Manuale Operativo

Servizio di Posta Elettronica Certificata

ITnet S.r.l.
Responsabile del Servizio PEC
Luigi Erardi

Redazione / Verifica / Approvazione	Data
Redatto: Antonello Pettazzi (Project & Quality)	14 marzo 2018
Approvato: Luigi Erardi (Responsabile servizio PEC)	14 marzo 2018

Distribuzione

Tipo di distribuzione	Golden Copy (Copia n. 1)	Copia n.
Pubblica	Archiviata presso: Qualità	Consegnata a: Data:

Storia delle revisioni

Rev. N.	Oggetto della revisione	Data
1.0	Prima emissione	26.01.2006
1.1	- Aggiornamento dei riferimenti per archiviazione Manuale; - Aggiornamento del Responsabile del Manuale; - Aggiornamento del Responsabile del Trattamento dei Dati	15.06.2006
1.2	Aggiornamento dei dati identificativi del Gestore (1.2.1)	31.07.2007
1.3	Revisione generale del Manuale Operativo	11.07.2008
1.4	- Aggiornamento modalità di vendita; - Migliore descrizione delle attività formative sul personale.	06.03.2009
1.5	- Aggiornamento dello strumento utilizzato per apporre le marche temporali ai log; - Adeguamento alla circolare CNIPA/CR/56 – Circolare CNIPA 21 Maggio 2009, n. 56.	22.03.2010
1.6	- Revisione annuale - Aggiornamento del Responsabile del Manuale; - Descrizione nuove funzionalità - Aggiornamenti dovuti alla installazione di una nuova release del SW PEC.	28.02.2011
2.0	Aggiornamento dei dati identificativi del Gestore	24.11.2011
2.1	- Nuovo logo; - Aggiornamento dei dati identificativi del Gestore - Aggiornamento riferimenti per Privacy	28.02.2013
3.0	- Aggiornamento Sede Legale - Aggiornamento elenco Data Center	03.12.2013
4.0	- Adeguamento alla circolare AgID sulla riassegnazione delle caselle di posta PEC	12.03.2014
4.1	- Aggiornamento Canali di comunicazione con il Gestore	14.04.2014
4.2	- Aggiornamento Amministratore Delegato Itnet s.r.l. - Aggiornamento dei dati identificativi del Gestore	26.05.2014
5.0	- Revisione annuale	02.03.2015

Rev. N.	Oggetto della revisione	Data
5.1	- Aggiornamento Amministratore Delegato Itnet s.r.l. - Aggiornamento indirizzo Servizio Clienti	10.06.2015
5.2	- Aggiornamento dimensione massima messaggi	12.05.2016
6.0	- Aggiornamento Amministratore Delegato Itnet s.r.l. - Aggiornamento descrizione infrastruttura di esercizio PEC	22.05.2017
6.1	- Nuova infrastruttura per il Disaster Recovery del servizio PEC	15.09.2017
7.0	- Revisione annuale - Adeguamento alla nuova organizzazione aziendale - Adeguamento alla versione 2015 della norma ISO 9001	14.03.2018

INDICE

1. GENERALITA' 7

1.1. GENERALITÀ DEL DOCUMENTO 7
1.1.1. Scopo e campo di applicazione 7
1.1.2. Identificazione del documento e gestione delle modifiche 7
1.1.3. Responsabile del manuale 7
1.1.4. Definizioni, abbreviazioni e acronimi 8
1.1.5. Riferimenti normativi 13
1.1.6. Tabella di corrispondenza 14
1.2. GENERALITÀ DEL GESTORE 16
1.2.1 Dati identificativi del Gestore 16
1.2.2 Canali di comunicazione con il Gestore 16
1.2.3 Accesso al sito WEB del gestore 17
1.2.4 Accesso al Manuale Operativo 17
1.2.5 Standard di sicurezza, qualità e tecnologici 17

2. GENERALITA' SUL SERVIZIO DI POSTA ELETTRONICA CERTIFICATA 20

2.1. FUNZIONAMENTO DEL SERVIZIO 20
2.2. FUNZIONAMENTO DEL SERVIZIO IN CASO DI PROBLEMI DI CONSEGNA 22
2.2.1. Descrizione del funzionamento in caso di messaggi non consegnabili 22
2.2.2. Descrizione del funzionamento in presenza di virus 22
2.3. CARATTERISTICHE DELLE RICEVUTE E DELLE BUSTE DI TRASPORTO 23
2.3.1. Firma elettronica delle ricevute e delle buste di trasporto 23
2.3.2. Riferimento temporale 23
2.3.3. Tipologia delle Ricevute di Avvenuta Consegna 23

3. IL SERVIZIO DI POSTA ELETTRONICA CERTIFICATA DI ITNET S.R.L. 25

3.1. TIPOLOGIA DEL SERVIZIO OFFERTO 25
3.1.1. "Profilo Base" 25
3.1.2. "Profilo Plus" 26
3.1.3. "Profilo Multidominio" 27
3.1.4. Gestione dei domini di Posta Elettronica Certificata 28
3.2. SERVIZI OPZIONALI 29
3.2.1. Rubrica, Lista attività e Calendario 29
3.3. PERSONALIZZAZIONI 29
3.4. ACCESSO AL SERVIZIO 29
3.4.1. Interfaccia WEB 29
3.4.2. Client di posta elettronica 30
3.4.3. Credenziali di accesso e parametri configurazione del servizio 31
3.4.4. Raccomandazioni per l'utenza 31

4. LIVELLI DI SERVIZIO E INDICATORI DI QUALITA' 32

5. CONDIZIONI DI FORNITURA 33

5.1. CANALI DI VENDITA, PROPOSTA E DOCUMENTAZIONE DEL SERVIZIO 33
5.1.1. Attivazione diretta del servizio 33
5.1.2. Attivazione del servizio tramite Partner commerciale 33
5.1.3. Attivazione del servizio tramite rivenditore (offerta Multidominio) 34
5.1.4. Modalità alternative per l'attivazione del servizio 35
5.2. ATTIVAZIONE DEL SERVIZIO 35
5.2.1. Gestione della registrazione del Titolare 35
5.3. DISDETTA DEL CONTRATTO 35
5.4. CORRISPETTIVO ECONOMICO 36
5.5. DESCRIZIONE GENERALI DEGLI ELEMENTI DEL CONTRATTO 36

5.6. OBBLIGHI E RESPONSABILITÀ 37
5.6.1. Obblighi del gestore – ITnet S.r.l. 37
5.6.2. Obblighi del Titolare del servizio 37
5.6.3. Responsabilità del Titolare 38
5.6.4. Cessione del servizio 38
5.7. ESCLUSIONI E LIMITAZIONE IN SEDE DI INDENNIZZO 38
6. SISTEMI TECNOLOGICI 40
6.1. INFRASTRUTTURE 40
6.2. CONNETTIVITÀ 42
6.3. DATA CENTER - CARATTERISTICHE PRINCIPALI 44
6.3.1. Caratteristiche comuni ai Data Center Itnet 44
6.3.2. Sito di Milano Ortles 44
6.3.3. Sito di Siziano (SuperNap) 45
6.4. PRECISIONE DEL RIFERIMENTO TEMPORALE 45
6.5. GESTIONE DEI LOG DEI MESSAGGI 46
6.5.1. Descrizione 46
6.5.2. Archiviazione e Conservazione 47
6.5.3. Reperimento e presentazione 48
7. INTEROPERABILITA' TRA GESTORI 50
8. MISURE DI SICUREZZA E SOLUZIONI FINALIZZATE A GARANTIRE IL COMPLETAMENTO DELLA TRASMISSIONE 51
8.1. ORGANIZZAZIONE DEL PERSONALE 51
8.2. APPROCCIO ORGANIZZATIVO 51
8.3. APPROCCIO TECNOLOGICO 52
8.3.1. Firma 52
8.3.2. Autenticazione 53
8.3.3. Colloquio Sicuro 53
8.3.4. Virus 53
8.3.5. Data Center - Standard di sicurezza 54
8.3.6. Backup dei dati 54
8.3.7. Monitoraggio 54
8.3.8. Gestione delle emergenze 55
9. MODALITA' DI CESSAZIONE DELL'ATTIVITA' DI GESTORE 56
10. PROTEZIONE DEI DATI PERSONALI 57
10.1. INFORMATIVA 57
10.2. PROCEDURE DI RIFERIMENTO 58
10.3. MISURE DI SICUREZZA PER LA PROTEZIONE DEI DATI PERSONALI 59
10.3.1. Trasmissione e accesso ai dati da parte dell'utente 59
10.3.2. Misure di sicurezza per la protezione dei dati 59

1. GENERALITA'

1.1. Generalità del Documento

1.1.1. Scopo e campo di applicazione

Il presente documento è stato redatto per descrivere le caratteristiche e le procedure adottate da ITnet S.r.l. per l'erogazione del Servizio di Posta Elettronica Certificata.

Nel presente manuale, oltre alle informazioni di carattere generale, sono state inserite tutte le informazioni necessarie per spiegare in maniera più completa possibile l'offerta di Posta Elettronica Certificata proposta da ITnet S.r.l.

1.1.2. Identificazione del documento e gestione delle modifiche

Questo documento è denominato Manuale Operativo di Posta Elettronica Certificata ed è identificato dalla data di emissione e dall'indice di revisione (inserito nell'intestazione di ogni pagina).

La versione attuale è la 6.1.

ITnet S.r.l. è responsabile della definizione, pubblicazione e aggiornamento del documento.

Il Manuale Operativo è pubblicato sul sito WEB del gestore (paragrafo 1.2.4 del presente documento) ed è scaricabile e consultabile telematicamente.

ITnet S.r.l. garantisce che la versione pubblicata sul sito è l'ultima aggiornata.

Il Manuale Operativo è stato organizzato in 10 (dieci) capitoli ognuno contenente tematiche ben definite in modo tale da permettere all'Utente un agevole orientamento all'interno del documento.

Le eventuali modifiche saranno sottoposte a ciclo di validazione (verifica e approvazione) da enti competenti e terranno conto di cambiamenti delle normative e dei regolamenti sui quali è basato tale Manuale Operativo.

Tali modifiche possono essere anche dettate da ottimizzazioni procedurali, da evoluzioni dell'offerta o da esigenze tecniche.

ITnet S.r.l. si impegna ad effettuare un controllo con cadenza annuale sui contenuti del documento al fine di garantirne la coerenza e l'aggiornamento.

1.1.3. Responsabile del manuale

Il responsabile del presente Manuale Operativo individuato da ITnet S.r.l. è ***Antonello Pettazzi.*** A cui ogni utente può rivolgersi per informazioni,

domande e chiarimenti riguardanti il presente manuale, contattandolo ai seguenti recapiti:

Antonello Pettazzi
PreSales & Qualiy
ITnet S.r.l.

Via del Bosco Rinnovato 8 – Palazzo U4
20090 Assago (MI)
a.pettazzi@it.net

1.1.4. Definizioni, abbreviazioni e acronimi

1.1.4.1 Definizioni

Di seguito sono elencate le definizioni utilizzate per la stesura del presente Manuale Operativo.

Per i termini già definiti nelle norme di riferimento si è riportata, se possibile in maniera integrale, la definizione data dalla norma (la codifica e l'elenco delle normative di riferimento sono riportate al paragrafo 1.1.5 del presente manuale) eventualmente integrata dalla particolare accezione con cui il termine viene utilizzato in ITnet S.r.l.

Termine	Definizione
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 del mittente è impossibilitato ad accettare il messaggio in ingresso, recante le motivazioni 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 del mittente, all'interno della quale sono inseriti il messaggio originale inviato dal Titolare di Posta Elettronica Certificata ed i relativi dati di certificazione.

Termine	Definizione
Casella di Posta Elettronica Certificata	È una casella di posta elettronica all'interno di un dominio di Posta Elettronica Certificata ed alla quale è associata una funzione che rilascia delle ricevute di avvenuta consegna al ricevimento di messaggi di Posta Elettronica Certificata.
Dati di certificazione	I dati, quali ad esempio data e 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 varie ricevute e sono trasferiti al titolare destinatario insieme al messaggio originale per mezzo di una busta di trasporto.
Destinatario	Utente che si avvale del servizio di Posta Elettronica Certificata per la ricezione dei documenti prodotti mediante strumenti informatici.
Dominio di Posta Elettronica Certificata	Dominio di Posta Elettronica Certificata che contiene unicamente caselle di Posta Elettronica Certificata.
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 garantiscono il controllo esclusivo da parte del Gestore.
Firma digitale	Il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore, 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 (art 1 lett. n del DPR n. 445/2000).
Firma elettronica	Insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica.

Termine	Definizione
Firma elettronica avanzata	Firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, 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.
Gestore di Posta Elettronica Certificata	È il soggetto che gestisce uno o più domini di Posta Elettronica Certificata con i relativi punti di accesso, di ricezione e di consegna. E' titolare della chiave usata per la firma delle ricevute e delle buste nel rispetto della normativa vigente. Si interfaccia con altri gestori di Posta Elettronica Certificata per l'interoperabilità con altri titolari.
Indice dei gestori di Posta Elettronica Certificata	E' il sistema, gestito dal DIGITPA, che contiene l'elenco dei domini e dei gestori di Posta Elettronica Certificata.
Log dei messaggi	Registro informatico delle operazioni relative alle trasmissioni effettuate mediante la Posta Elettronica Certificata tenuto dal Gestore.
Marca Temporale	È un'evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi secondo quanto previsto dal DPR 28 dicembre 200 n. 445 e dal decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 pubblicato nella Gazzetta Ufficiale n. 98 del 27 aprile 2004.
Messaggio di Posta Elettronica Certificata	E' un documento informatico composto dal testo del messaggio, dai dati di certificazione e dagli eventuali documenti informatici allegati.
Messaggio originale	È 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 l'invio di documenti prodotti mediante strumenti informatici.
PEC	Posta Elettronica Certificata

Termine	Definizione
Posta Elettronica Certificata	Ogni sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici.
Punto di 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 un virus informatico all'interno del messaggio, di emissione della ricevuta di accettazione e di imbustamento del messaggio originale nella busta di trasporto.
Punto di consegna	Il sistema che compie la consegna del messaggio nella casella di Posta Elettronica Certificata del destinatario titolare, 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.
Punto di ricezione	Il sistema che riceve il messaggio all'interno di un dominio di Posta Elettronica Certificata, effettua controlli sulla provenienza e sulla correttezza del messaggio ed emette la ricevuta di presa in carico, imbusta i messaggi errati in una busta di anomalia e verifica la presenza di virus informatici all'interno dei messaggi di posta ordinaria e della busta di trasporto.
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.

Termine	Definizione
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 del mittente per attestare l'avvenuta presa in carico del messaggio da parte del sistema di Posta Elettronica Certificata del destinatario 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.
Titolare	Il soggetto a cui sono assegnate una o più caselle di Posta Elettronica Certificata. All'interno del presente documento si identifica come Titolare il soggetto al quale viene erogato il servizio di PEC
Titolare del trattamento dei dati	E' il soggetto a cui compete la scelta in ordine di finalità e modalità del trattamento secondo quanto definito nel Decreto 196 del 2003
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, che sia mittente o destinatario di Posta Elettronica Certificata.
Virus Informatico	Un programma informatico avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati e dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale o l'alterazione del suo funzionamento.
Data Center	I Data Center di ITnet sono dislocate a Roma e Milano. Il servizio di Posta Elettronica Certificata è erogato dal Data Center di Milano.

1.1.4.1 Abbreviazioni e acronimi

Di seguito sono elencate le abbreviazioni e gli acronimi utilizzati.

Abbreviazione	Significato
AgID	Agenzia per l'Italia Digitale: istituita con decreto legge n. 83, convertito nella legge n. 134/2012 assorbe le competenze di DigitPA,
DPR	Decreto del Presidente della Repubblica
CAD	Codice dell'Amministrazione digitale (Decreto Legislativo 7 Marzo 2005 n.82)

Abbreviazione	Significato
CMS	Cryptographic Message Syntax
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
CRL	Certificate Revocation List
CRL DP	Certificate Revocation List Distribution Point
DNS	Domain Name Service
DigitPA	A decorrere dal 29 Dicembre 2009 a seguito del decreto del 1° Dicembre 2009, n.177 il CNIPA viene riordinato con nuova denominazione DigitPA
FQDN	Fully Qualified Domain Name
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format
MIME	Multipurpose Internet Mail Extensions
PEC	Posta Elettronica Certificata
S/MIME	Secure/MIME
SMTP	Simple Mail Transfer Protocol
TLS	Transport Layer Security
XML	eXtensible Markup Language
NTP	Network Time Protocol

1.1.5. Riferimenti normativi

Di seguito sono elencati i riferimenti normativi che sono stati presi in considerazione per la stesura del presente manuale:

[1] DPR n. 445/2000 - Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445,
Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa e successive modifiche ed integrazioni

[2] Decreto Legislativo n. 196 del 30 giugno 2003
Codice in materia di protezione dei dati personali

[3] DPR 68/2005 - 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 della legge 16 gennaio 2003, n. 3

[4] CAD - Decreto Legislativo 7 marzo 2005, n. 82
Codice dell'Amministrazione Digitale

[5] DM 2/11/2005 - Decreto della Presidenza del Consiglio dei Ministri Dipartimento per l'Innovazione e le Tecnologie 2 Novembre 2005
Recante le Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della Posta Elettronica Certificata

[6] CNIPA/CR/49 - Circolare CNIPA 24 Novembre 2005, n. 49
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.

[7] CNIPA/CR/51-Circolare CNIPA 7 Dicembre 2006, n. 51
Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell'elenco dei gestori di Posta Elettronica Certificata.

[8] FAQ-CNIPA/CR/51- Frequent asked questions su [7]

[9] CNIPA/CR/56 - Circolare CNIPA 21 Maggio 2009, n. 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
Abroga e sostituisce la Circolare CNIPA 24 Novembre 2005, n. 49

[10] Provvedimento Garante Privacy del 17 Gennaio 2008

in materia di "Sicurezza dei Dati di Traffico Telefonico e Telematico"

[11] Provvedimento Garante Privacy del 27 Novembre 2008

in materia di "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"

1.1.6. Tabella di corrispondenza

Per permettere un agevole orientamento all'interno del documento, di seguito è inserito un indice di corrispondenza tra quanto richiesto da AgID nella Circolare n. 56 del 21 Maggio 2009 [9] e i paragrafi del presente manuale.

Contenuto della Circolare CNIPA/CR/56 [9]	Inserimento nel Manuale Operativo
I dati identificativi del Gestore	Paragrafo 1.2.1
Nominativo del Responsabile del manuale stesso	Paragrafo1.1.3
Riferimenti normativi necessari per la verifica dei contenuti	Paragrafo 1.1.5
L'indirizzo del sito WEB del gestore ove è pubblicato il manuale ed è scaricabile	Paragrafo 1.2.4
L'indicazione delle procedure nonché degli standard tecnologici e di sicurezza utilizzati dal gestore nell'erogazione del servizio	Paragrafo 1.2.5
Le definizioni relative alle abbreviazioni e ai termini tecnici che figurano nel manuale	Paragrafo 1.1.4.1
Descrizione e modalità del servizio offerto	Capitolo 3

Contenuto della Circolare CNIPA/CR/56 [9]	Inserimento nel Manuale Operativo
La descrizione delle modalità di reperimento e di presentazione dei log dei messaggi	Paragrafi 6.5 e relativi sottoparagrafi
L'indicazione delle modalità di accesso e di fornitura del servizio	Paragrafo 3.4 e capitolo 5
I livelli di servizio e relativi indicatori di qualità di cui all'articolo 12 del Decreto del Ministro per l'innovazione e le tecnologie 2 Novembre 2005	Capitolo 4
L'indicazione delle modalità di protezione dei dati dei Titolari delle caselle, gli obblighi e delle responsabilità che ne discendono e le eventuali limitazioni in caso di indennizzo relativamente ai soggetti previsti all'articolo 2 del Decreto del Presidente della Repubblica n. 68/2005	Capitolo 10; Paragrafi 5.6, 5.7 e relativi sottoparagrafi
Le procedure operative da attuare nel caso di cessazione dell'attività di posta elettronica certificata	Capitolo 9
La versione del manuale	Paragrafi 1.1.2

1.2. Generalità del Gestore

1.2.1 Dati identificativi del Gestore

ITnet S.r.l. è il gestore di Posta Elettronica Certificata ai sensi del DM 2/11/2005 [5], che opera in conformità alle Regole Tecniche e secondo quanto descritto nel testo unico dal CAD [4] e dal DPR 68/2005 [3].

I dati completi del Gestore sono i seguenti:

Denominazione Sociale:
ITnet S.r.l.
Società con socio unico

Indirizzo sede legale:
Via Del Bosco Rinnovato, 8
20090 Assago (MI)

Legale rappresentante:
Eugenio Contatore
Amministratore Delegato

Capitale Sociale
Euro 1.004.00,00 interamente versato

Numero di iscrizione al Registro delle Imprese di Milano:
03458800103

Codice Fiscale:
03458800103

Numero di Partita IVA:
05895251006

R.E.A. di Milano:
MI-1453271

1.2.2 Canali di comunicazione con il Gestore

Itnet S.r.l. ha messo a disposizione ai Titolari ed ai Reseller del servizio di Posta Elettronica Certificata i seguenti canali attraverso cui è possibile effettuare segnalazioni di natura tecnica o amministrativa 24 ore su 24, 365 giorni all'anno:

- **Portale https://selfsolutions.it.net**

  Per aprire una segnalazione il Titolare o il Reseller si deve collegare al portale e, dopo essersi autenticato con username e password, compilare un form indicando la natura del problema.

- **Casella di posta elettronica servizioclienti@it.net**

  A questa casella possono essere fatte pervenire segnalazioni di problemi di tipo amministrativo e/o richieste di informazioni generiche.

- **Casella di posta elettronica certificata servizioclienti@pec.it.net**

  A questa casella possono essere fatte pervenire le richieste di log e le comunicazioni ufficiali (disdetta, modifica dati, ...).

- **Richiesta di Log**

  Eventuali richieste di log devono essere inviate dal Titolare tramite casella di Posta elettronica Certificata o Raccomandata A/R (su carta intestata debitamente firmata e allegando copia di un documento di riconoscimento) come indicato nel paragrafo 6.5.3 del presente manuale.

1.2.3 Accesso al sito WEB del gestore

Il sito **http://www.it.net** è il sito istituzionale di Itnet s.r.l. dove è possibile:

- consultare le informazioni relative al Gestore;
- trovare una sezione dedicata al servizio di Posta Elettronica Certificata;
- scaricare copia elettronica del presente Manuale Operativo.

1.2.4 Accesso al Manuale Operativo

Il presente manuale operativo è accessibile e scaricabile all'indirizzo **http://www.it.net**

1.2.5 Standard di sicurezza, qualità e tecnologici

⇛ ***Standard di qualità e di sicurezza***

ITnet S.r.l. garantisce l'adeguatezza dei propri principali processi operativi e la corretta gestione delle informazioni circolanti in azienda, facendo riferimento agli standard ISO 9001 (per cui è certificata dal 2004) e lo standard ISO 27001 (certificazione ottenuta nel 2007, che ha sostituito la BS 7799 ottenuta nel 2005)

Gli standard, relativi alla qualità, cui l'azienda fa riferimento sono:

UNI EN ISO 9001:2015
Sistemi di gestione per la qualità. Requisiti

UNI EN ISO 9000:2000
Sistemi di gestione per la qualità. Fondamenti e terminologia

UNI EN ISO 19011 :2003
Linee guida per gli audit dei sistemi di gestione per la qualità e/o di gestione ambientale

Gli standard, relativi alla sicurezza delle informazioni, cui l'azienda fa riferimento sono:

UNI ISO/IEC 27000
Fundamentals & Vocabulary

UNI ISO/IEC 27001:2013
ISMS Requirements

UNI ISO/IEC 27002
Code Of Practice for ISM

I certificati sono pubblicati sul sito aziendale **http://www.it.net**. Tutta la documentazione operativa e di sistema è distribuita al personale ITnet S.r.l. e pubblicata sulla intranet aziendale. Nel presente manuale sono esplicitati alcuni processi relativi alla gestione operativa del servizio di Posta Elettronica Certificata e laddove necessario sono fatti espliciti riferimenti alle procedure interne

⇛ ***Standard tecnologici***

In relazione ai processi ed alle applicazioni individuate nell'allegato tecnico del DM 2/11/2005 [5], il servizio di Posta Elettronica Certificata di ITnet S.r.l. è conforme ai seguenti standard tecnologici di riferimento di seguito dettagliati:

Codice	Titolo
RFC 1847	Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted
RFC 1891	SMTP Service Extension 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 Extensions (MIME) Part Five: Conformance Criteria and Examples
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

Codice	Titolo
RFC 2822	Internet Message Format
RFC 2849	The LDAP Data Interchange Format (LDIF) - Technical Specification
RFC 6234	US Secure Hash Algorithm (SHA256)
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

2. GENERALITA' SUL SERVIZIO DI POSTA ELETTRONICA CERTIFICATA

La Posta Elettronica Certificata (PEC) è un'estensione della Posta Elettronica che consente al mittente, qualora corrisponda con una controparte che utilizzi anch'essa un servizio di posta PEC, di avere la documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici.

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

2.1. Funzionamento del Servizio

Il funzionamento dell'applicazione, tra utenti di posta certificata, prevede le seguenti fasi:

- Il mittente invia un messaggio attraverso il servizio di Posta Elettronica Certificata. Il server di posta certificata del mittente (PUNTO DI ACCESSO) esegue una serie di controlli formali sul messaggio pervenuto.

  Prosegue poi:

  - inviando al mittente una **ricevuta di accettazione**, con la quale conferma al mittente che il suo messaggio è stato accettato dal sistema, ad una data e ora specifiche.

    La ricevuta di accettazione è un messaggio di posta elettronica firmato dal gestore del mittente nel quale sono riportati data ed ora di accettazione, l'oggetto ed i dati del mittente e del destinatario.
  - imbustando il messaggio originale in un **messaggio di trasporto** (BUSTA DI TRASPORTO) di tipo "S/MIME". Il messaggio di trasporto firmato dal gestore del mittente, è un messaggio che contiene, come allegato, il messaggio originale e tutti i dati che ne certificano il trasporto. Il messaggio di trasporto viene quindi inviato al dominio destinatario attraverso il PUNTO DI RICEZIONE del dominio destinatario;

  Questo accade sia nel caso che il destinatario ed il mittente appartengano ad uno stesso dominio di Posta Elettronica Certificata, sia che appartengano a domini di Posta Elettronica Certificata differenti.
- Il messaggio è poi ricevuto dal punto di ricezione che effettua i controlli sulla provenienza e la correttezza del messaggio.

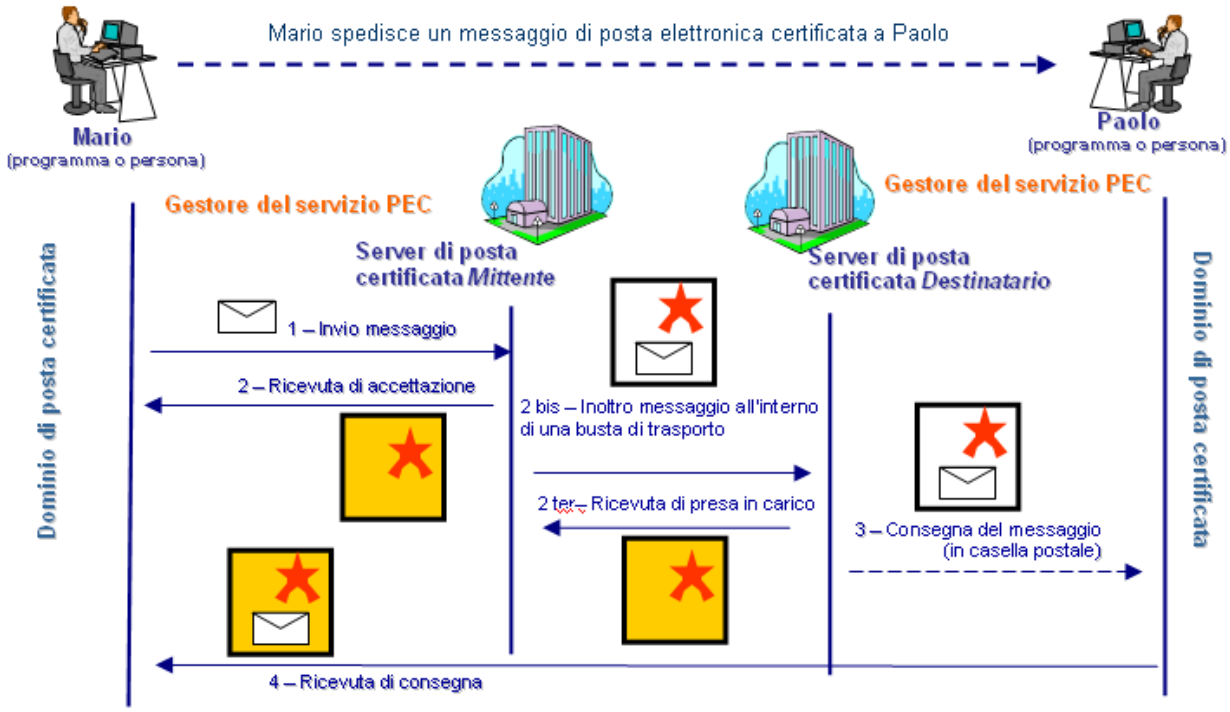
  In particolare viene verificata l'esistenza e la validità della firma del gestore che ha consegnato il messaggio del mittente.

  Se le verifiche sono positive il punto di ricezione emette una ricevuta di presa in carico verso il gestore mittente e provvede ad inoltrare il messaggio ricevuto verso il punto di consegna.

- Quando il messaggio di trasporto è stato consegnato PUNTO DI CONSEGNA, questo emette ed invia al mittente una ricevuta di avvenuta consegna, che conferma al mittente che il suo messaggio è stato effettivamente consegnato al destinatario specificato, certificando la data e l'ora dell'evento.

  L'emissione della ricevuta di avvenuta consegna avviene contestualmente alla disponibilità del messaggio nella casella di posta elettronica del destinatario, indipendentemente dalla lettura da parte del destinatario stesso.

La figura riassume il meccanismo di funzionamento del servizio di Posta Elettronica Certificata.



Nel caso in cui il destinatario di un messaggio di Posta Elettronica Certificata non appartenga ad un dominio PEC il processo di consegna del messaggio si svolge nel modo seguente:

- Il mittente invia un messaggio attraverso il servizio di Posta Elettronica Certificata. Il server di posta certificata del mittente (PUNTO DI ACCESSO) esegue una serie di controlli formali sul messaggio pervenuto.

  Prosegue poi:

  - inviando al mittente una **ricevuta di accettazione**, con la quale conferma al mittente che il suo messaggio è stato accettato dal sistema, ad una data e ora specifiche.

La ricevuta di accettazione è un messaggio di posta elettronica firmato dal gestore del mittente nel quale sono riportati data ed ora di accettazione, l'oggetto ed i dati del mittente e del destinatario. Nella ricevuta di accettazione è riportata la tipologia non PEC dei destinatari in modo da informare il mittente del differente flusso seguito dal messaggio.

- imbustando il messaggio originale in un **messaggio di trasporto** (BUSTA DI TRASPORTO) di tipo "S/MIME". Il messaggio di trasporto firmato dal gestore del mittente, è un messaggio che contiene, come allegato, il messaggio originale e tutti i dati che ne certificano il trasporto. Il messaggio di trasporto viene quindi inviato al dominio destinatario attraverso il gestore di posta del dominio destinatario;

Verso il mittente non viene generata alcuna ricevuta di avvenuta consegna.

2.2. Funzionamento del Servizio in caso di problemi di consegna

La situazione descritta nel paragrafo precedente costituisce la normalità dei casi. Possono verificarsi situazioni nelle quali il messaggio di Posta Elettronica Certificata non risulta consegnabile. In questi casi il flusso è quello descritto di seguito.

2.2.1. Descrizione del funzionamento in caso di messaggi non consegnabili

Il funzionamento del sistema prevede 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, allora il gestore del mittente stesso comunica al mittente che il gestore del destinatario potrebbe non essere in grado di realizzare la consegna del messaggio.
- se entro ulteriori 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.

2.2.2. Descrizione del funzionamento in presenza di virus

Il funzionamento del sistema di Posta Elettronica Certificata prevede delle attività a carico dei gestori nel caso in cui siano rilevati dei virus come descritto di seguito.

- 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 dall' art. 12, comma 1 del DPR 68/2005 [3].

- 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 dall' art. 12, comma 2 del DPR 68/2005 [3].

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

2.3. Caratteristiche delle ricevute e delle buste di trasporto

2.3.1. Firma elettronica delle ricevute e delle buste di trasporto

Le ricevute e le buste di trasporto rilasciate dal Gestore 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.

2.3.2. Riferimento temporale

Su tutti gli eventi che costituiscono la transazione di elaborazione dei messaggi (generazione di ricevute, buste di trasporto, ecc.) il Gestore appone un riferimento temporale in conformità con l'art. 10 del DPR 68/05 [3]

2.3.3. Tipologia delle Ricevute di Avvenuta Consegna

Coerentemente con quanto indicato dalle Regole Tecniche, 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 breve può essere richiesta dal mittente utilizzando appositi client di posta capaci di formare il messaggio di Posta Elettronica Certificata come specificato dall'allegato tecnico al DM 2 novembre 2005.

- 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. Anche questo tipo di ricevuta può essere richiesta dal mittente utilizzando un client di posta capace di formare il messaggio di Posta Elettronica Certificata come specificato dall'allegato tecnico al DM 2 novembre 2005.

3. IL SERVIZIO DI POSTA ELETTRONICA CERTIFICATA DI ITNET S.R.L.

In questo capitolo è descritta in maniera completa l'offerta di Posta Elettronica Certificata di ITnet S.r.l. destinata alle persone fisiche, alle Aziende e agli enti della Pubblica Amministrazione.

3.1. Tipologia del servizio offerto

ITnet S.r.l. offre il servizio di Posta Elettronica Certificata secondo i profili di seguito indicati:

- Profilo Base
- Profilo Plus
- Profilo Multidominio

3.1.1. "Profilo Base"

È l'offerta per i Clienti che desiderano utilizzare il servizio con il dominio predefinito *mailcert.it*.

Il Cliente può richiedere una o più caselle di Posta Elettronica Certificata del tipo risulta **nome_utente@mailcert.it**.

Il valore <nome_utente> verrà proposto dal richiedente. ITnet S.r.l. si riserva il diritto di rifiutare tale richiesta. Alcune cause di tale rifiuto del <nome_utente> possono essere, a titolo esemplificativo ma non esaustivo, casi di omonimia, nomi troppo lunghi, nomi simili a marchi noti o afferenti ad Enti ed Istituzioni pubbliche, ecc.

In ottemperanza alla comunicazione AgID del 17.12.2013 con oggetto *"**Prescrizione sulla riassegnazione delle caselle di posta elettronica certificata**"* in *cui "è posto, con decorrenza immediata, il divieto al Gestore di posta elettronica certificata, 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 utilizzato in precedenza.

Ciascuna casella di Posta Elettronica Certificata ha una dimensione standard minima di 50 MB.

Il dominio di Posta Elettronica Certificata mailcert.it è un dominio "aperto" che permette al Cliente di ricevere sia posta elettronica certificata che posta elettronica ordinaria.

Ogni Cliente ha la possibilità' di decidere se gestire la posta elettronica ordinaria in ingresso direttamente sul proprio account PEC oppure di ridirigere tale tipo di posta elettronica su un account di posta elettronica ordinaria non appartenente al dominio *mailcert.it*.

Per fare ciò il Cliente ha a disposizione una apposita sezione nella maschera "Opzioni" in cui può abilitare l'inoltro della posta ordinaria ad un indirizzo di posta elettronica "esterno". A seguito di questa configurazione i messaggi di posta elettronica ordinaria eventualmente ricevuti sulla casella PEC saranno reindirizzati alla casella indicata e poi eliminati dalla casella PEC. Tali messaggi potranno essere consultati solo nella casella "esterna" di destinazione.

3.1.2. "Profilo Plus"

L'offerta prevede:

- Un dominio personalizzato scelto dal Cliente tra le tipologie di seguito elencate:
  - nuovo dominio di 2° livello. In questo caso la registrazione del dominio verrà effettuata da ITnet S.r.l. per conto del Cliente stesso una volta ricevuta la documentazione correttamente compilata;
  - dominio di 3° livello a fronte di un dominio già registrato. In questo caso non è necessaria alcuna registrazione;
  - dominio di 3° livello del tipo nome_Cliente.mailcert.it dove <nome_Cliente> è scelto dal Cliente. In questo caso ITnet S.r.l. si riserva la facoltà di rifiutare tale scelta. Cause di rifiuto del <nome_cliente> possono essere, a titolo esemplificativo ma non esaustivo, casi di omonimia, nomi troppo lunghi, nomi simili a marchi noti o afferenti ad Enti ed Istituzioni pubbliche, ecc.
- La scelta del numero di caselle;
- La scelta dello spazio disco totale da associare successivamente a ciascuna casella in base alle esigenze;
- L'amministrazione delle caselle delegata al Cliente tramite interfaccia WEB

  Nel compiere questa attività il Cliente si impegna ad agire in conformità a quanto indicato nella comunicazione AgID del 17.12.2013 con oggetto "***Prescrizione sulla riassegnazione delle caselle di posta elettronica certificata***" in cui "*è posto, con decorrenza immediata, il divieto al Gestore di posta elettronica certificata, con riferimento agli indirizzi PEC dallo stesso gestiti, di riassegnare il medesimo indirizzo di posta elettronica certificata a soggetto diverso dal titolare originario"*.
- Il dominio è creato come "aperto", in grado cioè di ricevere sia posta elettronica certificata che posta elettronica ordinaria. Il Cliente ha la facoltà di modificare questo tipo di configurazione attraverso un apposito "check box" nel pannello di amministrazione del dominio stesso. In questo caso, il proprietario di ogni casella ha la possibilità' di decidere se gestire la posta elettronica ordinaria in ingresso direttamente sul proprio account PEC oppure di ridirigere tale tipo di

posta elettronica su un account di posta elettronica ordinaria non appartenente al dominio stesso;

- L'accesso al servizio tramite interfaccia WEB da parte dell'utente (WEB mail);
- La fruizione della funzionalità di notifica SMS. Il servizio prevede la possibilità di ricevere notifiche tramite SMS a fronte di eventi come l'arrivo di nuova posta, il superamento della soglia di attenzione della casella, la scadenza di attività, ecc. La notifica tramite SMS deve essere abilitata dall'amministratore del servizio sul singolo Utente utilizzando la propria interfaccia WEB. L'Utente abilitato, utilizzando l'interfaccia WEB, dovrà inserire il proprio numero di cellulare e selezionare gli eventi che vuole gli siano notificati via SMS;
- L'amministratore del servizio riceverà settimanalmente un report dettagliato dell'invio degli SMS per singolo Utente abilitato;
- L'invio degli SMS di notifica sarà fatturato utilizzando il listino disponibile con la documentazione contrattuale.

3.1.3. "Profilo Multidominio"

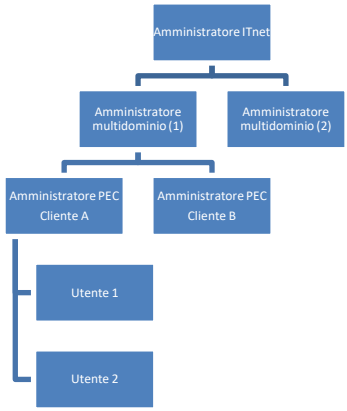
Con il "profilo Multidominio" si permette al Cliente di ITnet S.r.l. di offrire il servizio PEC ai propri Clienti finali consentendo l'amministrazione delegata dei domini di Posta Elettronica Certificata.

Come raffigurato di seguito, la gerarchia di amministrazione del servizio prevede i seguenti profili:

- ***Amministratore ITnet S.r.l.*** - Gestisce la piattaforma e configura il servizio "Multidomino" di Posta Elettronica Certificata al proprio Cliente;
- ***Amministratore del servizio Profilo Multidominio*** - Configura il servizio ai propri clienti finali, in particolare, associa ad ogni suo Cliente un dominio di Posta Elettronica Certificata e per ciascun dominio associa il numero di caselle, lo spazio disco ed eventuali funzionalità aggiuntive (ed es. se il dominio è "chiuso" o " aperto" rispetto alla posta elettronica ordinaria).
- ***Amministratore di dominio*** – Può creare/modificare/cancellare gli utenti relativi al proprio dominio associando a ciascuno le funzionalità disponibili.

  Nel compiere questa attività l'Amministratore di Dominio si impegna ad agire in conformità a quanto indicato nella comunicazione AgID del 17.12.2013 con oggetto "***Prescrizione sulla riassegnazione delle caselle di posta elettronica certificata***" in cui "*è posto, con decorrenza immediata, il divieto al Gestore di posta elettronica certificata, con riferimento agli indirizzi PEC dallo stesso gestiti, di riassegnare il medesimo indirizzo di posta elettronica certificata a soggetto diverso dal titolare originario"*.

- ***Utente*** – Utente del servizio di Posta Elettronica Certificata.



Con il "Profilo Multidominio" potranno essere utilizzati nomi a dominio appartenenti ad una delle tre tipologie elencate di seguito:

- nuovo dominio di 2° livello. In questo caso la registrazione del dominio verrà effettuata da ITnet S.r.l. per conto del Cliente stesso una volta ricevuta la documentazione correttamente compilata;
- dominio di 3° livello a fronte di un dominio già registrato. In questo caso non è necessaria alcuna registrazione;
- dominio di 3° livello del tipo nome_Cliente.mailcert.it dove <nome_Cliente> è scelto dal Cliente. In questo caso ITnet S.r.l. si riserva la facoltà di rifiutare tale scelta. Cause di rifiuto del <nome_cliente> possono essere, a titolo esemplificativo ma non esaustivo, casi di omonimia, nomi troppo lunghi, nomi simili a marchi noti o afferenti ad Enti ed Istituzioni pubbliche, ecc.

3.1.4. Gestione dei domini di Posta Elettronica Certificata

- Il dominio di Posta Elettronica Certificata scelto dal Cliente potrà contenere solamente caselle di Posta Elettronica Certificata.
- Tutti i messaggi in uscita dalle caselle di posta configurate nel dominio certificato del Cliente sono trattati come scambi di messaggi di posta certificata. Per ogni messaggio inviato a utenti di Posta Elettronica Certificata, il mittente riceverà una ricevuta di accettazione ed una ricevuta di consegna per ciascuno dei destinatari ai quali il messaggio è stato inviato.

  In caso di problemi di consegna o anomalie nell'utilizzo del servizio il mittente riceverà i corrispondenti avvisi.
- Nel caso in cui la gestione del dominio/sottodomino sia a carico del Cliente allora si richiede al Cliente stesso che il gestore del suo dominio configuri opportunamente i server DNS al fine di assicurare la visibilità in rete dei server coinvolti nel processo di gestione della Posta Elettronica Certificata. La responsabilità della corretta configurazione

del DNS è esclusiva competenza del Cliente come previsto nella specifica clausola contrattuale. I servizi relativi al dominio di Posta Elettronica Certificata verranno forniti dalla piattaforma di ITnet S.r.l..

- ITnet S.r.l. si occuperà sempre dell'inserimento dei domini nell'indice dei gestori di Posta Elettronica Certificata che contiene la lista di tutti i domini di Posta Elettronica Certificata gestiti da ciascun operatore.
- ITnet S.r.l. si riserva di non procedere alla registrazione di nomi dominio che non siano considerati conformi alla policy aziendale e che risultino violare i diritti di terzi in tema di proprietà industriale e intellettuale.

3.2. Servizi opzionali

Di seguito sono elencati in dettaglio i servizi opzionali messi a disposizione da ITnet S.r.l. per il servizio di Posta Elettronica Certificata.

3.2.1. Rubrica, Lista attività e Calendario

Le funzionalità di Rubrica, Lista attività e Calendario, rendono disponibile all'Utente una rubrica di destinatari, una lista di attività e un Calendario per gestire e pianificare gli invii di documenti tramite Posta Elettronica Certificata.

3.3. Personalizzazioni

L'offerta di ITnet S.r.l. relativa al profilo Plus e al profilo Multidominio prevede la possibilità di personalizzare alcuni elementi grafici nell'interfaccia WEB di accesso al servizio.

ITnet S.r.l. si riserva la facoltà di rifiutare l'inserimento di elementi grafici che possano impedire la corretta fruizione del servizio o di materiale che possa offendere o configurarsi come violazione di legge.

ITnet S.r.l. non assume, salvo caso di dolo o colpa grave, responsabilità in merito al controllo sugli elementi forniti dal Cliente e sulla legittimazione al loro uso da parte del Cliente stesso.

3.4. Accesso al servizio

Il servizio di Posta Elettronica Certificata è accessibile sia tramite interfaccia WEB sia tramite client di posta elettronica.

3.4.1. Interfaccia WEB

L'interfaccia WEB (HTTPS) è disponibile all'indirizzo https://pec.it.net (o altro indirizzo segnalato sul sito http://www.it.net) e prevede le seguenti principali funzionalità in base al profilo dell'Utente:

- Profilo "Amministratore del servizio del Cliente" (disponibile solo per l'offerta Plus e Multidominio):
  - gestione degli utenti (creazione/modifica/cancellazione);

- associazione a ciascuna casella dello spazio;
- impostazione del dominio come “aperto” o “chiuso” alla posta elettronica ordinaria;
- reset della password;
- reset della password ad un valore impostato nel caso in cui un Utente abbia dimenticato la propria;
- associare servizi opzionali agli utenti del dominio (notifica SMS e servizi di Rubrica, Calendario e Lista attività).

- Profilo “Utente” del servizio:
  - Gestione dei messaggi in arrivo;
  - Composizione di un nuovo messaggio;
  - Selezione della tipologia di ricevuta di avvenuta consegna (completa, breve, sintetica). Il tipo di ricevuta previsto di default dal sistema è “completa”;
  - Organizzazione dei messaggi in cartelle;
  - Ricerca dei messaggi;
  - Nel caso di dominio “aperto” (in grado di ricevere messaggi di posta elettronica ordinaria oltre che quelli di tipo certificato) definire una casella a cui effettuare il reindirizzamento dei messaggi di posta elettronica ordinaria;
  - Cambio della password;
  - Configurazione delle notifiche SMS (se abilitate dall’amministratore);
  - Accesso alle funzionalità di Rubrica, Calendario e Lista attività (se abilitate dall’amministratore).

3.4.2. Client di posta elettronica

L’accesso al servizio è possibile mediante l’utilizzo di un qualsiasi client di posta elettronica che preveda l’uso dei seguenti protocolli: SMTP/S per l’invio e POP3/S e IMAP/S per la ricezione. In questo caso le funzionalità disponibili sono quelle tipiche dello specifico client utilizzato.

Per poter utilizzare il servizio è necessario configurare il client con i parametri relativi a:

- Server di posta in arrivo (POP3/S o IMAP/S) e della relativa porta;
- Server di posta in uscita (SMTP/S) e della relativa porta.

Queste informazioni sono fornite al Cliente attraverso la *lettera di benvenuto (Welcome Letter)* del servizio.

La selezione della tipologia per la ricevuta di avvenuta consegna si ottiene facendo in modo che il client di posta inserisca nell’header della busta di consegna una delle righe seguenti:

- X-TipoRicevuta: breve
  se si vuole una ricevuta “breve”;
- X-TipoRicevuta: sintetica
  se si vuole una ricevuta “sintetica”.

Il tipo di ricevuta previsto di default dal sistema è “completa”.

3.4.3. Credenziali di accesso e parametri configurazione del servizio

Le credenziali di accesso al servizio sono inviate al Cliente all’interno della *lettera di benvenuto (Welcome Letter)* del servizio, all’indirizzo di posta elettronica o al numero di fax segnalato all’interno della documentazione contrattuale.

Nel caso il Cliente abbia richiesto:

- il profilo BASE riceverà le credenziali per gli utenti richiesti su dominio *mailcert.it*;
- il profilo Plus oppure Multidominio riceverà le credenziali di accesso dell’Utente Amministratore.

La password allegata alle credenziali di accesso del cliente, può essere modificata in qualunque momento dopo il primo accesso.

3.4.4. Raccomandazioni per l’utenza

Al fine di un corretto e sicuro utilizzo del servizio ITnet S.r.l. raccomanda di:

- procedere al cambiamento della password la prima volta che si accede al servizio utilizzando la funzionalità di modifica della password dall’interfaccia WEB e comunque di provvedere al cambiamento della password con cadenza periodica;
- consultare frequentemente la casella perché ogni messaggio ricevuto si intende pervenuto al titolare della casella stessa (DPR n. 68/2005 [3]);
- archiviare periodicamente i messaggi sul proprio computer e successivamente cancellarli dal server di posta per evitare che venga occupato tutto lo spazio disponibile e quindi i messaggi successivi vengano rifiutati;
- portare a conoscenza dei propri utilizzatori che si è in possesso di una casella di posta a valore legale da utilizzare esclusivamente per gli usi consentiti dalla legge e non come casella di posta elettronica ordinaria;
- dotare le stazioni di lavoro di un antivirus costantemente aggiornato per garantire maggiore sicurezza per quanto viene spedito e ricevuto. Anche se il servizio di Posta Elettronica Certificata di ITnet S.r.l. è dotato di antivirus, non è sempre possibile controllare tutti i contenuti potenzialmente dannosi (a titolo di esempio si evidenzia che contenuti messaggi e/o contenuti crittografati non possono essere sottoposti a controlli efficaci).

4. LIVELLI DI SERVIZIO E INDICATORI DI QUALITA'

Di seguito vengono riportati i livelli di servizio e gli indicatori di qualità del servizio di Posta Elettronica Certificata di ITnet S.r.l.:

Numero Destinatari

Numero massimo di destinatari per i messaggi originati da caselle di Posta Elettronica Certificata ITnet S.r.l.	**50**

Dimensione dei messaggi

La dimensione di ogni singolo messaggio che può essere accettata dal Servizio di Posta Elettronica Certificata di ITnet S.r.l. per cui è **garantita** la trasmissione (intesa come prodotto del numero dei destinatari e delle dimensioni del messaggio stesso)	**100 MB**

Disponibilità

Il periodo temporale di riferimento per il calcolo della disponibilità/Indisponibilità del servizio	**4 MESI (un QUADRIMESTRE)**
La disponibilità del servizio nel periodo di riferimento sopra indicato	**99,8%**
L'indisponibilità del servizio per il singolo fermo nel periodo sopra indicato	**≤ 50% del totale previsto per l'intervallo di tempo di riferimento**

Tempi

Tempo di consegna delle ricevute di accettazione nel periodo di disponibilità del servizio	**30 min.**

5. CONDIZIONI DI FORNITURA

5.1. Canali di vendita, proposta e documentazione del servizio

Il servizio di Posta Elettronica Certificata è commercializzato da ITnet S.r.l.:

- direttamente
- tramite partner commerciali autorizzati da ITnet S.r.l.
- tramite rivenditore

Il servizio è disciplinato e fornito in conformità con la vigente normativa e con quanto previsto dalla documentazione, di seguito elencata, che sarà fornita al Cliente:

- condizioni generali di contratto;
- proposta di contratto contenente gli elementi del servizio, i valori economici e la richiesta di attivazione del servizio;
- il presente Manuale Operativo;
- informativa sulla privacy.

5.1.1. Attivazione diretta del servizio

Il personale del Customer Service di ITnet raccoglie le informazioni relative al servizio (numero caselle, spazio totale, eventuali servizi opzionali, ecc.); procede all'identificazione del richiedente, alla definizione dell'accordo e alla firma del contratto verificandone la correttezza e la completezza.

Viene utilizzata la documentazione contrattuale predisposta da ITnet S.r.l. che contiene le condizioni del servizio che il Cliente richiede al Gestore.

Alla ricezione della documentazione richiesta, viene avviata la lavorazione del contratto.

5.1.2. Attivazione del servizio tramite Partner commerciale

Il Partner commerciale raccoglie le informazioni relative al servizio (numero caselle, spazio totale, eventuali servizi opzionali, ecc.); procede all'identificazione del richiedente, alla definizione dell'accordo e alla firma del contratto verificandone la correttezza e la completezza.

Tutta la documentazione contrattuale è predisposta da ITnet S.r.l. e contiene le condizioni del servizio che il Cliente richiede al Gestore.

Terminate queste attività, il Partner commerciale avvia la lavorazione del contratto inviandolo alle funzioni ITnet S.r.l. di competenza.

ITnet S.r.l. è integralmente responsabile della qualità del servizio nei confronti del Cliente finale.

5.1.3. Attivazione del servizio tramite rivenditore (offerta Multidominio)

ITnet S.r.l. può veicolare i propri servizi attraverso accordi di rivendita nel rispetto della normativa vigente e del presente Manuale Operativo.

Il rivenditore, come specificato negli accordi sottoscritti con ITnet S.r.l., è tenuto:

- a raccogliere le informazioni relative al servizio (numero caselle, spazio totale, eventuali servizi opzionali, ecc.);
- a procedere all'identificazione del richiedente (conservando le fotocopie del documento di riconoscimento), alla definizione dell'accordo e alla firma del contratto;
- a conservare la documentazione contrattuale originale firmata dal suo Cliente;
- ad indicare nelle Condizioni Generali di Fornitura con il proprio Cliente che
  - il Gestore del servizio di Posta Elettronica Certificata è ITnet S.r.l.;
  - ITnet S.r.l. è integralmente responsabile del servizio di Posta Elettronica Certificata;
  - eventuali richieste di Log devono essere inviate dal Titolare della casella ai riferimenti indicati a questo scopo al paragrafo 6.5.3 del presente manuale;
- gestire completamente l'help desk amministrativo dei propri Clienti
- gestire l'help desk tecnico di primo livello ossia:
  - accogliere le segnalazioni;
  - analizzare i problemi segnalati;
  - risolvere autonomamente le problematiche di tipo generale quali configurazioni, informazioni sul funzionamento del servizio PEC, ecc, ...;
  - scalare verso ITnet (riferimenti al paragrafo 1.2.2) le segnalazioni che necessitano di interventi tecnici;
- a fornire al suo Cliente copia del presente Manuale Operativo;
- ad inviare al suo Cliente (Titolare del Servizio) una lettera di benvenuto (Welcome Letter) contenente i dati necessari per l'accesso al servizio stesso (username, password, ...)
- a comunicare ad ITnet S.r.l. i dati necessari alla registrazione del Titolare. In particolare devono essere forniti:
  - Nome Cognome / Ragione Sociale;
  - Codice Cliente;
  - Codice Contratto;
  - Dominio di Posta Elettronica Certificata;
  - Data attivazione;
  - Data disattivazione;

- Copia del documento di identità;
- Copia della documentazione contrattuale (contratto e informativa privacy firmate, ...).

ITnet S.r.l. rimane integralmente responsabile del servizio nei confronti del Titolare.

5.1.4. Modalità alternative per l'attivazione del servizio

ITnet S.r.l. si riserva la facoltà di fornire nuove modalità e flussi per la richiesta di nuove attivazioni (ad esempio introducendo la modalità on-line via WEB). Le modalità oggi disponibili e quelle future garantiscono e garantiranno il rispetto delle norme relative alla privacy e alla normativa vigente relativa al servizio di Posta Elettronica Certificata.

5.2. Attivazione del Servizio

I tempi di attivazione del Servizio sono di cinque (5) giorni lavorativi da intendersi dalla data di ricezione di tutta la documentazione necessaria compresa quella eventuale per la registrazione di un nuovo dominio.

L'attivazione del servizio viene comunicata al Cliente inviando una lettera di benvenuto (Welcome Letter) all'indirizzo di posta indicato nella documentazione contrattuale contenente:

- La login e la password di accesso al servizio per l'Utente amministratore (nel caso di profilo Plus o Multidominio);
- La login e la password di accesso alla casella su dominio mailcert.it (nel caso di profilo Base);
- La URL di acceso al servizio tramite interfaccia WEB (WEB mail);
- I parametri di configurazione del client di posta elettronica;
- I riferimenti del sito WEB;
- Indicazioni dei riferimenti per accedere ai servizi di Customer Care di ITnet S.r.l. (caselle di posta elettronica per richiedere assistenza tecnica e amministrativa, le credenziali di accesso e l'indirizzo del portale per l'inoltro delle segnalazioni).

5.2.1. Gestione della registrazione del Titolare

ITnet S.r.l., come previsto dalla normativa, mantiene un registro dei Titolari.

5.3. Disdetta del contratto

Il Titolare, opportunamente identificato, può richiedere la risoluzione del contratto per il servizio di Posta Elettronica Certificata inviando una raccomanda all'indirizzo indicato nelle Condizioni Generali di contratto sottoscritte.

Il Gestore comunica al Titolare l'avvenuta disdetta/disattivazione.

La disdetta sarà operativa entro cinque (5) giorni lavorativi a partire dalla data di risoluzione richiesta dal Titolare.

Le richieste di disdetta/disattivazione sono conservate da ITnet S.r.l. per tre (3) anni.

5.4. Corrispettivo economico

Il servizio di Posta Elettronica Certificata di ITnet S.r.l. prevede un canone annuale dipendente dal numero dei domini/caselle di Posta Elettronica Certificata, dallo spazio totale richiesto e dalle funzionalità opzionali acquistate.

5.5. Descrizione generali degli elementi del contratto

- **Sospensione del servizio** – ITnet S.r.l. potrà sospendere temporaneamente il servizio per procedere alla manutenzione ordinaria e straordinaria degli impianti e delle apparecchiature necessarie all'erogazione del servizio dandone comunicazione al Cliente tramite e-mail con un preavviso di almeno 24 ore.

  ITnet S.r.l. potrà sospendere in ogni momento il Servizio, in tutto o in parte, anche senza preavviso, in caso di guasti alla rete e agli apparati di fornitura del Servizio, dipendenti da caso fortuito o forza maggiore, nonché nel caso di modifiche e/o manutenzioni straordinarie non programmabili e tecnicamente indispensabili.

  Costituiscono casi di forza maggiore gli eventi al di fuori del ragionevole controllo di ITnet S.r.l., quali, a titolo esemplificativo ma non esaustivo, attività e/o decisioni governative e/o della Pubblica Amministrazione, atti dell'Autorità Militare, limitazioni legali, catastrofi naturali, fulmini, incendi, esplosioni, sommosse, guerre, epidemie, e, purché siano su base nazionale, scioperi, mancanza di materie prime, energia, trasporti, ecc.

  ITnet S.r.l. potrà sospendere il Servizio anche in caso di violazione da parte del Titolare degli obblighi posti a suo carico in conformità a quanto previsto dal Manuale Operativo o dallo specifico accordo contrattuale, dandone comunicazione al Titolare tramite e-mail e fatta salva ogni eventuale azione di rivalsa nei riguardi del responsabile delle violazioni.

- **Risoluzione del contratto** – ITnet S.r.l. potrà procedere alla risoluzione del contratto:
  - nel caso in cui il servizio sia utilizzato per finalità contrarie a leggi, regolamenti, disposizioni e normative;
  - in caso di mancato pagamento entro giorni trenta (30) giorni dalla data di scadenza del pagamento indicato in fattura.

La comunicazione della risoluzione sarà comunicata al Cliente a mezzo di raccomandata a/r.

Rimane l'obbligo da parte del Cliente al pagamento dei corrispettivi non pagati.

5.6. Obblighi e responsabilità

5.6.1. Obblighi del gestore – ITnet S.r.l.

ITnet S.r.l. fornirà il Servizio conformemente a quanto stabilito dalla normativa vigente in materia, con le modalità indicate nel presente documento.

In particolare, ITnet S.r.l. assume i seguenti obblighi:

- garantire la fornitura del servizio di Posta Elettronica Certificata in conformità con le normative vigenti;
- assicurare l'erogazione del Servizio secondo i livelli minimi di servizio previsti dalla normativa vigente e dal presente Manuale;
- assicurare l'interoperabilità del Servizio con gli altri operatori iscritti nell'elenco pubblico dei gestori di PEC;
- rendere disponibili nei casi previsti dalla legge i log inerenti le trasmissioni tra caselle di Posta Elettronica Certificata.

ITnet S.r.l. si riserva il diritto di modificare le specifiche tecniche di erogazione del Servizio in base all'evoluzione tecnologica e/o normativa, aggiornando il presente manuale operativo così come specificato al paragrafo 1.1.2 del presente documento.

5.6.2. Obblighi del Titolare del servizio

Il Titolare assume i seguenti obblighi:

- fornire tutte le informazioni e la documentazione richiesta da ITnet S.r.l., necessarie ad una corretta identificazione garantendone, sotto la propria responsabilità, l'attendibilità ai sensi del DPR n. 68/2005 [3] e successive modifiche ed integrazioni;
- prestare il consenso al trattamento dei dati personali ai sensi del D.Lgs. n. 196 del 2003 [2] (ove richiesto);
- informare immediatamente ITnet S.r.l. in caso risulti compromessa la riservatezza dei codici di accesso per l'utilizzo del Servizio.

Il Titolare assume inoltre i seguenti obblighi e si impegna ad estenderli agli Utenti del servizio:

- consultare in maniera preventiva il Manuale Operativo per conoscerne i contenuti;
- conservare con la massima riservatezza e diligenza i codici di accesso al Servizio;
- non utilizzare 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;

Il Titolare prende atto che alla scadenza del contratto o in caso di sua risoluzione, non sarà più possibile accedere al Servizio e al suo contenuto, pertanto si impegna a darne informativa agli Utenti, sollevando ITnet S.r.l. da ogni responsabilità derivante dal mancato accesso.

5.6.3. Responsabilità del Titolare

Il Titolare manleva ITnet S.r.l. da ogni responsabilità, spesa, danno o pregiudizio, diretto od indiretto, di cui ITnet S.r.l. fosse chiamato a rispondere nei confronti di terzi per fatto

- riconducibile alla erronea o parziale indicazione dei dati forniti dal Titolare;
- imputabile al Titolare o all'Utente in relazione all'uso del Servizio

5.6.4. Cessione del servizio

Il Titolare non potrà cedere a terzi in tutto o in parte il Servizio regolato dalle presenti condizioni, senza la preventiva autorizzazione scritta di ITnet S.r.l.

5.7. Esclusioni e limitazione in sede di indennizzo

ITnet S.r.l. non sarà in alcun modo responsabile per danni di natura diretta od indiretta derivante da:

- atti della Pubblica Autorità, caso fortuito, forza maggiore ovvero da altra causa non imputabile a ITnet S.r.l. 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 di ITnet S.r.l., interruzioni nella fornitura di energia elettrica, terremoti, esplosioni, incendi), esclusi i casi di dolo o colpa grave;
- erroneo utilizzo di codici identificativi da parte dell'Utente;
- mancato invio o mancata consegna dei messaggi al di fuori dei livelli minimi di servizio previsti dalla normativa vigente, causati da anomalie segnalate al mittente o al destinatario, i quali non abbiano provveduto a riscontrare la comunicazione di anomalia inviata da ITnet S.r.l.;
- 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 tenuto da AgID.

Si evidenzia inoltre che ITnet S.r.l.

- non assume alcuna responsabilità, salvo eventuale dolo o colpa grave, dei ritardi che i messaggi di posta elettronica possono subire nella loro trasmissione via Internet;

- è esonerata da ogni potere di controllo, di mediazione o di vigilanza sul contenuto dei messaggi inviati dagli Utenti e non assume nessuna responsabilità riguardo al loro contenuto illecito o contrario alla morale o all'ordine pubblico, non sussistendo alcun obbligo di vigilanza o di cancellazione in capo al ITnet S.r.l. in riferimento al contenuto dei messaggi.
- non assume nessun obbligo, garanzia o responsabilità ulteriori rispetto a quelle scaturenti dal contratto di fornitura del Servizio per il tramite di ITnet S.r.l. e dalla normativa vigente.

ITnet S.r.l., nell'ambito della sua attività di Gestore di Posta Elettronica Certificata è dotato di polizza assicurativa a copertura dei rischi dell'attività e dei danni causati a terzi (DPR 68/05 [3]) con le seguenti caratteristiche:

Tipologia di risarcimento	Massimale annuo	Massimale per singolo sinistro
Perdite patrimoniali derivanti dall'attività di gestore di Posta Elettronica Certificata ai sensi del D.P.R. 11 Febbraio 2005, n°68	1.500.000 €	1.500.000 €
Perdite patrimoniali derivanti dalla diffusione involontaria o per infedeltà dei dipendenti, di dati personali	500.000 €	500.000 €

6. SISTEMI TECNOLOGICI

6.1. Infrastrutture

La piattaforma tecnologica utilizzata per erogare il Servizio di Posta Elettronica Certificata è installata presso il Data Center di Milano v.le Ortles e si basa su un'architettura progettata per garantire la massima disponibilità del servizio agli utenti.

Il core della piattaforma è rappresentato da un pool di server gestito dal sistema di virtualizzazione VMware rel. 5.5 che, attraverso le sue funzionalità, permette di raggiungere il livello di affidabilità richiesto dalla attuale normativa sul servizio di Posta Elettronica Certificata.

L'architettura logica del sistema, come descritto nella figura seguente, è così composta:

- Il modulo Firewall: composto di una coppia di sistemi in mutuo failover garantisce il primo livello di protezione permettendo l'accesso ai soli protocolli utilizzati per l'erogazione del servizio;
- Il modulo Bilanciatore: che permette di ridirigere il traffico diretto verso un dato servizio su più di un server del modulo di Front End e del modulo WEB garantendo una corretta distribuzione del carico;
- Il modulo Front-End: composto da più server, fornisce il punto di accesso agli Utenti attraverso vari protocolli (SMTP/S, POP3/S e IMAP/S) e si occupa dello scambio di corrispondenza con gli altri Gestori;
- Il modulo WEB: implementato da più server, permette di accedere al servizio tramite interfaccia WEB (HTTPS) da cui si possono eseguire tutte le attività indicate al paragrafo 3.4.1
- Il modulo Antivirus: fornisce il servizio di controllo e "pulizia" di eventuali virus informatici. Per garantire ridondanza e performance adeguate il modulo è composto di un sistema di Bilanciamento e di tre server con funzione di Antivirus;
- Il modulo Back-End: composto di più server fornisce i servizi di LDAP, di Message Store (Contenitore delle caselle di Posta). Ogni server di Back-End è interconnesso al modulo SAN attraverso una doppia connessione in fibra ottica;
- Il modulo DataBase: mantiene le informazioni che si riferiscono alle transazioni di Posta Elettronica Certificata. Su questo modulo sono implementate le procedure per l'estrazione dei file di log e per la loro marcatura temporale;
- Il modulo HSM (Hardware Security Module): composto da una batteria di appliance dedicate che ospitano i processori crittografici intelligenti utilizzate per
  - la memorizzazione delle chiavi private di firma;

- il processo di firma digitale delle Buste.

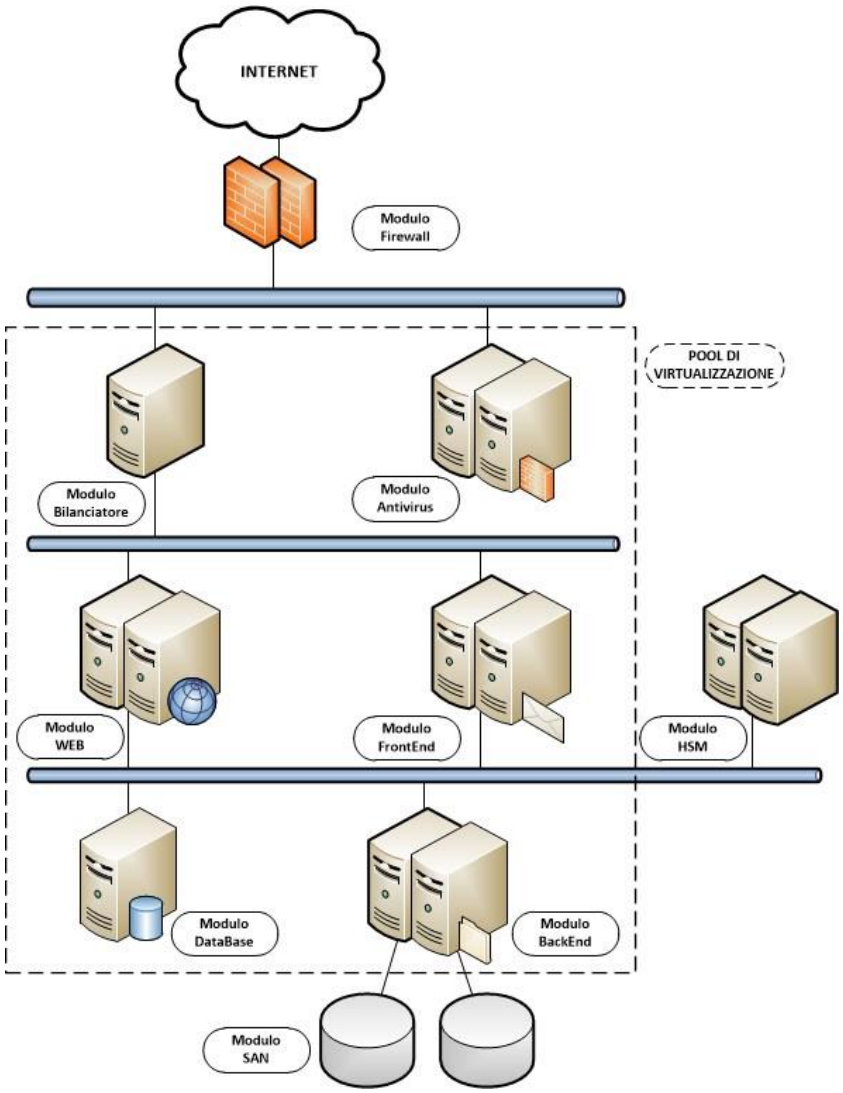
- Il modulo SAN (Storage Area Network): è il sistema su cui sono contenuti i dati acceduti da tutti i moduli che implementano il servizio di Posta Elettronica Certificata. E' implementato da uno storage in configurazione HA (completamente ridondato in tutte le sue parti critiche: processore, controller, alimentazione, interfacce in F.O., ...) con dischi in configurazione Raid5. La connessione tra i server e lo storage è realizzata attraverso una connessione fiber channel dual path.

Attraverso l'utilizzo di una soluzione di virtualizzazione ITnet S.r.l. è in grado di garantire le seguenti funzionalità:

- **Affidabilità:**
  - in caso di fault di uno dei nodi del modulo Firewall il secondo nodo continua a gestire il traffico garantendo l'applicazione delle policy di sicurezza in accesso;
  - in caso di fault di una macchina fisica del pool (o della necessità di un intervento di upgrading HW della macchina stessa) i server virtuali possono essere facilmente "spostati" su un altro nodo del pool (il software di gestione del pool supporta la funzionalità di Live Migration);
  - le caselle di posta degli utenti risiedono sul modulo SAN accessibile dai server tramite doppia connessione in fibra ottica;
  - in caso di fault di uno dei nodi di Load-Balancing del modulo Antivirus il funzionamento verrà garantito dal secondo elemento che prende in carico automaticamente tutte le attività di bilanciamento;
  - in caso di fault di un server con funzione Antivirus del modulo Antivirus il traffico viene automaticamente rediretto dal Load-Balancier sui server rimasti attivi;

- **Sicurezza:**
  - La presenza del modulo Firewall ove viene applicata la politica del tutto ciò che non è espressamente permesso è negato e l'utilizzo di elementi di Load-Balancing atti a disaccoppiare la corrispondenza tra il servizio erogato ed i server fisici che lo erogano garantisce un'elevata protezione di tutto il sistema diminuendo i rischi in caso di attacco informatico;
  - I sistemi utilizzati per l'erogazione del servizio sono sottoposti ad un intervento di hardening da parte del Responsabile della Sicurezza che, in collaborazione con il Responsabile dei Server, abilita i soli servizi indispensabili al funzionamento della PEC e disabilita tutti gli altri.

- **Scalabilità:**
  - L'utilizzo di una architettura virtualizzata permette di scalare facilmente sia in modalità orizzontale che in modalità verticale. A fronte del rilevamento di una crescita delle attività è infatti sufficiente aumentare le risorse disponibili alle macchine virtuali o inserire nel pool nuovi nodi fisici e "ridistribuire" i server virtuali sui nuovi nodi fisici.



6.2. Connettività

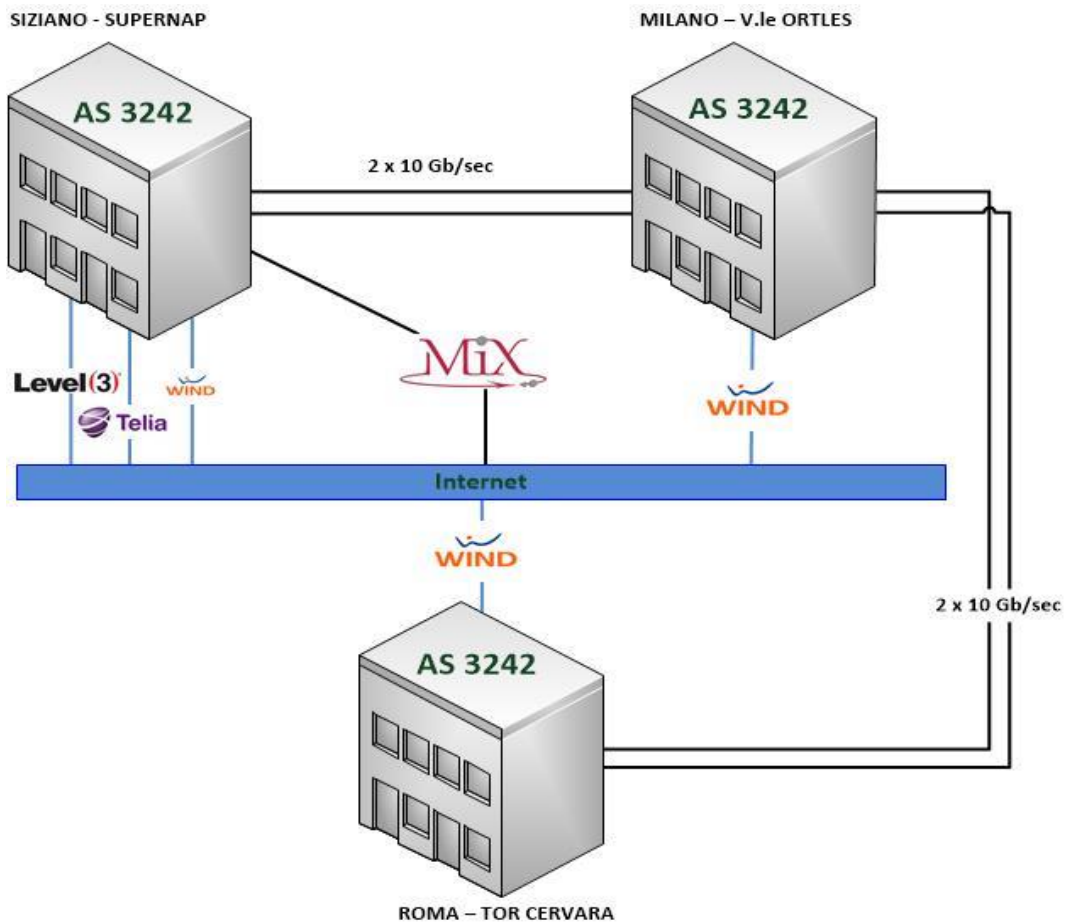
I Data Center di ITnet sono ubicati in facilities di WIND TRE (Roma - Tor Cervara e Milano – Ortles) e di Supernap Italia (Siziano, PV).

I Data Center sono poi interconnessi da circuiti in F.O. di ITnet (2 x 10Gb/s tra Milano – Ortles e Siziano, 2 x 10 Gb/s tra Milano – Ortles e Roma - Tor Cervara).

Questa infrastruttura permette di annunciare l'Autonomous System di ITnet (AS 3242) via BGP verso i carrier WIND TRE, Level 3, Telia, ...

La tabella seguente riassume la capacità trasmissiva verso Internet:

Data Center	Banda verso Internet	Banda verso MIX
Roma – Tor Cervara	2 x 10 Gb/s (WIND)	-
Milano – Ortles	2 x 5 Gb/s (WIND)	-
Siziano	n x 10 Gb/s (Multicarrier)	2 x 10 Gb/s



Tutto questo assicura ottima visibilità dei Data Center verso tutta l'utenza Internet nazionale ed internazionale.

L'infrastruttura di erogazione primaria del servizio di Posta Elettronica Certificata è posizionata presso il Data Center ITnet di Milano. Tale Data Center è direttamente connesso al POP Wind, presente nello stesso comprensorio, tramite connessioni multiple GigabitEthernet in fibra ottica terminate senza necessità di collegamenti WAN.

Sul sito di DR presso il Data Center di Siziano, l'infrastruttura Itnet è connessa al servizio Blended IP multicarier di Supernap con F.O. a 10 Gb/sec.

6.3. Data Center - Caratteristiche principali

Per garantire la continuità del servizio di Posta Elettronica Certificata, ITnet ha affiancato al sito primario di erogazione (Milano – v.le Ortles) un sito di Disaster Recovery (Siziano) da cui, in caso di grave disservizio sul sito primario, continuare ad erogare il servizio ai Titolari.

Entrambi i siti rispondono alle più rigorose indicazioni in termini di sicurezza fisica (controllo accessi, alimentazione elettrica, condizionamento, ...) e logica.

6.3.1. Caratteristiche comuni ai Data Center Itnet

Le facility in cui risiedono i DC ITnet presentano i seguenti sistemi:

- controllo degli accessi con badge e codice numerico a più livelli;
- sistema di rilevamento anti-intrusione e presidio con agenti di vigilanza 24hx7x365;
- telecamere a circuito chiuso con archiviazione digitale delle riprese nel rispetto delle attuali normative in termini di privacy;
- sistemi di rilevamento anti-fumo, anti-incendio e anti-allagamento;
- collegamento con gli altri DC per servizi di disaster recovery.

6.3.2. Sito di Milano Ortles

Alimentazione elettrica

- L'alimentazione principale del Data Center è appoggiata direttamente sull'anello regionale dell'ENEL (15.000 V).
- Ricevimento Media Tensione (M.T.) situato esternamente al corpo di fabbrica, in apposita struttura;
- Trasformatori di potenza Media Tensione/Bassa Tensione da 3150Kva ridondati al 100%;
- Gruppo di continuità ridondato al 100% CHLORIDE-SILECTRON, con raddrizzatore dodecafase, BYPASS statico completo di compensatore attivo in grado di ridurre le armoniche in ingresso al di sotto del 5%, predisposto per funzionare in parallelo;
- Accumulatori al piombo ermetici tipo Long Life EUROBAT 1;
- Gruppo elettrogeno da 2000 kVA in container, installato esternamente al fabbricato UPS (tempo di attivazione automatico < 10sec);
- Armadi rack (cabinet) con doppia alimentazione e potere d'interruzione del cortocircuito al primo interruttore a monte del rack;

Climatizzazione

- Climatizzazione completa in grado di mantenere un delta(t) < 1°C;
- Impianto di condizionamento ridondato al 100%;

6.3.3. Sito di Siziano (SuperNap)

Alimentazione elettrica

- Il campus è alimentato da una linea ridondata in alta tensione da 132 kV.
- Tutto il carico IT è protetto da un sistema UPS tri-ridondante in grado di assicurare il 100% di disponibilità (100% uptime).
- Certificazione Tier4 (modalità "system + system" (2N+1)).
- Sistema basato su due impianti elettrici separati e totalmente indipendenti (Feed A e Feed B), ognuno dei quali può sostenere, in ogni momento, il carico dell'intera Facility.
- Ogni impianto è dotato di un suo UPS (Uninterruptible Power Systems), System Bypass Modules, PDU (Power Distribution Units), RPP (Remote Power Panels) e altri componenti adeguati al livello di tiering.
- Tutti i rack sono dotati di una doppia alimentazione, ognuna afferente ad una "catena" di alimentazione (Feed A, Feed B).

Climatizzazione

- L'impianto di raffreddamento si basa su un set modulare di AHU (Air Handling Unit) che sfruttano il principio del raffrescamento evaporativo indiretto tramite scambiatori aria-aria opportunamente raffreddati da sistemi ad acqua (esterni al DC);
- L'infrastruttura in acciaio, che sostiene il sistema T-SCIF, ha anche la funzione di volano termico, permettendo alla Facility di raggiungere livelli di resilienza superiori ai più elevati standard di settore.

Questi sistemi di ultima generazione permetteranno di misurare un PUE inferiore a 1,4.

Con questi accorgimenti all'interno del DC possono essere ospitati rack ad alta densità (fino a 40KW) totalmente raffrescati ad aria.

6.4. Precisione del riferimento temporale

Per tutte le operazioni effettuate durante i processi di elaborazione dei messaggi, ricevute, log, ecc. svolte dai punti accesso/ricezione/consegna è disponibile il relativo riferimento temporale. Gli eventi (generazione di ricevute, buste di trasporto, log, ecc.) che costituiscono la transazione di elaborazione del messaggio presso i punti di accesso, ricezione e consegna, impiegano il riferimento temporale rilevato all'interno della transazione stessa. In questo modo l'indicazione dell'istante di elaborazione del messaggio è univoca all'interno dei log, delle ricevute, dei messaggi, ecc. generati dal server.

Le indicazioni temporali fornite dal servizio in formato leggibile dall'Utente sono fornite con riferimento all'ora legale vigente al momento indicato per l'operazione. Per la data il formato impiegato è "gg/mm/aaaa" mentre per l'indicazione oraria si utilizza la dicitura "hh:mm:ss", dove hh è in formato 24 ore. Al dato temporale è fatta seguire tra parentesi la "zona" ossia la

differenza (in ore e minuti) tra l'ora legale e UTC. La rappresentazione di tale valore è in formato "[+|-]hhmm", dove il primo carattere indica una differenza positiva o negativa.

Si considera come sorgente del riferimento temporale l'orologio di sistema, la cui precisione è garantita dalla sua sincronizzazione via NTP (Network Time Protocol) con IEN (Istituto Elettrotecnico Nazionale) Galileo Ferraris che fornisce un servizio di sincronizzazione per sistemi informatici collegati alla rete Internet, basato su due server primari installati nel Laboratorio di Tempo e Frequenza Campione.

Essi sono sincronizzati, attraverso un generatore di codice di data, dai campioni atomici a fascio di cesio utilizzati per generare la scala di tempo nazionale italiana UTC (IEN).

Lo scarto di tempo tra i server NTP dello IEN e la scala di tempo nazionale italiana viene tenuto sotto controllo ed è normalmente inferiore ad alcuni millisecondi. La precisione di sincronizzazione ottenibile dipende dalla tipologia della rete e dalla distanza interposta tra il server NTP ed il calcolatore che si vuole sincronizzare; i valori di scarto tipici sono inferiori al millisecondo per sistemi appartenenti alla stessa rete e possono arrivare a qualche centinaio di millisecondi per reti remote.

Il Network Time Protocol (NTP) è uno dei metodi più accurati e flessibili per disseminare l'informazione di tempo e di data sulla rete Internet. Esso permette di sincronizzare e mantenere sincronizzati tra loro computer collegati tramite reti locali, metropolitane o addirittura mondiali (Internet) utilizzando una struttura di tipo gerarchico.

Le specifiche tecniche di questo protocollo di sincronizzazione sono descritte nella *RCF-1305*.

6.5. Gestione dei Log dei messaggi

Il log dei messaggi è il registro informatico delle operazioni riguardanti le trasmissioni effettuate mediante Posta Elettronica Certificata che, come richiesto dalla normativa in vigore, è tenuto dal gestore.

In questo paragrafo sono descritte le modalità di gestione dei log del Servizio di Posta Elettronica Certificata adottati da ITnet S.r.l..

6.5.1. Descrizione

Durante le fasi di trattamento del messaggio presso i punti di accesso, ricezione e consegna, il sistema mantiene traccia delle operazioni svolte.

Tutte le attività sono memorizzate su una tabella di un Data Base dove vengono memorizzati i dati significativi dell'operazione:

- il codice identificativo univoco assegnato al messaggio originale
- la data e l'ora dell'evento

- il mittente del messaggio originale
- i destinatari del messaggio originale
- l'oggetto del messaggio originale
- il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.)
- il codice identificativo dei messaggi correlati generati (ricevute, errori, ecc.)
- il gestore mittente

Gli effettivi dati registrati sui singoli record dipendono dalla tipologia dell'operazione tracciata (ricezione messaggio, generazione buste, ecc.).

6.5.2. Archiviazione e Conservazione

Per aumentare l'efficienza e la velocità di trattamento, le informazioni che si riferiscono alle transazioni di Posta Elettronica Certificata sono mantenute dal sistema su un Data Base dedicato.

Ogni giorno, alle ore 01:00, una procedura automatica estrae dal Data Base tutti i dati relativi alle transazioni di Posta Elettronica Certificata che si sono verificate tra le 00:00:00 e le 23:59:59 del giorno precedente. Le informazioni così raccolte costituiscono i log della Posta Elettronica Certificata.

La normativa vigente relativa ai log della Posta Elettronica Certificata stabilisce che:

- immediatamente dopo la loro estrazione, i log vengano marcati temporalmente allo scopo di garantirne l'integrità e l'inalterabilità;
- i log vengano mantenuti per trenta (30) mesi a cura di ITnet S.r.l.;
- i log e le Buste di trasporto di Messaggi PEC contenenti virus informatici vengano sottoposti ad un processo di Conservazione.

Per svolgere l'attività di marcatura temporale ITnet S.r.l. si è dotata di software specifico (SMART_TSP_LOG distribuito da Aruba PEC S.r.l.).

Maggiori dettagli sul processo di Conservazione sono indicati nel "Manuale di Conservazione Sostitutiva" di Itnet S.r.l.

Per garantire la disponibilità dei log per il periodo richiesto, il processo di archiviazione si articola come segue:

- i log marcati temporalmente sono sottoposti al processo di Conservazione Sostitutiva presso un ente accreditato da AgID;
- i log marcati temporalmente sono depositati su un server locale dedicato all'archiviazione dei dati a scopo di magistratura (riferimento al Decreto del Garante Privacy 17 gennaio 2008);
- i log marcati temporalmente sono inviati su un server di backup presso una sede diversa da quella da cui viene erogato il servizio. Settimanalmente tali i log vengono masterizzati su dispositivo ottico non riscrivibile. La sede individuata a questo scopo è il Data Center ITnet di Roma – Tor Cervara.

I supporti ottici utilizzati per la archiviazione sono depositati all'interno di una cassaforte ignifuga previa etichettatura.

6.5.3. Reperimento e presentazione

Su richiesta dei soggetti aventi diritto, sono rese disponibili le informazioni contenute nei log, così come individuate dall'allegato tecnico al DM 2/11/2005 [5] (il codice identificativo univoco assegnato al messaggio originale, la data e l'ora dell'evento, il mittente del messaggio originale, i destinatari del messaggio originale, l'oggetto del messaggio originale, il tipo di evento oggetto del log, il codice identificativo dei messaggi correlati generati, il gestore mittente).

Il processo di richiesta, reperimento e presentazione dei log prevede le seguenti attività:

- Le richieste di estrazione dei log possono essere effettuate dal dai soggetti autorizzati dalla Legge o Titolari tramite l'invio di un documento cartaceo o informatico con il quale richiede il recupero e la presentazione dei log. In base alla tipologia adottata la richiesta può essere inviata:
  - tramite raccomandata A/R all'indirizzo

    ITnet S.r.l. - Servizio Clienti ITnet – Palazzo U4 - via del Bosco Rinnovato 8, 20090 Assago (MI).

    In questo caso la richiesta da parte dei Titolari deve essere effettuata su carta intestata e corredata da una copia di un documento di riconoscimento.

- tramite Posta Elettronica Certificata agli indirizzi **richiestalog@pec.it.net** oppure **servizioclienti@pec.it.net** utilizzando la propria casella di Posta Elettronica Certificata

La richiesta deve contenere i seguenti dati identificativi della e-mail per cui si richiede l'estrazione dei log:

- data della trasmissione (invio/ricezione)
- indicazione del mittente (From/da) e del destinatario (TO/a)
- codice identificativo della trasmissione (facoltativo)
- parte dell'oggetto (facoltativo)

- L'estrazione dei log è eseguita mediante accesso ai server o agli archivi ottici da parte del personale tecnico ITnet autorizzato.
- La presentazione dei log avviene tramite invio degli stessi all'indirizzo di Posta Elettronica Certificata del richiedente o, in alternativa, ad altro indirizzo specificato dal Titolare nella richiesta. Le informazioni rilasciate potranno essere utilizzate per gli usi consentiti dalla legge.

In ogni caso l'accesso ai log può avvenire su richiesta dell'Autorità Giudiziaria.

Se richiesto, il processo di estrazione dei file di log potrà essere effettuato a partire dall'Archivio di Conservazione. In questo caso il processo di estrazione e presentazione è quello descritto in "PSI10 Conservazione".

Ulteriori modalità di richiesta potranno essere comunicate attraverso il sito del Gestore.

7. INTEROPERABILITA' TRA GESTORI

In ottemperanza a quanto previsto dal DPR 68/2005 [3] ITnet S.r.l. garantisce l'interoperabilità con gli altri gestori in conformità alle regole di Posta Elettronica Certificata (DM 2/11/2005 [5]).

ITnet S.r.l. si è predisposta per verificare periodicamente l'invio e la ricezione di messaggi di Posta Elettronica Certificata verso gli altri gestori accreditati.

8. MISURE DI SICUREZZA E SOLUZIONI FINALIZZATE A GARANTIRE IL COMPLETAMENTO DELLA TRASMISSIONE

8.1. 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 e delle ispezioni (auditing);
- responsabile della sicurezza;
- responsabile della sicurezza dei log dei messaggi;
- responsabile del sistema di riferimento temporale.

Le figure sopra elencate possono avvalersi, per lo svolgimento delle funzioni di loro competenza, di addetti ed operatori.

Per tutte le figure coinvolte nel servizio sono predisposte apposite attività di formazione e di addestramento.

8.2. Approccio organizzativo

La continuità del servizio, anche al fine di assicurare il completamento delle fasi di trasmissione dei messaggi, è assicurata, oltre a tutti gli accorgimenti tecnologici messi in atto per garantire affidabilità/disponibilità e sicurezza, dalla continua supervisione del corretto funzionamento del sistema da parte del personale preposto, dal costante monitoraggio automatico, così come indicato al paragrafo 8.3.7, e anche attraverso procedure di escalation che mirino alla gestione affidabile e controllata del servizio di Posta Elettronica Certificata.

Per processo di escalation si intende l'esecuzione delle attività correlate alla risoluzione dei malfunzionamenti sugli elementi che compongono i moduli del sistema, per i quali sia necessario un passaggio al livello di competenza/responsabilità superiore.

Il processo di escalation viene attivato nel momento in cui è accertata l'impossibilità di risolvere la problematica a quel livello di competenza/responsabilità (se il problema risulta chiaramente identificato ed esistono le condizioni per procedere alla sua risoluzione, il caso non viene scalato).

- **Attività da effettuare entro 60 minuti dal malfunzionamento:**
  Il personale preposto al servizio di Posta Elettronica Certificata, coordinato dal Responsabile dei Servizi Tecnici, rilevato il guasto/anomalia identifica le azioni per il ripristino della situazione di esercizio; in particolare

- Informa L'Assistenza Tecnica di primo livello (AT) mediante apertura di Warning Trouble Ticket a cui dovranno essere correlati tutti i Customer Trouble Ticket generati dalle eventuali chiamate dei clienti;
- Richiede l'intervento di ulteriori risorse specialistiche (altri sistemisti o reperibile di secondo livello se fuori orario base), se non si è in grado di procedere autonomamente;
- Coinvolge l'eventuale fornitore interessato dal malfunzionamento in relazione alla tipologia del problema emerso;
- Se le contromisure adottate in tale circostanza si dimostrassero efficaci provvede a chiudere il Warning Trouble Ticket affinché ATpossa contattare tutti i clienti che hanno riscontrato problemi per comunicare l'avvenuta risoluzione.

o **Attività da effettuare entro 120 minuti dal malfunzionamento:**

- Il Responsabile dei Servizi Tecnici informa il diretto superiore che si attiva per individuare le azioni più opportune da mettere in atto al fine di effettuare una stima dei tempi necessari al superamento del problema;
- Viene avviato il processo di comunicazione verso i Clienti coinvolgendo gli enti preposti;
- Il processo termina con la risoluzione del problema registrandone la chiusura tramite i sistemi predisposti al monitoring e alla gestione dei guasti.

Se il malfunzionamento risultasse imputabile ad un incidente di sicurezza questo verrà registrato all'interno del Data Base degli Incidenti e sarà oggetto di analisi del Comitato Security.

8.3. Approccio Tecnologico

Come già enunciato la piattaforma tecnologica utilizzata per il Servizio di Posta Elettronica Certificata si basa su un'architettura completamente ridondata atta a garantire:

- affidabilità
- disponibilità
- sicurezza
- scalabilità

Di seguito sono riportati ulteriori aspetti tecnologici atti a garantire un'adeguata sicurezza del sistema di Posta Elettronica Certificata.

8.3.1. Firma

Le chiavi utilizzate da ITnet S.r.l. per le operazioni di firma nel proprio servizio di Posta Elettronica Certificata sono generate all'interno di un

apparato HW crittografico sicuro (HSM – Hardware Security Module), utilizzando l'algoritmo asimmetrico RSA con chiavi di lunghezza non inferiori a 1.024 bit. Gli HSM sono totalmente dedicati al servizio e ridondati, in modo da garantire la sicurezza e l'affidabilità necessaria in caso di guasti.

8.3.2. Autenticazione

Il sistema di Posta Elettronica Certificata ITnet S.r.l. prevede che tutti gli utenti debbano essere autenticati con username e password personali sia per l'invio di mail che per la ricezione.

Questo garantisce che il messaggio sia inviato da un Utente del servizio di Posta Elettronica Certificata i cui dati di identificazione siano congruenti con il mittente specificato al fine di evitare la falsificazione di questo ultimo.

8.3.3. Colloquio Sicuro

Al fine di garantire l'inalterabilità del messaggio originale spedito dal mittente si realizza l'imbustamento e la firma dei messaggi in uscita dal punto di accesso e la successiva verifica in ingresso al punto di ricezione.

Il messaggio originale (completo di header, testo ed eventuali allegati) è inserito come allegato all'interno di una busta di trasporto.

La busta di trasporto firmata dal gestore mittente permette di verificare che il messaggio originale non sia stato modificato durante il suo percorso dal dominio mittente al dominio destinatario.

La sicurezza del colloquio tra mittente e destinatario prevede un meccanismo di protezione per tutte le connessioni previste dall'architettura di Posta Elettronica Certificata (tra Utente e punto di accesso ITnet S.r.l., tra ITnet S.r.l. e gli altri gestori, tra punto di consegna ITnet S.r.l. ed Utente) attuato tramite l'impiego di canali sicuri.

L'integrità e la confidenzialità delle connessioni tra ITnet S.r.l. e l'Utente sono garantite mediante l'uso di protocolli sicuri (come dettagliato al paragrafo 3.4).

Il colloquio con gli altri gestori avviene con l'impiego del protocollo SMTP su trasporto TLS.

8.3.4. Virus

Un altro aspetto rilevante per la sicurezza, che riguarda l'intero sistema di Posta Elettronica Certificata, è relativo all'architettura tecnico/funzionale del sistema di antivirus.

ITnet S.r.l. utilizza un sistema Antivirus, composto da 3 unità, che ne garantiscono la ridondanza, e che impedisce quanto più possibile il trasporto di virus all'interno di messaggi di Posta Elettronica.

Le configurazioni adottate sono tali per cui tutti i messaggi in cui viene rilevato un virus vengono gestiti per analizzare se sia opportuno consegnare un messaggio di non “accettazione/rilevazione/mancata consegna per virus informatico” o respingere/cancellare il messaggio nel rispetto della normativa vigente.

Il sistema effettua automaticamente controlli per verificare la presenza di aggiornamenti del prodotto di antivirus con cadenza oraria e, se disponibili, li rende immediatamente operativi.

8.3.5. Data Center - Standard di sicurezza

Il Data Center ITnet S.r.l. dove risiedono i server per l’erogazione del servizio di Posta Elettronica Certificata è oggetto della certificazione ISO/IEC 27001:2013 (come dettagliato al paragrafo 1.2.5) Il campo di applicazione di detta norma, riportato sul certificato è:

“Gestione delle infrastrutture fisiche e di connettività di Data Center e dei processi a supporto con particolare riferimento a continuità elettrica, temperatura, controllo degli accessi e sicurezza fisica. Erogazione dei servizi Cloud e posta elettronica certificata (PEC)”.

Come ulteriore misura di sicurezza, in aggiunta a quanto già indicato, i server dedicati all’erogazione del servizio sono installati in un’area segregata ricavata all’interno del Data Center. L’accesso a tale area è consentito al solo personale incaricato ed è controllato da un lettore di badge.

8.3.6. Backup dei dati

I sistemi di erogazione del servizio di Posta Elettronica Certificata sono soggetti a regolare backup. Il prodotto utilizzato, Simpana CommVault, controlla e gestisce l’esecuzione dei salvataggi (sia a livello di File System che di intera macchina), la loro archiviazione su sistemi locali e la loro replica off site verso il Data Center ITnet di Roma Tor Cervara.

Le politiche di backup prevedono un salvataggio in forma incrementale con cadenza giornaliera, mentre settimanalmente viene effettuato un backup di tipo Full.

Il tempo di ritenzione dei salvataggi effettuati è di 1 (uno) mese.

8.3.7. Monitoraggio

Per verificare la disponibilità del servizio di Posta Elettronica Certificata sono state attivate sonde e strumenti per il controllo dei singoli elementi dei differenti moduli e per il test dei vari servizi.

Le sonde/controlli agiscono a livello di singolo sistema/servizio in modo da rilevare i malfunzionamenti prima che questi causino l’indisponibilità dell’intero servizio.

Al rilevamento di un malfunzionamento il sistema invia una e-mail ed un SMS ai sistemisti interessati affinché vengano attivate le procedure del caso.

Il sistema è sempre attivo 24 ore su 24.

8.3.8. Gestione delle emergenze

ITnet S.r.l., come Gestore Accreditato, allo scopo di garantire, i livelli di servizio richiesti dal DM 2/11/2005 [5], ha organizzato la sua infrastruttura tecnologica per l'erogazione del servizio con le modalità che vengono di seguito riepilogate:

- infrastruttura di virtualizzazione e Storage Area Network progettata e realizzata secondo criteri di alta affidabilità e ridondanza (vedi dettagli al paragrafo 6.1);
- gruppi di continuità distinti che servono i sistemi ridondati;
- generatore autonomo di elettricità nel caso in cui la mancanza di tensione della rete elettrica si prolunghi nel tempo (vedi dettagli al paragrafo 0);
- monitoring esterno continuo dei servizi con allarmi verso la struttura tecnica di gestione per l'implementazione di interventi di ripristino immediati (vedi dettagli al paragrafo 8.3.7);
- firewall ridondati che permettono l'accesso ai servizi in modalità sicura, come definito dalla normativa tecnica in vigore. Il collegamento per la gestione avviene attraverso connessioni criptate sicure da indirizzi autorizzati (vedi dettagli al paragrafo 6.1);
- le sedi di erogazione del servizio sono certificate ISO/IEC 27001:2013 (vedi dettagli al paragrafo 8.3.5)

ITnet S.r.l. si è predisposta definendo una procedura di urgenza in modo tale che a fronte ad un evento disastroso, venga coinvolto un gruppo di emergenza composto dai responsabili per analizzare la gravità dell'evento stesso e predisporre le azioni necessarie per minimizzarne i danni e per fornire indicazioni sulle modalità e politiche da adottare per il ripristino del servizio. Sempre in questa eventualità sono state comunque individuate le funzionalità indispensabili al fine di rendere minima l'interruzione del servizio e garantire il rispetto dei requisiti di legge in relazione alla reperibilità delle informazioni registrate sul log dei messaggi.

Per gli eventi non catastrofici la continuità del servizio è garantita in quanto la ridondanza dei sistemi, oltre a garantire la continuità di servizio a fronte di guasti hardware, permette di garantire continuità di servizio anche a fronte di upgrade software o hardware ai sistemi.

Nel caso si verificassero uno o più eventi sopra descritti, ITnet S.r.l., come gestore accreditato, effettuerà le necessarie comunicazioni ai Titolari e ad AgID così come previsto dalla normativa di riferimento vigente.

9. MODALITA' DI CESSAZIONE DELL'ATTIVITA' DI GESTORE

Nel caso in cui Itnet S.r.l. decidesse la cessazione dell'attività di Gestore verrebbero prontamente indirizzate le seguenti azioni:

- Comunicazione formale ai Titolari di caselle di Posta Elettronica Certificata della volontà di cessare l'attività di Gestore e le indicazioni su un eventuale gestore sostitutivo;
- Comunicazione formale ad AgID della volontà di cessare l'attività di Gestore, indicando la data di cessazione e l'eventuale Gestore subentrante;
- Comunicazione formale agli altri Gestori alla data presenti nell'elenco di AgID della volontà di cessare l'attività di Gestore;
- Indicazioni sul sito istituzionale riportando le indicazioni di cui sopra;
- Comunicazione al Supporto tecnico e al supporto Clienti in modo che possa fornire adeguate informazioni ai Titolari che abbiano bisogno di spiegazioni;
- Conservazione dei log per il tempo previsto dalla Normativa e non minore di trenta (30) mesi;
- Alla data di cessazione sono attuate le procedure per la cessazione delle chiavi di firma e dei relativi dispositivi.

10. PROTEZIONE DEI DATI PERSONALI

10.1. Informativa

La normativa di riferimento utilizzata per il trattamento dei dati da ITnet S.r.l. è rappresentata da:

- Decreto Legislativo 196 del 30 giugno 2003 [2];
- Provvedimento del 17 gennaio 2008 - Sicurezza dei dati di traffico telefonico e telematico [10];
- Provvedimento del 27 novembre 2008 - Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema [11].

In particolare, la normativa prevede l'individuazione di specifiche figure cui sono attribuiti ruoli e responsabilità ben definite:

- **Titolare del trattamento**: ITnet S.r.l., con sede legale in via del Bosco Rinnovato 8 20090 Assago (MI), è il titolare del trattamento dei dati ed è il soggetto a cui compete la scelta in ordine di finalità e modalità del trattamento.
- **Responsabile**: è la persona fisica, la persona giuridica, la pubblica amministrazione o qualsiasi altro ente preposto dal titolare alla vigilanza del corretto trattamento dei dati secondo le direttive impartite dal titolare.
- **Interessato,** la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.
- **Incaricati**: sono i dipendenti che per le loro attività lavorative gestiscono e trattano dati sensibili o personali.
- **Amministratori di sistema**: sono dipendenti scelti in base alla loro esperienza e competenza in materia che per le loro attività amministrano sistemi/macchine di proprietà di ITnet o dei clienti.

ITnet S.r.l. ha individuato l'elenco degli incaricati al trattamento e degli amministratori di sistema cui è stata data lettera formale con le indicazioni sul corretto utilizzo dei dati.

Ogni unità organizzativa è stata opportunamente formata con corsi finalizzati alla comprensione del decreto.

Si è inoltre sensibilizzato tutto il personale preposto dell'importanza di un utilizzo non improprio dei dati di cui vengono a conoscenza per le loro mansioni lavorative.

Le problematiche attinenti al tema privacy possono essere indirizzate a:

Servizio Clienti ITnet
ITnet s.r.l. – Palazzo U4

Via del Bosco Rinnovato 8
20090 Assago (MI).

10.2. Procedure di riferimento

ITnet S.r.l. rilascia al Cliente insieme ai documenti contrattuali che prevede l'informativa sulle finalità e il trattamento dei dati comunicati, così come stabilito dal decreto Legislativo 196/2003 [2], che viene sottoscritta per accettazione dall'interessato.

Di seguito sono definiti alcune procedure attivate dal Gestore per il Trattamento dei dati dell'interessato:

- **Principi che regolano il trattamento dei dati**

  I principi che regolano il trattamento dei dati sono i seguenti:

  - i dati sono raccolti presso l'interessato mediante compilazione di un apposito modulo che comprende l'informativa e l'esplicito consenso da parte dello stesso;
  - sono trattati solo i dati necessari per gli scopi per i quali sono raccolti e periodicamente ne viene verificata la pertinenza;
  - le operazioni effettuate sui dati sono solo quelle strettamente necessarie;
  - sono impartite precise istruzioni operative su come archiviare i dati in modo da evitare accessi non autorizzati;
  - I dati trattati in azienda sono accessibili solo a chi autorizzato.

- **Finalità del trattamento**

  I dati personali, direttamente forniti dall'interessato, saranno trattati da ITnet S.r.l. per le sole finalità proprie aziendali nei limiti stabiliti dalla legge.

  In particolare, i dati forniti saranno principalmente utilizzati per la fornitura del servizio ma, potranno essere comunicati a chi, avendone un lecito interesse, richieda un accertamento sulla titolarità della casella di posta elettronica di cui risulta assegnatario l'interessato.

  Ogni richiesta di comunicazione di dati deve essere scritta e motivata e deve indicare le norme di riferimento eventualmente su cui si basa. È compito della persona individuata su questi temi, accertarne la congruità e autorizzare la comunicazione.

  I dati forniti potranno essere inoltre utilizzati, previo consenso dell'interessato, al fine di vendita diretta di propri prodotti o servizi, comunicazioni, promozioni e presentazioni delle iniziative di ITnet S.r.l.

- **Diritti degli interessati**

  Come indicato all'art.7 del Decreto 196/2003 [2], l'interessato potrà esercitare tutti i diritti previsti da tale decreto.

  In particolare:

- diritto di opporsi per motivi legittimi al trattamento dei dati che lo riguardano pur se pertinente allo scopo della raccolta;
- diritto di opporsi ai dati raccolti per scopi commerciali, di invio di materiale pubblicitario, di vendita diretta, di compimento di ricerche di mercato o comunicazione commerciale interattiva;
- tutti gli altri diritti previsti dall'articolo suddetto.

Per esercitare tali diritti l'interessato dovrà inviare richiesta scritta a:

Servizio Clienti ITnet
ITnet s.r.l. – Palazzo U4
Via del Bosco Rinnovato, 8
20090 Assago (MI)

10.3. Misure di sicurezza per la protezione dei dati personali

Come previsto dalle norme vigenti in materia, ITnet S.r.l., in qualità di Titolare del trattamento, adotta almeno tutte le necessarie misure minime di sicurezza al fine di garantire sempre i seguenti principi relativi ai dati forniti dal Cliente:

- **Disponibilità**: i dati sono sempre fruibili, quando è necessario, e sono ridotti al minimo i rischi di perdita o distruzioni anche accidentali grazie ad un sistema di backup e di disaster recovery.
- **Integrità**: i dati sono difesi da manomissioni o da modifiche improprie da soggetti non autorizzati
- **Riservatezza**: i dati sono accessibili solo da persone che hanno le credenziali per accedervi e sono protette quindi da sistemi di identificazione con più punti di controllo.

10.3.1. Trasmissione e accesso ai dati da parte dell'utente

Si evidenzia che tutti i messaggi di Posta Elettronica Certificata e il colloquio attraverso l'interfaccia WEB o il client utilizzato tra l'Utente e il sistema avvengono attraverso protocolli e connessioni sicure come SMTP/S, IMAP/S, POP3/S e HTTPS.

Il sistema di Posta Elettronica Certificata ITnet S.r.l. prevede che tutti gli utenti debbano essere autenticati con username e password personali sia per l'invio sia per la ricezione di messaggi di Posta Elettronica Certificata.

Questo garantisce che il messaggio sia inviato da un Utente del servizio di Posta Elettronica Certificata i cui dati di identificazione siano congruenti con il mittente specificato al fine di evitare la falsificazione di questo ultimo.

10.3.2. Misure di sicurezza per la protezione dei dati

Dal punto di vista tecnico ITnet S.r.l., tramite i suoi incaricati, ha identificato le seguenti misure di sicurezza al fine di prevenire il rischio di distruzione, perdita, accessi non autorizzati e una scorretta trasmissione dei dati.

- **Misure di sicurezza fisiche**:

  Le misure di sicurezza fisica individuate da ITnet S.r.l. sono:

  - **Antincendio** – L'integrità fisica del personale e dei Data Center è garantita da meccanismi in grado di rilevare principi d'incendio, tramite rilevatori, allarmi automatici e un sistema centralizzato di controllo.
  - **Continuità nell'alimentazione elettrica** - Per soddisfare tale esigenza si ricorre all'utilizzazione di diverse sorgenti di energia elettrica quali:
    - fornitura di energia elettrica da parte dell'ente erogatore (ad esempio ENEL);
    - fornitura di sorgenti autonome di energia in grado di sopperire in diverso modo ma comunque efficacemente alla eventuale mancanza di energia da parte dell'ente erogatore. (ad esempio, sorgenti di continuità assoluta, come UPS, e sorgenti di alimentazione di emergenza, come gruppi elettrogeni G.E.).
  - **Perimetrazione/Anti-intrusione** – Gli accorgimenti principali adottati sono
    - Data Center fisicamente isolati;
    - Presidio con agenti di vigilanza 24 ore su 24, per sette giorni su sette;
    - Telecamere a circuito chiuso e archiviazione digitale delle riprese.
  - **Controllo degli accessi** - La limitazione dell'accesso con mezzi fisici è rappresentata da sorveglianza elettronica, serrature da sbloccare con schede magnetiche, carte intelligenti, chiavi classiche e barriere comandate a distanza.
    Tutti coloro che intendono accedere e circolare all'interno delle sedi aziendali di ITnet S.r.l. devono essere muniti di un tesserino di riconoscimento aziendale.

- **Misure di sicurezza di tipo informatico**

  Le misure di sicurezza di tipo informatico individuate da ITnet S.r.l. sono:

  - **Antivirus** - Per minimizzare i danni che possono essere causati dai virus informatici ITnet S.r.l. agisce con:
    - politiche di prevenzione per impedire l'introduzione dei virus all'interno dell'azienda;
    - politiche per la rilevazione della presenza dei virus all'interno di applicazioni, dati o boot record;
    - politiche di rimozione di eventuali virus presenti.

- **Backup dei dati e restore** – ITnet S.r.l. adotta una serie di procedure mirate attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nei sistemi su dispositivi opportuni.
  In caso di guasto hardware dei dischi è quindi possibile "ripristinare" il sistema nello stesso stato in cui si trovava nel momento dell'ultimo back-up.
  Le politiche di back-up sono organizzate in maniera tale da poter disporre di uno storico e poter così recuperare lo stesso dato in più stadi.
  I sistemi di back up sono posizionati in locali diversi da quelli che ospitano i sistemi con i dati. L'accesso fisico e logico ai sistemi di back up e al recupero dei dati è consentito esclusivamente a personale autorizzato.
- **Password** - Al fine di evitare che le informazioni vengano trattate e consultate da chi non ne sia preventivamente autorizzato e al fine di evitare possibili danni dovuti all'uso improprio (volontario o involontario) delle informazioni, sono previste formali procedure per l'allocazione dei diritti di accesso degli utenti, che potranno quindi accedere solamente ai dati per i quali sono abilitati. Identificazione e autenticazione è la tecnica che permette di riconoscere e verificare utenti o processi.

- **Formazione**

  Al fine di adempire quanto richiesto sia dal decreto Legislativo 196/2003 [2], da tutta la normativa in materia e dalla norma ISO 27001, sono erogate a tutti gli incaricati individuati e, comunque, a tutti i dipendenti della Società, sessioni di formazione volte a descrivere le parti principali del decreto e della normativa.

  Durante la formazione ad ogni struttura organizzativa sono impartite istruzioni differenziate a seconda dei trattamenti dei dati (identificativi, personali o giudiziari) svolti nel corso delle attività lavorative.

  L'obiettivo è quello di annullare o, comunque, ridurre al minimo il rischio di trattamento non consentito o improprio dei dati.

  I principali temi trattati in tali sessioni formative sono:

  - interpretazione del decreto legislativo 196, del provvedimento del 17 gennaio 2008 [10], e del provvedimento sugli amministratori di sistema del 28 novembre [11];
  - interpretazione della norma ISO 27001:2013;
  - descrizione del corretto utilizzo dei dati e dei trattamenti effettuati dalla struttura di cui il dipendente fa parte,
  - livelli di classificazione dei documenti e loro corretta gestione;

- corretto utilizzo delle dotazioni microinformatiche al fine di prevenire usi impropri o non autorizzati dei dati (gestione password, utilizzo corretto dei file di memoria, aree condivise ecc.).