali.

Cifratura
La trascrizione di una evidenza informatica secondo un codice riservato che la rende inintelligibile ai terzi. Le operazioni di cifratura e decifrazione si effettuano applicando algoritmi standard che prevedono l'utilizzo di chiavi segrete.

Dati di certificazione
I dati, quali ad esempio data ed ora di invio, mittente, destinatario, oggetto, identificativo del messaggio, che descrivono l'invio del messaggio originale e sono certificati dal gestore di posta elettronica certificata del mittente; tali dati sono inseriti nelle ricevute e sono trasferiti al titolare destinatario insieme al messaggio originale per mezzo di una busta di trasporto.

Destinatario
L'utente che si avvale del servizio di posta elettronica certificata del Gestore o di altro gestore di posta elettronica certificata per la ricezione di documenti prodotti mediante strumenti informatici.

Documento informatico
È la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Dominio di posta elettronica certificata
L'insieme di tutte e sole le caselle di posta elettronica certificata il cui indirizzo fa riferimento, nell'estensione, ad uno stesso dominio della rete internet, definito secondo gli standard propri di tale rete.

Evidenza informatica
È una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.

Firma elettronica
Insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

Firma elettronica qualificata
Firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.

Firma digitale
Un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Firma del gestore di Posta Elettronica Certificata
La firma elettronica avanzata, basata su un sistema di chiavi asimmetriche, che consente di rendere manifesta la provenienza e di assicurare l'integrità e l'autenticità dei messaggi del sistema di posta elettronica certificata, generata attraverso una procedura informatica che garantisce la connessione univoca al gestore e la sua univoca identificazione, creata automaticamente con mezzi che garantiscano il controllo esclusivo da parte del Gestore.

Gestore di Posta Elettronica Certificata
Il soggetto che gestisce uno o più domini di posta elettronica certificata con i relativi punti di accesso, di ricezione e di consegna, titolare della chiave usata per la firma delle ricevute e delle buste e che si interfaccia con altri gestori di posta elettronica certificata per l'interoperabilità con altri titolari.

Indice dei gestori di Posta Elettronica Certificata
Il sistema, che contiene l'elenco dei domini e dei gestori di posta elettronica certificata, con i relativi certificati corrispondenti alle chiavi usate per la firma delle ricevute, degli avvisi e delle buste, realizzato per mezzo di un server Lightweight Directory Access Protocol, di seguito denominato LDAP, posizionato in un'area raggiungibile dai vari gestori di posta elettronica certificata e che costituisce, inoltre, la struttura tecnica relativa all'elenco pubblico dei gestori di posta elettronica certificata.

LOG dei messaggi
Il registro informatico delle operazioni relative alle trasmissioni effettuate mediante posta elettronica certificata tenuto dal gestore.

Manuale operativo
Il presente documento pubblico che definisce e descrive le procedure applicate dal Gestore del servizio di PEC nello svolgimento della sua attività come definito dall'art. 23 del [DM]. Esso è depositato presso AgID ed è reso disponibile per la consultazione ed il download sul sito del Gestore stesso.

Manuale della qualità
Il manuale predisposto dal Gestore, finalizzato alla documentazione del proprio sistema di qualità certificato UNI EN ISO 9001:2015, come previsto dall'articolo 20, comma 2 del [DM].

Marca Temporale
Un'evidenza informatica che consente la validazione temporale.

Messaggio di posta elettronica certificata
Un documento informatico composto dal testo del messaggio, dai dati di certificazione e dagli eventuali documenti informatici allegati.

Messaggio originale
Il messaggio inviato da un utente di posta elettronica certificata prima del suo arrivo al punto di accesso e consegnato al titolare destinatario per mezzo di una busta di trasporto che lo contiene.

Mittente
Utente che si avvale del servizio di posta elettronica certificata per la trasmissione di documenti prodotti mediante strumenti informatici.

Piano per la Sicurezza
Il documento, previsto dall'articolo 16, del [DM], che definisce le adeguate misure adottate per garantire l'integrità, la sicurezza e la continuità del servizio di posta elettronica certificata. È un documento riservato a distribuzione controllata.

Posta elettronica certificata (PEC)
Ogni sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici.

Posta elettronica
Un sistema elettronico di trasmissione di documenti informatici.

Punto d'accesso
Il sistema che fornisce i servizi di accesso per l'invio e la lettura di messaggi di posta elettronica certificata, nonché i servizi di identificazione ed accesso dell'utente, di verifica della presenza di virus informatici all'interno del messaggio, di emissione della ricevuta di accettazione e di imbustamento del messaggio originale nella busta di trasporto.

Punto di ricezione
Il sistema che riceve il messaggio all'interno di un dominio di posta elettronica certificata, effettua i controlli sulla provenienza e sulla correttezza del messaggio ed emette la ricevuta di presa in carico, imbusta i messaggi errati in una busta d'anomalia e verifica la presenza di virus informatici all'interno dei messaggi di posta ordinaria e delle buste di trasporto.

Punto di consegna
Il sistema che compie la consegna del messaggio nella casella di posta elettronica certificata del titolare destinatario, verifica la provenienza e la correttezza del messaggio ed emette, a seconda dei casi, la ricevuta di avvenuta consegna o l'avviso di mancata consegna.

Ricevuta breve di avvenuta consegna
La ricevuta nella quale sono contenuti i dati di certificazione ed un estratto del messaggio originale.

Ricevuta completa di avvenuta consegna
La ricevuta nella quale sono contenuti i dati di certificazione ed il messaggio originale.

Ricevuta di accettazione
La ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del mittente, contenente i dati di certificazione, rilasciata al mittente dal punto di accesso a fronte dell'invio di un messaggio di posta elettronica certificata.

Ricevuta di avvenuta consegna
La ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, emessa dal punto di consegna al mittente nel momento in cui il messaggio è inserito nella casella di posta elettronica certificata del destinatario.

Ricevuta di presa in carico
La ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, emessa dal punto di ricezione nei confronti del gestore di posta elettronica certificata mittente per attestare l'avvenuta presa in carico del messaggio da parte del sistema di posta elettronica certificata di destinazione, recante i dati di certificazione per consentirne l'associazione con il messaggio a cui si riferisce.

Ricevuta sintetica di avvenuta consegna
La ricevuta che contiene i dati di certificazione.

Riferimento temporale
L'informazione contenente la data e l'ora che viene associata ad un messaggio di posta elettronica certificata.

Titolare
Il soggetto a cui è assegnata una casella di posta elettronica certificata.

Utente di Posta Elettronica Certificata
La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi ente, associazione o organismo, nonché eventuali unità organizzative interne ove presenti, che sia mittente o destinatario di posta elettronica certificata.

Validazione temporale
Il risultato della procedura informatica, con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale (informazione data e orario) opponibile ai terzi.

Virus informatico
Un programma informatico avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.

2.4 Termini tecnici

ISO – International Standard Organization
È un organismo internazionale per la definizione degli standard, composto da rappresentanze di organi nazionali, che produce standard industriali e commerciali a livello mondiale.

ITU – International Telecommunication Union
Organizzazione internazionale che funge da ente regolatore per gli standard nelle telecomunicazioni.

ITU – T
Sigla identificativa del Settore Telecomunicazioni ("Telecommunication Sector") dell'ITU.

LDAP – Lightweight Directory Access Protocol
È un protocollo standard per l'interrogazione e la modifica dei servizi di directory utilizzato per la gestione degli accessi al registro dei certificati e l'effettuazione di operazioni di prelievo di certificati e liste di revoca e sospensione.

DNS – Domain Name System
Il DNS è un servizio di directory, utilizzato soprattutto per la risoluzione di nomi di Host in indirizzi IP. Il servizio è realizzato tramite un database distribuito, costituito dai server DNS. Questa funzione è essenziale per l'usabilità di Internet, visto che gli esseri umani preferiscono ricordare nomi testuali, mentre gli Host ed i router sono raggiungibili utilizzando gli indirizzi IP. I nomi DNS, o "nomi di domino" sono una delle caratteristiche più visibili di Internet.

PIN – Personal Identification Number
Codice di sicurezza riservato che permette l'attivazione delle funzioni di firma.

HTTP – Hypertext Transfer Protocol
Usato come principale sistema per la trasmissione di informazioni sul web. L'HTTP funziona su un meccanismo richiesta/risposta: il client esegue una richiesta ed il server restituisce la risposta. Nell'uso comune il client corrisponde al browser ed il server al sito web. Vi sono quindi due tipi di messaggi HTTP: messaggi richiesta e messaggi risposta.

HTTPS – Secure Hypertext Transfer Protocol
Con il termine HTTPS ci si riferisce al protocollo HTTP (Hyper Text Transfer Protocol) utilizzato in combinazione con lo strato SSL (Secure Socket Layer); la porta standard dedicata a questo servizio è la 443/TCP.

ITSEC – Information Technology Security Evaluation Criteria
Criteri europei per la valutazione della sicurezza nei sistemi informatici.

PKCS – Public Key Cryptography Standard
Standard tecnici per applicazioni crittografiche (realizzati dalla RSA Data Security Inc.).

PKI – Public Key Infrastructure
Infrastruttura informatica costituita da applicazioni che utilizzano tecniche crittografiche a chiavi asimmetriche (pubblica e privata). Una infrastruttura di questo tipo include servizi di generazione e distribuzione di chiavi, di emissione e pubblicazione di certificati, di gestione dei registri dei certificati emessi e delle liste di sospensione e revoca, oltre ad altri servizi come la marcatura temporale. Esempi di utilizzazione basate sull'infrastruttura sono: la generazione di transazioni informatiche riservate (crittografia), la gestione di sistemi di autorizzazione, autenticazione e identificazione (firma digitale), riferibilità soggettiva ed integrità dei dati (firma digitale e marcatura temporale).

URL – Uniform Resource Locator
Sistema standard di nomenclatura indicante un sito, dominio o altro oggetto (file, gruppo di discussione, etc.) su Internet. La prima parte dell'URL (http:, ftp:, file:, telnet:, news:) specifica le modalità di accesso all'oggetto.

WWW – World Wide Web
L'insieme delle risorse e degli utenti su Internet che utilizzano il protocollo HTTP.

MIME – Multipurpose Internet Mail Extensions
Estensione del protocollo di posta elettronica standard che consente la trasmissione di contenuti binari con applicazioni specifiche.

S-MIME – Secure/MIME
Versione sicura del protocollo di posta elettronica MIME.

POP – Point of Presence
Punto di accesso alla rete Internet.

RFC – Request for Comments
Definizione scritte di protocolli o standard in uso su Internet.

TLS – Transport Layer Security
Protocollo standard per la gestione di transazioni sicure su Internet, basato sull'utilizzo di algoritmi crittografici a chiave pubblica.

XML
Extensible Mark-up Language. Un linguaggio sviluppato appositamente per la distribuzione di documenti su Web.

3 Descrizione generica del servizio PEC

La Posta Elettronica Certificata (PEC) è un'estensione della posta elettronica tradizionale, la quale consente di avere un riscontro certo, con valenza legale, dell'avvenuta consegna del messaggio.

In altre parole fornisce al processo di trasmissione elettronica valore equivalente a quello della notifica a mezzo posta raccomandata in tutti i casi previsti dalla legge.

Con una casella di Posta Elettronica Certificata è comunque possibile inviare e ricevere messaggi di posta elettronica ordinaria.

In particolare, il servizio PEC erogato da TWT, è un servizio conforme alla normativa italiana, con particolare riferimento al [DPR], al [DM] e ai suoi allegati.

Il titolare della casella PEC di TWT che invia una mail disporrà, come meglio specificato nei seguenti paragrafi, della ricevuta di accettazione e della successiva ricevuta di avvenuta consegna che potrà essere utilizzata per dimostrare l'avvenuto invio del messaggio e che certificherà la conclusione del processo di spedizione.

Il mittente, qualora dovesse inavvertitamente cancellare le ricevute dei messaggi inviati, può contare sul servizio del gestore TWT che conserverà traccia di tutti i messaggi inviati e ricevuti per un periodo minimo di 30 mesi.

L'utilizzatore di una casella di Posta Elettronica Certificata può accedere al servizio sia attraverso un client di posta elettronica tradizionale (Eudora, Outlook, etc) sia navigando con un internet browser (Firefox, Chrome, etc.) sul portale WebMail PEC di TWT.

3.1 Funzionamento del servizio

Nella figura seguente viene schematizzato il funzionamento del servizio di Posta Elettronica Certificata:

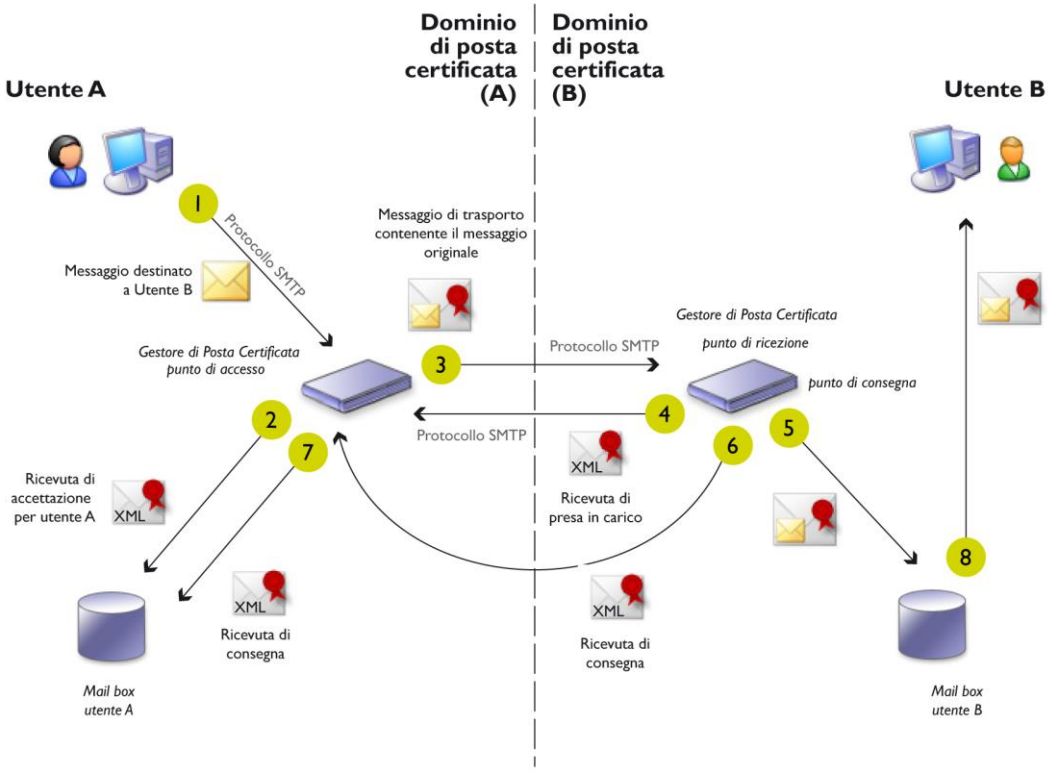


Figura 1: Funzionamento del servizio

1. Il mittente (utente A) invia un messaggio al destinatario attraverso il server di Posta Elettronica Certificata del suo gestore (punto di accesso), previa verifica delle credenziali di accesso.

2. Il gestore provvede ad inviare nella casella del mittente (utente A) una ricevuta di accettazione o di non accettazione sulla base dei controlli formali effettuati sul messaggio pervenuto. Le ricevute riportano la data e l'ora dell'evento, l'oggetto del messaggio e i dati del mittente e del destinatario e l'eventuale causa di non accettazione.

3. Il messaggio vieni quindi imbustato all'interno di un altro messaggio (chiamato busta di trasporto) di tipo S/MIME firmato digitalmente dal gestore ed inviato al punto di ricezione (gestore del destinatario).

4. Il punto di ricezione effettua il controllo della firma del gestore mittente e verifica la validità del messaggio, in caso di esito positivo provvede ad inviare al server del gestore mittente una ricevuta di presa in carico del messaggio e invia il messaggio verso il punto di consegna.

5. Il punto di consegna rende disponibile il messaggio nella casella del destinatario (utente B), a questo punto il destinatario (utente B) è in grado di leggere il messaggio di Posta Elettronica Certificata (punto 8, figura 1).

6. Il punto di consegna invia al gestore mittente una ricevuta di avvenuta consegna.

7. Il gestore mittente rende disponibile la ricevuta di avvenuta consegna nella casella del mittente (utente A).

Nel caso in cui il messaggio sia inviato contemporaneamente a più destinatari di Posta Elettronica Certificata il mittente si vedrà recapitare una sola ricevuta di accettazione e tante ricevute di avvenuta consegna, o di non avvenuta consegna (vedi paragrafo successivo), una per ogni destinatario.

Nel caso in cui il messaggio sia inviato ad uno o più destinatari di posta ordinaria (non certificata), oltre a non avere nessun valore legale, non verranno generate le ricevute di avvenuta consegna.

3.2 Funzionamento in caso di problemi di consegna

Il funzionamento del sistema prevede, nel rispetto della normativa di riferimento, che:

- Se il gestore del mittente non riceve dal gestore del destinatario, nelle dodici ore successive all'inoltro del messaggio, la ricevuta di presa in carico o di avvenuta consegna del messaggio inviato, comunica al mittente che il gestore del destinatario potrebbe non essere in grado di realizzare la consegna del messaggio.

- Se entro le successive dodici ore il gestore del mittente non riceve la ricevuta di avvenuta consegna del messaggio inviato, inoltra al mittente un ulteriore avviso relativo alla mancata consegna del messaggio entro le 24 ore successive all'invio.

3.3 Funzionamento in caso di presenza di virus

Il funzionamento del sistema di Posta Elettronica Certificata prevede le seguenti attività a carico dei gestori nel caso in cui siano rilevati dei virus:

- Se il gestore del mittente riceve messaggi con virus informatici è tenuto a non accettarli informando tempestivamente il mittente dell'impossibilità di dar corso alla trasmissione. In tal caso il gestore del mittente conserva i messaggi ricevuti per trenta mesi secondo le modalità definite dalla normativa di riferimento;

- Se il gestore del destinatario riceve messaggi con virus informatici è tenuto a non inoltrarli al destinatario informando tempestivamente il gestore del mittente affinché comunichi al mittente medesimo l'impossibilità di dar corso alla trasmissione. In tal caso il gestore del destinatario conserva i messaggi ricevuti per trenta mesi secondo le modalità definite dalla normativa di riferimento.

In tutti questi casi vengono generati e inviati al mittente specifici avvisi con i motivi della mancata consegna.

3.4 Ricezione della posta elettronica ordinaria

Nel caso in cui una casella di posta elettronica certificata (PEC) riceva un messaggio di posta elettronica ordinaria (PEO) questo viene imbustato dal gestore all'interno di un altro messaggio (chiamato Busta di Anomalia) di tipo S/MIME firmato dal gestore per segnalare al titolare che non si tratta di un messaggio di posta elettronica certificata.

È possibile, nelle impostazioni della webmail, configurare l'account PEC per non accettare la posta elettronica ordinaria, in questo caso il messaggio PEO verrà rifiutato dal sistema e il mittente riceverà un errore che indica che la posta PEO non è accettata da questo account PEC.

Nel caso in cui la PEO è abilitata, sempre nelle impostazioni della webmail, è possibile configurare un eventuale inoltro della PEO ad un'altra casella non certificata (la casella PEC riceverà comunque la busta di anomalia sopra citata mentre una copia del messaggio originale sarà inoltrata all'indirizzo specificato) e abilitare o meno il filtro AntiSPAM sulla PEO in ingresso.

3.5 Caratteristica delle ricevute e delle buste di trasporto

3.5.1 Firma elettronica delle ricevute e buste di trasporto

Le ricevute e le buste di trasporto rilasciate dal sottoscrittore sono sottoscritte dal gestore stesso mediante una firma elettronica avanzata,

generata automaticamente dal sistema di posta elettronica e basata su chiavi asimmetriche a coppia, una pubblica e una privata, che consente di renderne manifesta la provenienza e assicurarne l'integrità e l'autenticità.

3.5.2 Riferimento temporale

Come previsto dalla normativa, a ogni evento relativo al processo di elaborazione del messaggio di posta elettronica certificata, viene apposto dal gestore un riferimento temporale.

Per poter garantire la precisione del riferimento temporale, tutti gli apparati che costituiscono l'infrastruttura tecnologica di TWT S.p.A. sono sincronizzati con diversi Time Server pubblici tramite l'utilizzo del protocollo standard NTP (Network Time Protocol), fra cui il server NTP dell'Istituto Elettronico Nazionale Galileo Ferraris.

3.5.3 Tipologie delle ricevute di avvenuta consegna

Coerentemente con quanto indicato dalle Regole Tecniche AgID, il gestore può emettere tre differenti tipologie di Ricevute di Avvenuta Consegna, che possono soddisfare differenti esigenze dell'utenza e che sono di seguito riepilogate:

- la **Ricevuta Completa** è costituita da un messaggio di posta elettronica inviato al mittente che riporta, in formato leggibile, i dati di certificazione (mittente, destinatario, oggetto, data e ora di avvenuta consegna, codice identificativo del messaggio). Gli stessi dati sono inseriti all'interno di un file XML allegato alla ricevuta. Per le consegne relative ai destinatari primari del messaggio (che sono i destinatari diretti del messaggio diversi dai destinatari riceventi in copia), la ricevuta di avvenuta consegna contiene anche il messaggio originale, testo ed eventuali allegati.
- la **Ricevuta Breve** ha lo scopo di ridurre i flussi di trasmissione della Posta Elettronica Certificata, soprattutto in quei casi in cui la mole di documenti e di messaggi scambiati è molto consistente. Per questo, la Ricevuta Breve contiene il messaggio originale e gli *hash* crittografici degli eventuali allegati. Per permettere la verifica dei contenuti trasmessi, il mittente deve conservare gli originali non modificati degli allegati inseriti nel messaggio originale a cui gli *hash* fanno riferimento.
- la **Ricevuta Sintetica** segue le regole di emissione della ricevuta completa solo che l'allegato contiene esclusivamente il file XML con i dati di certificazione descritti. La ricevuta sintetica è particolarmente utile per i servizi che includono la Posta Elettronica Certificata come

strumento di trasporto a supporto di una forte automazione dei flussi di comunicazione.

4 Descrizione del servizio PEC TWT

Il servizio di posta elettronica certificata TWT viene offerto sotto forma di caselle attestate su un dominio inserito nell'apposito indice presso AgID.

4.1 Tipologie di servizio

TWT offre al cliente il servizio di posta elettronica certificata nelle seguenti tipologie:

1. Casella PEC sul dominio **TWTCERT.IT**
   La casella di posta elettronica certificata viene attivata sul dominio di posta certificata di TWT ed è quindi del tipo azienda@twtcert.it.

   Questa tipologia è dedicata a quella categoria di utenti per i quali non è particolarmente importante che il dominio di appartenenza sia esplicativo dell'organizzazione a cui appartengono.

2. Casella PEC sul sottodominio scelto dal cliente
   La casella di posta elettronica certificata viene attivata su un sottodominio scelto dal cliente ma all'interno di un dominio di posta certificata di proprietà TWT. In questo caso la casella PEC sarà del tipo nome@azienda.twtcert.it.

3. Caselle attestate su domini di proprietà del cliente
   Le caselle di posta elettronica certificata vengono attivate su un dominio di proprietà del cliente, tipo nome@azienda.it. E' consentito pertanto ai clienti di utilizzare anche sottodomini di domini in loro possesso, tipo nome@divisione.azienda.it.

   Questa tipologia è consigliata alle aziende che vogliono registrare un proprio dominio di posta elettronica certificata e attivare su di esso le proprie caselle. In questo caso il cliente ha la possibilità di amministrare le caselle, ovvero crearle e cancellarle, e di gestire in autonomia i suoi utenti.

In ottemperanza alla comunicazione AgID del 17.12.2013 con oggetto "Prescrizione sulla riassegnazione delle caselle di posta elettronica certificata" in cui "è posto il divieto al gestore, con riferimento agli indirizzi PEC dallo stesso gestiti, di riassegnare il medesimo indirizzo di posta elettronica certificata a soggetto diverso dal titolare originario",

saranno automaticamente rifiutati i "nome_utente" già utilizzati in precedenza.

TWT si riserva di verificare il nome della casella richiesta e di rifiutare l'attivazione e/o eseguire ulteriori verifiche nei casi in cui il nome richiesto richiami o evochi enti pubblici, nazionali o comunitari, o enti privati, assicurazioni, banche, istituti di credito o finanziari ovvero risulti offensivo o diffamatorio per altri utenti, gruppi e categorie sociali o risulti eccessivamente lungo o formato da sequenze totalmente alfanumeriche casuali.

Indipendentemente dalla tipologia di scelta, il servizio PEC di TWT prevede configurazioni personalizzabili a seconda delle esigenze del cliente, quali a titolo d'esempio:

- accesso via web;
- accesso tramite protocolli sicuri di posta elettronica;
- accesso tramite user e password;
- accesso con certificato digitale;
- amministrazione caselle;
- personalizzazioni webmail twt;
- dimensione spazio disco;

Tutte le caselle, indipendentemente dalla configurazione adottata dal cliente, soddisfano le funzionalità e caratteristiche previste per la posta elettronica certificata dalla normativa di riferimento: gestione delle ricevute di accettazione e di consegna, gestione delle buste di trasporto, conteggio dell'ora esatta, antivirus.

4.2 Modalità offerta

La posta elettronica certificata TWT viene commercializzata sia attraverso rete di vendita diretta, sia tramite partner: le modalità possono essere diverse a seconda della quantità di caselle richieste e della tipologia del cliente.

Per ricevere qualsiasi informazioni di dettaglio il richiedente può rivolgersi all'indirizzo di posta elettronica info@twtcert.it o visitare il sito www.twt.it.

L'offerta commerciale prevede un canone di attivazione ed un canone annuo che varia principalmente a seconda del numero di caselle PEC TWT acquistate dal cliente e dalla loro dimensione in termini di Mb di spazio

disponibile. Su questi prezzi TWT può praticare sconti di diversa consistenza in base ad elementi di vario genere.
Canoni di attivazione ed eventuali canoni annui sono inoltre previsti per i servizi opzionali da quotarsi a seconda della specifica personalizzazione richiesta.

A titolo d'esempio:
- la personalizzazione di alcuni elementi grafici nell'interfaccia webmail, per tutte le caselle di un dominio;
- lo spazio disco aggiuntivo rispetto allo standard;
- la notifica di ricezione di messaggi di posta certificata via SMS o tramite email di posta ordinaria.

5 Modalità di accesso al servizio

TWT offre alla propria clientela l'accesso al servizio tramite Mail Client (accesso standard) e Internet Browser (webmail).

5.1 Password

Le password d'accesso vengono create direttamente dall'utente finale in fase di attivazione e potranno da lui essere modificate in qualsiasi momento attraverso la Webmail.

Le password devono essere create seguendo alcune regole standard:
devono essere lunghe almeno 8 caratteri e devono contenere tre seguenti discriminanti: almeno una lettera maiuscola e una minuscola, almeno un carattere numerico (da 0 a 9), almeno un carattere speciale tra i seguenti: !$@#%^&*€

Le password vengono salvate sui database TWT già criptate e quindi nessuno all'interno dell'azienda è in grado di conoscerle. In caso di smarrimento, l'utente, selezionando il link "reset password" sulla pagina di login della Webmail, riceverà al proprio indirizzo di posta ordinaria, una email contenente un link per reimpostare la password.

5.2 Accesso standard / Webmail

Tutti i componenti della soluzione TWT fanno uso di protocolli sicuri standard per interagire tra loro e con le applicazioni esterne.

Ne consegue che la piattaforma è compatibile con tutti i mail client che fanno uso dei protocolli sicuri standard supportati (POP3S, IMAPS) e i browser che permettono l'utilizzo di TLS v1.2.

La seguente tabella mostra i client/browser e le piattaforme in cui i prodotti sono stati sperimentati con successo.

Sistemi Operativi	Versione minima supportata (OS)	Browser	Versione minima supportata (Browser)	Client di posta	Versione minima supportata (Client di posta)
Android	4.4.2	Tutti		Mail (Nativo)	5.x
Apple iOS	Tutte le versioni	Tutti		Mail	11.x
Windows Phone	8.1	Internet Explorer	11		
OSX	10.9	Safari	7.x	Apple Mail	Tutte
		Chrome	34.x	Outlook	2011 (solo su OSX da 10.11 a 10.13)
		Firefox	29.x	Thunderbird	45.6
Windows 7	Tutte	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	Tutte	Tutti		Tutti	

5.3 Protocolli

I protocolli utilizzati per comunicare col server di posta TWT sono i seguenti:

- per inviare messaggi di posta con client locale: SMTPS, porta 465;
- per ricevere messaggi di posta con client locale via POP3+SSL: POP3S, porta 995;
- per ricevere messaggi di posta con client locale via IMAP+SSL: IMAPS, porta 993;
- per utilizzare un browser internet: HTTPS, porta 443.

La versione minima accettata per i protocolli sicuri è il TLS v1.2.

5.4 Configurazione del client di posta.

Utilizzando un client di posta (utilizzeremo Microsoft outlook come esempio) è possibile scegliere la modalità di accesso al server via POP3S o via IMAPS.

Non ci dilunghiamo sulle differenze tra i due sistemi, se non dicendo che la differenza principale è che il protocollo IMAPS si basa sul concetto di elaborare tutta la posta su un server remoto e centralizzato, in modo di avere a disposizione l'intero insieme dei propri messaggi da qualsiasi macchina ci si connetta, al contrario di quanto accade tramite il protocollo POP3S, il quale scarica in locale i messaggi contenuti nella casella, lasciandone o meno una copia sul server.

5.4.1 Configurazione client Microsoft Outlook con POP3S.

Per creare l'account in Microsoft Outlook selezionare la voce di menu **File** (fig. 1).

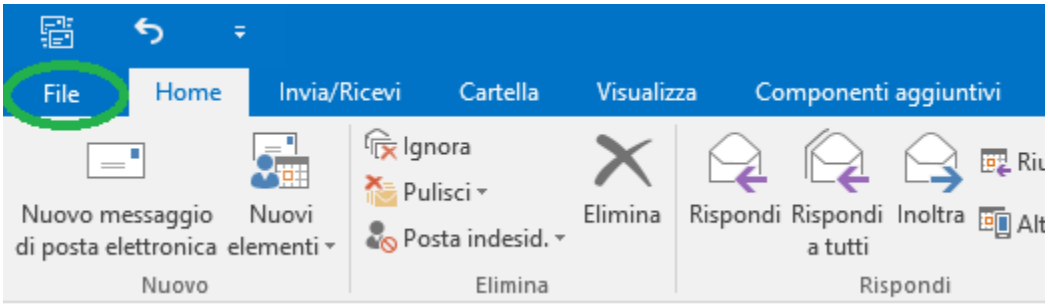


Figura 1: selezione voce di menu File

Dalla scheda **Informazioni account** cliccare il pulsante **Aggiungi account** (fig. 2).

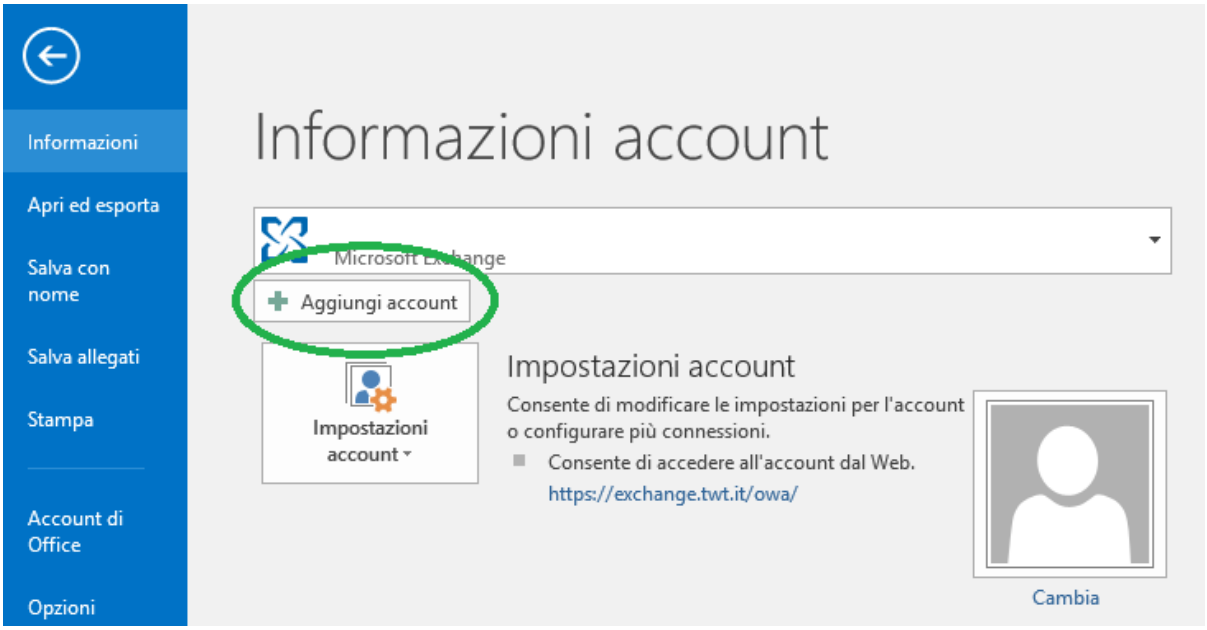


Figura 2: funzione Aggiungi account

Dalla finestra **Aggiungi account**, selezionare l'opzione **Configurazione manuale o tipi di server aggiuntivi**, e successivamente cliccare il pulsante ***Avanti*** (fig. 3).

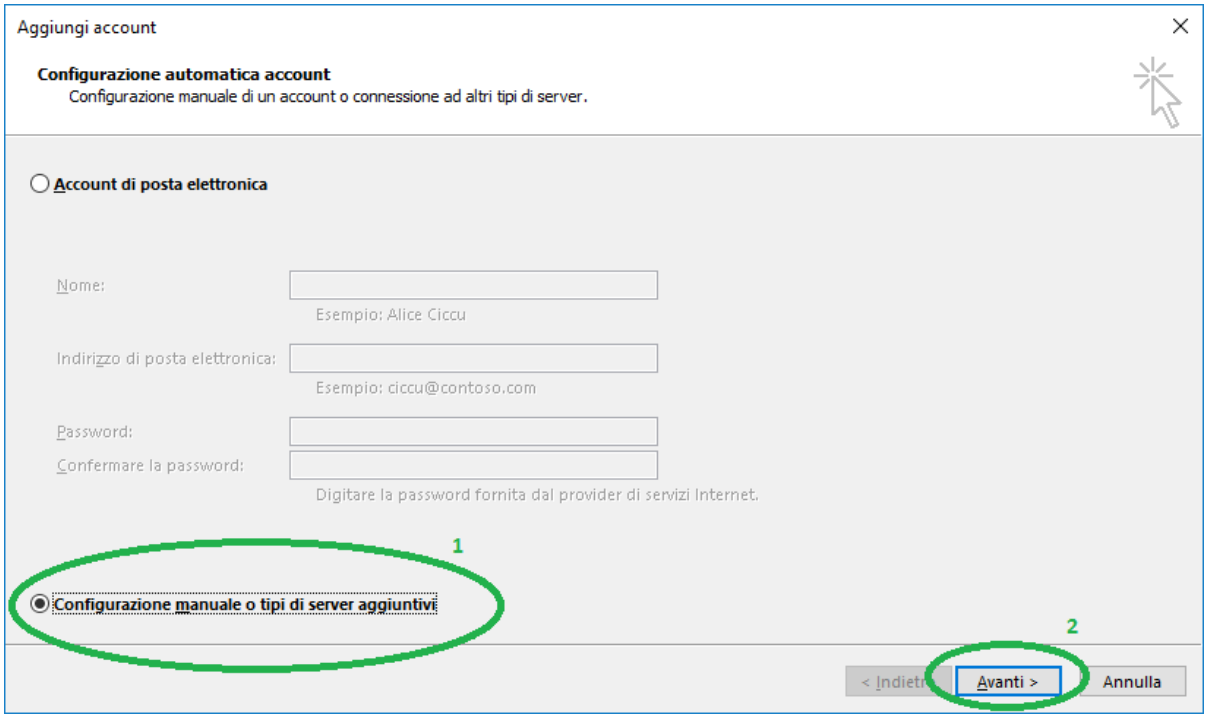


Figura 3: Configurazione manuale o tipi di server aggiuntivi.

Scegliere quindi l'opzione **POP o IMAP** (fig. 4).

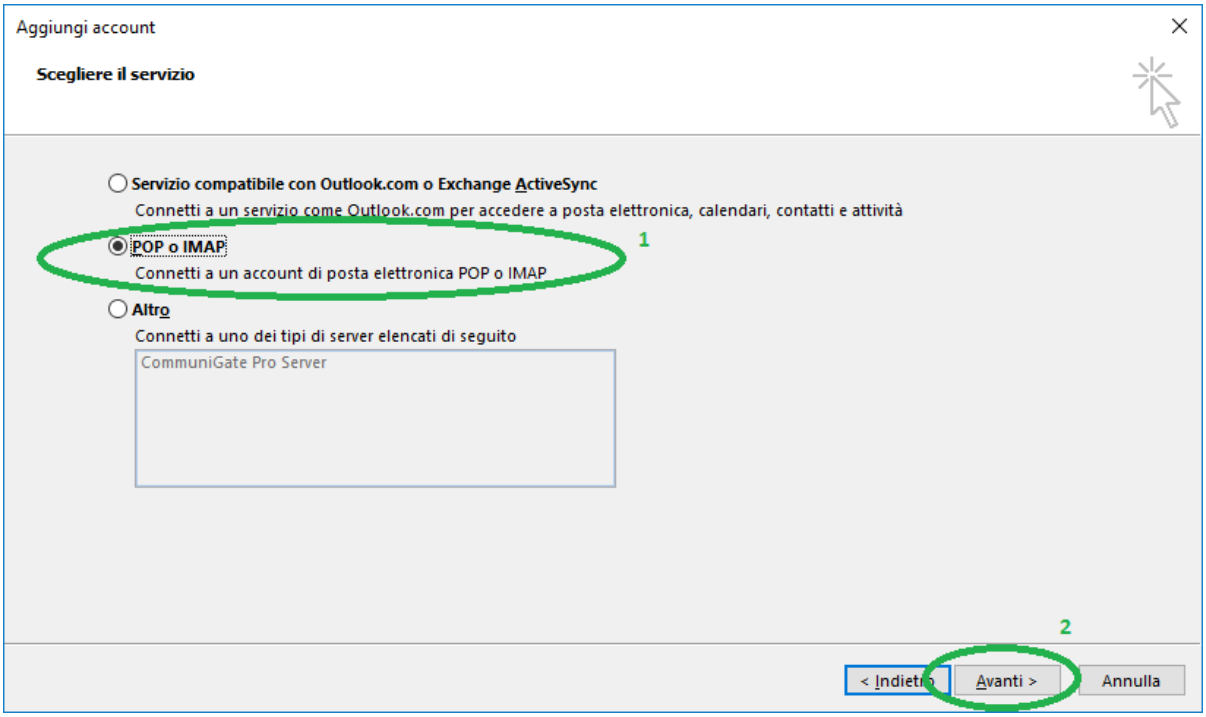


Figura 4: scelta del servizio

Dalla finestra **Impostazioni account POP e IMAP** si possono fornire tutte le informazioni dell'account e del server di posta.

Nella sezione **Informazioni utente**:

- indicare il proprio nome nel campo **Nome**.
- indicare l'indirizzo di posta certificata all'interno della casella **Indirizzo di posta elettronica**.

Nella sezione **Informazioni server**:

- come **Tipo account** selezionare la voce POP3
- all'interno della casella **Server di posta in arrivo** indicare *mail.twtcert.it*
- all'interno della casella **Server di posta in uscita (SMTP)** indicare *smtp.twtcert.it*

Nella sezione Informazioni di accesso:

- indicare il **Nome Utente** (precompilato da Microsoft Outlook con l'indirizzo di posta elettronica)
- indicare la **Password** impostata in fase di configurazione della casella di posta elettronica certificata.

La configurazione tipica di un account dovrebbe risultare simile a quella mostrata in figura (fig. 5).

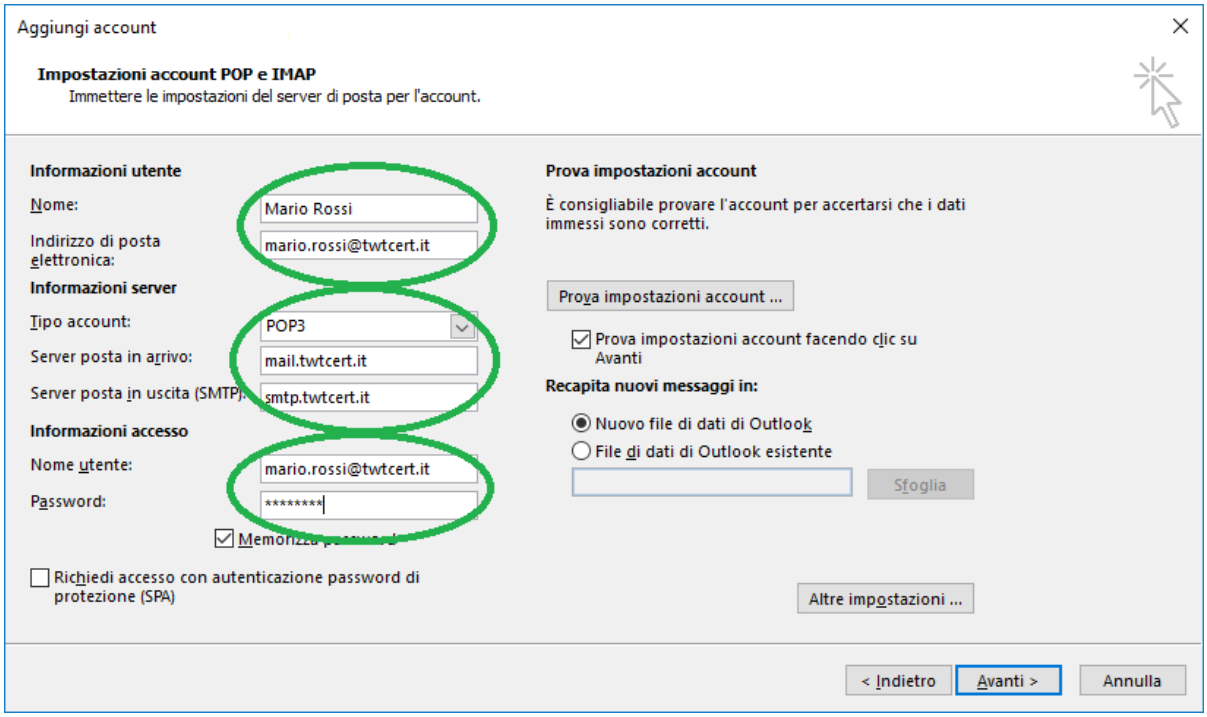


Figura 5: impostazioni account e server

Una volta completate le informazioni di base, cliccare sul pulsante Altre impostazioni, per accedere alla configurazione avanzata (fig. 6).

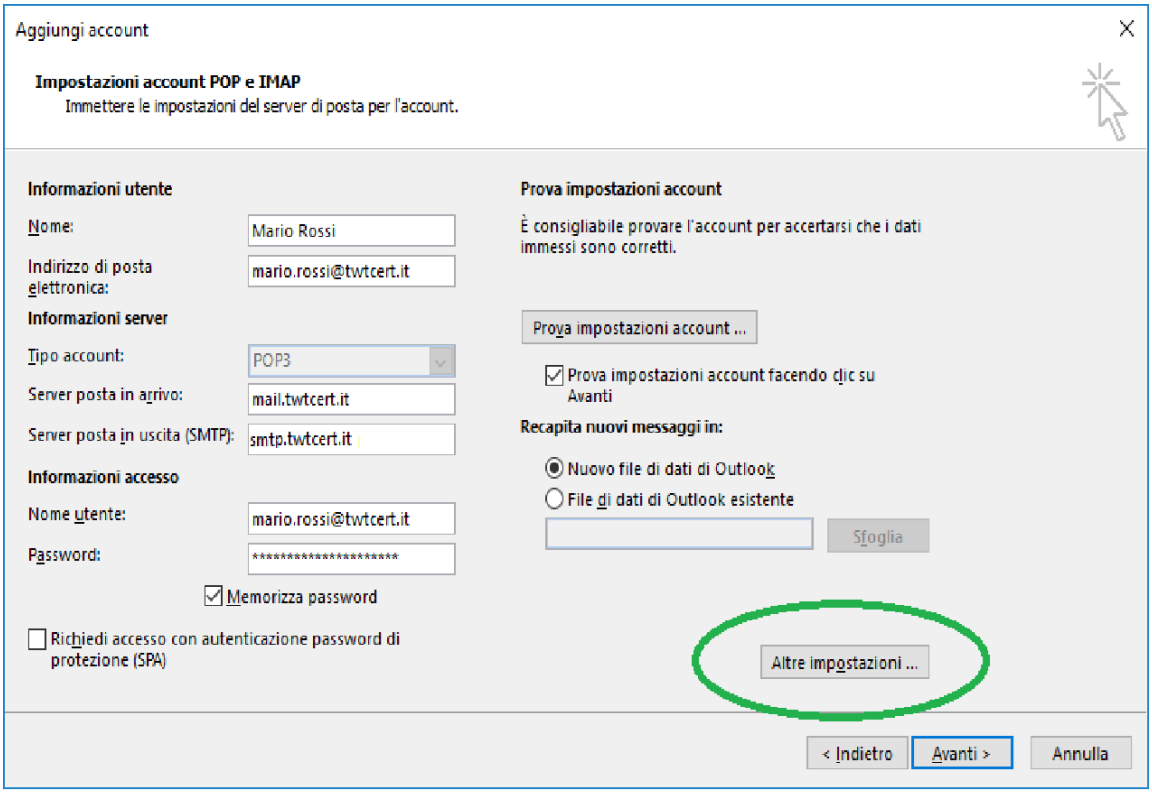


Figura 6: Altre impostazioni

Assicurarsi che nella finestra **Impostazioni posta elettronica Internet**, nella scheda **Generale**, sia indicato l'account di posta corretto (fig. 7).

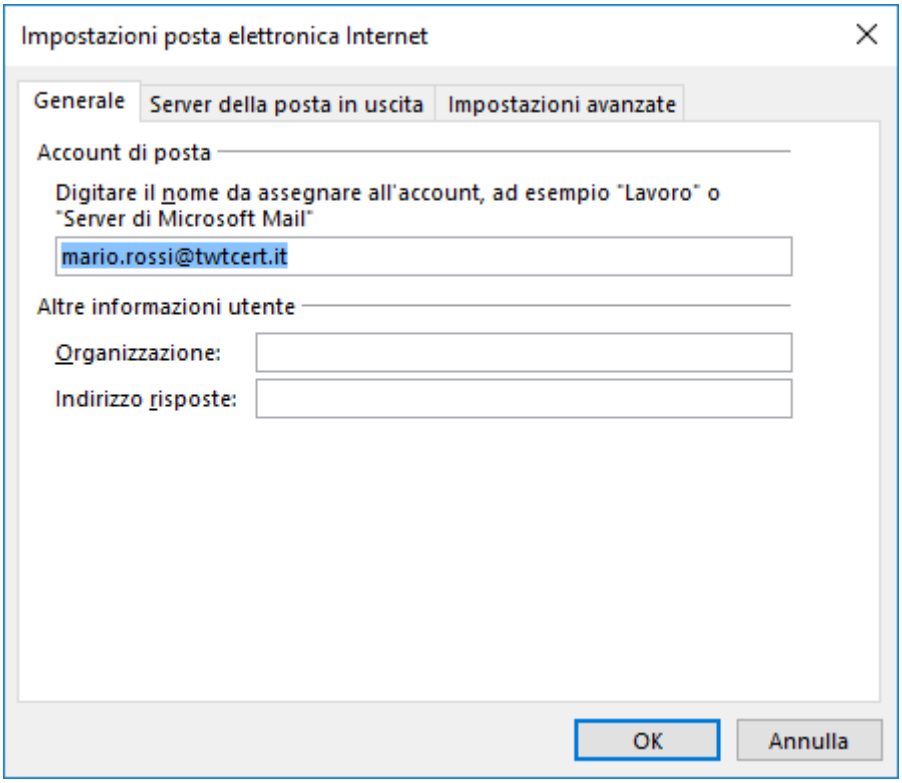


Figura 7: scheda generale

Nella scheda **Server della posta in uscita** selezionare la voce **Il server di posta in uscita (SMTP) richiede l'autenticazione** (fig. 8).

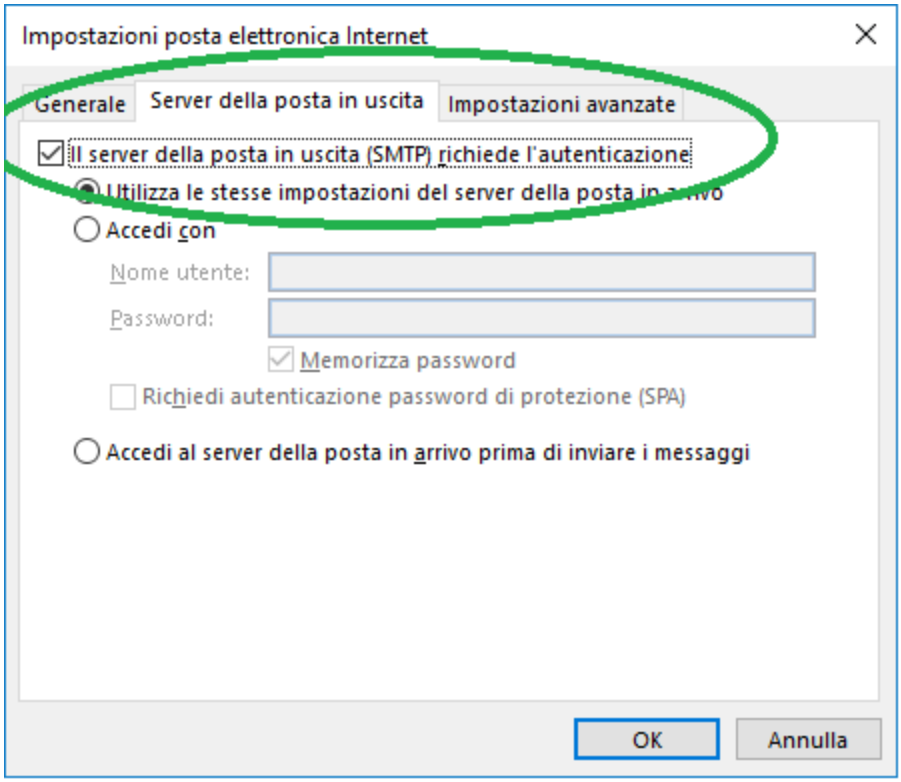


Figura 8: scheda Server della posta in uscita

Infine nella scheda **Impostazioni avanzate** indicare i seguenti parametri:

- **Server di posta in arrivo (POP3)**: 995
- **Il server richiede una connessione crittografata (SSL)**: sì
- **Server di posta in uscita (SMTP)**: 465
- **Utilizzare il tipo di connessione crittografata seguente**: TLS

La scheda di impostazioni avanzate dovrebbe risultare come in figura 9:

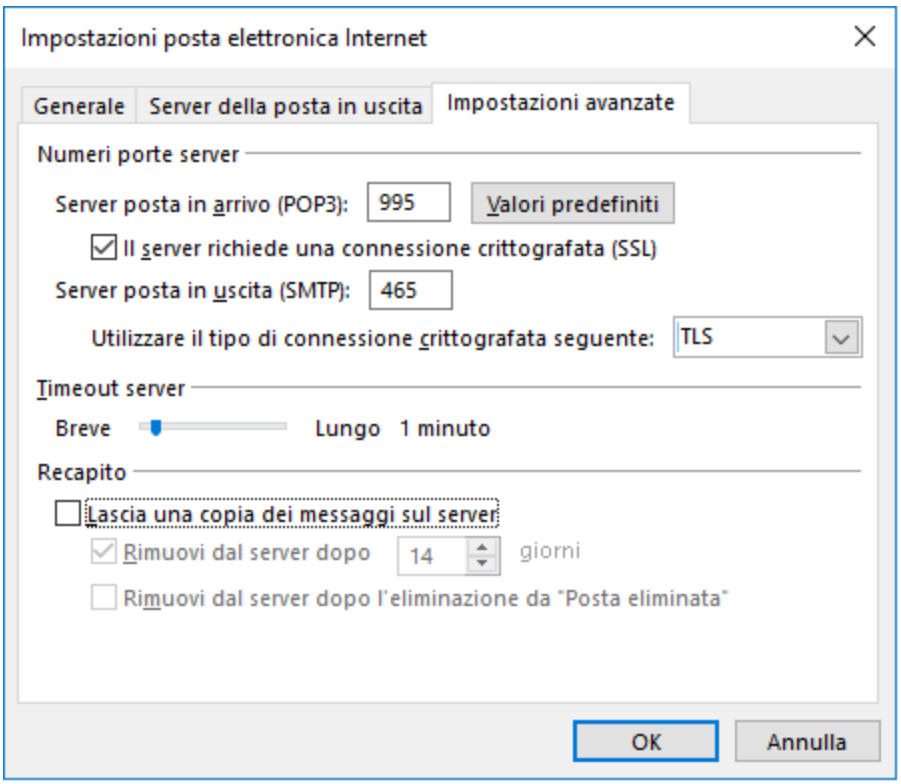


Figura 9: scheda Impostazioni avanzate

Cliccare quindi il pulsante OK per tornare alla finestra di configurazione di account e server.

Da qui è possibile fare un test immediato di configurazione dell'account, cliccando il pulsante **Prova impostazione account**. Oppure è possibile posticipare la prova una volta terminata la configurazione, selezionando la voce **Prova impostazioni account facendo clic su Avanti** e successivamente premendo il pulsante **Avanti** (fig. 10).

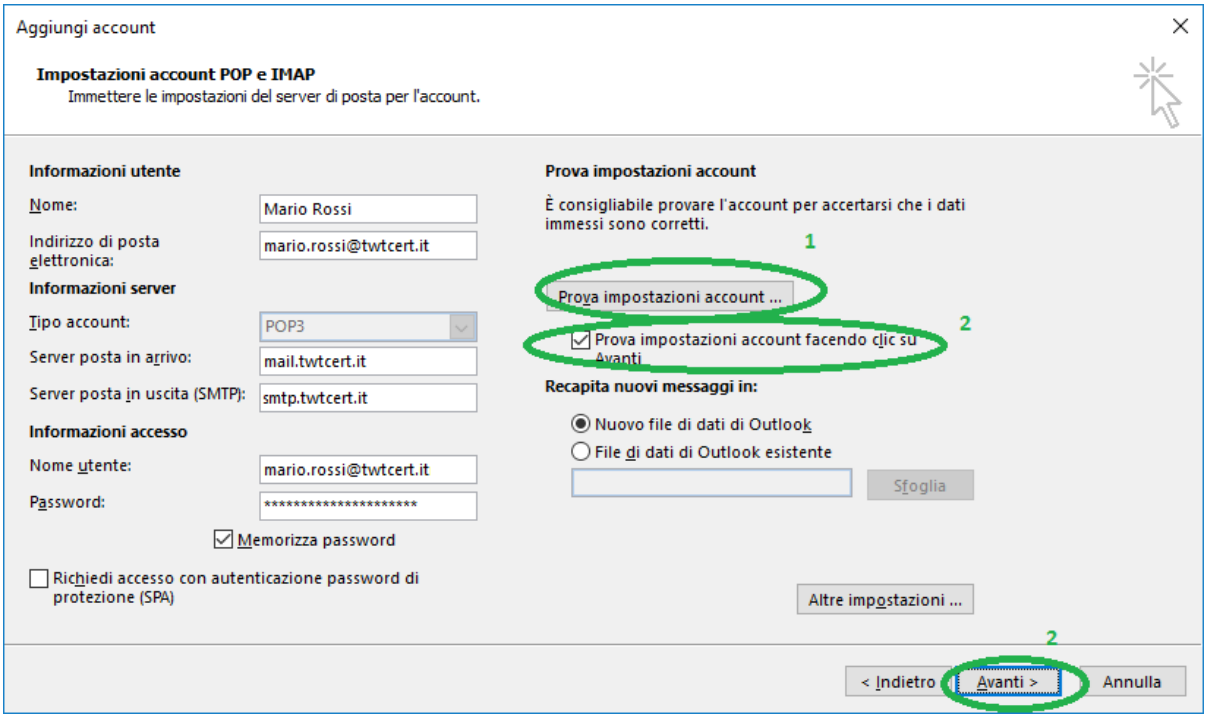


Figura 10: test di configurazione

Il client è ora pronto per ricevere e inviare posta sulla casella di posta elettronica certificata appena configurata.

5.5 Log dei Messaggi

Durante le fasi di trattamento del messaggio presso i punti di accesso, ricezione e consegna (funzionamento spiegato precedentemente nel capitolo 3), il sistema che eroga il servizio di posta elettronica certificata di TWT mantiene traccia delle operazioni svolte, memorizzandole su un registro informatico (LOG).

5.5.1 Richiesta dei log da parte del titolare

Come previsto dalla normativa vigente, qualora il titolare della casella di posta elettronica certificata non abbia più la disponibilità delle ricevute dei messaggi di posta elettronica certificata inviati, le informazioni contenute nel registro informatico memorizzato dal gestore, sono opponibili ai terzi, ai sensi della normativa vigente.

Le richieste relative alle informazioni sui log dei messaggi possono essere inoltrate esclusivamente dal titolare della casella di posta elettronica certificata TWT o dall'autorità giudiziaria.

Per richiedere le informazioni relative ai log dei messaggi, il titolare deve rivolgersi al Customer Care di TWT, inviando una mail dalla propria casella di posta elettronica certificata alla casella di posta elettronica certificata support@twtcert.it.

In caso d'impossibilità ad accedere alla propria casella pec, il titolare potrà far rivolgersi al Customer Care di TWT telefonicamente al numero verde 800.192.800 per ottenere maggiori ragguagli sull'invio della richiesta log via fax.

La richiesta dovrà contenere i seguenti dati:

- codice cliente TWT ed identificativo del sottoscrittore del contratto PEC TWT;
- data di riferimento del messaggio;
- indirizzo di posta elettronica certificata del titolare;
- indirizzo di posta elettronica certificata del destinatario;
- fotocopia di un documento d'identità.

Nel caso in cui la richiesta di informazione ed estrazione dei log sia relativa ad una singola mail PEC ("estrazione singola"), TWT effettuerà l'attività a titolo gratuito. Nel caso in cui la richiesta fosse relativa ai log di

molteplici mail PEC ("estrazione massiva"), TWT effettuerà l'attività previa apposita quotazione accettata dal Cliente.

Acquisiti i dati e, in caso di estrazione massiva, ottenuta l'accettazione della quotazione da parte del Cliente, il Customer Care di TWT inoltrerà la richiesta al responsabile dei servizi tecnici, che provvederà alla sua evasione in prima persona o delegando un operatore del suo servizio.

Reperite le informazioni, da inviare, il responsabile dei servizi tecnici (o la persona da lui delegata) le invierà al Titolare della casella di posta elettronica certificata come concordato durante la fase di richiesta.

Per le richieste da parte dell'autorità giudiziaria sarà necessaria comunicazione formale al gestore da parte della medesima.

6 Condizioni di fornitura

Il servizio è disciplinato e fornito in conformità con la normativa vigente e quanto previsto nel Contratto che comprende:

- la richiesta di attivazione;
- l'offerta commerciale;
- le condizioni generali di fornitura;
- l'allegato contenente il Manuale Operativo;
- l'informativa privacy;

Tutta la documentazione è reperibile sul sito istituzionale di TWT all'indirizzo http://www.twt.it.

6.1 Premessa

- Esiste una apposita normativa e delle precise specifiche tecniche emanate da AgID che regolano l'erogazione del servizio di posta elettronica certificata.
- Il servizio PEC può essere erogato solo dai gestori iscritti nell'elenco pubblico dei gestori di posta elettronica certificata tenuto da AgID (***Elenco Pubblico***).

Con queste premesse, di seguito, si riportano le condizioni di fornitura del servizio (***Condizioni***), da considerarsi come condizioni essenziali dell'offerta e specificamente accettate dal ***Titolare***, la cui inosservanza dà luogo all'applicazione dell'art.1456 c.c.

6.2 Obblighi e responsabilità

6.2.1 Soggetti del Servizio

Nell'ambito del ***SERVIZIO*** vengono identificati i seguenti soggetti:

GESTORE	TWT S.p.a., che stipula i contratti di vendita del ***Servizio*** nei confronti dei ***Titolari***, e opera in qualità Gestore di Posta Elettronica Certificata iscritto nell'***Elenco Pubblico*** di ***AgID*** e che gestisce i ***Domini*** di posta elettronica certificata con i relativi punti di accesso, ricezione e consegna definiti dalla normativa vigente.
TITOLARE	il soggetto che acquista il ***Servizio*** dal ***Gestore*** affinché sia utilizzato dai soggetti appartenenti alla propria organizzazione.
UTILIZZATORE	Il soggetto a cui il ***Titolare*** abbia rilasciato le credenziali di accesso al ***Servizio*** fornite dal ***Gestore***. Nel caso in cui il ***Servizio*** sia richiesto da un ***Titolare*** per uso personale, l'***Utilizzatore*** e il ***Titolare*** coincidono.
MITTENTE	L'***Utilizzatore*** che si avvale del ***Servizio*** del ***Gestore*** per l'invio di documenti prodotti mediante l'uso di strumenti informatici.
DESTINATARIO	L'***Utilizzatore*** che si avvale del ***Servizio*** del ***Gestore*** per la ricezione di documenti prodotti mediante l'uso di strumenti informatici.

6.2.2 Attività e obblighi del Gestore

Il ***Gestore*** fornirà il ***Servizio*** conformemente a quanto stabilito dalla normativa vigente in materia, con le modalità specificate nel presente ***Manuale Operativo***.

In particolare, il ***Gestore*** è tenuto a:

- attenersi alle regole tecniche cogenti;
- informare i ***Titolari*** sulle modalità di accesso al servizio e sui necessari requisiti tecnici per accedervi;
- porre in atto misure tecniche e organizzative idonee per garantire un livello di sicurezza dei propri sistemi adeguato al rischio relativo ai dati personali trattati come da normativa privacy vigente;
- garantire il funzionamento efficiente, puntuale e sicuro del ***Servizio***;

- fornire al ***Mittente***, appartenente ad un dominio di posta da lui gestito, la ricevuta di accettazione contenente i dati di certificazione;
- fornire al ***Mittente***, qualora il ***Destinatario*** appartenga ad un dominio di posta da lui gestito, la ricevuta di avvenuta consegna contenente i dati di certificazione;
- quando il messaggio di posta elettronica non risulta consegnabile, comunicare al ***Mittente***, entro le 24 ore successive all'invio, la mancata consegna;
- firmare le ricevute e la busta di trasporto con firma digitale;
- apporre il riferimento temporale su ciascun messaggio che transita nel sistema;
- conservare, a norma di legge, il file contenente i log dei messaggi transitati sul sistema. Il file deve essere generato giornalmente e deve contenere i log dei messaggi generati in un intervallo massimo di 24 ore. Su ogni file generato deve essere apposta una marca temporale;
- trasmettere il messaggio di posta certificata dal ***Mittente*** al ***Destinatario*** integro in tutte le sue parti, includendolo nella busta di trasporto;
- tenere traccia, durante tutte le fasi di trasmissione del messaggio di posta elettronica certificata, delle operazioni svolte su apposito log dei messaggi;
- conservare il registro contenente i log dei messaggi per trenta mesi;
- adottare opportune soluzioni tecniche ed organizzative che garantiscano la sicurezza, l'integrità e l'inalterabilità nel tempo delle informazioni contenute nel registro dei log dei messaggi di cui al punto precedente;
- Adottare procedure di emergenza che assicurino il completamento della trasmissione del messaggio ed il rilascio delle ricevute;
- Gestire messaggi contenenti virus informatici secondo quanto stabilito dalla normativa vigente;
- Assicurare i livelli minimi di servizio previste dalle allegate regole tecniche;
- Assicurare l'interoperabilità con gli altri gestori del servizio di posta elettronica certificata.

Il ***Gestore*** di posta elettronica certificata è responsabile dei danni causati, con dolo e colpa, a qualsiasi persona fisica o giuridica in seguito al mancato adempimento degli obblighi contrattuali e di quelli previsti dalla normativa vigente.

Il ***Gestore*** si riserva il diritto di apportare modifiche alle specifiche tecniche di erogazione del ***Servizio*** in base all'evoluzione normativa e/o tecnologica, rendendole note attraverso il ***Manuale Operativo*** e previa approvazione di AgID, ove tali modifiche risultassero essere di rilevante entità o la loro pubblicazione fosse richiesta dalla normativa vigente.

6.2.3 Esclusioni, Limitazione e polizza assicurativa

Il ***Gestore*** non sarà in alcun modo responsabile per quanto di seguito indicato:

- danni di qualsiasi natura, diretti o indiretti, o pregiudizi da chiunque patiti per eventi derivanti da atti della Pubblica Autorità, caso fortuito, forza maggiore ovvero da altra causa non imputabile al ***Gestore*** (quali, in via puramente esemplificativa e non esaustiva, mancato o erroneo funzionamento di reti, apparecchiature o strumenti di carattere tecnico al di fuori della sfera di controllo del ***Gestore***, interruzioni nella fornitura di energia elettrica, terremoti, esplosioni, incendi), esclusi i casi di dolo o colpa;
- danni di qualsiasi natura, diretti o indiretti, o pregiudizi da chiunque patiti nella misura in cui tali danni
    - derivino dalla violazione di obblighi che, in virtù di quanto previsto dal ***Manuale Operativo*** ovvero dalle vigenti disposizioni di legge, incombono, all'***Utilizzatore***, al ***Mittente***, al ***Destinatario***, a quanti ricevono messaggi trasmessi per il tramite del ***Servizio;***
    - avrebbero potuto essere evitati o limitati dalla conoscenza delle previsioni contenute nel ***Manuale Operativo*** da parte del ***Titolare***, dell'***Utilizzatore***, del ***Mittente***, del ***Destinatario***, da quanti ricevono messaggi trasmessi per il tramite del ***Servizio***
    - siano derivanti dall'erroneo utilizzo di codici identificativi da parte e dell'***Utilizzatore;***
    - siano derivanti dal mancato invio o dalla mancata consegna dei messaggi ove causati da anomalie segnalate, secondo i casi, al ***Mittente*** o al Destinatario i quali non abbiano provveduto a riscontrare la comunicazione di anomalia inviata dal ***Gestore;***
    - siano derivanti da ritardi, interruzioni, errori o malfunzionamenti del ***Servizio*** non imputabili al ***Gestore*** o derivanti dall'errata utilizzazione del ***Servizio*** da parte del ***Titolare*** o dell'***Utilizzatore;***
    - siano derivanti dall'applicazione delle previsioni normative in merito al trattamento dei messaggi con contenuto malevolo o contenenti virus informatici;
    - siano al di fuori dei livelli minimi di servizio previsti dalla normativa vigente;
    - siano derivanti dall'impiego del ***Servizio*** al di fuori delle previsioni normative vigenti o dall'utilizzo di servizi di posta elettronica forniti da gestori non inclusi nell'elenco pubblico tenuta da AgID;

I messaggi di posta elettronica possono subire dei ritardi nella loro trasmissione via Internet, pertanto il ***Gestore*** non assume alcuna responsabilità, salvo eventuale dolo o colpa, per detti ritardi.

Il ***Gestore*** è esonerato da ogni potere di controllo, di mediazione o di vigilanza sul contenuto dei messaggi inviati dagli ***Utilizzatori*** e non assume nessuna responsabilità riguardo al loro contenuto illecito o contrario alla morale o all'ordine pubblico, non sussistendo alcun obbligo di cancellazione in capo al ***Gestore*** in merito alla cancellazione del contenuto dei messaggi.

Il ***Gestore*** non assume nessun obbligo, garanzia o responsabilità ulteriori rispetto a quelle scaturenti dal contratto di fornitura del ***Servizio*** e dalla normativa vigente.

Il danneggiato decade dal diritto al risarcimento dei danni imputabili al ***Gestore*** qualora non ne faccia motivata denuncia scritta al ***Gestore*** entro il termine di 10 giorni dal verificarsi dell'evento dannoso.

Il ***Gestore*** ha stipulato un contratto assicurativo per la copertura dei rischi dell'attività e dei danni causati a terzi che ha come massimali:

- **1.000.000 euro per singolo sinistro**
- **1.000.000 euro per annualità.**

6.2.4 Obblighi del TITOLARE

Con l'accettazione di quanto stabilito in queste Condizioni di Fornitura il ***Titolare*** assume i seguenti obblighi:

- consultare preventivamente il ***Manuale Operativo*** e conoscerne i contenuti;
- fornire tutte le informazioni e la documentazione richieste dal ***Gestore***, necessarie ad una corretta identificazione personale garantendone, sotto la propria responsabilità, l'attendibilità ai sensi della normativa vigente;
- informare espressamente gli ***Utilizzatori*** riguardo agli obblighi da questi assunti in merito all'uso del ***Servizio;***
- ove richiesto, prestare il consenso al trattamento dei dati personali ai sensi della normativa privacy vigente;
- conservare e far conservare agli ***Utilizzatori*** con la massima riservatezza e diligenza i codici di accesso al ***Servizio;***
- informare immediatamente il ***Gestore*** in caso risulti compromessa la riservatezza dei codici di accesso per l'utilizzo del ***Servizio;***

- non utilizzare né permettere a terzi di utilizzare il ***Servizio*** per fini illeciti o per effettuare comunicazioni contrarie alla legge, alla morale o all'ordine pubblico;
- non utilizzare, e non far utilizzare agli Utilizzatori, il ***Servizio*** con lo scopo di depositare, inviare, pubblicare, trasmettere e/o condividere applicazioni o documenti informatici che siano in contrasto o violino diritti di proprietà intellettuale, segreti commerciali, marchi, brevetti o altri diritti di proprietà di terzi;
- non consentire a terzi non autorizzati dal ***Titolare*** l'uso del ***Servizio***, di cui sarà comunque responsabile il ***Titolare***

Il ***Titolare*** prende atto che alla scadenza del contratto o in caso di sua risoluzione, non sarà più possibile accedere al ***Servizio*** ed al suo contenuto, pertanto si impegna a darne informativa agli ***Utilizzatori***, sollevando il ***Gestore*** da ogni responsabilità derivante dal mancato accesso.
Il ***Titolare*** prende altresì atto che il contenuto della casella presente sull'Infrastruttura TWT al momento della cessazione, sarà conservato per ulteriori 6 mesi esclusivamente a mero titolo di cortesia, senza che il ***Gestore*** ne assuma l'obbligo: sarà quindi esclusa qualsiasi responsabilità di quest'ultimo in caso di perdita e danneggiamento totale o parziale della casella stessa. Trascorso tale periodo senza che il ***Servizio*** possa essere riattivato i dati presenti su detta Infrastruttura saranno definitivamente cancellati e non più recuperabili. Tale previsione si applica anche nel caso in cui sia attiva l'opzione di "Archivio storico" come specificata nell'offerta commerciale.

7 Livelli di servizio

Il gestore TWT garantisce agli utenti del servizio la possibilità di invio del messaggio di posta elettronica certificata in conformità con quanto previsto dalla normativa vigente:

- liste composte fino a 50 destinatari;
- un limite di 100 MB del prodotto tra numero di destinatari e dimensione del messaggio in caso di utilizzo tramite un client di posta;
- un limite di 50 MB del prodotto tra numero di destinatari e di dimensione del messaggio in caso di utilizzo tramite la webmail;
- un limite tecnico di 1000 invii all'ora, in caso di invio massivo, per motivazioni legate alla sicurezza del servizio.

La disponibilità del servizio di posta elettronica certificata è di 24 ore su 24, 7 giorni su 7, con un funzionamento pari al 99,8% del periodo temporale di riferimento pari ad un quadrimestre.

La durata massima di ogni singolo evento di non disponibilità del servizio non supera il 50% del totale previsto nel quadrimestre.

Le ricevute previste dal sistema e destinate agli utenti del servizio, durante il periodo di disponibilità del servizio, pervengono al mittente nei tempi previsti dalla normativa vigente.

TWT, ai sensi della CR/51, ha predisposto un'adeguata struttura informativa interna per fornire periodicamente ad AgID informazioni relative al funzionamento del servizio di posta elettronica certificata (n° caselle attivate, n° messaggi in entrata e in uscita, virus rilevati dal sistema, livelli di servizio erogati), e malfunzionamenti e disservizi rilevati.

Al fine di una elevata trasparenza nei confronti della propria clientela, TWT ha predisposto un sistema informativo che, in caso di impossibilità di utilizzo del servizio PEC, informi il cliente TWT in tempo reale del momento di downtime e di uptime del servizio.
L'informazione, a seconda del grado del malfunzionamento del Servizio, verrà fornita via e-mail sulla casella di posta elettronica tradizionale fornito al momento dell'attivazione del servizio.

Il livello di servizio è riferito ai sistemi TWT fino al collegamento a internet escludendo quindi la rete internet il cui livello di servizio è di competenza del provider del cliente.

7.1 Indicatori di qualità

Vengono di seguito descritti gli indicatori di qualità del servizio di posta elettronica certificata.

DESCRIZIONE	VALORI DI SOGLIA (O INTERVALLI DI VALORI)
Disponibilità di accesso al servizio di posta elettronica certificata (invio/ricezione mail)	7 giorni su 7 24 ore su 24
Tempo massimo di un singolo evento di manutenzione che implichi il fermo del servizio	1 ora e 20 minuti
Tempo massimo di tutti gli eventi di manutenzione che implichino il fermo del servizio nel periodo di riferimento (quadrimestre)	2 ore e 40 minuti
Monitoring automatico dei sistemi (vedi 8.4)	7 giorni su 7 24 ore su 24
Disponibilità del call center per l'assistenza clienti	giorni feriali dalle 8.30 alle 19.00

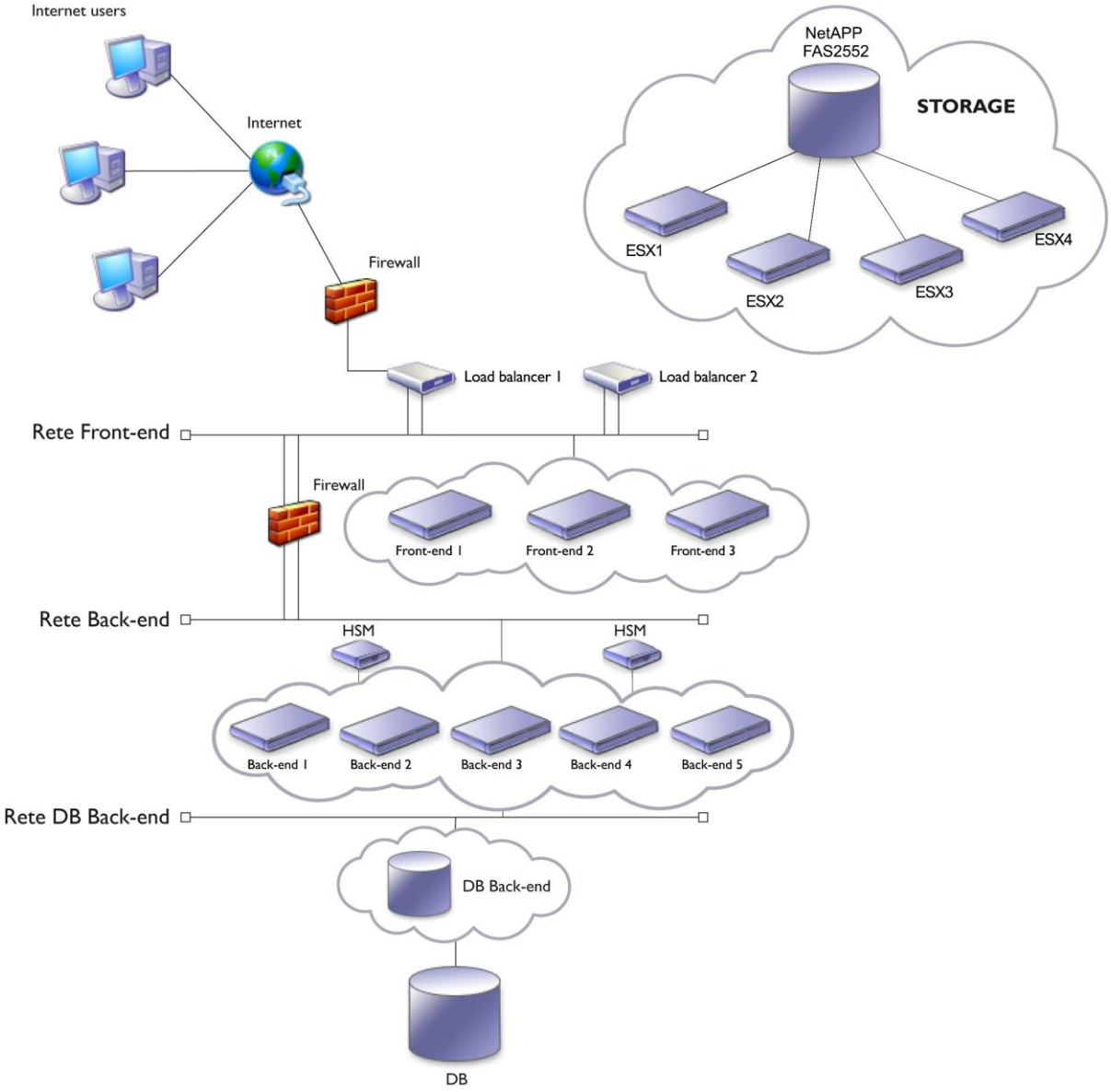
8 Sistemi tecnologici / infrastrutture

8.1 Sistema

Per garantire la massima disponibilità di servizio e la tolleranza ai Fault tutto il sistema tecnologico si basa su un'architettura completamente ridondata; tale architettura è sita presso il CED di TWT di Milano.

8.1.1 Struttura

La seguente figura schematizza la struttura tecnologica in uso:



La soluzione proposta prevede un firewall, collegato direttamente ai *Core Router* internet, che protegge la rete di Front-End da accessi indesiderati. A sua volta il Firewall è collegato al Load Balancer (Bilanciatore di Carico) che funge da livello di astrazione fra Internet e i server di Front-end. Gli utenti accedono ad un indirizzo IP Virtuale (VIP) attestato sul bilanciatore, il quale smista tutte le richieste verso i server di Front-End.

Questi server accettano e validano le richieste degli utenti e inoltrano la posta in arrivo verso le mailbox e quelle in partenza verso gli altri server di posta (altri gestori di posta certificata o altri server di posta ordinaria).

I server di Front-End per accedere ai dati di posta devono collegarsi al cluster di Back-End, tre o più server che si dividono le attività in modalità hot-standy (se un server ha problemi o deve essere fermato per manutenzione, gli altri membri del cluster si prendono in carico le sue attività), per farlo devono attraversare un altro firewall che crea un ulteriore livello di astrazione fra la rete di Front-End e la rete di Back-End.

I server che compongono il cluster di back-end hanno a loro volta la necessità di memorizzare i Log delle transazioni che gestiscono su un Database SQL esterno.

Tutti i server che compongono l'infrastruttura PEC (front-end, back-end e DB) sono dei server virtuali basati su 3 host in cluster su cui è installato l'Hypervisor VMWare ESXi.

Sia il cluster di Back-End sia Database SQL scrivono le proprie informazioni su una unità di storage esterna Fiber Channel equipaggiata con dischi RAID-5, completamente ridondata in tutte le sue parti.

8.1.2 Scalabilità

La scalabilità dell'intero servizio, ossia la capacità di adattarsi all'aumento dell'utenza e/o delle prestazioni, è basata sulla scalabilità delle singole componenti.

Tutte le componenti software presenti nell'infrastruttura sono infatti scalabili sia verticalmente (ossia incrementando le risorse interne di sistema per supportare maggiore potenza di calcolo), sia orizzontalmente (ossia aggiungendo nuovi server in affiancamento agli attuali).

8.1.3 Sicurezza Informatica

Come già detto il disaccoppiamento del livello logico di accesso degli utenti (Front-End) dal livello logico in cui vengono effettivamente conservati i dati (Back-End) e dall'ulteriore livello logico in cui vengono effettivamente conservati i log (DB-Back-End) aumenta la sicurezza del sistema. Il disaccoppiamento avviene tramite apparati Firewall.

Il sistema è protetto da virus tramite l'integrazione con il software antivirus ClamAV con l'integrazione di signature aggiuntivi commerciale.

Per le funzionalità di cifratura, decifratura e firma digitale i server di back-end si avvalgono di una coppia di HSM esterni.

Tutti i certificati di sicurezza utilizzati per queste funzioni sono memorizzati all'interno degli HSM, i quali, attraverso meccanismi di protezione, garantiscono che non venga fatto un uso improprio di tali informazioni (copia, alterazione, etc.).

8.1.4 Affidabilità e fault-tolerance

Sul Front End l'affidabilità del Servizio è garantita dalla ridondanza completa delle singole componenti del sistema e dal loro bilanciamento tramite l'apparato Load Balancer.

I sistemi di Back End per garantire l'alta affidabilità, si avvalgono della configurazione in cluster delle macchine e della clusterizzazione dei servizi.

Tutti i server coinvolti sono virtuali e l'alta affidabilità viene garantita da un cluster di 4 Host fisici VMWare ESXi 6.0 con funzionalità di Fault Tolerant e High Availability.

I dati (mailbox, log, etc.) sono fisicamente conservati su un *Disk Array* esterno, completamente ridondato (logica, connettività, alimentazione, etc.), il quale memorizza i dati su partizioni RAID-5.

Una peculiarità dell'alta affidabilità è la tolleranza ai "fault" di sistema: se un componente di una macchina si guasta c'è sempre un servizio ridondato che può venire in aiuto e sostituirlo temporaneamente, evitando così il disservizio.

8.2 Log di sistema

Tutti le componenti applicative del servizio di posta elettronica certificata registrano su appositi file di Log tutte le operazioni svolte tenendo traccia delle informazioni che compongono ogni singolo evento all'interno del sistema. A titolo di esempio ecco alcune delle informazioni memorizzate:

- eventi di sistema;
- connessione instaurate;
- presenze di virus;
- protocolli utilizzati;
- sincronizzazione dei sistemi;
- eventuali anomalie;
- controllo delle firme;
- codifica e decodifica dei messaggi.

I dati memorizzati possono variare da evento ad evento e da componente a componente.

Oltre ai Log su file (generati da tutte le componenti di sistema), vengono anche creati dei Log su Database esclusivamente per le componenti di back-end, relativamente a tutti gli eventi che hanno interessato ogni singolo messaggio. A titolo di esempio ecco alcune delle informazioni memorizzate:

- identificativo univoco originale di ogni messaggio;
- data e ora;
- tipo di evento (accettazione, spedizione, ricezione, avvisi, ricevute, ecc.);
- mittente;
- destinatari;
- oggetto del messaggio;
- anomalie.

Per garantire la sincronizzazione temporale di tutti le componenti del sistema viene utilizzato il protocollo NTP (Network Time Protocol). La sincronizzazione avviene utilizzando come riferimento temporale diversi ***Time Server*** pubblici.

8.2.1 Log su File

Tutti i componenti del sistema (back-end e front-end) che generano Log su File, chiudono e aprono un nuovo file di Log con cadenza giornaliera. Tali file di Log non risiedono sui server di Back-end / Front-end, ma su uno storage esterno completamente ridondato in configurazione ***Alta Affidabilità (HA)***.

8.2.2 Log su Database

Le componenti di back-end memorizzano, su un database esterno gestito dal cluster fisico VMWare, tutti gli eventi che hanno interessato ogni singolo messaggio gestito dal sistema di Posta Elettronica Certificata; come per il precedente paragrafo anche questi dati vengono memorizzati su uno storage esterno completamente ridondato in configurazione ***Alta Affidabilità (HA)***.

Questi database vengono giornalmente esportati su file e si aggiungono ai file di log già generati al punto precedente.

8.2.3 Archiviazione

Quotidianamente tutti i file di log generati vengono compressi in un unico file, questo file viene marcato temporalmente e conservato secondo le modalità definite nelle "istruzioni per la conservazione dei log dei messaggi e dei messaggi di posta elettronica certificata con virus" pubblicato sul sito AGID.

8.2.4 Interrogazione

In qualsiasi momento è possibile recuperare i file precedentemente archiviati per poter interrogare i log di una giornata intera o di una singola transazione elaborata dal sistema PEC.

8.3 Sicurezza dei dati

Come già accennato in precedenza, per garantire il più alto livello di servizio possibile, tutti i dati importanti (mailbox, log degli eventi, etc.) eventi vengono memorizzati su un Disk Array Fiber Channel esterno, equipaggiato con dischi in configurazione RAID-5, ridondato in tutte le sue parti.

8.3.1 Backup dei dati

Il sistema di storage in uso per il sistema PEC utilizza la logica di "Snapshot" per effettuare periodicamente una fotografia di tutti i dati. Queste fotografie avvengono ogni 2 ore per il giorno corrente e una al giorno per i giorni successivi fino a 30gg. Lo storage inoltre è replicato ogni 15 minuti su apparecchiatura gemella localizzato presso un sito distaccato; gli operatori di TWT sono responsabili, secondo le policy interne, di:

- verificare giornalmente il buon funzionamento degli storage e dello stato delle repliche;
- provvedere alla manutenzione ordinaria e straordinaria delle apparecchiature.

8.3.2 Restore dei dati

Nel caso in cui si renda necessario effettuare un ripristino dei dati, a causa di perdite accidentali o incidenti, è possibile ripristinare dal singolo log del messaggio fino all'intero sistema.
La procedura di restore è a carico del reparto tecnico TWT con l'impiego di personale opportunamente addestrato.

8.4 Monitoring

TWT S.p.A. ha sviluppato una suite di software proprietari per il monitoring e l'auditing di tutte le componenti hardware e software che compongono l'infrastruttura tecnologica.

Questi software sono sviluppati utilizzando i più diffusi protocolli standard (syslog, snmp, etc.) garantendo l'integrazione con la maggior parte dei

sistemi presenti sul mercato. Nel caso in cui si presenti la necessità di monitorare un sistema *non standard,* TWT sviluppa al suo interno un'integrazione specifica.

Fra le componenti che il sistema è in grado di monitorare abbiamo:

- PING Check
  Verifica che un indirizzo IP sia raggiungibile, è quindi possibile verificare che qualsiasi apparato collegato alla rete sia fisicamente operativo (pc, server, router, switch, etc. Etc.);

- TCP/UDP Port Check
  Verifica che su un dato indirizzo IP siano raggiungibili una o più porte TCP/UDP, in questo modo è possibile verificare che su quel determinato apparato sia attivo un particolare servizio;

- Service Check
  Verifica che un determinato programma sia in esecuzione sulla macchina che si sta controllando;

- Cluster Check
  Verifica l'operatività di tutte quelle macchine che lavorano in modalità cluster;

- Disk Space Check
  Verifica lo spazio disponibile sul disco di un determinato server, impostando delle soglie di allarme;

- HTTP Query
  Verifica la funzionalità di un server HTTP, verificando non solo la raggiungibilità del server ma anche interpretando la risposta dello stesso e agendo di conseguenza;

- SNMP Query
  Fra tutte le componenti monitorabili questa è considerata la più ampia in termini di possibilità, il protocollo SNMP (acronimo di Simple Network Management Protocol) è uno standard per cui tutte le componenti che ne fanno uso (sia hw che sw) mettono a disposizione una struttura logica e standard di accesso alle informazioni della componente che si interroga. Le informazioni che vengono messe a disposizione variano da componente a componente, da informazioni di stato a informazioni statistiche.
  A titolo puramente esemplificativo e non esaustivo, ecco alcuni esempi:

- *Server*
  - *Temperature (Fan, CPU, Power, Ambiente, ...);*
  - *Operatività di schede (Lan, SCSI, Fiber, ...);*
  - *Stato delle Memorie;*
  - *Processi attivi;*

- *Router*
  - *Temperature;*
  - *Memoria;*
  - *Carico di lavoro;*
  - *Stato dei peering;*

Quindi, tramite questa componente, è possibile monitorare in tutte le sue parti qualsiasi hw o sw che utilizzi questo standard.

Quando il sistema di monitoring rileva qualche anomalia, sulla base delle regole configurate, può intraprendere una serie di azioni informative e/o correttive:

- inviare mail a tutti gli indirizzi predefiniti per la regola specifica avvisando dell'anomalia rilevata;
- inviare SMS a tutti i numeri di cellulare predefiniti per la regola specifica avvisando dell'anomalia rilevata
- se previsto, eseguire dei software esterni passando come parametri quelli configurati sulla regola;
- se previsto, eseguire operazioni specifiche (riavvio delle apparecchiature, reset di software, restart applicativi, etc.) avvisando il personale preposto via mail e/o sms del risultato dell'operazione effettuata;
- se e quando il problema viene risolto (automaticamente o a seguito di intervento umano) il sistema avvisa (via mail e/o sms) tutti gli interessati del cambiamento di stato.

Il personale di TWT S.p.A. è adeguatamente e opportunamente formato per interpretare, gestire e risolvere le diverse anomalie che si presentano intervenendo da remoto quando possibile (tramite accesso VPN) o localmente presso il CED.

8.5 Marcatura Temporale

La marcatura temporale è come un messaggio firmato digitalmente che lega in modo sicuro un documento informatico (file) ad una data e ora certa e opponibile ai terzi.

Tutti i log delle trasmissioni, al momento di essere archiviati con cadenza giornaliera o anche in base al raggiungimento di una certa dimensione definita, vengono marcati temporalmente, apponendo un riferimento temporale (marca) opponibile ai terzi in base alla normativa. Il servizio di Time Stamping si intende erogato da un'autorità (Certification Autority, CA) iscritta nell'apposita lista stilata dal AgID relativa alle Time Stamping Autority.

8.6 Interoperabilità

In ottemperanza a quanto previsto dalla normativa vigente TWT S.p.A. si impegna a garantire l'interoperabilità con gli altri gestori in conformità alle regole di Posta Elettronica Certificata.

TWT, inoltre, effettua dei controlli periodici di interoperabilità tramite l'invio e la ricezione di messaggi di test verso gli altri gestori PEC accreditati.

8.7 Descrizione del CED

TWT S.p.A. dispone di un CED di circa 600mq nella quale sono ospitate tutte le infrastrutture tecnologiche dell'azienda.

Il palazzo è dotato di una cabina elettrica di media tensione da 23000 Volts, con 2 trasformatori da 1000 KVA; tutto il circuito è completamente ridondato. Alla cabina elettrica sono collegati 2 gruppi elettrogeni distinti, ridondati fra di loro in modalità warm/standby, di marca Perkins da 1000 KVA ciascuno, dotati di telecontrollo e avvisi ai responsabili dell'impianto in caso di anomalie.

Tutte le apparecchiature presenti nel CED sono protette da 2 gruppi UPS da 160 KVA l'uno.

Nel CED è presente un impianto di condizionamento della Schneider Electric ad acqua refrigerata costituito da 3 gruppi frigor con 2

compressori ciascuno, dotati della funzione free-cooling e controllati da un microprocessore proprietario; l'impianto è dotato di telecontrollo per l'invio di allarmi alla società manutentrice e ai responsabili TWT in caso di problemi/guasti.

Ogni armadio (rack) presente nel CED dispone di 2 alimentazioni da 16A o 32A provenienti da linee separate; questo permette alle apparecchiature con alimentazione ridondata di essere collegate a due linee elettriche distinte.

Onde poter garantire un livello di sicurezza sufficiente del CED e garantire che l'attività si svolga secondo i requisiti richiesti sono state approntate le seguenti misure di sicurezza:

L'accesso fisico ai locali è controllato da sistemi elettronici che permettono l'ingresso solo a personale autorizzato, tutte le persone che accedono al CED sono identificate grazie a un badge personale, in grado di inibire l'accesso al personale non autorizzato; il sistema è inoltre in grado di effettuare un sistema di *auditing* sull'ingresso/uscita del personale dal CED.

L'accesso logico ai sistemi informatici avviene attraverso l'utilizzo di una user e password personale in grado di identificare con sicurezza il personale che vi accede.

Il numero di persone autorizzate agli accessi fisici/logici è ridotta al minimo per poter garantire una maggior sicurezza.

Nei locali è in funzione un impianto di videosorveglianza a registrazione continua su Hard Disk (KDVR) collegato alla rete interna ed accessibile solo al personale responsabile della sicurezza con user/password personali.

È attivo anche un impianto Antifurto/Antintrusione con sensori di movimento nei locali e contatti di continuità a porte e finestre.

Questo impianto è dotato:

- sirene/lampeggianti che si attivano in caso di allarme;
- 2 combinatori telefonici (1 analogico e 1 cellulare GSM) che chiamano i responsabili di TWT in caso di allarme;
- collegamento IP alla rete interna per gestione e monitoring di tutto l'impianto;

9 Aspetti Operativi

9.1 Note sull'organizzazione del personale

Il personale preposto all'erogazione e controllo del servizio di posta elettronica certificata è organizzato nel rispetto dell'art. 21 del [DM].

In particolare, sono definite le seguenti figure organizzative:

- Responsabile della registrazione dei titolari;
- Responsabile dei servizi tecnici;
- Responsabile delle verifiche ed ispezioni (auditing);
- Responsabile della sicurezza;
- Responsabile della sicurezza dei log dei messaggi;
- Responsabile del sistema di riferimento temporale.

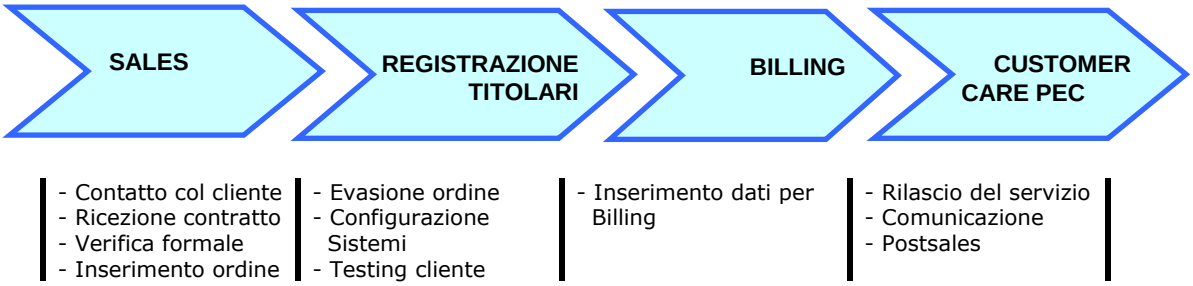
Talune figure professionali possono svolgere più funzioni tra loro compatibili. In particolare il responsabile della sicurezza è responsabile anche della sicurezza dei log dei messaggi e del sistema di riferimento temporale.

Le figure sopra elencate possono avvalersi, per lo svolgimento delle funzioni di loro competenza, di loro collaboratori che opereranno secondo le specifiche di comportamento definite dal responsabile.

Tutte le figure professionali coinvolte nella gestione/supervisione del sistema di Posta Elettronica Certificata vengono opportunamente addestrate mediante corsi di formazione tenuti internamente o esternamente.

9.2 Flusso Organizzativo

Il processo di attivazione del servizio PEC di TWT prevede il seguente flusso operativo che coinvolge diverse aree e funzioni aziendali dal primo contatto col cliente fino al rilascio del servizio.



Tale flusso è governato e controllato dai responsabili descritti nel paragrafo precedente.

Il contatto iniziale del cliente viene gestito dalla struttura commerciale interna che, ricevuta la richiesta di registrazione, ha in gestione le attività di inizializzazione del processo di inserimento ordine nel sistema gestionale TWT.

In generale ad ogni cliente viene assegnato un account commerciale che sarà il suo punto di contatto privilegiato con TWT.

La gestione operativa del servizio ed il relativo contatto è invece demandato al Customer Care di TWT, trai cui compiti principali di post sales è incaricato della gestione dell'assistenza alla clientela PEC.

9.3 Modalità di Gestione dell'Assistenza

La procedura di gestione dell'assistenza per il servizio di Posta Elettronica Certificata definisce e descrive i criteri e le modalità per l'espletamento della erogazione dell'assistenza richiesta.

Il servizio di assistenza è esplicitamente previsto contrattualmente ed erogato agli utenti registrati al servizio di posta elettronica certificata TWT e all'amministratore delle caselle di posta elettronica certificata attestate su un dominio di proprietà del cliente.

Il servizio erogato dal Customer Care TWT è attivo dalle 8.30 alle 19.00 dal lunedì al venerdì esclusi i festivi, raggiungibile:

- al numero verde 800.192.800
- via mail al support@twtcert.it

L'utente può richiedere supporto all'assistenza per i seguenti motivi:

- supporto durante la configurazione della casella di posta elettronica certificata;
- impossibilità di accedere al Mail Server;
- supporto all'utilizzo del client web;
- supporto durante la configurazione dei certificati elettronici nei client di posta;
- richiesta di informazioni sulla posta certificata (validità legale, caratteristiche, ecc.);
- richiesta informazioni riguardanti l'interoperabilità con gli altri operatori di posta certificata;
- smarrimento user-id per accesso al servizio;
- supporto in caso di smarrimento della password: TWT le invierà una email di reset contenente le relative istruzioni necessarie per impostarne una nuova;
- richiesta dei log dei messaggi;
- richieste relative al materiale di supporto degli utenti (ad esempio disponibilità del manuale utente o aggiornamento);
- compatibilità del client di posta con il servizio erogato da TWT;
- altre informazioni rilevanti al fine di poter fruire del servizio.

L'amministratore delle caselle di posta elettronica certificata attestate su un dominio di proprietà del cliente può, invece, richiedere supporto all'assistenza per i seguenti motivi:

- richiesta di assistenza durante la creazione di una casella di posta elettronica certificata nel proprio dominio di appartenenza;
- impossibilità di accedere al servizio;
- richiesta di informazioni sul servizio;
- richiesta di assistenza per modifica anagrafica utente;
- richiesta di assistenza per reset password utente;
- richiesta ripristino ricevute;
- richieste relative al materiale di supporto dell'amministratore;
- richiesta supporto registrazione utenti;
- altre informazioni rilevanti al fine di poter fruire del servizio.

9.4 Gestione delle emergenze

Al fine di garantire la continuità del servizio, i sistemi automatici di monitoraggio (paragrafo 8.4) avvisano tempestivamente i reperibili di TWT delle anomalie riscontrate e questi intervengono analizzando la problematica e, se possibile, risolvendola o eventualmente attuando l'escalation del problema verso il livello di competenza tecnica o responsabilità necessaria.

Al presentarsi del problema il reperibile compie le seguenti attività:

- Avvisa il suo diretto responsabile dell'anomalia riscontrata.
- Apre un Trouble Ticket Interno per tenere traccia del problema.
- Per ogni eventuale segnalazione da parte dei clienti viene aperto un altro Trouble Ticket che viene correlato al Trouble Ticket Interno aperto in precedenza.
- Se non è in grado di risolvere il problema in autonomia, coinvolge altri tecnici specializzati interni.
- Se si rende necessario contatta eventuali fornitori utili alla risoluzione del problema.
- Se il problema permane, informa, se non ne è già a conoscenza, il Responsabile del Servizio PEC con il quale verranno concordate le attività più consone necessarie alla risoluzione del problema.
- Informare, secondo le modalità previste dai contratti, tutta la clientela PEC dell'anomalia in corso.
- Informare, secondo le modalità e i tempi previsti dalla [CR/51], AgID.

Alla risoluzione del problema viene chiuso il Trouble Ticket Interno e tutti i Trouble Ticket correlati ad esso e vengono contattati i clienti che hanno riscontrato il problema per avvisarli della avvenuta risoluzione.

10 Protezione dei dati personali (Privacy)

Titolare del trattamento dei dati è TWT S.p.A., con sede legale in Milano, Via Abbondio Sangiorgio n. 12, 20145, e Sede Operativa in Milano, Viale E. Jenner n. 33, 20159.
TWT ha nominato il proprio Responsabile della protezione dei dati che può essere contattato all' indirizzo mail dpo@twt.it.

I dati personali trattati sono:

- i dati forniti in sede di registrazione dal titolare della casella;
- i dati presenti sulla copia del documento di identità del titolare della casella;
- i dati derivanti dall'esecuzione delle prestazioni richieste (invio e ricezione di messaggi pec)
- gli eventuali dati personali contenuti nei messaggi pec e nei relativi allegati.

I dati sono trattati per la fornitura del servizio. Potranno essere comunicati a chi, avendone un lecito e comprovato interesse, anche al di fuori dell'Unione Europea, richieda di accertare la titolarità della casella di posta elettronica di cui risulta assegnatario l'interessato o di avere conto dei messaggi scambiati e/o del contenuto degli stessi.

Il conferimento dei dati personali richiesti in sede di registrazione è obbligatorio e l'eventuale rifiuto comporta l'impossibilità di svolgere il servizio.

Con il consenso dell'interessato, i dati forniti dall'interessato in sede di registrazione potranno essere utilizzati a fini di vendita diretta di propri prodotti o servizi, a fini di marketing, promozione delle attività e presentazione delle iniziative di TWT.

La durata di conservazione dei dati è fissata dalla legge.

I dati potranno altresì essere comunicati o resi accessibili alle società controllate e/o collegate a TWT, ad altre Società che si occupano della manutenzione dei sistemi informatici nonché ai soggetti che si occupano di specifiche fasi dei trattamenti, in qualità di responsabili di TWT, i cui nominativi sono a disposizione a richiesta degli interessati.

L'interessato ha il diritto di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi e la limitazione del trattamento. Ha, inoltre, il diritto di opporsi al trattamento dei dati

personali e il diritto alla portabilità degli stessi. Può esercitare i suoi diritti rivolgendosi a dpo@twt.it.
L'interessato ha, infine, il diritto di proporre reclamo al Garante per la protezione dei dati personali.

10.1 Misure di sicurezza a protezione dei dati personali

Il gestore tratta i dati personali nel rispetto della normativa vigente in materia di dati personali adottando le misure tecniche e organizzative necessarie per garantire un livello di sicurezza dei propri sistemi adeguato al rischio relativo ai dati personali trattati.

Con riferimento al DB di registrazione si evidenzia che:

- il DB di registrazione e la relativa applicazione di gestione risiedono su un elaboratore dedicato, ubicato in una sala tecnica ad accesso controllato;
- per accedere all'applicazione, gli operatori si identificano mediante credenziali univoche e personali;
- l'applicazione mantiene accuratamente traccia, in un apposito giornale di controllo, di ogni operazione effettuata;
- viene prodotta periodicamente una copia di sicurezza (backup) della base dati e di altre informazioni essenziali per il ripristino del sistema in caso di guasto all'elaboratore o di perdita accidentale di dati.

Con riferimento ai messaggi di posta elettronica certificata si evidenzia che il colloquio tra l'interfaccia web dell'utente ed il sistema PEC di TWT avviene attraverso protocolli e connessioni sicuri (SMTP+SSL, IMAP+SSL, POP3+SSL, HTTPS), e che solo utenti accreditati che abbiano superato i controlli di sicurezza possono accedere alle proprie caselle di posta elettronica certificata TWT.