

VINCENZO GAMBETTA

Laureato in Fisica Nucleare, ha trascorso oltre trent'anni in IBM Italia ricoprendo, in Italia e all'estero, incarichi manageriali e professionali. Attualmente è analista di mercato e consulente per la gestione dati, informazioni e documenti presso aziende (fornitrici ed utenti) di medie e grandi dimensioni.

Tra i clienti è Assinform per la quale tiene i rapporti con AIPA/CNIPA, il Ministero dell'economia e delle finanze e le altre istituzioni coinvolte per garantire la miglior applicabilità delle norme sulla conservazione, sulla fatturazione elettronica e sul documento informatico e firma digitale. In Assinform è, anche, coordinatore dei gruppi di lavoro gestione documentale e outsourcing nonché del centro di competenza per le PMI. È autore delle prime due ricerche sul mercato della gestione elettronica dei documenti in Italia, realizzate per ITER, in collaborazione con le Università Cattoliche di Piacenza (1998) e Milano (2000). È abitualmente relatore in seminari e conferenze e scrive per testate specializzate su temi quali gestione elettronica documenti/contenuti, BPM&A, conservazione, fatturazione elettronica, documento informatico e firma digitale. È direttore contenuti del periodico iged.it, specializzato in gestione elettronica dei documenti, e ha la responsabilità scientifica della manifestazione OMAT.

PEC. POSTA ELETTRONICA CERTIFICATA



VINCENZO GAMBETTA

PEC

PEC. POSTA ELETTRONICA CERTIFICATA

8

POSTA ELETTRONICA CERTIFICATA



La Fondazione Siav Academy è il Centro per la Ricerca e lo Sviluppo dell'Innovazione Tecnologica nell'ambito di Siav Group. Attraverso il proprio Comitato Scientifico, costituito da alcuni dei più autorevoli esperti a livello internazionale, la Fondazione intende contribuire al dibattito e all'evoluzione scientifica, normativa e applicativa sui temi della dematerializzazione. La Fondazione, attiva nell'organizzazione di convegni e seminari formativi, opera anche nell'ambito dei Beni Culturali attraverso sponsorizzazioni e progetti dedicati alla conservazione e valorizzazione del patrimonio storico, culturale e artistico.

La Collana "Tecnologia dei processi documentali" rientra nelle attività pubblicistiche che la Fondazione promuove. Curata e coordinata dal Comitato Scientifico, con la supervisione puntuale del prof. Pierluigi Ridolfi, la Collana ha l'obiettivo di approfondire le più importanti e attuali tematiche che riguardano la gestione documentale, per quanto riguarda la normativa, le tecnologie, gli standard e le applicazioni.

in collaborazione con



VINCENZO GAMBETTA

8



Collana di Minigrafie

Tecnologia dei Processi Documentali

FONDAZIONE SIACV ACADEMY



FONDAZIONE SIAV ACADEMY

VINCENZO GAMBETTA

PEC
POSTA ELETTRONICA
CERTIFICATA

Contributi di Stefano Pigliapoco e Alessandro Fabris

Collana di Minigrafie sulla

Tecnologia dei processi documentali

A cura di Pierluigi Ridolfi

© 2011 Fondazione Siav Academy - Edizione fuori commercio

È consentita la copia di qualunque parte di questo testo purché venga citata la fonte.

ISBN 978-88-97222-08-8



Collana di Minigrafie
Tecnologia dei Processi Documentali

INDICE

Capitolo I Cos'è la PEC?	<i>pag. 7</i>
• <i>Evoluzione delle email</i> • <i>Gli attori</i> • <i>Terminologia</i> • <i>Lo schema di funzionamento</i> • <i>Statistiche</i> • <i>L'offerta</i>	
Capitolo II Vantaggi e svantaggi	<i>pag. 37</i>
• <i>Introduzione</i> • <i>Confronto con la raccomandata ed altri sistemi di corrispondenza</i>	
Capitolo III La PEC nella normativa italiana	<i>pag. 45</i>
• <i>Introduzione</i> • <i>Il quadro normativo di riferimento</i> – <i>DPR 11 febbraio 2005, n. 68</i> – <i>Decreto Ministeriale 2 novembre 2005</i> – <i>Circolari CNIPA di accreditamento n. 56 del 21 maggio 2009, e di vigilanza n. 51 del 7 dicembre 2006</i> – <i>Decreto legge del 29 novembre 2008, n. 185</i> – <i>Decreto Legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale"</i>	
Capitolo IV La PEC per il cittadino	<i>pag. 61</i>
• <i>La PostaCertificat@</i> • <i>Come si ottiene</i> • <i>Caratteristiche e servizi</i> – <i>I servizi base</i> – <i>I servizi avanzati</i>	
Capitolo V Interoperabilità e alternative	<i>pag. 67</i>
• <i>La REM (Registered Email)</i>	

Capitolo VI *pag. 75* **Gestione e archiviazione dei messaggi di Posta Elettronica Certificata**

di Stefano Pigliapoco

- *Introduzione*
 - *Gestione informatica dei documenti*
 - *Formazione e conservazione dell'archivio digitale*
- *Gestione dei messaggi di PEC*

Capitolo VII *pag. 89* **Alcuni ambiti di applicazione**

Capitolo VIII *pag. 93* **Le soluzioni Siav per la gestione della PEC**

di Alessandro Fabris

- *Introduzione*
- *La gestione della PEC*
- *PEC Manager*
- *PEC Manager PA*
- *PEC Manager SE*
- *Ergon*
- *Sinthesi*

Testi delle norme principali *pag. 115*

- *DPR del 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”*
- *Decreto del Ministro per l'innovazione e le tecnologie, 2 novembre 2005 “Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata”*
- *Decreto legge del 29 novembre 2008, n. 185, recante “misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale”, convertito in legge, con modificazioni, con la Legge 28 del gennaio 2009, n. 2*
- *DPCM 6 maggio 2009 “Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini”*

Capitolo I

Cos'è la PEC?

1. Evoluzione delle email

La posta elettronica è uno strumento di comunicazione a diffusione “universale”, con caratteristiche di immediatezza, versatilità ed efficacia, accompagnate da una concreta semplicità che tutti abbiamo avuto modo di verificare.

Questo strumento, nel giro di pochi lustri, ha avuto una diffusione talmente insperata, imprevedibile ed inimmaginabile¹ che consente oggi, a milioni di persone in tutto il mondo, di scambiarsi ogni tipo di informazione, praticamente in ogni situazione e con l'impiego di strumenti sempre più diversi e di utilizzo comune.

Con il tempo le modalità d'accesso alla posta elettronica ed ai suoi servizi hanno seguito e soddisfatto le crescenti esigenze degli utenti, si pensi alla possibilità di accedervi via web, all'impiego di smartphone, tablet ed altro ancora, ...

Con la posta elettronica, universalmente impiegata nelle comunicazioni interpersonali e d'ufficio, ci si scambia di tutto: dagli ordini, ai contratti, alle notifiche, ai file di qualunque tipo, agli auguri per festività e ricorrenze, ai pettegolezzi, agli appuntamenti, agli inviti, alle più disparate informazioni di tipo personale, tecnico/scientifiche e di business, ai messaggi pubblicitari, ai tentativi di frode, ed altro ancora: qualunque “cosa” in formato digitale può essere trasferita via posta elettronica.

¹ Sebbene la prima email sia del 1971, esse presero piede solo negli anni 90: le mail spedite giornalmente nel 2010 si stima siano state mediamente superiori a 290 miliardi, contro i 60 del 2006.

Questo strumento consente, inoltre, di inviare la stessa comunicazione contemporaneamente a molti soggetti, i quali possono, a loro volta, re-inviarla a molti altri ancora.

Oggi la posta elettronica è un qualcosa di talmente insito nelle “abitudini” di ognuno di noi, privati o facenti parte di un qualunque tipo di organizzazione, ed è così integrata nei processi aziendali che si può parlare di “dipendenza” da essa vuoi nei comportamenti dei singoli vuoi per la sua capacità di condizionare l’operatività di tutti i giorni.

Nel corso del 2010 è diventato, però, sempre più evidente quanto la comunicazione, in particolare quella interpersonale, si sia progressivamente spostata in rete sui social network.

Secondo Morgan Stanley, il numero di utenti dei social network, oggi stimato superiore ai 1,2 miliardi, ha effettuato il “sorpasso” degli utenti di email all’incirca a settembre del 2009, quando valevano entrambi sugli 800 milioni.

Ciò nonostante la posta elettronica resta il più importante mezzo di comunicazione a livello business e, comunque, formale.

Proprio a causa di questa enorme (universale) diffusione dello strumento e dei contenuti che tramite essa possono essere inviati sono emersi alcuni limiti (difetti?) di questo strumento.

La posta elettronica, così come oggi realizzata e utilizzata, non è, infatti, in grado di offrire certezze circa l’identità del mittente, di quando è avvenuto l’invio, del fatto che ciò che è stato spedito sia arrivato integro al/ai ricevente/i nonché sulla effettiva ricezione da parte del/i ricevente/i.

Non sono queste cose di poco conto nell’ambiente “globale” nel quale lo strumento è impiegato per trasmettere informazioni e documenti di qualunque tipo e rilevanza.

Proprio prendendo le mosse dall’esigenza di colmare le lacune appena citate è nata, in Italia, la Posta Elettronica Certificata, familiarmente rinominata Raccomandata Elettronica, che va ad affiancarsi alla tradizionale Posta Elettronica un po’ come la raccomandata con ricevuta di ricevimento si affianca (o dovrei dire ... affiancava) alla normale corrispondenza.

La Posta Elettronica Certificata può, dunque, essere impiegata in qualunque contesto ove sia necessario, o si desideri, disporre di uno strumento opponibile a terzi che comprovi l’invio, la consegna ed il contenuto di un documento elettronico.

In altri termini consente di disporre di una prova legalmente valida, con preciso riferimento temporale, dell’avvenuta spedizione di un determinato messaggio, con l’eventuale documentazione allegata, nonché della sua consegna integro ai destinatari designati.

2. Gli attori

Gli “attori” di un sistema di Posta Elettronica Certificata sono:

- Il gestore di Posta Elettronica Certificata: il soggetto che gestisce uno o più domini² 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 (vedi seguito), che si interfaccia con altri gestori di Posta Elettronica Certificata garantendo l’interoperabilità tra i titolari.

² Un dominio di Posta Elettronica Certificata è un dominio DNS (Domain Name System) dedicato alle caselle di posta elettronica degli utenti di Posta Certificata. Un Domain Name System - DNS (sistema dei nomi a dominio) è un sistema impiegato per risolvere i nomi dei nodi di rete in Indirizzi IP. Il servizio è realizzato da un sistema di Data Base distribuiti: i server DNS, appunto. All’interno di un tale dominio le caselle di posta elettronica devono appartenere ad utenti di Posta Certificata.

Esso è inserito in elenco pubblico dei gestori di Posta Elettronica Certificata gestito da DigitPA.

- Gli utenti o titolari (di Posta Elettronica Certificata): le persone fisiche o giuridiche, gli enti, le associazioni o qualunque organizzazione nonché le Pubbliche Amministrazioni cui sia stata assegnata una casella di Posta Elettronica Certificata da parte di un gestore di Posta Elettronica Certificata incluso nell'apposito elenco gestito e pubblicato da DigitPA. Essi assumono, di volta in volta, il ruolo di mittente o destinatario in funzione dell'attività svolta.

La comunicazione tra i gestori di Posta Elettronica Certificata è assicurato da un indice (l'elenco pubblico, appunto) che contiene l'elenco dei domini e dei gestori di Posta Elettronica Certificata, con i relativi certificati corrispondenti alle chiavi usate per la firma delle ricevute, degli avvisi e delle buste.

L'indice è realizzato per mezzo di un server LDAP (Lightweight Directory Access Protocol)³ posizionato in un'area raggiungibile da tutti i gestori e costituisce la struttura tecnica relativa all'elenco pubblico dei gestori di Posta Elettronica Certificata.

L'Elenco dei gestori di Posta Elettronica Certificata è riportato nella tabella I (aggiornamento al 30 luglio 2011).

N°	Ragione sociale	Indirizzo Internet	Data iscrizione elenco
1	ACI Informatica	http://www.informatica.aci.it	16-12-2009
2	Actalis	http://www.actalis.it/	21-12-2005
3	Ancitel	http://www.pec.ancitel.it/	18-07-2007
4	ARUBA PEC	http://www.pec.it/	11-10-2006
5	Cedacri	http://www.cedacri.it/	08-02-2006
6	Consiglio Nazionale del Notariato	http://www.notariato.it	21-12-2005
7	Fastweb	http://www.fastweb.it	03-10-2007
8	HP ES Italia (già EDS Italia)	https://www.eds.com/ssl/about/locations/italy/	12-07-2006
9	IN.TE.S.A.	http://trustedmail.intesa.it	11-10-2006
10	Infocert	http://www.legalmail.it	18-10-2007
11	Innova Puglia (già Tecnopolis Csata)	http://www.rupar.puglia.it	13-06-2007
12	Intred	http://www.intred.it	04-05-2011
13	IT Telecom	http://www.firmasicura.it	21-12-2005
14	ITnet	http://www.it.net	29-03-2006
15	IWBank	http://www.iwbank.it	23-01-2008
16	KPNQwest Italia	http://www.kqi.it/	13-12-2010
17	Lombardia Informatica	http://www.lispa.it	04-05-2011
18	Namirial	http://www.namirial.com	26-02-2007
19	Numera Sistemi e Informatica	http://www.numera.it	26-07-2006
20	Poste Italiane	http://www.poste.it	18-01-2006
21	Postecom	http://www.poste.it	21-12-2005
22	Regione Marche	http://www.postaraffaello.it	18-10-2007
23	Sogei – Società Generale d'Informatica	http://www.sogei.it	20-09-2006
24	TWT	http://www.twt.it	25-06-2007
25	Università degli studi di Napoli Federico II	http://www.unina.it	31-12-2008

Tabella I - I gestori di Posta Elettronica Certificata compresi nell'elenco pubblico (aggiornamento al 30 luglio 2011)

³ RFC 2849 - The LDAP Data Interchange Format (LDIF) - Technical Specification.

3. Terminologia

È utile, prima di descrivere brevemente il funzionamento della Posta Elettronica Certificata, passare all'illustrazione dei principali termini utilizzati⁴.

Innanzitutto definiamo un dominio PEC; esso è un dominio DNS che comprende solo caselle di Posta Elettronica Certificata.

Lo scambio di posta è possibile tra utenti dello stesso dominio sia con utenti appartenenti a differenti domini PEC.

Lo scambio di messaggi email è possibile anche con utenti non appartenenti a domini PEC, in questo caso però non saranno disponibili molte delle funzioni proprie della PEC.

All'interno di ognuno di suddetti domini si possono individuare tre funzionalità:

- Il punto di accesso - Consente l'accesso al servizio, effettua i controlli previsti per i messaggi da spedire e si occupa di generare la ricevuta di accettazione e la busta di trasporto;
- Il punto di ricezione – Riceve i messaggi di Posta Elettronica Certificata da altro dominio, effettua i dovuti controlli, genera la ricevuta di presa in carico e, se del caso, l'eventuale busta di anomalia;
- Il punto di consegna – Provvede alla consegna del messaggio PEC nella casella di posta del destinatario, dopo averne verificato la correttezza e la provenienza, ed emette la/e ricevuta/e di avvenuta consegna.

I dati di certificazione, dal canto loro, sono l'insieme dei dati che descrivono ed identificano il messaggio (originale) e sono

⁴ Si fa riferimento al Decreto del Ministro per l'Innovazione e le Tecnologie, 2 novembre 2005 "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata" (Pubblicato nella Gazzetta Ufficiale n. 266 del 15 novembre 2005).

generati e certificati dal gestore di Posta Elettronica Certificata del mittente.

I dati di certificazione sono inseriti nelle ricevute e sono trasferiti all'utente di Posta Certificata di destinazione insieme al messaggio originale per mezzo di un messaggio di trasporto.

Tra i dati di certificazione sono:

- la data e l'ora di invio;
- il mittente;
- il/i destinatario/i;
- l'oggetto;
- l'identificativo messaggio.

Questi dati (di certificazione) sono inseriti in un file XML che accompagna sempre le ricevute, le buste e gli avvisi sotto riportati. Il file XML contiene tutti i dati utili, in formato direttamente elaborabile, da parte del ricevente la ricevuta, la busta o l'avviso.

Un sistema di Posta Elettronica Certificata nel corso dello svolgimento del processo genera, dunque, ricevute, buste e avvisi. Tecnicamente si tratta di messaggi, firmati con la firma (elettronica) del gestore che li ha generati.

Tali messaggi sono:

- Ricevuta di accettazione - La ricevuta di accettazione è un messaggio di posta elettronica inviato al mittente dal proprio gestore all'atto della ricezione al punto di accesso del messaggio che il mittente intende inviare. Esso contiene la data ed l'ora di accettazione, i dati del mittente e del/i destinatario/i, l'oggetto del messaggio ed il suo identificativo. La ricevuta di accettazione è firmata dal gestore. Il corpo del messaggio della ricevuta è composto da un testo in formato leggibile, secondo il seguente schema:

“Ricevuta di accettazione.

Il giorno (data) alle ore (ora e fuso orario) il messaggio (oggetto del messaggio) proveniente da (mittente) e indirizzato a (elenco dei destinatari con gli indirizzi di Posta Elettronica, certificata o meno) è stato accettato dal sistema ed inoltrato. L'identificativo del messaggio è: (identificativo).”

La ricevuta può contenere ulteriori informazioni e/o allegati a fronte di specifiche funzionalità offerte dal gestore di Posta Certificata.

- Busta di trasporto - La busta di trasporto è un messaggio generato dal gestore del mittente, che contiene il messaggio originale con i relativi dati di certificazione.

La busta è sottoscritta con la firma del gestore di Posta Elettronica Certificata del mittente.

Il gestore del mittente genera una busta per ogni gestore cui i destinatari fanno capo.

Il corpo della busta di trasporto è composto da un testo che costituisce la parte immediatamente leggibile dal destinatario del messaggio di Posta Certificata secondo il seguente schema:

“Messaggio di posta certificata.

Il giorno (data) alle ore (ora e fuso orario) il messaggio (oggetto del messaggio) è stato inviato da (mittente) e indirizzato (elenco dei destinatari con gli indirizzi di Posta Elettronica, certificata o meno).

Il messaggio originale è incluso in allegato.

L'identificativo del messaggio è: “(identificativo).”

La busta può contenere ulteriori informazioni e/o allegati a fronte di specifiche funzionalità offerte dal gestore di PEC.

- Ricevuta di presa in carico - Quando un messaggio di Posta Elettronica Certificata passa dal dominio del mittente al dominio del destinatario, il gestore di quest'ultimo emette una ricevuta di presa in carico nei confronti del gestore del mittente.

Questa ricevuta attesta l'avvenuta presa in carico del messaggio da parte del dominio di Posta Certificata di destinazione.

Nella ricevuta di presa in carico sono inseriti i dati di certificazione per consentirne l'associazione con il messaggio a cui si riferisce ed è firmata dal gestore del destinatario.

Oltre ai dati di certificazione sono elencati i destinatari cui la stessa fa riferimento. A fronte di un messaggio preso in carico, ogni gestore dei destinatari dovrà emettere una o più ricevute di presa in carico relative ai destinatari di propria competenza.

L'insieme di tali ricevute coprirà, in assenza di errori di trasporto, il complessivo dei destinatari del messaggio.

Il corpo del messaggio di ricevuta è composto da un testo in formato leggibile, secondo il seguente schema:

“Ricevuta di presa in carico.

Il giorno (data) alle ore (ora e fuso orario) il messaggio (oggetto del messaggio) proveniente da (mittente) e indirizzato a (elenco dei destinatari con gli indirizzi di Posta Elettronica, Certificata o meno) è stato accettato dal sistema.

L'identificativo messaggio è: (identificativo).”

La ricevuta può contenere ulteriori informazioni e/o allegati a fronte di specifiche funzionalità offerte dal gestore di Posta Certificata.

- Busta di anomalia - Nel caso in cui uno dei test che il gestore del destinatario è tenuto ad eseguire evidenzia un errore nel messaggio in arrivo, oppure quest'ultimo sia un mes-

saggio di posta elettronica ordinaria e il gestore ne preveda, comunque, l'inoltro al destinatario, il messaggio è inserito in una busta di anomalia, sottoscritta con la firma del gestore stesso.

Nella busta è inserito un messaggio che evidenzia l'errore riscontrato ovvero che il messaggio trasportato non è di PEC. Il corpo della busta di anomalia è composto da un testo che costituisce la parte immediatamente leggibile dal destinatario del messaggio di Posta Certificata secondo il seguente schema:

“Anomalia nel messaggio.

Il giorno (data) alle ore (ora e fuso orario) è stato ricevuto il messaggio (oggetto del messaggio) proveniente da (mittente) e indirizzato a (elenco dei destinatari con gli indirizzi di Posta Elettronica, certificata o meno).

Tali dati non sono stati certificati per il seguente errore: (descrizione sintetica dell'errore riscontrato).

Il messaggio originale è incluso in allegato.

L'identificativo del messaggio è: “(identificativo).”

Nella busta di anomalia non sono inseriti allegati oltre al messaggio pervenuto al punto di ricezione (es. dati di certificazione) data l'incertezza sull'effettiva provenienza/correttezza del messaggio.

- Avviso di non accettazione – Questo avviso è emesso dal gestore del mittente quando non è in grado di procedere all'inoltro del messaggio a causa del mancato superamento dei controlli formali che è tenuto ad eseguire.

Esso è sottoscritto con la firma del gestore e porta la motivazione per cui non è possibile accettare il messaggio ed esplicita che il messaggio non potrà essere consegnato al/i destinatario/i.

Il corpo del messaggio di questa ricevuta è composto da un testo in formato leggibile, secondo il seguente schema:

“Errore nell'accettazione del messaggio.

Il giorno (data) alle ore (ora e fuso orario) nel messaggio (oggetto del messaggio) proveniente da (mittente) e indirizzato a (elenco dei destinatari con gli indirizzi di Posta Elettronica, certificata o meno) è stato rilevato un problema che ne impedisce l'accettazione a causa di (descrizione errore).

Il messaggio non è stato accettato.

L'identificativo del messaggio è: (identificativo).”

La ricevuta può contenere ulteriori informazioni e/o allegati a fronte di specifiche funzionalità offerte dal gestore di Posta Certificata, in nessun caso, però, può esservi inserito il messaggio originale.

- Avviso di mancata consegna - Nel caso in cui il gestore del mittente, entro le dodici ore successive all'inoltro del messaggio, non abbia ricevuto dal gestore del destinatario la ricevuta di presa in carico, o di avvenuta consegna, del messaggio inviato comunica al mittente l'eventualità che il messaggio possa non essere consegnato.

Tale comunicazione è effettuata mediante un avviso di mancata consegna per superamento dei tempi massimi, sottoscritto con la Firma del gestore.

Il corpo del messaggio di questo avviso è composto da un testo in formato leggibile, secondo il seguente schema:

“Avviso di mancata consegna.

Il giorno (data) alle ore (ora e fuso orario) il messaggio (oggetto del messaggio) proveniente da (mittente) e destinato all'utente (destinatario) non è stato consegnato nelle

prime dodici ore dal suo invio. Non escludendo che questo possa avvenire in seguito, si ritiene utile considerare che l'invio del messaggio potrebbe non andare a buon fine. Il sistema provvederà comunque ad inviare un ulteriore avviso di mancata consegna se nelle prossime dodici ore non vi sarà la conferma della ricezione da parte del destinatario. L'identificativo del messaggio è: (identificativo).”

L'avviso può contenere ulteriori informazioni e/o allegati a fronte di specifiche funzionalità offerte dal gestore di Posta Certificata, in nessun caso, però, vi è inserito il messaggio originale.

Se, entro le successive dodici ore, al gestore del mittente non sia pervenuta la ricevuta di avvenuta consegna del messaggio inviato, questi inoltra al mittente un ulteriore avviso relativo alla mancata consegna del messaggio entro le 24 e non prima delle 22 ore successive all'invio.

- Avvisi conseguenti il rilevamento di virus informatici - Così come prescritto dall'Articolo 12 (Virus informatici) del DPR 11 febbraio 2005 n. 68, sia il gestore del mittente sia quello del destinatario hanno l'obbligo di verificare che i messaggi di posta elettronica da loro trattati non contengano virus informatici.

I gestori hanno l'obbligo, in tal evenienza, di non accettare il messaggio o di non inoltrarlo (a seconda della situazione), di informare tempestivamente chi lo ha inviato e di conservarlo almeno per trenta mesi.

Possono, pertanto, essere generati i seguenti avvisi.

- Avviso di non accettazione per virus informatico. Nel caso in cui sia il gestore del mittente ad individuare un messaggio con virus informatici questi avviserà il mittente stesso con una chiara comunicazione riportante i motivi che hanno causato il rifiu-

to del messaggio. Il corpo del messaggio di questo avviso è composto da un testo in formato leggibile, secondo il seguente schema:

“Errore nell'accettazione del messaggio per presenza di virus.

Il giorno (data) alle ore (ora e fuso orario) nel messaggio (oggetto del messaggio) proveniente da (mittente) e destinato a (elenco dei destinatari con gli indirizzi di Posta Elettronica, certificata o meno) è stato rilevato un problema di sicurezza (identificativo del tipo di contenuto rilevato).

Il messaggio non è stato accettato.

L'identificativo del messaggio è: (identificativo).”

L'avviso può contenere ulteriori informazioni e/o allegati a fronte di specifiche funzionalità offerte dal gestore di Posta Certificata, in nessun caso vi è inserito il messaggio originale.

- Avviso di rilevazione virus informatico. Qualora sia il gestore del destinatario a ricevere un messaggio di Posta Elettronica Certificata con virus informatici, ne accerta la provenienza, tramite la verifica della Firma del gestore del mittente e lo informa tempestivamente affinché comunichi al mittente l'impossibilità di dar corso alla trasmissione.

Ciò avviene tramite un avviso di rilevazione virus. Nel corpo del messaggio deve essere specificato il motivo per il quale è stato impossibile dar corso alla trasmissione.

Il corpo del messaggio di questo avviso è composto da un testo, in formato leggibile, secondo il seguente schema:

“Avviso di rilevazione virus informatico.

Il giorno (data) alle ore (ora e fuso orario) nel messaggio (oggetto del messaggio) proveniente da (mittente) e destinato all'utente (destinatario) è stato rilevato un problema di sicurezza (identificativo del tipo di contenuto rilevato).

L'identificativo del messaggio è: (identificativo).”

- Avviso di mancata consegna per virus informatico. All'arrivo di un avviso di rilevazione di virus informatico da parte del gestore del destinatario, il gestore del mittente, sulla base dell'avviso ricevuto, emette un avviso di mancata consegna da restituire al mittente. Il corpo del messaggio di questo avviso è composto da un testo, in formato leggibile, secondo il seguente schema:

“Avviso di mancata consegna per virus.

Il giorno (data) alle ore (ora e fuso orario) nel messaggio (oggetto del messaggio) destinato all'utente (destinatario) è stato rilevato un problema di sicurezza (identificativo del tipo di contenuto rilevato).

Il messaggio non è stato consegnato.

L'identificativo del messaggio è: (identificativo).”

Un discorso a parte meritano le ricevute di avvenuta consegna, non solo per la loro importanza, ma anche perché possono essere strutturate in vario modo con conseguenti differenti comportamenti per il mittente.

La ricevuta di avvenuta consegna è uno degli aspetti chiave della Posta Elettronica Certificata ed è fatta pervenire al mittente, sot-

toscritta con la firma del gestore del destinatario, al momento in cui il messaggio entra nella disponibilità del destinatario, ossia quando è inserito nella casella di Posta Elettronica Certificata del destinatario⁵. La ricevuta di avvenuta consegna è emessa, nel formato richiesto dal mittente, per ognuno dei destinatari a cui è consegnato il messaggio.

Essa può essere completa, breve o sintetica.

- Ricevuta completa di avvenuta consegna – La ricevuta completa di avvenuta consegna è emessa per ognuno dei destinatari a cui è consegnato il messaggio.

Il corpo del messaggio della ricevuta è composto da un testo, in formato leggibile, secondo il seguente schema:

“Ricevuta di avvenuta consegna.

Il giorno (data) alle ore (ora e fuso orario) il messaggio (oggetto del messaggio) proveniente da (mittente) e indirizzato a (destinatario) è stato consegnato nella casella di destinazione.

L'identificativo del messaggio è: (identificativo).”

La ricevuta può contenere ulteriori informazioni e/o allegati a fronte di specifiche funzionalità offerte dal gestore di Posta Certificata.

Nel rilascio delle ricevute di avvenuta consegna, è effettuata una distinzione tra i messaggi consegnati

⁵ Si ricorda, a questo proposito, quanto stabilito dal comma 2 dell'Articolo 45 (Valore giuridico della trasmissione) del Codice dell'amministrazione digitale: “Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore”.

ai destinatari primari e a quelli in copia.

Il messaggio originale completo (header, testo ed eventuali allegati) è inserito all'interno della ricevuta di avvenuta consegna solo se relativo ai destinatari primari.

- Ricevuta breve di avvenuta consegna - Il mittente può richiedere la ricevuta di avvenuta consegna in formato breve. Nella ricevuta di avvenuta consegna breve è sempre allegato il messaggio originale, ma gli eventuali allegati sono sostituiti con le loro impronte; ciò ha principalmente lo scopo di ridurre le dimensioni della ricevuta stessa.

Attenzione: al fine di rendere possibile la verifica dei contenuti trasmessi è “indispensabile” che il mittente conservi immutati (così come sono stati spediti) gli allegati, inseriti nel messaggio originale, a cui le impronte fanno riferimento.

Il corpo del messaggio della ricevuta è composto da un testo, in formato leggibile, secondo il seguente schema:

“Ricevuta breve di avvenuta consegna

Il giorno (data) alle ore (ora e fuso orario) il messaggio (oggetto del messaggio) proveniente da (mittente) e indirizzato a (destinatario) è stato consegnato nella casella di destinazione.

L'identificativo del messaggio è: (identificativo).”

La ricevuta è emessa per ognuno dei destinatari a cui è consegnato il messaggio.

Nel caso in cui il messaggio originale sia stato originato in formato S/MIME è effettuata un'ulteriore analisi del formato.

Questo formato consente, infatti, di cifrare, firmare il messaggio o fare entrambe le cose.

Nel caso il mittente abbia firmato il messaggio questo si presenta in due parti: la prima è quella che è stata generata prima della firma e successivamente firmata, la seconda comprende i dati aggiunti nel processo di firma. In questa situazione gli allegati possono essere sostituiti dalle relative impronte, ma si deve tener conto che, a causa della sostituzione degli allegati con le impronte, il messaggio genererà un errore in un'eventuale fase di verifica dell'integrità della firma. Se il messaggio è stato cifrato, data l'impossibilità di analizzare la sua originale struttura e distinguere il testo dagli eventuali allegati, la ricevuta breve avrà gli stessi contenuti della normale ricevuta di avvenuta consegna.

- Ricevuta sintetica di avvenuta consegna – Questa ricevuta non prevede l'invio del messaggio originale ed è identica sia per i destinatari primari sia per quelli in copia. Il corpo del messaggio della ricevuta è composto da un testo, in formato leggibile, secondo il seguente schema:

“Ricevuta sintetica di avvenuta consegna.

Il giorno (data) alle ore (ora e fuso orario) il messaggio (oggetto del messaggio) proveniente da (mittente) e indirizzato a (destinatario) è stato consegnato nella casella di destinazione.

L'identificativo del messaggio è: (identificativo).”

La ricevuta può contenere ulteriori informazioni e/o allegati a fronte di specifiche funzionalità offerte dal gestore di Posta Certificata.

4. Lo schema di funzionamento

Tutti gli eventi (generazione di ricevute, buste di trasporto, log, ecc.) che si succedono nel processo dall'accettazione alla consegna del messaggio di Posta Elettronica Certificata presso i punti di accesso, ricezione e consegna devono fare riferimento allo stesso, univoco, accurato ed affidabile riferimento temporale.

La risoluzione del riferimento è al minuto secondo.

I riferimenti temporali forniti dal servizio di PEC (in chiaro nel testo delle ricevute, buste di trasporto, ecc.) devono fare riferimento al tempo UTC e indicare la differenza tra quest'ultima e l'ora legale vigente.

In questa prima fase si considera il caso in cui mittente e destinatario dispongano entrambi di una casella di PEC.

Nel caso più generale, i due soggetti faranno riferimento a due differenti gestori; se così non fosse il processo sostanzialmente non cambia.

Il mittente predispone (o ha già predisposto) eventuali documenti informatici che diventeranno gli allegati del messaggio di PEC che si accinge ad inviare.

Un messaggio PEC, come per tutti gli strumenti di posta elettronica, oltre a poter esso stesso contenere informazioni nel suo testo (essere anch'esso un documento) è anche un vettore di documenti che possono avere qualunque formato ed, eventualmente, essere sottoscritti elettronicamente o cifrati.

Una volta generato il messaggio di posta, con gli eventuali allegati, il mittente si collega al proprio gestore di PEC nelle modalità previste, e concordate, e si fa riconoscere: la modalità più diffusa è quello che prevede la copia identificativo (codice

utente/user ID) e codice segreto (password), ma sono possibili altre modalità più sofisticate e sicure che si basano, ad esempio, sull'impiego di smartcard (ad esempio, la CNS).

Su richiesta i gestori possono garantire un secondo livello di autenticazione quale ad esempio la digitazione del codice generato da un Token crittografico o da una sequenza di caratteri corrispondenti a quelle individuabili dall'incrocio delle coordinate proposte dal sistema che fanno riferimento ad una tabella consegnata dal gestore all'utente (vedasi Tabella II).

	1	2	3	4	5	6	7	8	9	10
A	A	F	I	D	D	O	L	U	I	Y
B	Q	5	F	I	E	C	Z	9	J	O
C	3	C	S	V	I	O	X	G	A	S
D	E	H	E	7	A	K	C	0	N	2
E	N	O	1	N	O	E	R	V	E	W

Tabella II. Esempio di tabella consegnata all'utente per un secondo livello di identificazione.
(Alla proposta delle coordinate B9, D1, D5 l'utente dovrà digitare "JEA")

Il collegamento può avvenire utilizzando l'abituale Client di posta elettronica adottato dal mittente o direttamente tramite Internet con un semplice Web Browser. Il messaggio è così inviato al punto di accesso del proprio gestore (Figura 1, passo 1).

Il gestore, ricevuto il messaggio effettua, come previsto, tutta una serie di controlli "formali" e, nel caso non riscontri alcuna anomalia, (Figura 1, passo 2) predispone una ricevuta di accettazione nella quale inserisce il messaggio così come gli è stato trasmesso dal mittente, la firma elettronicamente e la restituisce al mittente.

Questa operazione serve anche a proteggere da eventuali modifiche il messaggio appena inviato.

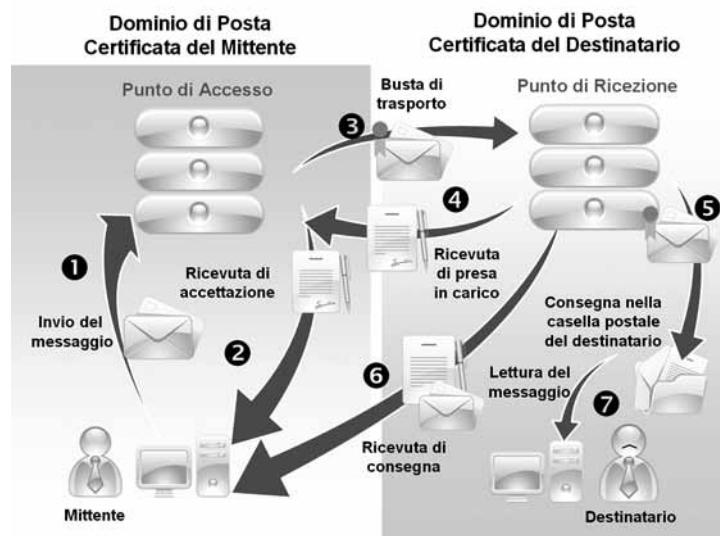


Figura 1. Scambio di messaggi tra due domini di Posta Elettronica Certificata (passi da 1 a 7)

Qualora il gestore del mittente rilevi irregolarità formali, o la presenza di virus informatici, provvederà ad inviare al mittente rispettivamente un avviso di non accettazione (con le relative motivazioni) o un avviso di non accettazione per virus informatico. Il processo qui si arresta.

Il gestore, nel caso rilevi virus nella posta inoltratagli non solo è tenuto a non inoltrarla, ma deve provvedere a conservarla almeno per trenta mesi.

Accettato il messaggio, il gestore del mittente provvede ad inviare lo stesso al punto di ricezione del gestore del destinatario. Per fare ciò si avvale di una busta di trasporto (Figura 1, passo 3).

Il gestore del destinatario, al ricevimento della busta, effettua tutta una serie di controlli per verificare, tra l'altro, la corretta

provenienza (da un gestore PEC riconosciuto) nonché l'integrità del messaggio ricevuto e l'assenza di virus informatici.

Il punto di ricezione informa, quindi, il gestore del mittente del corretto trasferimento del messaggio e dalla sua presa in carico ritornandogli una ricevuta di presa in carico (Figura 1, passo 4).

Nel caso in cui, nello svolgere i dovuti controlli, il gestore del destinatario rilevi nel messaggio appena ricevuto dei virus informatici arresta il processo di invio del messaggio e ne informa tempestivamente, con un avviso di rilevazione virus, il gestore del mittente, affinché quest'ultimo possa comunicare al mittente del messaggio l'impossibilità di procedere con la trasmissione. Il mittente sarà, dunque informato di quanto avvenuto tramite un avviso di mancata consegna per virus informatico.

Il gestore del destinatario può procedere, a questo punto, a depositare il messaggio nella casella postale a disposizione del destinatario (Figura 1, passo 5) che, da questo momento, è in grado di prenderne visione (Figura 1, passo 7) come farebbe nel caso di un sistema di posta elettronica tradizionale.

Quale ultimo atto del processo, il gestore destinatario provvede ad inviare la prevista ricevuta di avvenuta consegna al mittente (Figura 1, passo 6).

È questa ricevuta che prova che il messaggio inviato sia stato ricevuto (= depositato nella casella del destinatario corrispondente all'indirizzo telematico da questi dichiarato).

È importante ricordare che il sistema di PEC, essendo un sistema di posta elettronica, non prevede l'effettiva lettura del messaggio quale prova della sua avvenuta consegna: così come precedentemente chiarito a proposito delle ricevute di avvenuta consegna, il messaggio si intende consegnato quando è reso disponibile nella casella di posta elettronica del destinatario.

Il processo appena sommariamente descritto non si modifica nella sostanza nel caso in cui mittente e destinatario appartenano allo stesso dominio di Posta Elettronica Certificata, anzi si semplifica in quanto non saranno effettuati i trasferimenti⁶ di cui ai passi 3 e 4 della figura 1 con tutte le attività conseguenti.

Una mail di PEC può essere, anche, indirizzata ad un indirizzo non appartenente ad un dominio PEC.

In questa situazione (Figura 2) i primi tre passi avvengono come precedentemente descritto; il provider del destinatario, però non è in grado di analizzare la busta di trasporto che riceve ed è costretto a consegnarla, così come la ha ricevuta, nella casella postale del destinatario che sarà, comunque, in grado di prendere visione del messaggio e dei suoi allegati.

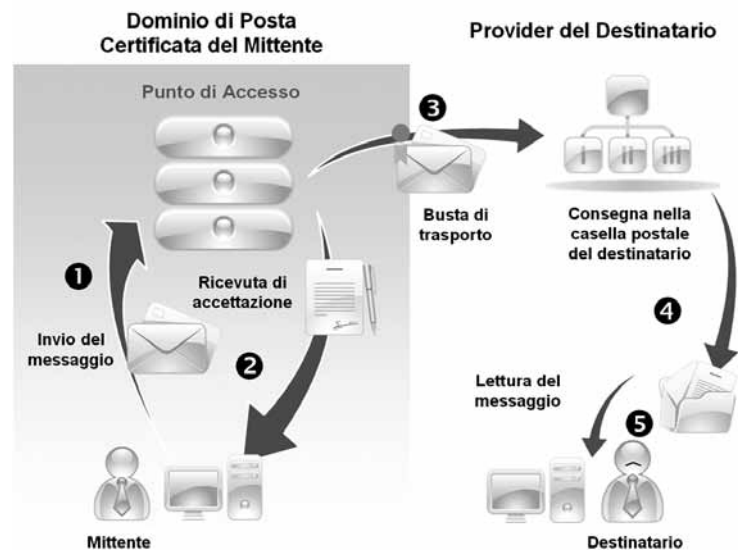


Figura 2. Scambio di messaggi tra un dominio di Posta Elettronica Certificata e un destinatario che non possiede una Casella di PEC

⁶ L'elaborazione dei messaggi di posta certificata (ricevute utente, messaggi di trasporto, ecc.) deve avvenire anche nel caso che mittente e destinatario appartengano allo stesso dominio.

Può, evidentemente, presentarsi il caso che un messaggio di posta elettronica tradizionale/ordinaria sia inviato ad un indirizzo di PEC (Figura 3).

L'accettazione di un messaggio di posta elettronica tradizionale è a discrezione del gestore di Posta Elettronica Certificata del destinatario.

Le modalità con cui sono gestiti tali messaggi devono essere comunicate all'utente di PEC.

In generale al momento del ricevimento di un messaggio di posta elettronica tradizionale il punto di ricezione genererà una busta di anomalia, contenente il messaggio originale ricevuto, che consegnerà nella casella postale del destinatario.

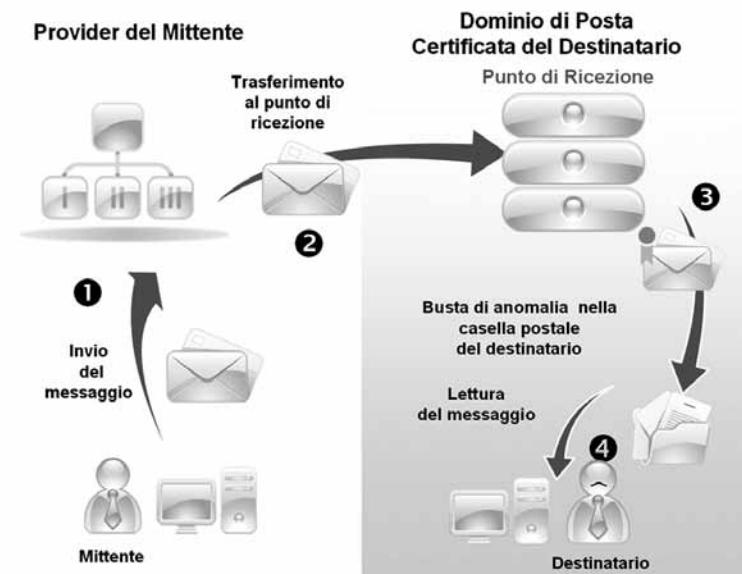


Figura 3. Invio di un messaggio di posta elettronica tradizionale ad un destinatario in un dominio di Posta Elettronica Certificata

5. Statistiche

Nel suo Marketing Consumer Report 2010, Contactlab valuta in 62 milioni le caselle di posta elettronica utilizzate in Italia, con un corrispondente traffico giornaliero di circa 560 milioni di messaggi.

Contactlab stima, inoltre, che ogni utente disponga in media 2,5 caselle di posta elettronica. Si può, pertanto ragionevolmente ipotizzare che, nel nostro Paese, i singoli utenti di posta elettronica siano circa 25 milioni ed essi ricevano ogni giorno, mediamente, 23 messaggi (messaggi indesiderati compresi).

A fronte di questi volumi come si posiziona attualmente la diffusione e l'impiego della Posta Elettronica Certificata?

Nel fare il confronto bisogna tenere conto che la PEC è utilizzata per esigenze reali di comunicazione (formale) e non è certo utilizzata per attività di marketing, per scambio di informazioni personali, per fare spam o per altre attività illecite.

Così come richiesto dalla Circolare del CNIPA del 7 dicembre 2006, ogni gestore di PEC comunica ogni due mesi a DigitPA (prima CNIPA) una certa serie di informazioni tra le quali sono il numero di caselle per ogni dominio di PEC ed il numero totale di messaggi che hanno coinvolto le caselle gestite. In Tabella III sono riportati i più recenti di tali dati.

Periodo	N° domini	N° caselle	N° messaggi
Gennaio Febbraio 2010	115.995	2.340.848	52.818.441
Marzo Aprile 2010	88.310	1.686.958	55.956.190
Maggio Giugno 2010	95.912	1.850.958	71.274.138
Marzo-Aprile 2011	122.987	2.534.097	54.518.176
Maggio-Giugno 2011	130.203	2.643.147	54.487.937

Tabella III. Comunicazioni del gestore di PEC

Raffrontati con i dati sopra riportati, relativi alla posta elettronica ordinaria, si vede che il numero delle caselle di PEC è di poco superiore al 10% del numero di singoli utenti di posta elettronica ordinaria, mentre il rapporto tra il numero di messaggi coinvolti è di circa il 4 % dei messaggi utili di posta elettronica ordinaria (che, per omogeneità di confronto si sono stimati nel 40% circa del volume totale di traffico); in altre parole una casella di PEC riceve, oggi, poco più di un messaggio ogni tre giorni.

Anche se l'impiego della PEC è uno strumento molto “giovane” e, per sua stessa concezione, limitato alle comunicazioni di tipo “formale”, l'attuale adozione sembra abbastanza limitata. Esso è, peraltro, un sistema chiuso: il valore probatorio della trasmissione e della ricezione di un messaggio tramite PEC si realizza solo se entrambi gli attori (mittente e destinatario) appartengono al sistema stesso (dispongono di una casella PEC).

Si aggiunga il fatto che è un sistema praticamente applicabile al solo territorio nazionale e che, per precisa disposizione inserita nella sua norma costitutiva, la PEC non può (ancora) essere impiegata⁷ in importanti procedimenti quali quelli del processo amministrativo, del processo tributario e del processo dinanzi alle sezioni giurisdizionali della Corte dei conti. Altro elemento che in qualche modo potrebbe frenarle l'adozione potrebbero essere il limite ancora abbastanza diffuso alle dimensioni dei messaggi.

Se da un lato, poi, la sua peculiare caratteristica di rendere sicuro ed opponibile un qualunque flusso comunicativo la può rendere una “piattaforma” sulla quale realizzare utili applicazioni, dall'altro il suo impiego limitato fa da freno all'individuazione e alla realizzazione di applicazioni che possono trarre vantaggio dalla sua adozione.

⁷ DPR del 11 febbraio 2005 n. 68, Articolo 15, comma 4.

Pur essendo un sistema chiuso è, anch'esso, soggetto alle leggi che regolano il valore dei sistemi di comunicazione, in particolare vale la regola che “il valore di un sistema di comunicazione cresce con il quadrato del numero di “persone/nodi” collegati”⁸.

Appare evidente, quindi, che solo una sua più capillare diffusione (in termini sia di numero di soggetti che la utilizzano sia di applicazioni che inducono vantaggi impiegandola) renderà veramente efficace lo strumento in questione. In questa direzione vanno tutte le iniziative normative sostenute, peraltro, da una precisa volontà politica.

Basti pensare all'obbligo di dotarsi di una casella di Posta Elettronica Certificata per professionisti e imprese⁹ nonché alla possibilità per il cittadino di disporre a titolo gratuito di una casella di PEC.

Queste norme avrebbero potuto essere più efficaci, in particolare l'ultima, ma l'indiscutibile spinta affinché tutte le pubbliche amministrazioni dialoghino tra loro e con i cittadini e le imprese in modalità digitale sono sicuramente un importante elemento che contribuisce alla diffusione dell'impiego della PEC: non solo la maggior parte delle comunicazioni suddette rivestono un carattere formale, ma sono, in quantità molto rilevanti e coinvolgono tutti i soggetti, il diffondersi della digitalizzazione, infine, tende a far crescere il numero delle applicazioni che potranno essere interessate (vedasi, usa per tutte, ad esempio la fatturazione elettronica).

⁸ Legge di Metcalfe.

⁹ Il potenziamento, in termini di numero di Caselle PEC, di queste due categorie è di circa 2.000.000 per i professionisti e oltre 2.710.000 per le imprese (quelle costituite in forma societaria). Con riferimento a queste ultime, a fine luglio le caselle di PEC presenti nel Registro delle Imprese erano di poco superiori alle 350.000, l'87% circa delle quali corrisponde ad aziende costituite dopo il 29 novembre 2008 per le quali vi è l'obbligo di comunicare al Registro un indirizzo PEC all'atto della costituzione.

Un altro fattore che potrebbe facilitarne la diffusione sarebbe la disponibilità e la facile accessibilità ad un'anagrafe¹⁰ degli indirizzi “ufficiali” di PEC dei singoli soggetti. Il problema però non è di facile soluzione per i problemi di privacy che lo caratterizza.

A solo titolo di proposta/provocazione positiva vorrei semplicemente ricordare che così come, nell'impiego della PostaCertificat@, si può accedere in sicurezza per cittadini e pubbliche amministrazioni ai rispettivi indirizzi PEC (l'accesso è monitorato dal fatto che la richiesta può essere fatta per indirizzi singoli e da una casella “controllabile”) perché non pensare all'istituzione di un'anagrafe nazionale accessibile tramite i gestori PEC?

6. L'offerta

Come visto, attualmente sono 25 i gestori di Posta Elettronica Certificata: apparentemente molti per le attuali dimensioni del mercato.

L'offerta attuale è abbastanza diversificata ed il costo varia in funzione sia delle strategie di mercato dei singoli gestori, sia dei servizi standard e/o aggiuntivi offerti.

Le caselle offerte possono andare da circa 30, 50 o 100 Mbyte per i privati e da 1 Gbyte a 10 Gbyte, e oltre, per le aziende.

In genere questo spazio, a parte per quelle di minor dimensione, è suddiviso in spazio a disposizione della casella vera e propria e in spazio da dedicare all'archiviazione sicura delle email che

¹⁰ Per quanto riguarda le imprese si può ottenere l'indirizzo PEC dal Registro delle Imprese (<http://www.registroimprese.it/>) con una semplice interrogazione. Per evitare indesiderate acquisizioni automatiche di massa di tali indirizzi è anche prevista, individuata l'impresa che interessa, l'inserimento di un codice di sicurezza suggerito dall'applicazione stessa.

può non essere presente per le disponibilità minori in termini di spazio; esempi possono essere: 2 Gbyte (di cui 1 per la casella e 1 per l'archiviazione), 5 Gbyte (di cui 2 per la casella e 3 per l'archiviazione), 10 Gbyte (di cui 2 per la casella e 8 per l'archiviazione).

Tra i servizi aggiuntivi normalmente offerti sono la disponibilità di funzioni antivirus e antispam, la ricezione di email da domini non di posta certificata, l'accesso al servizio via client o via Web, la notifica di ricezione di un messaggio di posta certificata con SMS e/o tramite email ordinaria.

Tra le funzionalità non offerte da tutti i gestori, da richiedersi se previste in aggiunta all'offerta prescelta o disponibili solo per le offerte più complete e onerose, sono le possibilità di stabilire filtri e regole sui messaggi, di inoltrare automaticamente la posta ricevuta ad altra mail, di attuare del mass mailing e di disporre di report sull'impiego della casella.

Alcuni gestori offrono per i "pacchetti" più completi anche un servizio di gestione delle caselle, a carico di un amministratore, con il quale si possono, ad esempio, creare nuove caselle, cancellare caselle, assegnare lo spazio disco agli utenti e modificare le password.

Vi sono, poi, gestori in grado di completare la propria offerta con la possibilità di apporre al messaggio una firma digitale o una firma elettronica qualificata, di cifrare il messaggio e di conservare a norma la corrispondenza, degli avvisi e delle ricevute.

Per quanto concerne l'identificazione del domino di Posta Elettronica Certificata tutti i gestori offrono come standard il dominio fisso (@dominiogestore.it), è anche possibile disporre di un sottodominio del gestore (@nomecliente.dominiogestore.it); per il nome di dominio può anche essere utilizzato un proprio dominio nella forma @pec.dominiocliente.it.

Dal punto di vista dei costi¹¹ la situazione è ancora più complessa in quanto, oltre a tenere conto delle funzionalità offerte sono da tenere in considerazione le offerte di "pacchetti" che, oltre a differenti mix di funzioni e di spazio offerti, possono prevedere impegni pluriennali, più caselle o rivolgersi a target specifici (categorie di professionisti ad esempio).

Con il solo obiettivo di dare degli ordini di grandezza si riporta che il costo annuo di una casella di PEC può variare da 5,00 a 80,00 Euro (dove la principale discriminante è data dallo spazio a disposizione, ma influiscono anche i servizi offerti in modo standard e gli impegni pluriennali).

Sempre per fornire ordini di grandezza, un dominio personalizzato può costare dai 100,00 ai 500,00 Euro mentre la conservazione a norma può essere fatturata a circa 500,00 Euro per Gbyte l'anno.

¹¹ I valori di costo indicati si intendono al netto di IVA.

Capitolo II

Vantaggi e svantaggi

1. Introduzione

La Posta Elettronica Certificata nasce, in un momento storico che vede l'ineludibile passaggio dalla carta al digitale (con tutto ciò che ne consegue), per offrire una valida e più efficace alternativa alla raccomandata, in particolare a quella con avviso di Ricevimento.

La PEC, infatti, offre garanzia di integrità di ciò che è stato spedito e ricevuto; le ricevute di avvenuta consegna, inoltre, non solo danno la certezza al mittente che il destinatario ha ricevuto esattamente quanto spedito, ma sono una prova opponibile a terzi¹².

Il processo di PEC, infine, è tracciato con un riferimento temporale affidabile nella registrazione di tutti gli eventi che lo compongono, riferimento che è a tutti gli effetti una validazione temporale (riferimenti temporali opponibili ai terzi)¹³.

Va evidenziato che la Posta Elettronica Certificata non garantisce l'autenticità¹⁴ di ciò che è stato spedito; per ottenere questa garanzia i documenti spediti devono essere sottoscritti con firma digitale o firma elettronica qualificata.

¹² Articolo 48 - Posta Elettronica Certificata del Codice dell'amministrazione digitale.

¹³ Articolo 37, comma 4, punto c) del Decreto del Presidente del Consiglio dei Ministri del 30/03/2009 - Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici (Pubblicato nella Gazzetta Ufficiale n. 129 del 06/06/2009).

¹⁴ Caratteristica che garantisce che un documento è ciò che dichiara di essere senza aver subito alterazioni o modifiche.

La PEC, dunque, è un sistema di “trasporto” che assicura, trasporto, ricezione, integrità, ..., ma non aggiunge autenticità a ciò che ha trasportato.

La tradizionale raccomandata AR, dal canto suo, ha sì la possibilità di provare la spedizione, la ricezione, ma non che ci sia il contenuto che si dichiara di aver spedito (ad esempio la busta può esser vuota).

Altra cosa da chiarire è che un messaggio di PEC non è detto che dia garanzia sull'identità del mittente.

Ciò è sicuramente vero per una raccomandata tradizionale e lo è anche per una email convenzionale: chiunque potrebbe configurare il proprio client di posta per far figurare che sia stata spedita da `chidicoio@suoserver.it`.

Nel caso di una casella di PEC quanto sopra non è possibile, ma vi è da prendere in esame una serie di situazioni.

Il gestore generalmente non identifica il mittente al momento dell'assegnazione di una casella di Posta Elettronica Certificata e si limita, al momento dell'accesso al servizio, a verificare che il messaggio sia inviato da un utente abilitato al servizio, ma non controlla che il mittente specificato nel messaggio che è inviato sia congruente con i dati di identificazione forniti.

Molte caselle di PEC, inoltre, sono di gruppo, assegnate pertanto ad una azienda, ad una funzione, ad una amministrazione, ecc.; in questo caso si può essere sufficientemente certi che il messaggio sia stato spedito da un appartenente a quel gruppo e, comunque, si può ipotizzare che tale azienda, funzione, amministrazione, ecc. ne risponda.

In questa situazione l'unico controllo possibile è quello di verificare con un'interrogazione al Registro delle Imprese, se azienda,

o sul sito www.indicepa.it, nel caso di una pubblica amministrazione, se tale indirizzo esiste veramente.

Analogamente può essere fatto con gli indirizzi di Posta Elettronica Certificata di professionisti iscritti agli albi od elenchi istituiti con leggi dello Stato.

Nel caso dei professionisti la procedura di rilascio di una casella è, in genere, più controllata: il richiedente è identificato e la richiesta deve essere presentata tramite la compilazione di una domanda, con tutte le informazioni atte ad identificare il soggetto richiedente (persona fisica o soggetto giuridico) al quale sarà assegnata la casella di posta, opportunamente sottoscritta e inviata, se non consegnata personalmente, con raccomandata.

Può essere prevista la sottoscrizione digitale; in questa situazione può essere altresì richiesto che la sottoscrizione sia attuata con lo strumento di firma rilasciato dall'ordine (ciò avviene, ad esempio, nel caso di PEC rilasciata dal Consiglio Nazionale del Notariato).

Questa limitazione potrà essere superata al momento dell'emanazione delle Regole Tecniche richieste al punto c-bis¹⁵ del comma 1 dell'articolo 65 - Istanze e dichiarazioni presentate

¹⁵ 65. Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica.

1. Le istanze e le dichiarazioni presentate alle pubbliche amministrazioni per via telematica ai sensi dell'articolo 38, commi 1 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, sono valide:

[...]

c-bis) ovvero se trasmesse dall'autore mediante la propria casella di posta elettronica certificata purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite con regole tecniche adottate ai sensi dell'articolo 71, e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato. In tal caso, la trasmissione costituisce dichiarazione vincolante ai sensi dell'articolo 6, comma 1, secondo periodo. Sono fatte salve le disposizioni normative che prevedono l'uso di specifici sistemi di trasmissione telematica nel settore tributario.

[...]

alle pubbliche amministrazioni per via telematica del Codice dell'amministrazione digitale.

Come previsto dal citato articolo il gestore deve identificare il titolare della casella di posta prima di rilasciare le credenziali di accesso e deve certificare tale identità in ogni messaggio o in un suo allegato.

In questa situazione sarà, molto probabilmente, rafforzato il modo con cui il titolare potrà accedere al servizio adottando un doppio livello di autenticazione¹⁶.

Si può pensare all'impiego della carta nazionale dei servizi o alla carta d'identità elettronica così come ad un rafforzamento, in termini di sicurezza, dell'uso di user-id e password (magari adeguandosi più rigidamente a quanto stabilito in materia nell'allegato B del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", oppure associando ad essi l'impiego di una password monouso da acquisire, di volta in volta, con modalità già sufficientemente adottate; si può pensare all'utilizzo di un token crittografico rilasciato dal gestore o alla sua trasmissione/ricezione attraverso sistemi di telefonia mobile).

¹⁶ Si parla di autenticazione (riconoscimento) forte (Strong Authentication) quando si fa riferimento a due o più metodi di autenticazione.

Tali metodi si fondano sull'esibizione di informazioni distintive generate da tre differenti sorgenti:

- Qualcosa che si conosce (esempio: una password o il classico codice chiamato PIN),
- Qualcosa che si possiede (in modo esclusivo) come una carta di credito, una CNS, un token crittografico, un telefono cellulare, una lista di codici ricevuti in modo esclusivo e sicuro, ...
- Qualcosa che distingue/individua il soggetto, quali le impronte digitali, l'iride o altre caratteristiche biometriche.

Si parla di autenticazione a due fattori se si utilizzano congiuntamente due delle tipologie di informazioni sopra citate. Ciò rappresenta un metodo più sicuro rispetto alla comune autenticazione basata sulla sola conoscenza di una password.

Le più comuni forme di autenticazione a due fattori adottano "Qualcosa che si conosce" (la classica password, ad esempio) in congiunzione ad un'informazione originata da "Qualcosa che si possiede" (come una "one time password" originata da un token crittografico).

Si può ragionevolmente pensare, infine, che la previsione dell'obbligo di identificazione del titolare di una casella di Posta Elettronica Certificata sopra citato, non introduca una nuova forma di PEC, ma porti ad ampliare i servizi attuali di PEC con l'aggiunta di questa funzionalità.

Si fa rilevare che un messaggio con suddette caratteristiche rappresenta, nei confronti delle pubbliche amministrazioni a tutti gli effetti una firma elettronica avanzata, così come sarà regolata dalle emanande regole tecniche in materia.

2. Confronto con la raccomandata ed altri sistemi di corrispondenza

Le forme di comunicazione che si intende mettere qui a confronto sono: la PEC, la raccomandata con A/R, il fax e l'email tradizionale.

Il metodo più economico tra queste forme di comunicazione è certamente l'email tradizionale il cui costo è praticamente nullo e, se si impiegano le caselle di posta offerte dal mercato (da Google, a Hotmail e altre ancora), di fatto esso si riduce ad una parte del costo fisso del collegamento ad Internet. Ovviamente si può voler disporre di fornitori che mettono a disposizione funzioni più ricche; in questo caso si paga un canone che, comunque, è molto limitato.

Confrontando, sempre dal punto di vista dei soli costi, la PEC con la raccomandata con AR è facile verificare che, dovendo inviare più di qualche raccomandata al mese, la PEC diventa sicuramente più conveniente e ... non si prendono in considerazione in questo momento gli altri vantaggi.

Continuando il confronto con l'email tradizionale la PEC garanti-

sce il valore legale di quanto inviato e l'identificazione certa della casella del mittente (ovviamente se è un'altra casella di PEC); si noti che non si parla di mittente, ma di casella del mittente.

La PEC, inoltre, offre maggiori garanzie nei confronti di spam, phishing e quant'altro.

Passando alla raccomandata i vantaggi che la PEC può vantare sono innanzi tutto la certezza del contenuto trasmesso, i risparmi di costi di spedizione e archiviazione (oltre ai risparmi di tempo) nonché la tracciabilità della casella del mittente (ovviamente se di PEC), ma non sono da sottovalutare la possibilità di invio multiplo, la rapidità (immediatezza) di consegna, la possibilità di invio da qualunque sito che disponga di un collegamento ad Internet ed in qualunque momento.

Per completezza confrontiamo la PEC con il fax.

Il fax è uno strumento ormai abbastanza obsoleto, ma, anche se la tendenza è quella di dismettere sempre più le attrezzature fisiche per l'invio e la ricezione, proprio per la struttura stessa di suddetta strumentazione¹⁷ il modo di generare, trasmettere e ricevere i fax si è nel tempo trasformato in una attività completamente digitale.

Un fax (inteso come documento da trasferire) può essere generato, inviato e ricevuto in modalità completamente digitale, acquisendone pertanto tutte le caratteristiche.

Al fax comunque è riconosciuto valore legale, ha consegna praticamente immediata, in genere si ha la conferma che è stato spedito, ma non si ha la certezza che sia stato ricevuto e, anche

¹⁷ Le apparecchiature fax, sostanzialmente, in input funzionano come uno scanner convertendo il documento cartaceo in immagini digitali che sono trasmesse come tali, tramite linea telefonica, all'unità di output che provvede a stamparle.

se trasmettendo un'immagine si può sostenere che non possa essere alterato, non si può altrettanto essere certi che non possa essere ripudiato.

La semplicità e la comodità d'uso sono un fatto abbastanza relativo, se si pensa alle attrezzature fisiche, ma non è certamente vero se si pensa ai processi completamente digitali, oggi largamente diffusi, che consentono anche l'invio massivo a molti destinatari. Anche la possibilità di inviare un fax da luoghi diversi ed in tempi non obbligati non è totalmente sostenibile.

Resta la struttura dei costi che, anche se i processi si sono digitalizzati, non si è modificata.

La Tabella IV riassume e completa quanto appena illustrato.

	PEC	email	Racc. A/R	fax
Valore Legale	√	=	√	√
Velocità di consegna (immediatezza)	√	√	=	√
Semplicità e comodità d'uso	√	√	=	(√)
Accesso da luoghi diversi ed in tempi non obbligati	√	√	=	=
Possibilità di invii multipli	√	√	=	(√)
Certificazione della Spedizione	√	=	√	√
Ricevuta di Avvenuta Consegna	√	√	√	=
Certezza di cosa è stato consegnato	√	=	=	(√)
Inalterabilità del contenuto del messaggio	√	=	=	√
Non ripudio del messaggio consegnato	√	=	=	(√)
Costo per invio	=	=	√	√
Costo fisso	√	√	=	√

Tabella IV. Caratteristiche di PEC, email, raccomandata A/R e fax

Capitolo III

La PEC nella normativa italiana

1. Introduzione

La posta elettronica, come si è visto, è uno strumento di fatto largamente utilizzato non solo nelle comunicazioni interpersone, ma soprattutto nelle comunicazioni di business (più o meno formali) e nella trasmissione di file e documenti di qualunque tipo ed importanza.

Questo nuovo strumento di comunicazione, se pur affermatissimo, ha una caratteristica peculiare che non si ritrova nelle comunicazioni tradizionali, essendo propria dello strumento in questione: se da un lato esso è uno strumento di trasmissione di documenti, dall'altro può essere esso stesso documento.

Si aggiunga il fatto, non secondario, che con le comunicazioni digitali molto spesso si coinvolgono soggetti non noti l'uno all'altro.

La posta elettronica tradizionale, così come oggi impiegata, ha tutta una serie di "debolezze" quando la si utilizza per scambi di informazioni, specialmente se formali.

Il problema si può schematicamente dividere in due principali capitoli:

1. dare sostanza probatoria al documento che la mail trasmette (sia esso allegato o insito nel testo della stessa);
2. attribuire valore giuridico al sistema di trasmissione (attribuzione certa dell'invio e della ricezione).

Al primo dei problemi citati si è da tempo data una soluzione. Tutta la normativa sul documento informatico - conseguente a quanto stabilito dal comma 2¹⁸ dell'articolo 15 della legge del 15 marzo 1997 n. 59 (la famosa Bassanini 1) - ha consentito, con la sottoscrizione digitale di un documento informatico, di attribuire ad esso la stessa efficacia probatoria di un testo sottoscritto con firma autografa.

Attualmente è il Codice dell'amministrazione digitale che all'articolo 21 stabilisce quanto sopra.

Ciò è vero anche nel caso in cui sia la mail ad essere così sottoscritta, come prescritto dal suddetto articolo 21.

In caso contrario "la sua idoneità a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio"; in parole più semplici, una normale email ha valore di prova solo se colui contro il quale è prodotta ne riconosca la sottoscrizione (in questo caso con firma elettronica "semplice") o non disconosca la conformità al vero di quanto in essa rappresentato.

Con l'introduzione della Posta Elettronica Certificata si è voluto dare soluzione al secondo dei problemi sopra evidenziati: lo stabilisce, infatti, l'articolo 4 al comma 1 del DPR n. 68 del 2005: "La posta elettronica certificata consente l'invio di messaggi la cui trasmissione è valida a tutti gli effetti di legge".

¹⁸ L. 59/1997 - Articolo 15 - Rete unitaria delle pubbliche amministrazioni.
[...]

2. Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge. I criteri e le modalità di applicazione del presente comma sono stabiliti, per la pubblica amministrazione e per i privati, con specifici regolamenti da emanare [...].

2. Il quadro normativo di riferimento

L'istituzione, il funzionamento e la portata giuridica della Posta Elettronica Certificata è normata dalle disposizioni seguenti e dalle loro successive modifiche:

- DPR 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" (pubblicato in Gazzetta Ufficiale n. 97 del 28 aprile 2005);
- Decreto Ministeriale 2 novembre 2005, "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata" (pubblicato in Gazzetta Ufficiale n. 265 del 14 novembre 2005);
- Circolare CNIPA 56 del 21 maggio 2009, "Modalità per la presentazione delle domande di iscrizione all'elenco pubblico dei gestori di posta elettronica certificata di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005 n. 68" (pubblicata in Gazzetta Ufficiale n. 283 del 5 dicembre 2005);
- Circolare CNIPA 51 del 7 dicembre 2006, "Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell'elenco dei gestori di posta elettronica certificata (PEC) di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68" (pubblicata in Gazzetta Ufficiale n. 296 del 21 dicembre 2006);
- Decreto legge del 29 novembre 2008, n. 185 "Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale" (pubblicato in Gazzetta Ufficiale n. 280 del 29 novembre 2008 – supplemento ordinario). Convertito in legge, con modificazioni, con la Legge 28 del gennaio 2009, n. 2 (pubblicata in Gazzetta Ufficiale n. 22 del 28 gennaio 2009 - supplemento ordinario);

- Decreto Legislativo 7 marzo 2005, n. 82 “Codice dell’amministrazione digitale” (pubblicato in Gazzetta Ufficiale n. 112 del 16 maggio 2005 – supplemento ordinario);
- DPCM 6 maggio 2009 - “Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini” (pubblicato in Gazzetta Ufficiale n. 119 del 25 maggio 2009).

Di seguito sono illustrati gli elementi più significativi delle principali norme sopra elencate.

DPR 11 febbraio 2005, n. 68

La norma che segna l’inizio e definisce la disciplina della Posta Elettronica Certificata è, appunto, il DPR 11 febbraio 2005, n. 68.

Questo regolamento, come ben specificato nel titolo e nelle premesse, tra origine dai due dettami di legge:

1. l’Articolo 27¹⁹ della Legge del 16 gennaio 2003 n. 3 - Disposizioni ordinamentali in materia di pubblica amministrazione, e
2. l’Articolo 14²⁰ del DPR del 28 dicembre 2000, n. 445.

¹⁹ Articolo 27 - Disposizioni in materia di innovazione tecnologica nella pubblica amministrazione [...]

8. Entro un anno dalla data di entrata in vigore della presente legge sono emanati uno o più regolamenti, [...] per introdurre nella disciplina vigente le norme necessarie ai fini del conseguimento dei seguenti obiettivi:

[...]

e) estensione dell’uso della posta elettronica nell’ambito delle pubbliche amministrazioni e dei rapporti tra pubbliche amministrazioni e privati;

[...]

²⁰ Il citato Articolo 14 - Trasmissione del documento informatico, prima dell’entrata in vigore del regolamento in questione, era composto dai seguenti 3 commi:

1. Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario, se trasmesso all’indirizzo elettronico da questi dichiarato.
2. La data e l’ora di formazione, di trasmissione o di ricezione di un documento informatico,

La prima e più importate affermazione di tale Regolamento è che “la posta elettronica certificata consente l’invio di messaggi la cui trasmissione è valida agli effetti di legge” [comma 1 dell’Articolo 4]: la validità della trasmissione e ricezione di un messaggio di Posta Elettronica Certificata è attestata rispettivamente dalla ricevuta di accettazione e dalla ricevuta di avvenuta consegna [comma 4 dell’Articolo 4].

I privati²¹ poi, che intendono utilizzare il servizio di Posta Elettronica Certificata, per ciascun procedimento con le pubbliche amministrazioni o per ogni singolo rapporto tra privati o tra questi e le pubbliche amministrazioni, devono dichiarare espressamente l’indirizzo di posta valido ad ogni effetto giuridico.

Tale dichiarazione obbliga solo il dichiarante e può essere revocata nella stessa forma con cui è stata effettuata [commi 2, 3 e 5 dell’Articolo 4].

Gli altri principali contenuti del Regolamento, oltre alle definizioni di cui all’articolo 1, si possono sintetizzare come segue:

- L’individuazione dei soggetti coinvolti (mittente, destinatario e gestore) [Articolo 2].
- Le componenti e le modalità di funzionamento dei sistemi di Posta Elettronica Certificata [Articolo 5 e commi da 1 a 6 dell’Articolo 6]; in particolare stabilisce che:
 - le ricevute rilasciate dai gestori, al fine di renderne manifesta la provenienza e di assicurarne l’integrità

redatto in conformità alle disposizioni del presente testo unico e alle regole tecniche di cui agli articoli 8, comma 2 e 9, comma 4, sono opponibili ai terzi.

3. La trasmissione del documento informatico per via telematica, con modalità che assicurino l’avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge.

²¹ Per quanto riguarda Imprese e Professionisti si veda quanto stabilito dal Decreto Legge 29 novembre 2008, n. 185, convertito in legge dalla Legge 28 gennaio 2009, n. 3.

e l'autenticità siano sottoscritte mediante una firma elettronica avanzata²², generata automaticamente dal sistema di posta elettronica e basata su chiavi asimmetriche a coppia, una pubblica e una privata [Articolo 9];

– su ciascun messaggio sia apposto un riferimento temporale, opportunamente generato, e che quotidianamente sia apposta sui log dei messaggi una marca temporale [Articolo 10].

- L'importante modifica del comma 1 dell'art. 14 del DPR 445 del 2000 [Articolo 3] che ridefinisce in modo più chiaro e puntuale la sequenza di invio e ricezione di un documento informatico.

La nuova formulazione è “Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore”.

Questa formulazione, senza subire alcuna modifica è tutt'ora vigente (comma 2 dell'Articolo 45 del Codice dell'amministrazione digitale).

- L'istituzione dell'elenco dei gestori, tenuto da CNIPA, oggi DigitPA, che deve verificarne i requisiti soggettivi ed oggettivi quali l'onorabilità degli amministratori, la solidità, o copertura, finanziaria adeguata a condurre l'attività,

²² Come fatto già rilevare nella nota a pie' di pagina dell'articolo 9 del testo del DPR 68/2005, per firma elettronica avanzata si intende quella definita nell'articolo 2, comma 1, lettera g), del decreto legislativo 23 gennaio 2002, n. 10, che riflette la definizione del comma 2 dell'articolo 5 della Direttiva Europea 1999/93/CE.

Per quanto riguarda la sicurezza dei dispositivi di firma impiegati, vale la pena di evidenziare che essi sono degli HSM (Hardware Security Module) certificati (o in via di certificazione) e che DigitPA esercita attività di vigilanza su tutto il processo nonché sugli HSA affidati ai gestori.

la capacità ed esperienza tecnico-organizzativa, la dimestichezza con procedure e metodi per la gestione della sicurezza e la certificazione ISO9000 del processo [commi 1, 2, e da 7 a 12 dell'articolo 14] e conseguente definizione dei requisiti che il gestore deve dimostrare di possedere per essere iscritto nell'elenco pubblico [commi dal 3 al 6 dell'Articolo 14].

- L'attribuzione a DigitPA, delle funzioni di vigilanza e controllo sulle attività dei gestori [comma 13, dell'Articolo 14].
- L'obbligo per i gestori di:

- garantire l'interoperabilità dei servizi di Posta Elettronica Certificata offerti [comma 2, dell'Articolo 5,];
- tenere traccia delle operazioni svolte, in un apposito log, per una durata di trenta mesi garantendone la riservatezza, la sicurezza, l'integrità e l'inalterabilità [commi 2 e 3 dell'Articolo 11,].

Tali informazioni nel caso il mittente non abbia più la disponibilità delle ricevute dei messaggi di posta elettronica certificata inviati sono opponibili a terzi anche al fine di dare valenza alla avvenuta trasmissione del messaggio di notificazione a mezzo posta, nei casi consentiti dalla legge [comma 7 dell'Articolo 5];

- garantire livelli minimi di servizio [Articolo 13];
- verificare l'eventuale presenza di virus nelle email, bloccandone, in caso positivo, la trasmissione ed informandone il mittente; il gestore deve conservare tali email per trenta mesi [Articolo 12].

Il comma 4 dell'Articolo 16 stabilisce, infine, gli ambiti entro i quali quanto stabilito da tale regolamento non è applicabile,

restando valide le specifiche disposizioni normative in vigore. Specificatamente si tratta dell'uso degli strumenti informatici e telematici nel processo civile, nel processo penale, nel processo amministrativo, nel processo tributario e nel processo dinanzi alle sezioni giurisdizionali della Corte dei conti.

Decreto Ministeriale 2 novembre 2005

Il Decreto Ministeriale definisce nel dettaglio le regole e le norme tecniche per la realizzazione, il funzionamento e l'interoperabilità dei sistemi di Posta Elettronica Certificata.

Il Decreto descrive, inoltre, la struttura dell'elenco pubblico dei gestori e le modalità con cui accedervi [Articolo 18], le modalità di iscrizione a tale indice [Articolo 16], la struttura organizzativa minima dei gestori [Articoli 21 e 22] e la struttura del manuale operativo [Articolo 23].

Delle caratteristiche dei messaggi (ricevute, avvisi e buste) generati e gestiti dai sistemi di Posta Elettronica Certificata e del funzionamento di tali sistemi si è già dato conto nei paragrafo 3 e 4 del Capitolo I.

Il Decreto stabilisce, inoltre, che:

- i certificati da allegare alla sottoscrizione dei messaggi generati all'interno dei sistemi di Posta Elettronica Certificata sono rilasciati al gestore da DigitPA al momento della sua iscrizione all'elenco pubblico dei gestori [Articolo 7];
- i riferimenti temporali da impiegare devono essere generati in modo da garantire che non abbiano uno scarto superiore ad un minuto secondo rispetto al Tempo Universale Coordinato (UTC) [Articolo 9];
- la conservazione del log dei messaggi deve essere eseguita

a norma di legge, con apposizione della Marca Temporale, senza soluzione di continuità, con cadenza non superiore alle 24 ore [Articolo 10];

- anche la conservazione dei messaggi contenenti virus deve essere eseguita a norma di legge [Articolo 11];
- i livelli minimi di servizio che devono essere garantiti sono i seguenti:
 - la disponibilità del servizio di Posta Elettronica Certificata deve essere maggiore o uguale al 99,8% nel quadrimestre; la durata massima di ogni evento di indisponibilità non deve superare il 50% del totale previsto per il quadrimestre stesso;
 - il limite di tempo entro il quale deve essere restituita la ricevuta di presa in carico/accettazione di un messaggio di posta inoltrato va concordata tra gestore e titolare;
 - il gestore ha l'obbligo di mettere in opera le soluzioni tecnico/operative di emergenza che consentano di completare, in ogni caso, la trasmissione del messaggio e il rilascio delle ricevute relative. Tali soluzioni vanno descritte nel manuale operativo;
 - il gestore ha la facoltà di definire il numero massimo di destinatari cui inviare un messaggio e la dimensione massima che accetta per ogni singolo messaggio, sia esso generato da un suo titolare o a questo diretto. In ogni modo deve garantire l'invio di un messaggio indirizzato ad almeno 50 destinatari e per il quale il prodotto, tra numero di destinatari e dimensione del messaggio (allegati inclusi), non superi i 30 Mbyte.

Circolari CNIPA di accreditamento n. 56 del 21 maggio 2009, e di vigilanza n. 51 del 7 dicembre 2006

La circolare di accreditamento definisce i dettagli per la presentazione della domanda di iscrizione all'elenco pubblico dei gestori di Posta Elettronica Certificata.

La documentazione richiesta è suddivisa in cinque aree principali:

- societaria;
- economico/patrimoniale;
- organizzativa;
- tecnico/operativa
- sicurezza.

La circolare fornisce, inoltre, le indicazioni circa la modalità di esame della domanda di iscrizione all'elenco pubblico dei gestori e le azioni conseguenti (da parte sia di DigitPA sia del gestore) l'accettazione della domanda.

La circolare di vigilanza entra nei dettagli delle modalità con le quali il DigitPA esercita la vigilanza nei confronti dei gestori iscritti nell'elenco pubblico.

In particolare descrive:

- le modalità di svolgimento dei test di interoperabilità;
- il controllo esercitato, da parte di DigitPA, sul modello di business relativo all'offerta dei servizi di PEC;
- le comunicazioni periodiche a DigitPA delle statistiche relative al traffico gestito ed ai livelli di servizio erogati, le modalità con cui effettuare tali comunicazioni nonché la struttura informativa necessaria per adempiere a tale obbligo;
- la classificazione dei disservizi che potrebbero verificarsi nell'erogazione del servizio;

- le modalità ed i tempi con i quali effettuare la tempestiva segnalazione a DigitPA di malfunzionamenti gravi del servizio di Posta Elettronica Certificata offerto;
- gli obblighi e le modalità di sospensione del servizio erogato in caso di malfunzionamenti gravi e gli obblighi informativi conseguenti;
- le verifiche periodiche che tutti i gestori sono tenuti ad effettuare e l'effettuazione di sopralluoghi da parte di DigitPA presso le strutture dei gestori, al fine di verificare la conformità del sistema Posta Elettronica Certificata;
- la disposizione, da parte di DigitPA, di provvedimenti nei confronti dei gestori inadempienti.

Decreto legge del 29 novembre 2008, n. 185

Questo decreto copre un ampio spettro di problematiche (comprese quelle dirette ad incentivare la digitalizzazione).

Per quanto interessa in questa sede esso riveste una particolare importanza per l'impiego e la diffusione della Posta Elettronica Certificata.

Il decreto legge 185/2008 contiene, infatti, importanti modifiche al Codice dell'amministrazione digitale ed al DPR n.68/2005.

Riferendoci alle sole prescrizioni introdotte in materia di Posta Elettronica Certificata²³ è da sottolineare l'obbligo di dotarsi di una casella di Posta Elettronica Certificata per tutte le attività di

²³ In effetti il testo convertito in legge del Decreto in oggetto oltre a far riferimento alla PEC, consente anche analoghi sistemi di posta elettronica "basati su tecnologie che certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità del contenuto delle stesse, garantendo l'interoperabilità con analoghi sistemi internazionali". Ciò premesso per completezza di informazione, d'ora in poi si farà solo riferimento alla PEC non essendo disponibili altri sistemi di posta elettronica che garantiscano quanto richiesto.

“business”: mi riferisco in particolare alle imprese costituite in forma societaria [comma 6 dell’Articolo 16] ed ai professionisti [comma 7 dell’Articolo 16] iscritti in albi ed elenchi istituiti con leggi dello Stato.

Per quanto riguarda le tempistiche, il Decreto fa riferimento al 29 novembre 2008, data di entrata in vigore del Decreto medesimo (Tabella V).

Imprese costituite in forma societaria	Devono indicare il proprio indirizzo PEC all’atto di iscrizione al registro delle imprese, se posteriore al 29 novembre 2008
	Entro tre anni (a decorrere dal 29 novembre del 2008) tutte le imprese devono aver comunicato il proprio indirizzo di PEC al Registro delle Imprese
Professionisti iscritti agli albi od elenchi istituiti con leggi dello Stato	Entro un anno (a decorrere dal 29 novembre del 2008) comunicano ai rispettivi ordini o collegi il proprio indirizzo di PEC
Pubbliche amministrazioni (di cui al Decreto Legislativo n° 165/2001, articolo 1, comma 2)	Istituiscono una casella di PEC per ogni registro di protocollo e ne danno comunicazione a CNIPA/ DigitPA
	Le amministrazioni centrali lo avrebbero già dovuto fare entro 8 mesi dalla entrata in vigore del CAD (art. 47, c. 3, lettera a) (1/1/2006)

Tabella V. Riferimenti relativi al Decreto del 29 novembre 2008

I professionisti entro un anno da tale data avrebbero dovuto fornire il loro indirizzo PEC ai propri ordini o collegi che avrebbero dovuto provvedere a pubblicarli sui propri siti in un elenco.

Le imprese di nuova costituzione, dal canto loro, sin dalla entrata in vigore del Decreto hanno l’obbligo di comunicare il loro indirizzo di PEC al Registro delle Imprese. Per le imprese preesistenti l’obbligo di comunicazione scatta a partire dal 29 novembre 2011.

La consultazione e l’estrazione in via elettronica degli indirizzi PEC di professionisti e imprese è possibile solo per le pubbliche amministrazioni.

Le regole tecniche per la consultazione e l’estrazione degli indirizzi PEC, da parte delle sole pubbliche amministrazioni [comma 10 dell’Articolo 16], dagli elenchi di indirizzi PEC dei professionisti, dagli elenchi di indirizzi PEC dal Registro delle Imprese e dagli elenchi gestiti dall’affidatario del servizio di posta certificata al cittadino sono da definire da parte di DigitPA (vedi seguito), saranno pubblicate sul suo sito e saranno efficaci dal momento in cui saranno pubblicate.

Anche alle pubbliche amministrazioni, che non avessero già provveduto a dotarsi di una casella di PEC, ai sensi dell’Articolo 47 del Codice dell’amministrazione digitale (pubbliche amministrazioni centrali), è richiesto di dotarsi di una²⁴ casella di PEC per ogni registro di protocollo: questo indirizzo, comunicato a CNIPA/DigitPA è pubblicato sull’indice delle PA (<http://www.indicepa.gov.it/>).

L’importanza di quanto qui stabilito non sta tanto (anche se importante) nella volontà di diffondere quanto più possibile l’impiego della PEC, quanto nel fatto che le comunicazioni tra i soggetti di cui sopra possono avvenire tramite Posta Elettronica Certificata (con tutte le implicazioni e le valenze del caso) senza

²⁴ Questa prescrizione con la recente modifica (Decreto legislativo 235/2010) all’articolo 47 del CAD trasforma “una” in “almeno una”.

che il destinatario debba dichiarare la propria disponibilità ad accettarle in tale forma e presso tale indirizzo.

Viene, dunque, attribuito valore legale all'invio di atti e notifiche in formato elettronico. Di fatto per tali soggetti l'indirizzo PEC equivale ad un indirizzo fisico.

Si ricorda, come già visto, che i privati che intendono utilizzare il servizio di Posta Elettronica Certificata, devono dichiarare espressamente l'indirizzo di posta valido ad ogni effetto giuridico per ciascun procedimento con le pubbliche amministrazioni o per ogni singolo rapporto tra privati o tra questi e le pubbliche amministrazioni [Articolo 4 DPR 68/2005]. Il decreto in esame, con l'obiettivo di raggiungere la massima diffusione delle tecnologie telematiche nelle comunicazioni, ha previsto l'attribuzione, senza oneri, ai cittadini che lo richiedono di una casella di Posta Elettronica Certificata [Articolo 16-bis].

Le modalità di attribuzione e di utilizzo delle suddette caselle vengono rinviate ad un apposito decreto del Presidente del Consiglio dei Ministri (maggiori dettagli sono riportati nel capitolo seguente).

Decreto Legislativo 7 marzo 2005, n. 82 “Codice dell'amministrazione digitale”

Per quanto concerne il Codice, la norma primaria che regola la digitalizzazione non solo nella pubblica amministrazione, ma anche nel più ampio contesto nazionale, vi sono precise disposizioni che interessano la Posta Elettronica Certificata.

La più importate è proprio nell'articolo 48 (Posta Elettronica Certificata) che stabilisce in modo esplicito che:

- salvo eventuali altre soluzioni tecnologiche che potranno, in un futuro, essere individuate con un opportuno DPCM,

la Posta Elettronica Certificata è lo strumento da impiegare per le comunicazioni per via telematica che necessitino di una ricevuta di invio e di una di consegna;

- suddetta modalità di trasmissione di un documento informatico equivale, salvo specifiche diverse disposizioni, alla notificazione per mezzo della posta;
- la data e l'ora di trasmissione e di ricezione, così come ottenute tramite PEC sono opponibili a terzi.

A salvaguardia del corretto funzionamento del processo di trasmissione proprio della Posta Elettronica Certificata, è demandato a DigitPA il compito di esercitare la dovuta vigilanza sull'attività dei gestori di PEC [Articolo 31].

L'articolo 6 (Utilizzo della Posta Elettronica Certificata) riassume e ribadisce poi quanto già definito in altre norme, ossia l'impiego della Posta Elettronica Certificata da parte della pubblica amministrazione, per l'invio di atti e provvedimenti che li riguardano, nei confronti di professionisti, imprese e cittadini che abbiano ottenuto una casella di PostaCertificat@ (il servizio gratuito previsto per il cittadino. Si veda il Capitolo IV) o che abbiano preventivamente dichiarato la loro disponibilità all'impiego di un loro indirizzo PEC per determinati procedimenti.

Conseguenza di quanto appena riportato è l'obbligo da parte delle pubbliche amministrazioni di istituire almeno un indirizzo PEC per ciascun indirizzo di protocollo e di pubblicarlo sull'Indice PA [Articolo 31, comma 3] nonché di pubblicare sui propri siti un indirizzo “istituzionale” di PEC a cui il cittadino possa rivolgersi [Articolo 54, comma 2-ter].

L'articolo 47 (Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni) stabilisce inoltre che le comunicazioni di documenti tra le pubbliche amministra-

zioni sono valide ai fini del processo amministrativo anche se trasmesse tramite sistemi di PEC.

Infine il comma c-bis dell'articolo 65 (Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica) stabilisce che, fatte salve le disposizioni che prevedono l'uso di specifici sistemi di trasmissione telematica nel settore tributario, le istanze e le dichiarazioni presentate alle pubbliche amministrazioni per via telematica sono valide anche quando trasmesse dall'autore mediante la propria casella di Posta Elettronica Certificata se il suo gestore, prima di rilasciargli le credenziali di accesso, lo abbia identificato come titolare della casella di PEC e lo attesti nel messaggio o in un suo allegato.

Capitolo IV

La PEC per il cittadino

1. La PostaCertificat@

Il servizio di Posta Elettronica Certificata previsto dal comma 5 dell'Articolo 16-bis del Decreto legge n.185//2008, ha avuto definite le modalità di rilascio e utilizzo delle sue caselle dal DPCM 6 maggio 2009.

L'affidatario del servizio gli ha attribuito il nome di PostaCertificat@.

Il servizio si rivolge:

- a tutti i cittadini²⁵ che ne facciano richiesta;
- ai cittadini dipendenti della PA esclusivamente per le comunicazioni tra dipendente e PA oltre che tra cittadino e PA (i dipendenti pubblici che attivano la casella PostaCertificat@ potranno attivare a proprio carico anche i servizi accessori previsti per i cittadini);
- a tutte le amministrazioni pubbliche locali e centrali per i propri registri di protocollo, utilizzati per le comunicazioni tra PA e cittadino.

In questa sede ci si riferisce d'ora in poi al solo cittadino.

²⁵ In maggior dettaglio il servizio è disponibile a tutti i cittadini maggiorenni siano essi italiani (anche se residenti all'estero) o di nazionalità straniera residenti sul territorio italiano in possesso di un Codice Fiscale e, nel caso di cittadini extra-UE, con permesso di soggiorno o "modello 22A con Ologramma" (documento rilasciato dagli Uffici Postali all'atto della presentazione della domanda per il rinnovo del permesso di soggiorno) validi.

Questo servizio, citato spesso anche come CEC-PAC (Comunicazione Elettronica Certificata tra Pubblica Amministrazione e Cittadino) consiste nel rilascio, a titolo gratuito, ai cittadini che ne facciano richiesta di una casella di posta con tutte le caratteristiche di una casella di Posta Elettronica Certificata, con i vincoli che saranno di seguito illustrati.

Va detto subito che questa modalità di Posta Certificata è un sistema di comunicazione chiuso ed esclusivo che consente al cittadino di dialogare con la pubblica amministrazione e viceversa; non sono, infatti previsti altri tipi di comunicazione quali, ad esempio, quelle tra cittadino e cittadino o quelle intercorrenti con altre realtà di business (aziende, banche, clienti, fornitori, ...) o con altre utenze private di PEC.

Il possesso di una casella di PostaCertificat@ non è, pertanto, sufficiente a rispettare l'obbligo, per imprese, professionisti e pubbliche amministrazioni, di dotarsi di una casella di Posta Elettronica Certificata introdotto dal decreto legge 185/2008.

Questo tipo di comunicazione, tecnicamente equivalente a quella che avviene tramite un sistema di PEC, consente di inviare e ricevere messaggi la cui trasmissione è valida ad ogni effetto di legge.

Esso, infatti, attribuisce al messaggio di posta elettronica la piena validità legale nei casi previsti fornendo tutte le garanzie offerte dalla Posta Elettronica Certificata compresa quella relativa alla data e all'ora dell'accettazione e della consegna del messaggio nonché all'integrità del contenuto

Superando quanto stabilito per i privati, al comma 2 dell'Articolo 4 del DPR 68/2008, per il cittadino cui è assegnato un indirizzo di PostaCertificat@ quest'ultimo è valido ad ogni effetto giuridico ai fini dei rapporti con le pubbliche amministrazioni: la volontà espressa dal cittadino all'atto della richiesta di asse-

gnazione di una casella di PostaCertificat@ rappresenta, infatti, esplicita accettazione dell'invio tramite la stessa di tutti i provvedimenti e gli atti che lo riguardano da parte delle pubbliche amministrazioni²⁶.

Ciò premesso tramite la PostaCertificat@ il cittadino può dialogare elettronicamente con le pubbliche amministrazioni sia per richiedere e ricevere comunicazioni, documenti ed informazioni, sia per inviare istanze o per ricevere da queste comunicazioni e notifiche.

Le caselle PostaCertificat@ attivate dalla pubblica amministrazione per i propri dipendenti (in qualità di cittadini) sono del tutto equivalenti alle caselle PostaCertificat@ per il cittadino.

Si noti che in questa situazione, viste le modalità di riconoscimento previste per l'assegnazione di una casella di PostaCertificat@, il gestore dispone già di tutti gli elementi per produrre l'attestato, richiesto dal comma c-bis dell'articolo 65 del CAD, affinché le istanze e le dichiarazioni presentate alle pubbliche amministrazioni via PostaCertificat@ siano riconosciute valide. Deve solo sapere quale sarà la struttura prevista.

Va infine sottolineato che, in funzione delle "emanande" nuove "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, firme elettroniche qualificate, firme elettroniche digitali e validazione temporale dei documenti informatici" l'invio di un messaggio tramite una casella di PostaCertificat@ costituisce a tutti gli effetti sottoscrizione con firma elettronica avanzata.

Tutti gli indirizzi di posta elettronica della pubblica amministrazione, in particolare quelli di PEC o di PostaCertificat@, sono consultabili all'Indice delle pubbliche amministrazioni (www.

²⁶ Articolo 3 del DPCM 6 maggio 2009.

indicepa.gov.it/) e all'interno del portale dedicato (<https://www.postacertificata.gov.it>).

A fine agosto il numero di richieste di caselle di PostaCertificat@ era di circa un milione e centomila.

2. Come si ottiene

Per richiedere l'attivazione del servizio PostaCertificat@ ci si deve collegare al portale web dedicato (www.postacertificata.gov.it) e seguire i passi indicati dalla procedura interattiva guidata.

Tra i dati da inserire richiesti sono:

- dati anagrafici, comprensivi del codice fiscale;
- domicilio postale per le eventuali comunicazioni in forma cartacea;
- contatti telefonici (fisso e mobile);
- indirizzo di posta elettronica tradizionale.

Si potranno anche selezionare i servizi di base (forniti gratuitamente) o avanzati (a pagamento) che il cittadino desidera attivare.

Il cittadino deve anche inserire la password che desidera utilizzare per il successivo accesso ai servizi offerti dal portale web e per utilizzare la casella PostaCertificat@ ed i servizi associati.

Importante è l'accettazione esplicita che il cittadino deve formulare in questa sede delle condizioni contrattuali del servizio nonché delle implicazioni dell'adesione allo stesso nei rapporti con la PA.

Al termine delle suddette operazioni il cittadino è informato dell'esito positivo della richiesta ed è invitato, per completare la procedura di attivazione, a recarsi presso uno degli uffici postali

abilitati, dove avverrà l'identificazione, a partire dalle 24 ore successive (comunque entro tre mesi).

All'attivazione dell'indirizzo della casella di PostaCertificat@ assegnata, unitamente ai dati anagrafici e di domicilio/residenza, ed altri eventuali indirizzi di posta elettronica, sarà inserita all'interno dell'elenco degli indirizzi dei cittadini e resa quindi visibile a tutte le PA attive sul circuito cittadino – PA.

Il cittadino ha facoltà, in ogni momento, di recedere dal servizio.

3. Caratteristiche e servizi

Per accedere alla casella di PostaCertificat@ è sufficiente disporre di una connessione ad Internet.

L'accesso alla casella è possibile sia tramite client (configurabile alla stregua di un normale client di posta elettronica) o direttamente dal portale PostaCertificat@.

Le caselle di PostaCertificat@ hanno una dimensione standard di 250 Mbyte, mentre il numero massimo dei destinatari è stabilito in 50 e la dimensione massima (intesa come prodotto del numero di destinatari e la dimensione del messaggio più i suoi allegati) deve essere al massimo di 30 Mbyte.

I servizi offerti sono divisi in base (gratuiti) e avanzati (per questi ultimi è previsto un addebito).

I servizi base

I servizi base forniti in forma gratuita al cittadino, ossia l'insieme dei servizi necessari a garantire la creazione di un canale di comunicazione semplice, diretto e sicuro tra cittadino e pubblica amministrazione, sono, oltre alla casella di posta elettronica Po-

staCertificat@ di dimensioni standard:

- La possibilità di ricevere le notifiche relative all'attività di ricezione della propria casella PostaCertificat@ (ad esempio la ricezione di un messaggio o di ricevute di accettazione e consegna) tramite posta elettronica tradizionale;
- uno spazio, per memorizzare i documenti scambiati tramite la casella di PostaCertificat@, delle dimensioni di 500 Mbyte (fascicolo elettronico personale).

I servizi avanzati

Ai cittadini che ne facciano richiesta saranno messi a disposizione, a pagamento, ulteriori servizi quali:

- la notifica multicanale, ad esempio tramite SMS o posta cartacea, degli eventi collegati alla casella stessa;
- la firma digitale;
- il fascicolo elettronico personale avanzato (1 Gbyte di spazio disponibile).

Ulteriori servizi potranno essere in futuro messi a disposizione del cittadino; una descrizione di tali possibili servizi è consultabile sul portale www.postacertificata.gov.it alla voce “guida utente/servizi”.

Capitolo V

Interoperabilità e alternative

1. La REM (Registered Email)

La PEC è una “invenzione” tutta nazionale o le sue funzionalità rappresentano concrete esigenze, sentite anche in altri Paesi?

In altri termini, nel caso della posta elettronica, quanto è sentita l'esigenza di avere la certezza sull'identità del mittente, sul fatto che l'invio sia realmente avvenuto (e quando) e, non ultimo, che ciò che è stato spedito sia arrivato, integro, al ricevente?

Il problema ha interessato anche ETSI (European Telecommunications Standards Institute)²⁷, uno dei tre Enti di Standardizzazione europei riconosciuti dall'Unione Europea.

Nel settembre 2006, fu pertanto avviata un'indagine a livello europeo per approfondire l'argomento²⁸: la conseguenza è stata la redazione delle specifiche della REM (Registered Email), pubblicate nell'agosto del 2008 come ETSI TS (Technical Specification) 102 640²⁹.

²⁷ ETSI produce standard per l'Information and Communications Technologies (ICT). Essi riguardano le tecnologie di comunicazione di tipo fisso, mobile, “Converged”, di broadcast ed Internet. ETSI è riconosciuto ufficialmente dalla Commissione Europea come una Organizzazione Europea di standardizzazione (European Standards Organization – ESO). ETSI è una organizzazione “not-for-profit”. 700 soci, da 60 paesi di tutto il mondo, beneficiano della partecipazione diretta all'organizzazione.

Ulteriori informazioni sono disponibili al sito: www.etsi.org.

²⁸ I risultati di questa indagine sono stati riportati nel documento ETSI TR 102 605. Sistemi con finalità simili alla PEC italiana sono operativi almeno in Belgio, Germania, Spagna e Svizzera.

²⁹ Tutti i documenti prodotti da ETSI, possono essere scaricati dall'indirizzo <http://pda.etsi.org/pda/queryform.asp>.

Queste specifiche sono composte da 5 parti:

1. Architecture;
2. Data requirements, Formats and Signatures for REM;
3. Information Security Policy Requirements for REM Management Domains;
4. REM-MD Conformance Profiles;
5. REM-MD Interoperability Profiles.

A queste entro fine 2011 si aggiungerà una sesta parte che presenta i profili di interoperabilità con i protocolli UPU e Busdix (“Business Document Exchange Network service metadata and transport specification”) di PEPPOL³⁰ (parti 6-1 e 6-2 del TS 102 640), oltre a un profilo per il collegamento con soluzioni di tipo REM basate sul protocollo di tipo SOAP sviluppato dal progetto SPOCS³¹ (parte 6-3).

Nelle figure che seguono è rappresentata schematicamente la struttura architeturale della REM. Come si vedrà, essa comprende tutte le funzionalità della PEC più altre; è importante, inoltre, ricordare che, anche se non evidenziato espressamente, la REM dispone di interfacce che consentono di colloquiare correttamente con sistemi di posta analoghi, quali appunto la PEC; inoltre entro fine 2011 la REM disporrà anche di interfacce che

³⁰ PEPPOL (Pan-European Public Procurement OnLine) è un progetto finanziato dall’Unione Europea che ha l’obiettivo di espandere le connessioni di mercato e l’interoperabilità tra comunità di eProcurement (www.peppol.eu). SPOCS (Simple Procedures Online for Cross-Border Services) è un progetto lanciato dalla Commissione Europea a maggio 2009 per aiutare le imprese a rispettare tutti gli innumerevoli regolamenti che valgono nei vari paesi europei, per esempio quando si tratta di chiedere licenze, permessi e rispettare procedure amministrative. Rispettare queste procedure in paesi diversi da quello di residenza può risultare a volte anche molto complesso (www.eu-spocs.eu).

³¹ SPOCS (Simple Procedures Online for Cross-Border Services) è un progetto lanciato dalla Commissione Europea a maggio 2009 per aiutare le imprese a rispettare tutti gli innumerevoli regolamenti che valgono nei vari paesi europei, per esempio quando si tratta di chiedere licenze, permessi e rispettare procedure amministrative. Rispettare queste procedure in paesi diversi da quello di residenza può risultare a volte anche molto complesso (www.eu-spocs.eu).

consentiranno di colloquiare con i sistemi conformi con le specifiche SOAP, con quelle sviluppate dal progetto PEPPOL e con i sistemi realizzati in base alle specifiche tecniche UPU S52-1 sviluppate dalla UPU (Unione Postale Universale) per il “Postal Registered electronic Mail”.

Ciò significa che chi la realizzerà potrà agevolmente garantire l’interoperabilità con analoghi sistemi di posta, se non proprio attuare una facile migrazione.

I domini di posta sono chiamati, nella terminologia adottata per la REM, “REM Management Domain – REM-MD”. Per analogia, i domini non REM sono stati chiamati “Standard E-Mail Management Domain – SEM-MD”. Si noti che, così come per la PEC, i REM-MD possono dialogare con i SEM-MD.

Anche se il protocollo di trasmissione raccomandato è lo SMTP, la struttura è stata progettata in una prospettiva più ampia in modo da poter essere realizzato anche con altri protocolli.

La modalità di trasmissione della posta è stata concepita in modo da poter scegliere tra due delle seguenti modalità: “Store and Forward” (S&F), ossia ricezione e spedizione della mail, o “Store and Notify” (S&N) ovvero ricezione della mail da parte del REM-MD del mittente il quale la rende disponibile per il download da parte del destinatario.

I REM-MD possono adottare l’una o l’altra; le combinazioni possibili sono:

- “S&F to S&F” - In questa modalità lo scambio tra i due REM-MD, operanti in S&F, avviene in modo analogo a quello della PEC; il messaggio originale, incluso in un nuovo messaggio creato appositamente dal REM-MD del mittente (proprio come si fa con la PEC), è inviato al REM-MD del destinatario e poi depositato nella casella di quest’ultimo;

- “S&N to S&F” - In questo caso il messaggio originale è custodito in un repository del REM-MD del mittente che invia a quello del destinatario un nuovo messaggio, detto “di notifica”, che contiene la URL da cui il destinatario può scaricare il messaggio originale. Questo nuovo messaggio creato appositamente dal REM-MD del mittente è inviato al REM-MD del destinatario e infine a quest’ultimo;
- “S&F to S&N”. Qui le possibilità sono due:
 1. il REM-MD del destinatario si limita a trasferire al destinatario il messaggio ricevuto dal REM-MD del mittente che contiene il messaggio originale in allegato; in pratica opera come nel caso S&F to S&F;
 2. Il REM-MD del destinatario conserva il messaggio ricevuto in un suo repository e crea un messaggio di notifica che inoltra al destinatario il quale, mediante la URL contenuta nel messaggio ricevuto, potrà scaricarsi dal repository del suo REM-MD il messaggio predisposto dal REM-MD del mittente.

Nelle figure 4, 5 e 6 sono illustrate graficamente le tre principali situazioni di gestione del messaggio in ambiente REM.

La REM, come la PEC, prende in considerazione tutta una serie di messaggi, anzi sono molto più ricchi visto il più ampio spettro di situazioni che prevede.

Essi si dividono principalmente in:

- REM-MD Evidence – insieme di informazioni create all’interno di un REM-MD che provano che un dato evento si è verificato in un certo momento;
- REM Dispatch – busta firmata, generata dal REM-MD del mittente, che contiene il messaggio originale e le REM-MD Evidence collegate;
- REM-MD Message – messaggio generato da un REM-MD

sotto la sua responsabilità tecnico/legale; il mittente ed il destinatario possono riceverlo come notifica o ricevuta. È costituito da una busta firmata che contiene le opportune REM-MD Evidence. Il messaggio è strutturato in formati MIME e può contenere il messaggio originale.

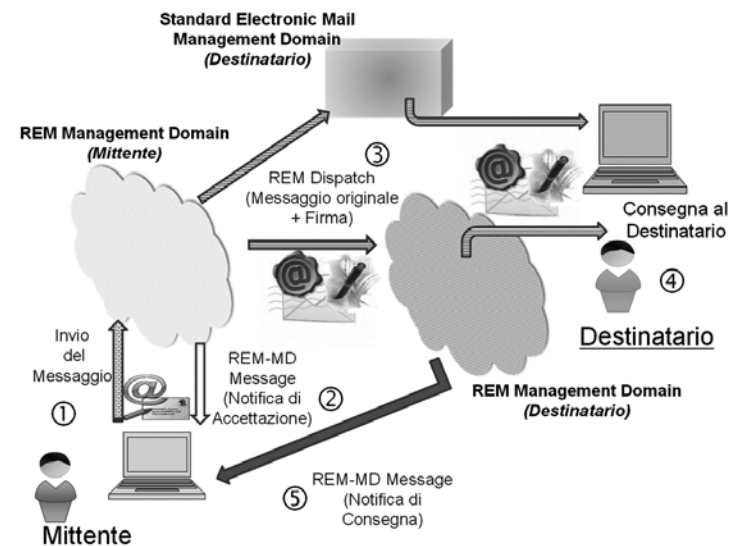


Figura 4. Store & Forward utilizzato da REM-MD di utente e destinatario

Tra le informazioni contenute nelle “Evidence”, a parte quelle che la PEC chiama “Dati di Certificazione”, c’è anche l’impronta dell’intero messaggio (allegati compresi) così come è stato originariamente inviato dal mittente. Essendo tale impronta allegata anche alla notifica di accettazione, il mittente può dimostrare di aver inviato un determinato messaggio anche a destinatari che non siano utenti REM. Esempi di altre informazioni in esse contenute sono:

- l’accettazione o il rigetto (con motivazioni) del messaggio o del suo inoltra;

- la notifica di consegna o di mancata consegna (con motivazioni);
- le notifiche di disponibilità per il download;
- l'inoltro (con successo o meno) del messaggio originale ad un indirizzo in un dominio di posta elettronica tradizionale;
- L'informazione che il messaggio è stato ricevuto da un dominio di posta elettronica tradizionale, ...

Le firme apposte durante il processo dai REM-MD sono delle firme elettroniche avanzate, così come previste dal comma 2 dell'articolo 2 della Direttiva Europea 1999/93/CE e impiegano un dispositivo sicuro di firma di cui al comma 6 dell'articolo 2 della direttiva medesima. Esse non sono da confondere con la firma elettronica avanzata recentemente introdotta dal Decreto legislativo 30 dicembre 2010, n. 235, mentre sono molto simili, nella sostanza, alla Firma del gestore di cui al Decreto Ministeriale del 2 novembre 2011.

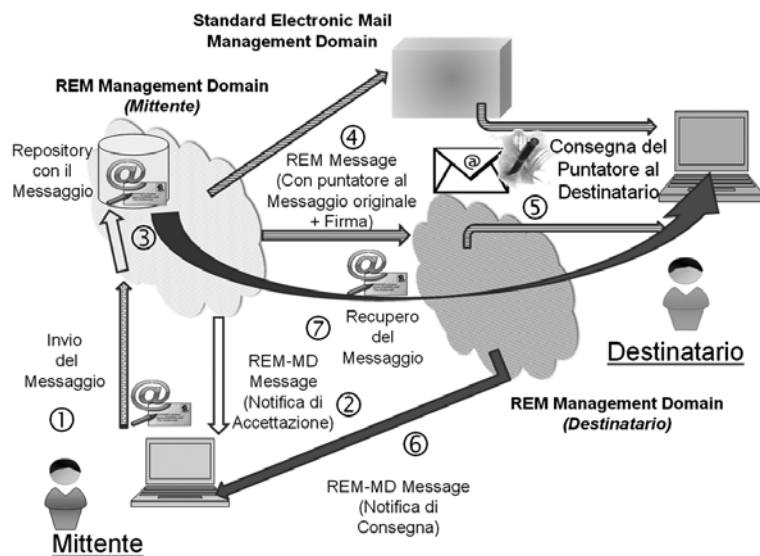


Figura 5. Store & Notify: il messaggio di notifica è generato dal REM-MD del mittente (se un destinatario del messaggio originale appartiene ad un SEM-MD è sempre possibile inviargli il puntatore per recuperare il messaggio inviato)

Sempre a proposito di firme la REM prevede che i certificati di firma siano rilasciati da una Certification Authority indipendente dall'azienda che gestisce la REM-MD: ciò per garantire la necessaria indipendenza ed autorevolezza.

La Time Stamping Authority, invece, non è sempre necessaria, a patto che il gestore sia considerato affidabile (cosa che è certamente vera per i gestori di PEC sui quali DigitPA opera attività di vigilanza).

In ambito REM, affinché due o più REM-MD si possano riconoscere a vicenda è necessario che le loro "politiche" (il modo in cui operano e le misure di sicurezza adottate) siano compatibili, se non le stesse, e che ciò venga reso pubblico. È stato previsto anche il mutuo riconoscimento tra i differenti domini di REM.

In Italia (limitatamente alla PEC) il problema è stato risolto con l'introduzione dell'Indice dei gestori di PEC, gestito e pubblicato da DigitPA: tramite questo indice si è, infatti, in grado di sapere se un messaggio PEC sia effettivamente stato prodotto da un gestore riconosciuto da DigitPA.

Ciò che non vi è nel nostro Paese (in quanto non è stato proprio previsto) è la possibilità di riconoscimento della PEC da parte di operatori estranei al circuito PEC.

Le specifiche REM lasciano ai singoli REM-MD come organizzarsi in tal senso. Quello che conta è che almeno i REM-MD che operano all'interno di un insieme di politiche accettate e riconosciute siano informati in modo affidabile su quali sono i REM-MD riconosciuti. Ciò lascia aperto il problema del coordinamento.

Il modo per risolvere tale problema è l'adozione, così come è stato fatto per i Certificatori, del meccanismo denominato

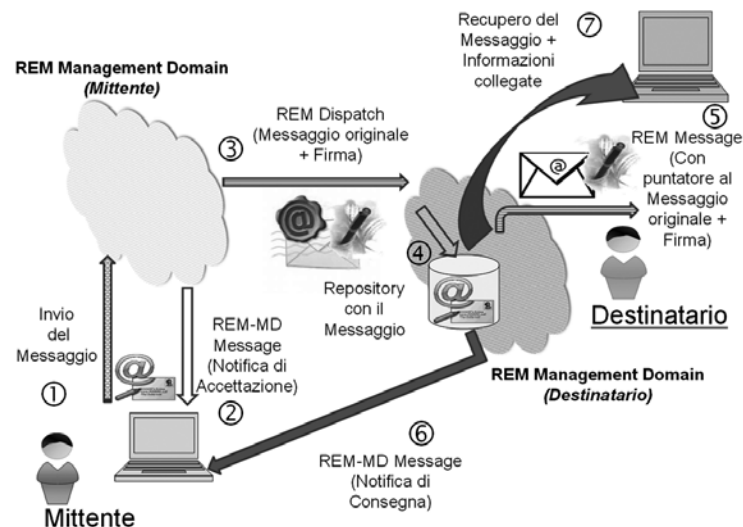


Figura 6. Store & Notify: il messaggio di notifica è generato dal REM-MD del destinatario

“Trust-service Status List” (TSL³²) le cui specifiche sono pubblicate nello ETSI TS 102 231. La TSL è utilizzabile proprio per fornire le informazioni sullo stato di valutazione, presente e passata, di ogni singolo fornitore di servizi collegato all’impiego di firme elettroniche. Per quanto riguarda futuri sviluppi, i presupposti ci sono tutti, ma se ci sono voluti cinque anni affinché la TSL fosse riconosciuta come la soluzione al problema della circolazione delle firme elettroniche all’interno dell’Unione Europea, non è il caso di fare previsioni sul tempo necessario a comprendere che oltre a PEPPOL (che è “solo” pubblico) serve anche per i privati e che la REM è ad oggi la soluzione.

³² Questa “Lista”, che mutua i concetti ed il meccanismo dell’originario Elenco nazionale dei Certificatori Accreditati in Italia, è stata pensata principalmente per trovare una soluzione al problema del mutuo riconoscimento legale delle firme digitali così come previste dalle norme dei vari Paesi della Comunità Europea; oggi è stata di fatto pienamente adottata.

Capitolo VI

Gestione e archiviazione dei messaggi di Posta Elettronica Certificata

di Stefano Pigliapoco³³

1. Introduzione

Le operazioni di protocollazione, classificazione e archiviazione dei messaggi di Posta Elettronica Certificata ricadono nell’insieme delle attività finalizzate alla gestione informatica dei documenti e alla formazione della memoria digitale delle pubbliche amministrazioni.

Pertanto, si premettono alcune considerazioni su questi argomenti per facilitare il lettore nella comprensione dei concetti che saranno esposti nei successivi paragrafi.

1.1 Gestione informatica dei documenti

Per gestione informatica dei documenti s’intende “l’insieme delle attività finalizzate alla formazione, ricezione, registrazione di protocollo, classificazione, organizzazione, assegnazione e reperimento dei documenti amministrativi formati o acquisiti da una pubblica amministrazione, nell’ambito del sistema di classi-

³³ Docente di Informatica documentale e multimediale presso l’Università degli Studi di Macerata. La sua attività di studio e ricerca riguarda il documento informatico, la comunicazione digitale, la dematerializzazione della documentazione amministrativa, il reengineering dei processi, la formazione, gestione e conservazione di archivi digitali in ambito pubblico e privato. È componente di diversi comitati scientifici e gruppi di ricerca sulla digital preservation.

ficazione d'archivio adottato; essa è effettuata mediante sistemi informativi automatizzati³⁴.

Tra queste attività, la registrazione di protocollo, la classificazione dei documenti e la formazione dei fascicoli archivistici rivestono un'importanza fondamentale.

La registrazione di protocollo è l'operazione che permette di identificare e descrivere i documenti ricevuti o spediti da una pubblica amministrazione, fissando con certezza giuridica la data dell'ingresso o dell'uscita. Il registro di protocollo è un atto pubblico cui è riconosciuta la fede privilegiata³⁵ in virtù "del rapporto assolutamente inscindibile che collega, o almeno che dovrebbe collegare, tra di loro il numero progressivo, gli estremi cronologici relativi al preciso momento dell'ingresso in memoria, l'indicazione del mittente o del destinatario e la descrizione dell'oggetto"³⁶. In altri termini, tra una registrazione di protocollo e il relativo documento, che può essere un'entità unica, oppure costituito da un atto primario (ad esempio, la lettera di trasmissione di un progetto a una pubblica amministrazione) e da uno o più allegati (il progetto), deve esserci una corrispondenza biunivoca e inscindibile, che trova evidenza nella cosiddetta segnatura di protocollo la quale, nel caso dei documenti cartacei, è rappresentata da un timbro apposto sul documento e compilato con i dati identificativi della registrazione di protocollo, mentre nel caso dei documenti informatici i dati di protocollo sono inseriti in un file XML associato al documento in modo permanente e non modificabile.

³⁴ Art. 1, c. 1, lett. q), del DPR 28 dicembre 2000, n. 445, recante il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

³⁵ Sentenza della Cassazione penale, sez. V, del 6 ottobre 1987.

³⁶ Cfr. A. Romiti, *Le principali sentenze sul protocollo delle pubbliche amministrazioni: casistica, commento e note sentenza per sentenza*, Viareggio, SAL editoriale, 1995, p. 43.

Una registrazione di protocollo contiene dati obbligatori e dati accessori. Quelli obbligatori sono:

- numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- mittente per i documenti ricevuti, o in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
- oggetto del documento, registrato in forma non modificabile;
- data e numero di protocollo del documento ricevuto, se disponibili;
- impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.

Come dati opzionali o accessori si segnalano:

- numero degli allegati al documento principale (se esistono) e loro descrizione;
- mezzo di ricezione o di spedizione;
- ufficio di competenza ed eventuali copie per conoscenza.

La descrizione dell'oggetto deve essere sufficientemente accurata da far capire il contenuto del documento e le sue finalità anche in mancanza dell'originale.

Ai sensi dell'art. 53, c. 5, del DPR n. 445/2000, sono soggetti a registrazione sul sistema di protocollo i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Non lo sono, invece, le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubbli-

citari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione.

Nell'articolo citato, risalta l'obbligo imposto dal legislatore alle pubbliche amministrazioni riguardo alla registrazione di tutti i documenti informatici; non solo quelli ricevuti o spediti, ma anche quelli prodotti internamente dalle varie unità organizzative³⁷.

Le operazioni di classificazione e fascicolazione rendono evidenti le relazioni che esistono tra i documenti dell'archivio e tra questi e le attività del soggetto produttore. Nello specifico, l'operazione di classificazione consiste nell'associare a un documento la voce del titolario – titolo, classe e sottoclasse - corrispondente alla funzione cui si riferisce, mentre la fascicolazione consiste nel riunire in un'unica entità (il fascicolo) i documenti riguardanti uno stesso procedimento amministrativo, o riferiti a una stessa attività, affare, persona fisica o giuridica. I fascicoli sono le unità di base, indivisibili, di un archivio e la loro formazione deve essere garantita specialmente in ambiente digitale, dove i documenti non hanno la consistenza della carta.

1.2 Formazione e conservazione dell'archivio digitale

I vincoli cui sono soggette le pubbliche amministrazioni per la tenuta e la conservazione dei loro archivi, sono chiaramente esposti nel d. lgs. 22 gennaio 2004, n. 42, recante il codice dei beni culturali e del paesaggio:

- l'art. 10 dichiara che gli archivi e i singoli documenti dello Stato, delle regioni, degli enti pubblici territoriali, nonché di ogni altro ente o istituto pubblico, sono beni culturali e quindi soggetti alle disposizioni in materia di tutela e valorizzazione;
- l'art. 30 impone allo Stato, alle regioni, agli altri enti pub-

³⁷ Come si vedrà nel successivo paragrafo, tale disposizione è funzionale alla formazione dell'archivio digitale.

blici territoriali nonché ad ogni altro ente o istituto pubblico, l'obbligo di garantire la sicurezza e la conservazione dei beni culturali di loro appartenenza, nonché di conservare i propri archivi nella loro organicità e di ordinarli;

- l'art. 53 afferma che i beni culturali appartenenti allo Stato, alle regioni e agli altri enti pubblici territoriali costituiscono il demanio culturale e quindi sono inalienabili.

La transizione dal documento cartaceo al documento informatico, che determina la trasformazione dell'archivio cartaceo in archivio digitale o ibrido, non introduce modifiche alle disposizioni sopra richiamate le quali, pertanto, devono essere attuate anche dalle cosiddette “amministrazioni pubbliche digitali”. In altri termini, dalla lettura combinata del codice dell'amministrazione digitale, contenuto nel d. lgs. 8 marzo 2005, n. 82, recentemente modificato con il d. lgs. 30 dicembre 2010, n. 235, e del codice dei beni culturali e del paesaggio, si rileva per le pubbliche amministrazioni l'obbligo di garantire sia la produzione, ricezione, trasmissione e gestione dei documenti informatici, anche sottoscritti con firma elettronica, sia la formazione e la conservazione degli archivi digitali o ibridi.

Preso atto di quest'obbligo, le pubbliche amministrazioni devono domandarsi quali sono i documenti informatici da archiviare e conservare. La risposta è nella definizione di archivio, che lo indica come il “complesso di documenti prodotti o acquisiti da persone fisiche o giuridiche durante l'espletamento delle proprie funzioni e/o per il raggiungimento delle proprie finalità”. Ogni documento amministrativo³⁸ informatico, quindi, deve essere ar-

³⁸ Ai sensi dell'art. 1, c. 1, lett. a), del DPR n. 445/2000, sono documenti amministrativi “ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa”. Rientrano, pertanto, nella categoria dei documenti amministrativi anche gli atti di diritto privato, formati anche da soggetti privati, purché il loro contenuto sia espressione di attività finalizzate alla cura di interessi amministrativi.

chiviato e conservato perché necessario per dimostrare la regolare esecuzione dei procedimenti amministrativi e la legittimità dei provvedimenti adottati.

Le pubbliche amministrazioni, inoltre, devono stabilire dove e come formare l'archivio digitale. Un documento informatico, non avendo la fisicità della carta, può essere riunito ai suoi precedenti e susseguenti, formando un'unità archivistica equivalente al fascicolo cartaceo, solo con l'ausilio di un sistema che permetta l'esecuzione delle operazioni di protocollazione, classificazione e fascicolazione.

Pertanto, il mezzo con cui si formano le unità archivistiche digitali e il luogo dove sono archiviate insieme ai documenti che le compongono è il sistema di gestione informatica dei documenti, che ai sensi dell'art. 1, c. 1, lett. r), del DPR 28 dicembre 2000, n. 445, è "l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti".

Grazie alle funzionalità di questo sistema si ricostruiscono i fascicoli, collegandoli alle attività del soggetto produttore e ai documenti ricevuti o prodotti per il loro svolgimento.

Siccome l'archivio digitale deve accogliere tutti i documenti informatici ricevuti o prodotti da una pubblica amministrazione durante l'esercizio delle sue funzioni e poiché esso si forma sul sistema di gestione informatica dei documenti con le operazioni di protocollazione, classificazione e fascicolazione, appare logico implementare una soluzione organizzativa, archivistica e tecnologica, che faccia convergere su questo sistema non soltanto i documenti ricevuti o spediti, ma anche quelli prodotti internamente dalle varie unità organizzative dell'ente. Ecco perché il legislatore nell'art. 53, c. 5, del DPR n. 445/2000, ha obbligato le pubbliche amministrazioni a registrare sul sistema di proto-

collo tutti i documenti informatici.

In questa prospettiva, il sistema di gestione informatica dei documenti assume la fisionomia di un vero e proprio servizio infrastrutturale, e gli altri sistemi utilizzati per l'informatizzazione dei procedimenti amministrativi dovrebbero interoperare con esso per evitare la dispersione irrazionale dei documenti informatici nei vari computer collegati alla rete dell'amministrazione.

Spostando l'attenzione dalla formazione alla conservazione dell'archivio digitale, si rileva la necessità di regolare la produzione documentaria per evitare che siano archiviate entità elettroniche soggette a rapida obsolescenza o mancanti delle necessarie informazioni di contesto.

In particolare, i documenti informatici, anche sottoscritti con firma digitale, non devono contenere macroistruzioni o codice eseguibile, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati in esso rappresentati³⁹. Inoltre, essi devono essere prodotti in un formato elettronico compatibile con il processo di conservazione digitale, cioè un formato elettronico di tipo aperto, standard, ben documentato e indipendente dalle piattaforme tecnologiche utilizzate per la loro rappresentazione.

2. Gestione dei messaggi di PEC

L'art. 1, c. 1, lett. g), del DPR n. 68/2005, definisce 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". Si tratta di un sistema di comunicazione elettronica introdotto dal legislatore italiano

³⁹ Si veda l'art. 3, c. 3, del DPCM 30 marzo 2009, recante le regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici.

con l'obiettivo di fornire alle pubbliche amministrazioni, ai cittadini, ai professionisti e alle imprese uno strumento affidabile per trasmettere e ricevere contenuti digitali con garanzia di recapito, riservatezza, integrità e provenienza.

La garanzia della provenienza di un'email certificata, ossia l'identificazione del titolare della casella da cui proviene un messaggio di PEC⁴⁰, discende da tre caratteristiche del servizio:

- a. il soggetto che trasmette il messaggio, all'atto della connessione al punto di accesso, viene identificato - con ragionevole sicurezza - dal suo gestore tramite le credenziali (user id e password) che gli ha rilasciato insieme alla casella;
- b. il canale di comunicazione tra mittente e destinatario implementa meccanismi tecnici tali da garantire la sicurezza e la riservatezza di tutte le connessioni: tra mittente e punto di accesso, tra gestore e gestore, tra punto di consegna e destinatario;
- c. i gestori del servizio di PEC tengono traccia, per almeno trenta mesi, in un registro informatico denominato log dei messaggi, delle operazioni effettuate per la trasmissione delle email certificate. E tale registro è conservato con modalità tali da assicurare la riservatezza, sicurezza, integrità ed inalterabilità nel tempo delle informazioni in esso contenute.

Allo stato attuale, per effetto della normativa vigente, accanto ai canali tradizionali della posta cartacea e degli apparecchi fax, nelle pubbliche amministrazioni è operativo il canale della PEC che, al pari degli altri mezzi di comunicazione, può essere utilizzato da cittadini, professionisti, imprese o altri enti pubblici, per

⁴⁰ Il titolare di una casella di Posta Elettronica Certificata di cui al DPR n. 68/2005 può essere una persona fisica o giuridica, una pubblica amministrazione o qualsiasi ente, associazione o organismo, mentre il titolare di una casella certificata del cittadino (servizio PostaCertificat@ di cui DPCM 6 maggio 2009) può essere solo una persona fisica.

inoltrare messaggi rilevanti ai fini amministrativi.

Il Codice dell'amministrazione digitale riconosce piena efficacia alle trasmissioni di documenti informatici eseguite con una casella di PEC:

- l'art. 45, c. 1, dichiara che "i documenti trasmessi da chiunque a una pubblica amministrazione con qualsiasi mezzo telematico o informatico, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale";
- l'art. 47, c. 1, sottolinea che le comunicazioni di documenti tra le pubbliche amministrazioni avvengono di norma mediante l'utilizzo della posta elettronica e sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza";
- l'art. 47, c. 2, precisa che "ai fini della verifica della provenienza, le comunicazioni sono valide se: 1) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata; 2) ovvero sono dotate di protocollo informatizzato; 3) ovvero è comunque possibile accertarne altrimenti la provenienza secondo quanto previsto dalla normativa vigente; 4) ovvero sono trasmesse attraverso sistemi di Posta Elettronica Certificata di cui al DPR n. 68/2005";
- l'art. 65, c. 1, lett. c-bis), considera valide le istanze e le dichiarazioni presentate alle pubbliche amministrazioni dall'autore per via telematica mediante la propria casella di PEC, purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato⁴¹.

⁴¹ Qui il legislatore pone l'accento sull'esigenza di associare le caselle di PEC ai rispettivi titolari in modo che sia possibile attribuire ad essi la paternità dei messaggi inoltrati.

Queste disposizioni sono sufficienti a tracciare il profilo giuridico dei messaggi di PEC. Essi soddisfano il requisito della forma scritta, possono rappresentare un'istanza o una dichiarazione presentata a una pubblica amministrazione per via telematica, equivalgono a un documento informatico sottoscritto con firma elettronica⁴², costituiscono comunicazione valida ai fini del procedimento amministrativo.

Pertanto, ricordando quanto esposto nei precedenti paragrafi in merito alle tipologie di documenti informatici soggetti alla registrazione sul sistema di protocollo, non ci sono dubbi sul fatto che i messaggi di PEC devono essere registrati sul sistema di gestione informatica dei documenti, classificati in base al titolare di archivio, inseriti nei fascicoli elettronici relativi alle attività cui si riferiscono, archiviati e conservati digitalmente. Oltretutto, il legislatore, nell'art. 40-bis, c. 1, del Codice dell'amministrazione digitale, ha confermato l'obbligo della registrazione di protocollo per:

- le comunicazioni che pervengono o sono inviate attraverso la casella di PEC istituzionale e gli altri eventuali indirizzi di posta elettronica dichiarati all'Indice degli indirizzi delle amministrazioni pubbliche (www.indicepa.gov.it);
- i messaggi ricevuti o trasmessi attraverso l'indirizzo di PEC pubblicato sul sito istituzionale dell'amministrazione per accogliere le richieste dei cittadini;
- i documenti scambiati tra le pubbliche amministrazioni per

⁴² Si segnala che nella bozza delle nuove regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, firme elettroniche qualificate, firme elettroniche digitali e validazione temporale dei documenti informatici, recentemente pubblicata sul sito di DigitPA, l'invio tramite Posta Elettronica Certificata di cui all'art. 65, comma 1, lettera c-bis), del CAD, effettuato richiedendo la ricevuta completa di cui all'art. 1, comma 1, lettera i) del decreto 2 novembre 2005, recante le regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della Posta Elettronica Certificata, costituisce, nei confronti della pubblica amministrazione, firma elettronica avanzata del messaggio spedito.

posta elettronica o in cooperazione applicativa;

- le istanze e le dichiarazioni presentate per via telematica con le modalità di cui all'articolo 65, c. 1, lett. c-bis).

La protocollazione dei messaggi di PEC deve seguire, ovviamente, le stesse regole fissate per i documenti informatici.

In primo luogo, un messaggio di PEC da protocollare deve possedere le caratteristiche di leggibilità e stabilità nel tempo. In particolare, non deve contenere macroistruzioni o codice eseguibile, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati in esso rappresentati. Ad esempio, se una pubblica amministrazione ricevesse un messaggio di PEC nel cui testo è presente il link ad un file memorizzato sul sito web del mittente, si troverebbe nella condizione di dover protocollare e archiviare un documento il cui contenuto può cambiare in qualsiasi momento, semplicemente modificando sul sito web l'oggetto digitale collegato.

In secondo luogo, poiché per effetto delle operazioni di protocollazione, classificazione e fascicolazione, un messaggio di PEC entra nell'archivio digitale dell'amministrazione, esso deve possedere i requisiti che ne permettono la conservazione nel tempo. In particolare, gli eventuali file allegati al messaggio di PEC devono essere prodotti in un formato elettronico di tipo aperto, standard, documentato e indipendente dalle piattaforme tecnologiche utilizzate per la loro rappresentazione. Inoltre, nelle email non devono essere presenti parti crittografate che richiedono l'uso di software proprietari e/o chiavi di decodifica (specialmente se in possesso di soggetti terzi).

Come rilevato nel precedente paragrafo, al registro di protocollo è riconosciuta la valenza di atto pubblico di fede privilegiata per effetto della corrispondenza biunivoca e inscindibile che esiste tra le registrazioni e i relativi documenti. L'esigenza di rispetta-

re il vincolo della corrispondenza biunivoca e inscindibile tra i messaggi di Posta Elettronica Certificata e le relative registrazioni di protocollo si traduce nella necessità di formarli in modo che ciascuno di essi costituisca un documento informatico.

In altre parole, occorre evitare che in un'unica email certificata vi siano nidificati più documenti informatici riguardanti funzioni diverse dell'amministrazione.

L'invito a formare i messaggi di PEC in modo che ognuno di essi costituisca un documento informatico viene anche dal legislatore, il quale, nell'art. 15, c. 2, del DPCM 31 ottobre 2000, recante le regole tecniche per il protocollo informatico, ha stabilito che "ad ogni messaggio di posta elettronica ricevuto da una area organizzativa omogenea (AOO) corrisponde un'unica operazione di registrazione di protocollo, la quale si può riferire sia al corpo del messaggio sia a uno o più dei file ad esso allegati".

Da queste considerazioni, appare evidente che la protocollazione dei messaggi di PEC, in entrata o in uscita, è un'operazione che può raggiungere un livello di complessità elevato e richiede un'adeguata formazione del personale unitamente all'utilizzo di un sistema di gestione informatica dei documenti tecnologicamente avanzato e dotato di funzionalità ad hoc per la trattazione della PEC.

Riguardo alle esigenze di formazione, oltre alla preparazione degli operatori del protocollo sulle peculiarità dei documenti informatici, dei messaggi di PEC e dell'archivio digitale, è necessario che le pubbliche amministrazioni, o in alternativa DigitPA a livello nazionale, predispongano e diffondano le istruzioni per la corretta produzione dei messaggi di Posta Elettronica Certificata, al fine di ricevere e archiviare documenti informatici ben formati e conservabili in forma digitale.

Sotto il profilo tecnologico, si deve perseguire l'integrazione funzionale tra il servizio di Posta Elettronica Certificata e il sistema di gestione informatica dei documenti, sia per acquisire i messaggi in entrata direttamente sul sistema di protocollo informatico e sia per utilizzare lo stesso sistema per formare automaticamente quelli in uscita, allegandovi i documenti registrati con le relative segnature di protocollo. Così facendo, si evita la dispersione dei messaggi di PEC in tanti sistemi e si spinge il personale alla loro protocollazione e archiviazione prima della trattazione da parte degli uffici competenti, o prima della loro spedizione ai destinatari.

Verso l'integrazione funzionale tra il sistema di gestione informatica dei documenti e il servizio di Posta Elettronica Certificata indirizza anche la Circolare 19 aprile 2010, n. 2, del Dipartimento per la digitalizzazione della pubblica amministrazione e l'innovazione tecnologica della Presidenza del Consiglio dei Ministri, nella quale si rileva la necessità di "convogliare il flusso delle email relativo alle caselle di PEC sullo stesso sistema di protocollazione utilizzato per i documenti tradizionali" e l'opportunità di "adottare prodotti di gestione del protocollo informatico predisposti per il trattamento dei messaggi e degli allegati veicolati via PEC, o soluzioni in grado di "collegare" il sistema di gestione della posta elettronica di tipo PEC e quello di gestione del protocollo". Per motivi analoghi, nella stessa Circolare, si raccomanda di "adottare sistemi di gestione documentale che consentano la gestione integrata e la tenuta dei messaggi, degli allegati e delle ricevute nell'ambito della gestione del fascicolo informatico".

Proseguendo nell'analisi dei requisiti tecnologici, un buon sistema di gestione informatica dei documenti, all'atto della registrazione di un messaggio di PEC, dovrebbe presentare all'operatore del protocollo le parti che lo compongono, cioè il testo del

messaggio, i dati di certificazione che identificano il titolare della casella di provenienza, gli eventuali file allegati che possono anche essere sottoscritti con firma digitale e gli altri dati tecnici propri della comunicazione per via telematica, permettendogli di selezionare e descrivere correttamente il documento principale, che può essere rappresentato dal testo del messaggio o da un file allegato all'email, e gli eventuali allegati al documento.

In ogni caso, occorre sempre abbinare alla soluzione tecnologica e alla formazione del personale un modello organizzativo e archivistico che eviti l'eccessiva proliferazione delle caselle di PEC dichiarate all'Indice degli indirizzi delle amministrazioni pubbliche (www.indicepa.gov.it) e/o pubblicate su siti istituzionali. Innanzitutto, perché queste caselle devono essere costantemente monitorate per gestire prontamente i documenti informatici in arrivo e rispettare i tempi fissati per lo svolgimento dei procedimenti amministrativi, e ciò appare tanto più difficile quanto più elevato è il numero degli indirizzi di PEC assegnati ai vari uffici, dirigenti e responsabili di procedimento. In secondo luogo, perché tanto maggiore è il numero delle caselle di PEC attive e tanto più grande è il rischio che i messaggi finiscano per essere memorizzati nei sistemi sui quali sono ricevuti o prodotti, con conseguente dispersione dei documenti informatici nei vari computer dell'ente, che rende difficile, se non addirittura impossibile, la formazione di fascicoli elettronici completi.

Capitolo VII

Alcuni ambiti di applicazione

Si è visto come la Posta Elettronica Certificata possieda, almeno, tutte le caratteristiche della raccomandata con AR (compresa l'opponibilità a terzi dell'avvenuta consegna) a cui si aggiungono indubbi, e facilmente quantificabili, vantaggi in termini di costi e di tempo (non solo relativamente alla durata del processo di comunicazione, ma anche in termini operativi).

Essa, inoltre, consente di effettuare un flusso comunicativo completamente sicuro ed opponibile a terzi in termini sia di certificazione della spedizione e del ricevimento, sia del contenuto oggetto della trasmissione medesima.

È proprio la sua peculiare caratteristica di rendere sicuro ed opponibile un qualunque flusso comunicativo che ne fa una "piattaforma" sulla quale realizzare utili applicazioni.

Un uso "produttivo" della Posta Elettronica Certificata può essere, quindi, di valido supporto ad aziende e pubbliche amministrazioni in svariati processi legali, amministrativi e operativi.

Di fatto qualunque processo che preveda, o possa essere trasformato in, un trasferimento "controllato" e "controllabile" di informazioni in formato digitale può essere realizzato tramite Posta Elettronica Certificata.

Se, poi, alle caratteristiche di impiego della PEC ed alla sua versatilità si associa la sottoscrizione digitale (firma digitale o firma elettronica qualificata) si può disporre di comunicazioni ufficiali, oltre che più semplici, con la garanzia della piena efficacia della posizione assunta.

Esempi di impiego della PEC possono essere:

- l'invio di comunicazioni interne non disconoscibili (circolari, informative, disposizioni operative, revisioni e finalizzazione di delibere assembleari, ...) all'interno di un determinato sistema (azienda, circuito, ..);
- la trasmissione di cedolini o di altra documentazione rilevante ai fini del corretto e completo svolgimento di un processo (pratica di fido, rimborsi sanitari o a fronte di incidenti automobilistici o meno, ...);
- l'inoltro di documentazione commercialmente rilevante tra partner - all'interno della catena del valore - quali contratti, fatture, estratti conto, ordini, conferme d'ordine, ordini e conferme di pagamento,

Ciò può essere molto utile quando non sono operativi altri canali comunicativi affidabili: ciò è particolarmente vero in un sistema produttivo fatto da piccole e micro imprese.

Altri impieghi posso riguardare tutte quelle comunicazioni tra le parti che rappresentano la conferma ad un impegno assunto o servono a rendere formalmente esecutiva una posizione; si pensi ad esempio alla disdetta di un contratto nei termini previsti o all'adeguamento di un canone.

Si pensi, infine, a tutti quei processi in cui si vuole attribuire data certa (opponibile a terzi) a determinati atti che non richiedono per la loro stipula/finalizzazione la presenza di un Pubblico Ufficiale/Notaio, a partire dalla semplice "auto-prestazione postale", ossia l'apposizione di un timbro postale allo sportello su un documento con l'obiettivo di renderne certa la data di produzione.

Sia pure nei limiti dei vincoli già illustrati in questa sede, vi sono tutti gli elementi per ritenere che, con il progressivo adattamento al digitale della nostra cultura, la Posta Elettronica Certificata, ancorché non si veda ancora una qual forma di "killer applica-

tion", assumerà sempre maggiore importanza nelle attività quotidiane di aziende, amministrazioni, professionisti e ... persone.

Il vincolo del raggiungimento della massa critica degli utenti dovrebbe già di fatto essere superato con l'obbligo, già più volte citato, di dotarsi di almeno una casella di Posta Elettronica Certificata per professionisti, imprese e pubbliche amministrazioni. Ciò rende sufficientemente ottimisti per quanto concerne la diffusione della PEC nelle attività produttive o di "business".

Resterebbe fuori il singolo individuo che più difficilmente può trovare sufficienti stimoli a dotarsi di una casella di PEC e ad utilizzarla per comunicare anche se, riflettendo sulle sole cose sopra esposte, non sono poche le situazioni nelle quali potrebbe ritenere utile impiegarla.

Certo la realizzazione della PostaCertificat@ - in assenza della possibilità di un suo impiego al di fuori del dialogo cittadino-pubblica amministrazione e viceversa, non spinge nella direzione della diffusione del suo impiego. In direzione opposta, di contro, spinge, l'obbligo di adozione diffusa dello strumento in questione per tutte le pubbliche amministrazioni e il suo sempre più diffuso impiego, vuoi nelle comunicazioni tra pubbliche amministrazioni vuoi, soprattutto, nel dialogo con i cittadini non solo per gli obblighi a cui questi devono fare fronte, ma soprattutto per migliorare e rendere più accessibili i servizi offerti.

Si può ragionevolmente sperare, infine, che questa barriera possa essere superata grazie anche alla "forza d'urto" che la pubblica amministrazione rappresenta nei comportamenti di tutti i soggetti di una nazione.

Molto probabilmente nel nostro, molto complesso, sistema socio/economico, bisogna che maturi una nuova "forma mentis" che abbia nel digitale uno dei pilastri che la sorreggono.

Capitolo VIII

Le soluzioni Siav per la gestione della PEC

di Alessandro Fabris⁴³

1. Introduzione

La Posta Elettronica Certificata poggia su basi di natura tecnologica e normativa che ne consentono (e sempre più consentiranno in futuro) un proficuo utilizzo nella comunicazione formale tra soggetti. Nel Capitolo VII è stato elencato un insieme di ambiti applicativi che possono trarre giovamento dall'uso della PEC, e sicuramente con il diffondersi di questo strumento si creeranno numerose nuove occasioni per l'utilizzo della Posta Elettronica Certificata, il che comporterà inevitabilmente il moltiplicarsi delle comunicazioni di questo tipo.

Se oggi infatti la quantità di messaggi che mediamente vengono recapitati ad ogni singola casella di Posta Elettronica Certificata è piuttosto ridotta (v. Capitolo I), in futuro è ipotizzabile che tale numero sia destinato a crescere in modo considerevole, essendo uno strumento trasversale rivolto a tutti: a partire dal mondo della pubblica amministrazione, indirizzato dall'azione del legislatore, per passare ai professionisti e alle imprese, incentivati dalle

⁴³ Laureatosi nel 1997 in Ingegneria Informatica presso l'Università di Padova, è stato Responsabile del Laboratorio di sviluppo software di Siav, per poi diventare Responsabile del Siav Education & Knowledge Center, ruolo che ricopre tuttora. Da oltre 10 anni lavora nel mondo della gestione documentale, realizzando soluzioni innovative in ambiti quali OCR, image processing, document e process management, business process intelligence, conservazione sostitutiva, protocollo informatico.

opportunità di risparmio nei costi e dalla maggiore efficienza, per arrivare ai privati cittadini che, con il progressivo radicarsi di una “cultura e società digitale”, troveranno nella PEC un canale di comunicazione per interloquire più facilmente con enti, imprese, professionisti e altri cittadini. Con la sua diffusione si porrà quindi in modo sempre più evidente il problema di trovare una soluzione adeguata per gestire la propria Posta Elettronica Certificata.

2. La gestione della PEC

Per chi utilizza questo strumento, che consente di definire una comunicazione sicura ed opponibile a terzi sia relativamente al tracciamento della spedizione (e della ricezione) che per il suo contenuto, si pone l'esigenza di affrontare la responsabilità di una corretta gestione dei contenuti trattati e della loro fruizione. Infatti (v. Capitolo VI), chiunque abbia a che fare con la Posta Elettronica Certificata – quindi tutti, prima o poi – deve chiedersi come archivarla in modo corretto. La gestione della posta elettronica tradizionale già oggi pone seri problemi ad enti, aziende e professionisti, che si trovano nel corso degli anni ad accumulare quantità enormi di messaggi, i cui contenuti possono essere di scarso valore (ad esempio comunicazioni di natura promozionale) oppure estremamente importanti (contratti, reclami, ordini, richieste, ecc.). Come rintracciare i messaggi nel mare magnum delle email ricevute se non si dispone di sistemi di classificazione adeguati?

Questo problema è ancora più evidente per le comunicazioni PEC, vista la sicura rilevanza dei contenuti trattati. Serve quindi dotarsi di strumenti con cui archiviare in modo ottimale e conservare correttamente la Posta Elettronica Certificata e ciò che vi ruota attorno, a partire dalle ricevute generate dai gestori.

Gestire la PEC significa da un lato garantirne la continuità del va-

lore legale nel tempo, dall'altro essere capaci di valorizzarne al meglio il contenuto, per consentirne la reperibilità e la immediata fruizione a chiunque e in qualunque momento. Una risposta efficace consiste quindi nel trovare una soluzione di gestione documentale che includa le logiche applicative per una corretta archiviazione e conservazione della PEC. In quest'ottica Siav, attingendo al patrimonio di competenze e di componenti software sviluppati in oltre venti anni di attività nell'ambito della gestione dei documenti e dei processi, ha realizzato una serie di prodotti che sono espressamente pensati per risolvere in modo ottimale le esigenze di gestione della PEC. Le molteplici esigenze dei tanti fruitori di questo strumento, che vanno dal privato cittadino al grande ente pubblico, hanno infatti richiesto di trovare risposte adeguate e personalizzate, che si sono tradotte in differenti tipi di soluzioni.

La figura 7 rappresenta nel cerchio interno l'insieme delle soluzioni Siav che includono le logiche di gestione della PEC, mentre nel cerchio esterno sono indicati i soggetti a cui tali soluzioni si rivolgono.



Figura 7. Soluzioni Siav di gestione della PEC e fruitori

I software attualmente disponibili sono:

- PEC Manager, la soluzione per i privati cittadini, i professionisti e le piccole imprese (gratuita);
- PEC Manager PA, la soluzione per gli Enti pubblici con limitate esigenze di archiviazione della PEC (gratuita);
- PEC Manager SE, modulo per integrare nelle soluzioni di gestione documentale proposte da Siav le funzioni di gestione della PEC; è disponibile nei seguenti prodotti: Archiflow e Archidoc, Koinè, Logiko, SimpleFlow e SimpleFlow PA;
- Ergon, la soluzione per la gestione della corrispondenza in ingresso e in uscita via PEC;
- Sinthesi, la piattaforma completa per una gestione multi-canale della corrispondenza in ingresso e in uscita (tramite documenti cartacei e digitali, posta elettronica tradizionale e certificata, fax).

Come anticipato in precedenza, esiste una grande varietà di soggetti interessati ad adottare sistemi di gestione della PEC, ciascuno con le proprie esigenze. Perciò la valutazione di un'applicazione per la gestione della PEC è opportuno venga fatta tenendo sotto controllo questi fattori:

- numero di caselle di Posta Elettronica Certificata monitorate;
- modalità di gestione dei messaggi inviati e ricevuti;
- numero di messaggi che possono essere gestiti;
- numero di utenti che possono utilizzare l'applicazione;
- disponibilità di funzionalità aggiuntive.

Nei prossimi paragrafi saranno descritte le principali caratteristiche delle soluzioni proposte da Siav.

3. PEC Manager

PEC Manager è una soluzione che fornisce alle piccole imprese, ai professionisti, agli studi legali, ai consulenti, ed anche ai privati cittadini, uno strumento integrato non solo per la gestione della PEC ma anche per archiviare i propri documenti in modo semplice, sicuro ed altamente automatizzato.

Il pacchetto applicativo, liberamente utilizzabile a titolo gratuito, può essere scaricato dal sito www.siav.it.

3.1 Caratteristiche

Per descrivere le caratteristiche dell'applicazione si possono individuare tre ambiti di azione: la gestione della corrispondenza in arrivo, la spedizione di nuovi messaggi PEC, e la gestione di documenti di altra natura (analogici e digitali).

3.1.1 Corrispondenza in entrata

Per i messaggi in entrata, PEC Manager verifica periodicamente tutte le caselle di Posta Elettronica Certificata (o di Posta-Certificat@, v. Capitolo IV) indicate in fase di configurazione dell'applicazione e, per ogni comunicazione ricevuta su questo canale, provvede a registrarla all'interno di un apposito archivio informatico, dandone automaticamente evidenza ai destinatari del messaggio tramite un'interfaccia applicativa di semplice ed intuitivo utilizzo. In questo modo il sistema garantisce che tutta la corrispondenza elettronica in arrivo sia effettivamente sottoposta all'attenzione dei destinatari, che potranno consultarla e decidere come elaborarla. PEC Manager include inoltre una serie di funzionalità per la condivisione e lo smistamento delle comunicazioni tra gli utenti del sistema, in modo da garantire, nell'ambito delle regole di sicurezza e protezione dei documenti, un efficace interscambio delle informazioni tra gli utenti.

3.1.2 Corrispondenza in uscita

Per la PEC in partenza si possono individuare due fasi principali.

Fase 1

La prima operazione da compiere consiste nella stesura del contenuto che si vuole spedire. Per facilitare la gestione di questa fase del lavoro PEC Manager fornisce una serie di strumenti per la condivisione dei documenti e per la gestione dei flussi di attività i quali permettono ai vari utenti di partecipare in modo ordinato e controllato alla preparazione dei contenuti. Questo tipo di operatività consente di migliorare la propria efficienza grazie alla rapidità con cui transitano le informazioni.

Fase 2

La seconda fase inizia quando il documento è pronto per la spedizione, momento in cui il sistema si occupa di preparare la comunicazione elettronica, di inviarla ai destinatari, di gestire il monitoraggio del suo stato, e di archiviarne automaticamente le ricevute di ritorno, che vengono allegate al messaggio originale.

3.1.3 Gestione documentale estesa

PEC Manager non gestisce solo la PEC, ma permette di trattare qualunque tipologia di documento, in formato cartaceo o digitale; ciò consente di avere un unico archivio documentale centralizzato, facilmente consultabile, e di usufruire di tutte le funzioni che il sistema offre per rendere semplice ed immediata la gestione, la condivisione e la conservazione dei contenuti e della conoscenza.

PEC Manager permette inoltre di creare dei “raccoltori digitali” in cui inserire tutti i documenti tra loro collegati e realizzare una struttura di fascicoli elettronici multilivello.

3.2 Funzionalità principali

Si riportano nel seguito le principali funzionalità della soluzione PEC Manager.

Pacchetto autoinstallante

PEC Manager si presenta come un pacchetto applicativo autoinstallante e completo di tutti i componenti software necessari al suo funzionamento. Può essere utilizzato su una singola postazione di lavoro, oppure in una rete interna in configurazione client/server.

Sistema pre-configurato

PEC Manager viene installato con un archivio informatico pre-configurato, così da essere immediatamente pronto all'uso per l'utente finale. L'applicazione fornisce quindi una serie di tipologie documentali predefinite con cui è possibile classificare i contenuti archiviati nel sistema; essa permette anche di modificare la rappresentazione dei documenti per venire incontro a specifiche esigenze.

Gestione automatica massiva delle comunicazioni PEC e PostaCertificat@

PEC Manager include un motore per il monitoraggio continuo delle caselle PEC istituzionali; essa è in grado di individuare automaticamente le ricevute di ritorno ed associarle alle comunicazioni in uscita che le hanno generate. È possibile condividere la medesima casella di posta PEC tra più utenti che, in tal caso, saranno però in grado di inviare in modo indipendente le proprie comunicazioni usando lo stesso mittente.

Funzionalità di gestione documentale

PEC Manager è stato realizzato come componente software per la gestione documentale che permette di salvare in formato digitale tutta la documentazione archiviata e i relativi metadati.

Questo include funzionalità quali:

- definizione dei permessi di accesso ai singoli documenti archiviati;
- integrazione nativa con sistemi di scansione e salvataggio diretto in formato PDF (importazione cartaceo);
- importazione dei documenti in formato digitale nativo (PDF, office, immagini,...);
- funzioni per la creazione di fascicoli elettronici multilivello per raccogliere tutti i documenti tra loro correlati;
- possibilità di inserire annotazioni relative ai documenti in archivio;
- visualizzazione della storia delle azioni svolte sul documento.

Strumenti di predisposizione delle comunicazioni

PEC Manager include una serie di strumenti per gestire il flusso di composizione delle comunicazioni e definire un eventuale ciclo di approvazione delle medesime.

Customizzazione tramite linguaggi di scripting

PEC Manager fornisce la possibilità di personalizzarne il funzionamento mettendo a disposizione una serie di interfacce applicative programmabili tramite linguaggi di scripting.

Conversione in PDF

PEC Manager mette a disposizione gli strumenti per convertire i documenti in PDF prima della spedizione (tramite printer driver).

Firma digitale

PEC Manager include le funzioni per apporre la firma digitale sui documenti elettronici senza l'ausilio di librerie di terze parti. Questa funzionalità, unitamente alla possibilità di generare documenti in formato PDF, permette di spedire messaggi di Posta

Elettronica Certificata in cui non solo è garantita la sicurezza della trasmissione e la notifica dell'avvenuta ricezione, ma in cui anche il contenuto stesso del messaggio è sottoscritto digitalmente e opponibile a terzi.

Conservazione Sostitutiva

PEC Manager può fornire, come estensione del prodotto, un componente per la conservazione a lungo termine delle comunicazioni, secondo quanto previsto dalla normativa vigente.

3.3 Posizionamento nell'offerta Siav

Lo schema della Tabella VI fornisce una sintesi delle caratteristiche di PEC Manager e il suo posizionamento in relazione alle esigenze di un utente.

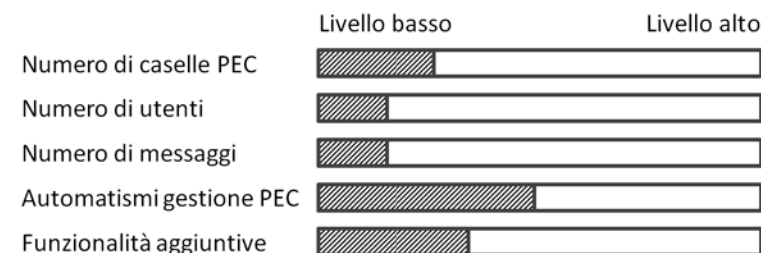


Tabella VI. Livello di funzionalità di PEC Manager

4. PEC Manager PA

PEC Manager PA è la soluzione applicativa che consente agli enti pubblici di avere un sistema per la gestione massiva della Posta Elettronica Certificata in arrivo ed in partenza, rispettando le peculiari esigenze delle amministrazioni pubbliche in materia di gestione dei messaggi in ingresso ed in uscita.

PEC Manager PA è un prodotto liberamente scaricabile ed installabile; esso è stato riconosciuto come valida soluzione per la gestione della PEC dal Dipartimento per la Digitalizzazione della Pubblica Amministrazione e l'Innovazione Tecnologica della Presidenza del Consiglio, il quale ha siglato con Siav un Protocollo d'Intesa in data 14 luglio 2010 che consente ad ogni ente pubblico di usufruire a titolo gratuito di questo prodotto (per ulteriori informazioni si consulti il sito www.innovazione-pa.gov.it).

Il download è disponibile sul sito www.pecmanagerpa.it

4.1 Caratteristiche

Le caratteristiche funzionali di PEC Manager PA sono molto simili a quelle di PEC Manager; pertanto ne saranno di seguito descritte le sole peculiarità necessarie per rispondere alle esigenze della PA. In particolare sono state realizzate le funzionalità che permettono una corretta gestione della PEC nell'ambito dell'inserimento nel registro di Protocollo in uso presso l'ente.

Con riferimento anche a quanto descritto nel Capitolo VI, PEC Manager PA permette di effettuare queste operazioni:

- individuare, all'interno di un messaggio ricevuto, quale sia il documento principale, quali gli allegati significativi e quali gli eventuali allegati da ignorare;
- generare più registrazioni a partire dalla medesima email ricevuta, qualora lo stesso messaggio contenga varie comunicazioni da protocollare in modo distinto;
- interagire con il sistema di gestione del Protocollo Informatico in uso presso l'ente, in modo da garantire la corretta registrazione di ogni comunicazione in ingresso ed in uscita.

4.2 Funzionalità principali

Si riportano nel seguito le principali funzionalità della soluzione PEC Manager PA. Come già indicato, l'applicazione ha le stesse caratteristiche di base di PEC Manager, a cui sono state aggiunte alcune ulteriori funzionalità (standard od opzionali), che rendono la soluzione adatta alle esigenze delle amministrazioni pubbliche. Di seguito sono riportate le peculiarità di PEC Manager PA rispetto a PEC Manager.

Interazione con il Protocollo Informatico dell'ente

Le comunicazioni in ingresso e in uscita vengono protocollate appoggiandosi al sistema di gestione del Protocollo Informatico già in uso presso l'ente.

Esistono due modalità di interazione tra le due applicazioni.

- **Protocollazione manuale.** In questo caso PEC Manager PA dopo avere archiviato la comunicazione ne calcola l'impronta informatica. Questa impronta può essere riportata dall'utente nel sistema di Protocollo Informatico utilizzato dall'ente, da cui recupererà il numero di protocollo che aggiungerà manualmente ai metadati salvati in PEC Manager PA.
- **Protocollazione automatica.** PEC Manager PA fornisce inoltre la possibilità di integrarsi con altri sistemi tramite co-operazione applicativa (es: Web Services), per richiedere in modo automatico il numero e la data di protocollo al sistema di Protocollo Informatico dell'ente. Sono inoltre disponibili le interfacce per restituire il documento a sistemi informatici che vogliano interoperare con PEC Manager PA.

Protocollo Informatico

Qualora l'ente non abbia a disposizione un sistema di gestione del Protocollo Informatico, o sia interessato a sostituire quello in uso, PEC Manager PA può attivare un componente aggiuntivo

per la gestione a norma del Protocollo Informatico. Tra le funzionalità disponibili vi sono: fascicolazione, segnatrice, titolare di classificazione, stampa del registro di Protocollo.

4.3 Posizionamento nell'offerta Siav

Lo schema della Tabella VII fornisce una sintesi delle caratteristiche di PEC Manager PA e il suo posizionamento in relazione alle esigenze di un utente.

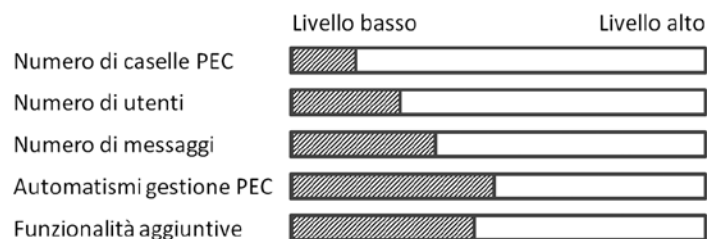


Tabella VII. Livello di funzionalità di PEC Manager PA

5. PEC Manager SE

PEC Manager SE è un componente software sviluppato da Siav per dotare i propri sistemi di gestione elettronica dei documenti delle funzioni necessarie alla corretta gestione della PEC. Si tratta dunque di un modulo che si integra in una soluzione esistente, e che permette in tal modo ad un'Organizzazione di conservare in un unico archivio informatico tutti i propri documenti, in un'ottica di "visione multicanale" che garantisca la convergenza in un solo sistema di tutti i contenuti e informazioni che transitano nell'Organizzazione.

Attualmente è possibile attivare PEC Manager SE su queste applicazioni software: Archidoc e Archiflow, Koinè, Logiko, SimpleFlow e SimpleFlow PA.

5.1 Caratteristiche

In termini funzionali il modulo PEC Manager SE ha le medesime caratteristiche di PEC Manager e PEC Manager PA.

La peculiarità di questo componente sta nel fatto che permette di integrare, in un sistema di gestione documentale che l'utente già conosce, la gestione dei messaggi PEC. Ciò consente di accedere con semplicità ed immediatezza ai contenuti ricevuti ed inviati via PEC, che sono visti esattamente allo stesso modo di tutti gli altri contenuti salvati nel sistema.

Per le soluzioni che prevedono la presenza di un motore di workflow integrato (Archiflow, SimpleFlow, Logiko e Koinè) è inoltre possibile implementare logiche di gestione automatizzata nella predisposizione delle comunicazioni in uscita in cui, a fianco delle attività svolte dai singoli operatori, si aggiungono altre operazioni che possono essere svolte automaticamente dall'applicazione, in base ai dati di profilazione del documento.

5.2 Funzionalità principali

Nel caso di PEC Manager SE le funzionalità disponibili dipendono essenzialmente dalle caratteristiche del prodotto all'interno del quale il modulo viene attivato. Di seguito vengono quindi riportate le sole caratteristiche comuni a tutte le soluzioni.

Gestione automatica massiva delle comunicazioni PEC e PostaCertificat@

PEC Manager SE include un motore per il monitoraggio continuo delle caselle PEC e PostaCertificat@ dell'Organizzazione, ed è in grado automaticamente di individuare le ricevute di ritorno ed associarle alle comunicazioni in uscita che le hanno generate.

Integrazione nel sistema di gestione documentale

PEC Manager SE viene attivato come componente integrato di un più ampio sistema di gestione documentale; pertanto può essere utilizzato sfruttandone tutte le caratteristiche tra cui: funzioni di collaborazione e condivisione dei contenuti, gestione dei processi di workflow (ove previsto), supporto dei cicli approvativi, firma digitale, fascicolazione, gestione del Protocollo Informatico (ove previsto), customizzazione tramite scripting, ecc.

5.3 Posizionamento nell’offerta Siav

Lo schema della Tabella VIII fornisce una sintesi delle caratteristiche del modulo PEC Manager SE e il suo posizionamento in relazione alle esigenze di un cliente.

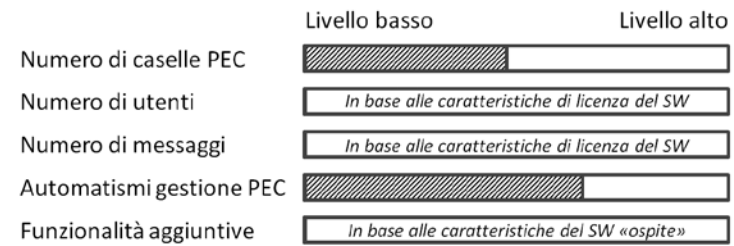


Tabella VIII. Livello di funzionalità di PEC Manager SE

6. Ergon

Ergon è la soluzione per la gestione della PEC basata su una piattaforma tecnologica di classe *enterprise*, che permette di operare in un’ampia varietà di scenari applicativi, a partire da piccoli enti per arrivare a Organizzazioni pubbliche complesse ed articolate.

Grazie alle caratteristiche di scalabilità con cui è stato realizzato, Ergon è in grado di gestire il monitoraggio continuo di centinaia di cassette postali e di fornire l’accesso ai suoi servizi anche ad Organizzazioni costituite da un numero molto elevato di utenti.

6.1 Caratteristiche

Questa soluzione, insieme a Sinthesi, costituisce la punta di diamante tra i sistemi di gestione della PEC offerti da Siav.

Ergon fornisce un’applicazione completa per la gestione dei flussi di lavoro relativi alle comunicazioni PEC in ingresso ed in uscita, e include un motore di workflow che consente di definire le regole di accettazione e registrazione delle comunicazioni in arrivo, di smistare le medesime ai destinatari di competenza, nonché di supportare l’Organizzazione nella predisposizione delle comunicazioni in uscita.

6.1.1 Corrispondenza in ingresso

Il sistema esegue il monitoraggio continuo sull’arrivo di PEC e PostaCertificat@ su una o più caselle istituzionali.

Per ciascun messaggio ricevuto il sistema ne legge il contenuto e valuta automaticamente se sussistono le condizioni per la protocollazione automatica del documento. Infatti, se il messaggio risponde a determinate caratteristiche di interoperabilità e di sicurezza può essere automaticamente sottoposto al sistema di Protocollo Istituzionale affinché possa essere protocollato senza alcun intervento da parte di un operatore di protocollo.

Qualora il documento ricevuto attraverso PEC non soddisfi le condizioni per la protocollazione automatica, Ergon lo sottopone ad un operatore di protocollo che provvederà a rendere il documento protocollabile.

Come accennato, Ergon prevede la possibilità di integrarsi con il sistema di Protocollo Informatico in uso presso l’ente, a cui può trasmettere i dati di protocollazione in modo automatico tramite cooperazione applicativa, tipicamente utilizzando Web Services.

6.1.2 Corrispondenza in uscita

La PEC in partenza, così come avviene per PEC Manager e PEC Manager PA, prevede in Ergon un processo distinto in più fasi.

Fase 1

La prima fase consiste nella predisposizione del documento che dovrà essere spedito tramite Posta Elettronica Certificata. In questo ambito Ergon mette a disposizione una serie di strumenti per coadiuvare gli utenti nella redazione del contenuto, ed inoltre include un motore di workflow che permette di governare in modo automatico il “percorso” seguito dal documento in fase di stesura, nonché di rendere automatica la compilazione di parte del documento (es: inserimento dell’elenco dei destinatari, compilazione del campo oggetto o di altri dati ricavabili in autonomia dal profilo di classificazione del documento stesso).

In questa fase vengono inoltre individuati i destinatari a cui andrà spedito il messaggio PEC, che potranno essere selezionati da una serie di rubriche presenti nel sistema o inseriti manualmente dall’operatore, o recuperati automaticamente dal sistema in base alle caratteristiche di profilazione del documento.

Fase 2

La seconda fase consiste nel cosiddetto “consolidamento” del documento, che prevede la sua conversione in formato PDF/A e la successiva applicazione di un ciclo di approvazione tramite apposizione di firme digitali sul documento oppure di una serie di “visti approvativi” di cui viene tenuta traccia nel sistema.

Fase 3 (opzionale)

Quando il documento è stato definitivamente approvato può essere sottoposto a protocollazione (in caso di ente pubblico) tramite cooperazione applicativa così come descritto per la corrispondenza in ingresso.

Fase 4

L’ultima operazione consiste nella generazione automatica del messaggio PEC a partire dai dati di profilazione del documento, e nella successiva spedizione. Il sistema rimane a quel punto in attesa delle ricevute previste, che vengono allegate al messaggio inviato e sottoposte all’attenzione degli operatori, i quali potranno anche decidere di ripetere una spedizione in caso di anomalie.

6.1.3 Conservazione sostitutiva

Tutti i messaggi PEC ricevuti ed inviati sono sottoposti a conservazione sostitutiva secondo le normative vigenti, tramite una serie di componenti software che, in base alle regole configurate nel sistema, provvedono in autonomia a generare i supporti di conservazione, a monitorare nel tempo l’integrità dei documenti conservati e la loro validità legale, a segnalare al Responsabile della Conservazione quali attività deve svolgere (es: sottoscrizione del file di chiusura – o indice di conservazione –, risoluzione di anomalie nello stato dell’archivio, ecc.).

6.2 Funzionalità principali

Di seguito vengono riportate le principali peculiarità che caratterizzano Ergon.

Soluzione web-based

Ergon utilizza un’interfaccia completamente web-based, ed è progettato per poter essere utilizzato anche delle medie e grandi Organizzazioni, che necessitano di gestire centinaia di caselle PEC, migliaia di allegati e le tutte le relative ricevute.

Sistema di monitoraggio della PEC di classe enterprise

Ergon prevede un sistema di spedizione e ricezione dei messaggi basato su un motore BPM interamente realizzato da Siav.

La soluzione consente di definire con facilità regole di smistamento e assegnazione delle email in arrivo verso gli uffici o ruoli di competenza.

Include inoltre un sistema per il tracciamento dello stato delle email, che analizza le ricevute di ritorno e fornisce all'utente un'evidenza immediata di eventuali anomalie, con la possibilità di re-invio dei messaggi in errore.

Gestione della predisposizione dei documenti

Ergon prevede la possibilità di definire una serie di rubriche in cui registrare i destinatari dei messaggi, a cui applicare differenti livelli di sicurezza.

Fornisce il supporto per la realizzazione di cicli approvativi per l'invio delle comunicazioni in uscita.

Integrazione con il Protocollo Informatico dell'ente

Se utilizzato da un ente pubblico, prevede la possibilità di integrarsi in modo automatico con i sistemi di Protocollo Informatico già in uso presso il cliente, tramite Web Services.

Conversione automatica in PDF

Integra un modulo per la conversione automatica in PDF dei documenti che sono stati predisposti e che sono pronti per la spedizione verso destinatari esterni.

Conservazione Sostitutiva

Ergon include un componente che permette di sottoporre a Conservazione Sostitutiva l'archivio dei messaggi PEC ricevuti e spediti.

Sistema di classe enterprise

Ergon è sviluppato utilizzando una piattaforma tecnologica stu-

diata per essere scalabile ed altamente affidabile, pertanto consente di definire la distribuzione ottimale dei suoi componenti applicativi in relazione alle esigenze del cliente.

6.3 Posizionamento nell'offerta Siav

Lo schema della Tabella IX fornisce una sintesi delle caratteristiche di Ergon e il suo posizionamento in relazione alle esigenze di un cliente.

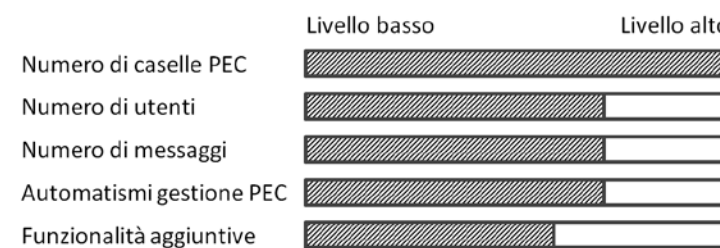


Tabella IX. Livello di funzionalità di Ergon

7. Sintesi

Sintesi costituisce la più completa piattaforma di gestione della corrispondenza in ingresso ed in uscita per le amministrazioni pubbliche, in un'ottica di convergenza multicanale. Sintesi ha l'obiettivo di far convivere nello stesso archivio tutti i contenuti provenienti da fonti eterogenee (cartaceo, elettronico, fax, posta elettronica tradizionale e certificata).

Sintesi include una serie completa di funzioni per la gestione documentale e per la gestione dei procedimenti amministrativi, che è pensata per rendere efficiente il flusso di lavoro, per velocizzare il transito e la condivisione delle informazioni, per garantire la necessaria sicurezza nell'accesso ai dati e ridurre le attività svolte manualmente dagli utenti.

7.1 Caratteristiche

Nell'ambito delle funzioni di gestione della PEC, Sinthesi ha le medesime caratteristiche di Ergon, di cui condivide la piattaforma tecnologica di base.

La specificità di Sinthesi sta nell'insieme complessivo delle funzionalità che sono presenti nello stesso prodotto, di cui la gestione dei messaggi PEC costituisce un elemento essenziale.

7.2 Funzionalità principali

Di seguito vengono riportate le funzionalità principali di Sinthesi.

Gestione elettronica dei documenti

Sinthesi è una soluzione completa di gestione documentale, ed include tutte le funzionalità necessaria ad una gestione efficace di un archivio informatico (profilazione dei documenti, gestione allegati, fascicolazione, check-in/check-out, versioning, tracciatura delle attività, definizione dei diritti, cassetta postale interna per lo smistamento dei documenti, assegnazione per competenza e per conoscenza, ecc.)

Gestione automatica dei procedimenti

Sinthesi include un motore di gestione dei processi, che permette di disegnare i flussi di lavoro, di assegnare le attività automaticamente in base ai ruoli, di applicare regole per la verifica del corretto svolgimento delle attività, di eseguire funzioni custom per l'automazione di parte della lavorazione, ecc.

Gestione corrispondenza

Sinthesi fornisce un'unica interfaccia per la gestione completa della corrispondenza in ingresso ed in uscita, sia essa cartacea o digitale.

Protocollo Informatico

Il sistema prevede tutte le funzionalità per la gestione del Protocollo Informatico secondo quanto richiesto dalle normative vigenti (classificazione, fascicolazione, titolare, ecc.)

Firma digitale

Sinthesi include tutte le funzioni per l'apposizione della firma digitale sui documenti in formato elettronico, ed è in grado di supportare la firma nativa dei file in formato PDF.

Integrazione con Microsoft Office

Sinthesi prevede un flusso controllato dal motore di workflow per la predisposizione dei documenti in uscita. Tale flusso permette di compilare automaticamente parte del documento e di stabilire il "percorso" che deve seguire il documento in lavorazione per essere verificato e approvato prima dell'effettiva spedizione.

Gestione nativa PDF e PDF/A

Sinthesi archivia i documenti in formato PDF (PDF/A ove possibile), così da garantire un rapido e capillare accesso alle informazioni, nonché l'utilizzo di un formato universalmente riconosciuto come standard.

Conservazione Sostitutiva

Sinthesi include un potente sistema per la Conservazione Sostitutiva dei documenti secondo quanto previsto dalle normative vigenti. Il componente è in grado in autonomia di generare i supporti di conservazione applicando le regole definite in fase di configurazione, di monitorare costantemente l'integrità dell'archivio sostitutivo, di sottoporre all'attenzione del Responsabile della Conservazione le attività di sua competenza (firma dei file di chiusura - o indice di conservazione -, gestione delle anomalie, ecc.).

Postalizzazione dei documenti in forma cartacea

Il sistema è pensato come applicazione multicanale, pertanto anche per le comunicazioni in uscita è possibile scegliere la modalità di trasmissione del documento, tra: PEC, postalizzazione cartacea massiva, stampa su carta con apposizione di firma autografa e successiva spedizione manuale.

7.3 Posizionamento nell’offerta Siav

Lo schema della Tabella X fornisce una sintesi delle caratteristiche di Sinthesi e il suo posizionamento in relazione alle esigenze di un cliente.

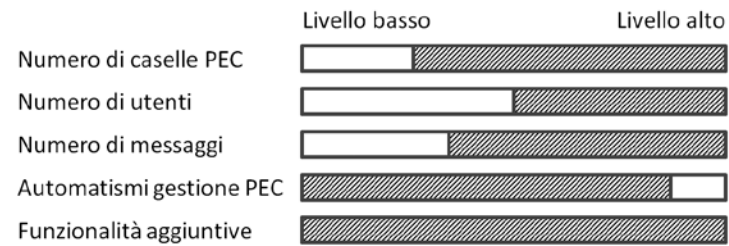


Tabella X. Livello di funzionalità di Sinthesi

Testi delle norme principali

DPR del 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”

(pubblicato in Gazzetta Ufficiale n. 97 del 28 aprile 2005)

Articolo 1

Oggetto e definizioni

1. Il presente regolamento stabilisce le caratteristiche e le modalità per l'erogazione e la fruizione di servizi di trasmissione di documenti informatici mediante posta elettronica certificata.
2. Ai fini del presente regolamento si intende per:
 - a) busta di trasporto, il documento informatico che contiene il messaggio di posta elettronica certificata;
 - b) Centro nazionale per l'informatica nella pubblica amministrazione, di seguito denominato: "CNIPA", l'organismo di cui all'articolo 4, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, come modificato dall'articolo 176, comma 3, del decreto legislativo 30 giugno 2003, n. 196;
 - c) dati di certificazione, i dati inseriti nelle ricevute indicate dal presente regolamento, relativi alla trasmissione del messaggio di posta elettronica certificata;
 - d) dominio di posta elettronica certificata, l'insieme di tutte e sole le caselle di posta elettronica certificata il cui indirizzo fa riferimento, nell'estensione, ad uno stesso dominio della rete Internet, definito secondo gli standard propri di tale rete;
 - e) log dei messaggi, il registro informatico delle operazioni relative alle trasmissioni effettuate mediante posta elettronica certificata tenuto dal gestore;
 - f) messaggio di posta elettronica certificata, un documento informatico composto dal testo del messaggio, dai dati di certificazione e dagli eventuali documenti informatici allegati;
 - g) 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;
 - h) posta elettronica, un sistema elettronico di trasmissione di documenti informatici;

- i) riferimento temporale, l'informazione contenente la data e l'ora che viene associata ad un messaggio di posta elettronica certificata;
- l) utente di posta elettronica certificata, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi ente, associazione o organismo, nonché eventuali unità organizzative interne ove presenti, che sia mittente o destinatario di posta elettronica certificata;
- m) virus informatico, un programma informatico avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.

Articolo 2

Soggetti del servizio di posta elettronica certificata

1. Sono soggetti del servizio di posta elettronica certificata:
 - a) il mittente, cioè l'utente che si avvale del servizio di posta elettronica certificata per la trasmissione di documenti prodotti mediante strumenti informatici;
 - b) il destinatario, cioè l'utente che si avvale del servizio di posta elettronica certificata per la ricezione di documenti prodotti mediante strumenti informatici;
 - c) il gestore del servizio, cioè il soggetto, pubblico o privato, che eroga il servizio di posta elettronica certificata e che gestisce domini di posta elettronica certificata.

Articolo 3

Trasmissione del documento informatico

1. Il comma 1 dell'articolo 14 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è sostituito dal seguente:
 "1. Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore."

Articolo 4

Utilizzo della posta elettronica certificata

1. La posta elettronica certificata consente l'invio di messaggi la cui trasmissione è valida agli effetti di legge.
2. Per i privati che intendono utilizzare il servizio di posta elettronica certificata, il solo indirizzo valido, ad ogni effetto giuridico, è quello espressamente dichiarato ai fini di ciascun procedimento con le pubbliche amministrazioni o di ogni singolo rapporto intrattenuto tra privati o tra questi

e le pubbliche amministrazioni. Tale dichiarazione obbliga solo il dichiarante e può essere revocata nella stessa forma.

3. La volontà espressa ai sensi del comma 2 non può comunque dedursi dalla mera indicazione dell'indirizzo di posta certificata nella corrispondenza o in altre comunicazioni o pubblicazioni del soggetto.

4. (Comma abrogato)

5. Le modalità attraverso le quali il privato comunica la disponibilità all'utilizzo della posta elettronica certificata, il proprio indirizzo di posta elettronica certificata, il mutamento del medesimo o l'eventuale cessazione della disponibilità, nonché le modalità di conservazione, da parte dei gestori del servizio, della documentazione relativa sono definite nelle regole tecniche di cui all'articolo 17.

6. La validità della trasmissione e ricezione del messaggio di posta elettronica certificata è attestata rispettivamente dalla ricevuta di accettazione e dalla ricevuta di avvenuta consegna, di cui all'articolo 6.

7. Il mittente o il destinatario che intendono fruire del servizio di posta elettronica certificata si avvalgono di uno dei gestori di cui agli articoli 14 e 15.

Articolo 5

Modalità della trasmissione e interoperabilità

1. Il messaggio di posta elettronica certificata inviato dal mittente al proprio gestore di posta elettronica certificata viene da quest'ultimo trasmesso al destinatario direttamente o trasferito al gestore di posta elettronica certificata di cui si avvale il destinatario stesso; quest'ultimo gestore provvede alla consegna nella casella di posta elettronica certificata del destinatario.
2. Nel caso in cui la trasmissione del messaggio di posta elettronica certificata avviene tra diversi gestori, essi assicurano l'interoperabilità dei servizi offerti, secondo quanto previsto dalle regole tecniche di cui all'articolo 17.

Articolo 6

Ricevuta di accettazione e di avvenuta consegna

1. Il gestore di posta elettronica certificata utilizzato dal mittente fornisce al mittente stesso la ricevuta di accettazione nella quale sono contenuti i dati di certificazione che costituiscono prova dell'avvenuta spedizione di un messaggio di posta elettronica certificata.
2. Il gestore di posta elettronica certificata utilizzato dal destinatario fornisce al mittente, all'indirizzo elettronico del mittente, la ricevuta di avvenuta consegna.
3. La ricevuta di avvenuta consegna fornisce al mittente prova che il suo messaggio di posta elettronica certificata è effettivamente pervenuto all'indirizzo

elettronico dichiarato dal destinatario e certifica il momento della consegna tramite un testo, leggibile dal mittente, contenente i dati di certificazione.

4. La ricevuta di avvenuta consegna può contenere anche la copia completa del messaggio di posta elettronica certificata consegnato secondo quanto specificato dalle regole tecniche di cui all'articolo 17.

5. La ricevuta di avvenuta consegna è rilasciata contestualmente alla consegna del messaggio di posta elettronica certificata nella casella di posta elettronica messa a disposizione del destinatario dal gestore, indipendentemente dall'avvenuta lettura da parte del soggetto destinatario.

6. La ricevuta di avvenuta consegna è emessa esclusivamente a fronte della ricezione di una busta di trasporto valida secondo le modalità previste dalle regole tecniche di cui all'articolo 17.

7. Nel caso in cui il mittente non abbia più la disponibilità delle ricevute dei messaggi di posta elettronica certificata inviati, le informazioni di cui all'articolo 11, detenute dai gestori, sono opponibili ai terzi ai sensi dell'articolo 14, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

Articolo 7

Ricevuta di presa in carico

1. Quando la trasmissione del messaggio di posta elettronica certificata avviene tramite più gestori il gestore del destinatario rilascia al gestore del mittente la ricevuta che attesta l'avvenuta presa in carico del messaggio.

Articolo 8

Avviso di mancata consegna

1. Quando il messaggio di posta elettronica certificata non risulta consegnabile il gestore comunica al mittente, entro le ventiquattro ore successive all'invio, la mancata consegna tramite un avviso secondo le modalità previste dalle regole tecniche di cui all'articolo 17.

Articolo 9

Firma elettronica delle ricevute e della busta di trasporto

1. Le ricevute rilasciate dai gestori di posta elettronica certificata sono sottoscritte dai medesimi mediante una firma elettronica avanzata ai sensi dell'articolo 1, comma 1, lettera dd), del decreto del Presidente della

Repubblica 28 dicembre 2000, n. 445⁴⁴, generata automaticamente dal sistema di posta elettronica e basata su chiavi asimmetriche a coppia, una pubblica e una privata, che consente di rendere manifesta la provenienza, assicurare l'integrità e l'autenticità delle ricevute stesse secondo le modalità previste dalle regole tecniche di cui all'articolo 17.

2. La busta di trasporto è sottoscritta con una firma elettronica di cui al comma 1 che garantisce la provenienza, l'integrità e l'autenticità del messaggio di posta elettronica certificata secondo le modalità previste dalle regole tecniche di cui all'articolo 17.

Articolo 10

Riferimento temporale

1. Il riferimento temporale e la marca temporale sono formati in conformità a quanto previsto dalle regole tecniche di cui all'articolo 17.

2. I gestori di posta elettronica certificata appongono un riferimento temporale su ciascun messaggio e quotidianamente una marca temporale sui log dei messaggi.

Articolo 11

Sicurezza della trasmissione

1. I gestori di posta elettronica certificata trasmettono il messaggio di posta elettronica certificata dal mittente al destinatario integro in tutte le sue parti, includendolo nella busta di trasporto.

2. Durante le fasi di trasmissione del messaggio di posta elettronica certificata, i gestori mantengono traccia delle operazioni svolte su un apposito log dei messaggi. I dati contenuti nel suddetto registro sono conservati dal gestore di posta elettronica certificata per trenta mesi.

3. Per la tenuta del registro i gestori adottano le opportune soluzioni tecniche e organizzative che garantiscano la riservatezza, la sicurezza, l'integrità e l'inalterabilità nel tempo delle informazioni in esso contenute.

4. I gestori di posta elettronica certificata prevedono, comunque, l'esistenza di servizi di emergenza che in ogni caso assicurano il completamento della trasmissione ed il rilascio delle ricevute.

⁴⁴ dd) Firma elettronica avanzata ai sensi dell'articolo 2, comma 1, lettera g), del decreto legislativo 23 gennaio 2002, n. 10, la 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;

Articolo 12**Virus informatici**

1. Qualora il gestore del mittente riceva messaggi con virus informatici è tenuto a non accettarli, informando tempestivamente il mittente dell'impossibilità di dar corso alla trasmissione; in tale caso il gestore conserva i messaggi ricevuti per trenta mesi secondo le modalità definite dalle regole tecniche di cui all'articolo 17.
2. Qualora il gestore del destinatario riceva 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 tale caso il gestore del destinatario conserva i messaggi ricevuti per trenta mesi secondo le modalità definite dalle regole tecniche di cui all'articolo 17.

Articolo 13**Livelli minimi di servizio**

1. I gestori di posta elettronica certificata sono tenuti ad assicurare il livello minimo di servizio previsto dalle regole tecniche di cui all'articolo 17.

Articolo 14**Elenco dei gestori di posta elettronica certificata**

1. Il mittente o il destinatario che intendono fruire del servizio di posta elettronica certificata si avvalgono dei gestori inclusi in un apposito elenco pubblico disciplinato dal presente articolo.
2. Le pubbliche amministrazioni ed i privati che intendono esercitare l'attività di gestore di posta elettronica certificata inviano al CNIPA domanda di iscrizione nell'elenco dei gestori di posta elettronica certificata.
3. I richiedenti l'iscrizione nell'elenco dei gestori di posta elettronica certificata diversi dalle pubbliche amministrazioni devono avere natura giuridica di società di capitali e capitale sociale interamente versato non inferiore a un milione di euro.
4. I gestori di posta elettronica certificata o, se persone giuridiche, i loro legali rappresentanti ed i soggetti preposti all'amministrazione devono, inoltre, possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche di cui all'articolo 26 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1 settembre 1993, n. 385, e successive modificazioni.
5. Non possono rivestire la carica di rappresentante legale, di componente del consiglio di amministrazione, di componente del collegio sindacale, o di soggetto

comunque preposto all'amministrazione del gestore privato coloro i quali sono stati sottoposti a misure di prevenzione, disposte dall'autorità giudiziaria ai sensi della legge 27 dicembre 1956, n. 1423, e della legge 31 maggio 1965, n. 575, e successive modificazioni, ovvero sono stati condannati con sentenza irrevocabile, salvi gli effetti della riabilitazione, alla reclusione non inferiore ad un anno per delitti contro la pubblica amministrazione, in danno di sistemi informatici o telematici, contro la fede pubblica, contro il patrimonio, contro l'economia pubblica, ovvero per un delitto in materia tributaria.

6. Il richiedente deve inoltre:

- a) dimostrare l'affidabilità organizzativa e tecnica necessaria per svolgere il servizio di posta elettronica certificata;
 - b) impiegare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia della posta elettronica e della dimestichezza con procedure di sicurezza appropriate;
 - c) rispettare le norme del presente regolamento e le regole tecniche di cui all'articolo 17;
 - d) applicare procedure e metodi amministrativi e di gestione adeguati e tecniche consolidate;
 - e) utilizzare per la firma elettronica, di cui all'articolo 9, dispositivi che garantiscono la sicurezza delle informazioni gestite in conformità a criteri riconosciuti in ambito europeo o internazionale;
 - f) adottare adeguate misure per garantire l'integrità e la sicurezza del servizio di posta elettronica certificata;
 - g) prevedere servizi di emergenza che assicurano in ogni caso il completamento della trasmissione;
 - h) fornire, entro i dodici mesi successivi all'iscrizione nell'elenco dei gestori di posta elettronica certificata, dichiarazione di conformità del proprio sistema di qualità alle norme ISO 9000, successive evoluzioni o a norme equivalenti, relativa al processo di erogazione di posta elettronica certificata;
 - i) fornire copia di una polizza assicurativa di copertura dei rischi dell'attività e dei danni causati a terzi.
7. Trascorsi novanta giorni dalla presentazione, la domanda si considera accolta qualora il CNIPA non abbia comunicato all'interessato il provvedimento di diniego.
8. Il termine di cui al comma 7 può essere interrotto una sola volta esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità del CNIPA o che questo non possa acquisire autonomamente.

In tale caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.

9. Il procedimento di iscrizione nell'elenco dei gestori di posta elettronica certificata di cui al presente articolo può essere sospeso nei confronti dei soggetti per i quali risultano pendenti procedimenti penali per delitti in danno di sistemi informatici o telematici.

10. I soggetti di cui al comma 1 forniscono i dati, previsti dalle regole tecniche di cui all'articolo 17, necessari per l'iscrizione nell'elenco dei gestori.

11. Ogni variazione organizzativa o tecnica concernente il gestore ed il servizio di posta elettronica certificata è comunicata al CNIPA entro il quindicesimo giorno.

12. Il venire meno di uno o più requisiti tra quelli indicati al presente articolo è causa di cancellazione dall'elenco.

13. Il CNIPA svolge funzioni di vigilanza e controllo sull'attività esercitata dagli iscritti all'elenco di cui al comma 1.

Articolo 15

Gestori di posta elettronica certificata stabiliti nei Paesi dell'Unione europea

1. Può esercitare il servizio di posta elettronica certificata il gestore del servizio stabilito in altri Stati membri dell'Unione europea che soddisfi, conformemente alla legislazione dello Stato membro di stabilimento, formalità e requisiti equivalenti ai contenuti del presente decreto e operi nel rispetto delle regole tecniche di cui all'articolo 17. È fatta salva in particolare, la possibilità di avvalersi di gestori stabiliti in altri Stati membri dell'Unione europea che rivestono una forma giuridica equipollente a quella prevista dall'articolo 14, comma 2. Per i gestori di posta elettronica certificata stabiliti in altri Stati membri dell'Unione europea il CNIPA verifica l'equivalenza ai requisiti ed alle formalità di cui al presente decreto e alle regole tecniche di cui all'articolo 17.

Articolo 16

Disposizioni per le pubbliche amministrazioni

1. Le pubbliche amministrazioni possono svolgere autonomamente l'attività di gestione del servizio di posta elettronica certificata, oppure avvalersi dei servizi offerti da altri gestori pubblici o privati, rispettando le regole tecniche e di sicurezza previste dal presente regolamento.

2. L'utilizzo di caselle di posta elettronica certificata rilasciate a privati da pubbliche amministrazioni incluse nell'elenco di cui all'articolo 14, comma 2, costituisce invio valido ai sensi del presente decreto limitatamente ai rapporti intrattenuti tra le amministrazioni medesime ed i privati cui sono

rilasciate le caselle di posta elettronica certificata.

3. Le pubbliche amministrazioni garantiscono ai terzi la libera scelta del gestore di posta elettronica certificata.

4. Le disposizioni di cui al presente regolamento non si applicano all'uso degli strumenti informatici e telematici nel processo civile, nel processo penale, nel processo amministrativo, nel processo tributario e nel processo dinanzi alle sezioni giurisdizionali della Corte dei conti, per i quali restano ferme le specifiche disposizioni normative.

Articolo 17

Regole tecniche

1. Il Ministro per l'innovazione e le tecnologie definisce, ai sensi dell'articolo 8, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, sentito il Ministro per la funzione pubblica, le regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata. Qualora le predette regole riguardino la certificazione di sicurezza dei prodotti e dei sistemi è acquisito il concerto del Ministro delle comunicazioni.

Articolo 18

Disposizioni finali

1. Le modifiche di cui all'articolo 3 apportate all'articolo 14, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, (Testo A) si intendono riferite anche al decreto del Presidente della Repubblica 28 dicembre 2000, n. 444 (Testo C).

**Decreto del Ministro per l'innovazione e le tecnologie,
2 novembre 2005
“Regole tecniche per la formazione, la trasmissione e la
validazione, anche temporale, della posta elettronica certificata”
(pubblicato in Gazzetta Ufficiale n. 266 del 15 novembre 2005)**

**Capo I
PRINCIPI GENERALI**

Articolo 1

Definizioni

1. Ai fini del presente decreto si applicano le definizioni contenute nell'art. 1 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, citato nelle premesse. Si intende, inoltre, per:

- a) 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 virus informatici all'interno del messaggio, di emissione della ricevuta di accettazione e di imbustamento del messaggio originale nella busta di trasporto;
- b) punto di ricezione: il sistema che riceve il messaggio all'interno di un dominio di posta elettronica certificata, effettua i controlli sulla provenienza e sulla correttezza del messaggio ed emette la ricevuta di presa in carico, imbusta i messaggi errati in una busta di anomalia e verifica la presenza di virus informatici all'interno dei messaggi di posta ordinaria e delle buste di trasporto;
- c) punto di consegna: il sistema che compie la consegna del messaggio nella casella di posta elettronica certificata del titolare destinatario, verifica la provenienza e la correttezza del messaggio ed emette, a seconda dei casi, la ricevuta di avvenuta consegna o l'avviso di mancata consegna;
- d) firma del gestore di posta elettronica certificata: la firma elettronica avanzata, basata su un sistema di chiavi asimmetriche, che consente di rendere manifesta la provenienza e di assicurare l'integrità e l'autenticità dei messaggi del sistema di posta elettronica certificata, generata attraverso una procedura informatica che garantisce la connessione univoca al gestore e la sua univoca identificazione, creata automaticamente con mezzi che garantiscano il controllo esclusivo da parte del gestore.
- e) 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;

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

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

h) 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;

i) ricevuta completa di avvenuta consegna: la ricevuta nella quale sono contenuti i dati di certificazione ed il messaggio originale;

l) ricevuta breve di avvenuta consegna: la ricevuta nella quale sono contenuti i dati di certificazione ed un estratto del messaggio originale;

m) ricevuta sintetica di avvenuta consegna: la ricevuta che contiene i dati di certificazione;

n) 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;

o) messaggio originale: il messaggio inviato da un utente di posta elettronica certificata prima del suo arrivo al punto di accesso e consegnato al titolare destinatario per mezzo di una busta di trasporto che lo contiene;

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

q) 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;

r) dati di certificazione: i dati, quali ad esempio data ed ora di invio, mittente, destinatario, oggetto, identificativo del messaggio, che descrivono l'invio del messaggio originale e sono certificati dal gestore di posta elettronica certificata

del mittente; tali dati sono inseriti nelle ricevute e sono trasferiti al titolare destinatario insieme al messaggio originale per mezzo di una busta di trasporto;
 s) gestore di posta elettronica certificata: il soggetto che gestisce uno o più domini di posta elettronica certificata con i relativi punti di accesso, di ricezione e di consegna, titolare della chiave usata per la firma delle ricevute e delle buste e che si interfaccia con altri gestori di posta elettronica certificata per l'interoperabilità con altri titolari;

t) titolare: il soggetto a cui è assegnata una casella di posta elettronica certificata;
 u) dominio di posta elettronica certificata: dominio di posta elettronica certificata che contiene unicamente caselle di posta elettronica certificata;
 v) indice dei gestori di posta elettronica certificata: il sistema, che contiene l'elenco dei domini e dei gestori di posta elettronica certificata, con i relativi certificati corrispondenti alle chiavi usate per la firma delle ricevute, degli avvisi e delle buste, realizzato per mezzo di un server Lightweight Directory Access Protocol, di seguito denominato LDAP, posizionato in un'area raggiungibile dai vari gestori di posta elettronica certificata e che costituisce, inoltre, la struttura tecnica relativa all'elenco pubblico dei gestori di posta elettronica certificata.

z) casella di posta elettronica certificata: la casella di posta elettronica posta all'interno di un dominio di posta elettronica certificata ed alla quale è associata una funzione che rilascia ricevute di avvenuta consegna al ricevimento di messaggi di posta elettronica certificata;

aa) marca temporale: un'evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi secondo quanto previsto dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e dal decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, pubblicato nella Gazzetta Ufficiale n. 98 del 27 aprile 2004.

Articolo 2

Obiettivi e finalità

1. Il presente decreto definisce le regole tecniche relative alle modalità di realizzazione e funzionamento della posta elettronica certificata di cui al decreto del Presidente della Repubblica n. 68 del 2005.

Articolo 3

Norme tecniche di riferimento

1. Sono di seguito elencati gli standard di riferimento delle norme tecniche, le cui specifiche di dettaglio vengono riportate in allegato al presente decreto:

a) RFC 1847 (Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted);

b) RFC 1891 (SMTP Service Extension for Delivery Status Notifications);
 c) RFC 1912 (Common DNS Operational and Configuration Errors);
 d) RFC 2252 (Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions);
 e) RFC 2315 (PKCS \ 7: Cryptographic Message Syntax Version 1.5);
 f) RFC 2633 (S/MIME Version 3 Message Specification);
 g) RFC 2660 (The Secure HyperText Transfer Protocol);
 h) RFC 2821 (Simple Mail Transfer Protocol);
 i) RFC 2822 (Internet Message Format);
 l) RFC 2849 (The LDAP Data Interchange Format (LDIF) - Technical Specification);
 m) RFC 3174 (US Secure Hash Algorithm 1 - SHA1);
 n) RFC 3207 (SMTP Service Extension for Secure SMTP over Transport Layer Security);
 o) RFC 3280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List - CRL Profile).

Articolo 4

Compatibilità operativa degli standard

1. DigitPA, verifica, in funzione dell'evoluzione tecnologica, la coerenza operativa degli standard così come adottati nelle specifiche tecniche, dando tempestiva informazione delle eventuali variazioni nel proprio sito istituzionale.

Capo II

DISPOSIZIONI PER I TITOLARI E PER I GESTORI DI POSTA ELETTRONICA CERTIFICATA

Articolo 5

Comunicazione e variazione della disponibilità all'utilizzo della posta elettronica certificata

1. La dichiarazione di cui all'art. 4, comma 4, del decreto del Presidente della Repubblica n. 68 del 2005, può essere resa mediante l'utilizzo di strumenti informatici, nel qual caso la dichiarazione deve essere sottoscritta con la firma digitale di cui all'art. 1, comma 1, lettera n) del decreto del Presidente della Repubblica n. 445 del 2000.

2. La dichiarazione di cui al comma 1 è resa anche nei casi di variazione dell'indirizzo di posta elettronica certificata o di cessazione della volontà di avvalersi della posta elettronica certificata medesima.

Articolo 6Caratteristiche dei messaggi gestiti dai sistemi di
posta elettronica certificata

1. Sistemi di posta elettronica certificata generano messaggi conformi allo standard internazionale S/MIME, così come descritto dallo standard RFC 2633.
2. I messaggi di cui al comma 1 si dividono in tre categorie:
 - a) ricevute;
 - b) avvisi;
 - c) buste.
3. La differenziazione dei messaggi, come indicato nel comma 2, è realizzata dai sistemi di posta elettronica certificata utilizzando la struttura header, prevista dallo standard S/MIME, da impostare per ogni tipologia di messaggio in conformità a quanto previsto dalle specifiche tecniche di cui all'allegato.
4. I sistemi di posta elettronica certificata in relazione alla tipologia di messaggio da gestire realizzano funzionalità distinte e specifiche.
5. L'elaborazione dei messaggi di posta elettronica certificata avviene anche nel caso in cui il mittente ed il destinatario appartengano allo stesso dominio di posta elettronica certificata.
6. Le ricevute generate dai sistemi di posta elettronica certificata sono le seguenti:
 - a) ricevuta di accettazione;
 - b) ricevuta di presa in carico;
 - c) ricevuta di avvenuta consegna completa, breve, sintetica.
7. La ricevuta di avvenuta consegna è rilasciata per ogni destinatario al quale il messaggio è consegnato.
8. Gli avvisi generati dai sistemi di posta elettronica certificata sono i seguenti:
 - a) avviso di non accettazione per eccezioni formali ovvero per virus informatici;
 - b) avviso di rilevazione di virus informatici;
 - c) avviso di mancata consegna per superamento dei tempi massimi previsti ovvero per rilevazione di virus informatici.
9. Le buste generate dai sistemi di posta elettronica certificata sono le seguenti:
 - a) busta di trasporto;
 - b) busta di anomalia.
10. La busta di trasporto è consegnata imm modificata nella casella di posta elettronica certificata di destinazione per permettere la verifica dei dati di certificazione da parte del ricevente.

Articolo 7

Firma elettronica dei messaggi di posta elettronica certificata

1. I messaggi di cui all'art. 6, generati dai sistemi di posta elettronica certificata, sono sottoscritti dai gestori mediante la firma del gestore di posta elettronica certificata, in conformità a quanto previsto dall'allegato.
2. I certificati di firma di cui al comma 1 sono rilasciati da DigitPA al gestore al momento dell'iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata e sino ad un numero massimo di dieci firme per ciascun gestore.
3. Qualora un gestore abbia ravvisato la necessità di utilizzare un numero di certificati di firma superiore a dieci, può richiederli a DigitPA documentando tale necessità. DigitPA, previa valutazione della richiesta, stabilisce se fornire o meno al gestore ulteriori certificati di firma.

Articolo 8

Interoperabilità

1. Le specifiche tecniche finalizzate a garantire l'interoperabilità sono definite nell'allegato.

Articolo 9

Riferimento temporale

1. A ciascuna trasmissione è apposto un unico riferimento temporale, secondo le modalità indicate nell'allegato.
2. Il riferimento temporale può essere generato con qualsiasi sistema che garantisca stabilmente uno scarto non superiore ad un minuto secondo rispetto alla scala di tempo universale coordinato (UTC), determinata ai sensi dell'art. 3, comma 1, della legge 11 agosto 1991, n. 273.

Articolo 10

Conservazione dei log dei messaggi

1. Al fine della conservazione dei log dei messaggi, di cui alle deliberazioni di DigitPA in materia di riproduzione e conservazione dei documenti su supporto ottico, ogni gestore provvede a:
 - a) definire un intervallo temporale unitario non superiore alle ventiquattro ore;
 - b) eseguire senza soluzioni di continuità il salvataggio dei log dei messaggi generati in ciascun intervallo temporale come sopra definito.
2. Ai file generati da ciascuna operazione di salvataggio deve essere associata la relativa marca temporale.

Articolo 11**Conservazione dei messaggi contenenti virus e relativa
informativa al mittente**

1. Il gestore è tenuto a trattare il messaggio contenente virus secondo le regole tecniche indicate nell'allegato.
2. Il gestore è tenuto ad informare il mittente che il messaggio inviato contiene virus.
3. Il gestore è tenuto a conservare il messaggio contenente virus per un periodo non inferiore ai trenta mesi secondo le modalità indicate nelle deliberazioni di DigitPA in materia di riproduzione e conservazione dei documenti su supporto ottico.

Articolo 12**Livelli di servizio**

1. Il gestore di posta elettronica certificata può fissare il numero massimo di destinatari e la dimensione massima del singolo messaggio, sia per i messaggi che provengono da un suo titolare, sia per i messaggi che provengono da titolari di caselle di altri gestori di posta elettronica certificata.
2. In ogni caso il gestore di posta elettronica certificata deve garantire la possibilità dell'invio di un messaggio:
 - a) almeno fino a cinquanta destinatari;
 - b) per il quale il prodotto del numero dei destinatari per la dimensione del messaggio stesso non superi i trenta megabytes.
3. La disponibilità nel tempo del servizio di posta elettronica certificata deve essere maggiore o uguale al 99,8% del periodo temporale di riferimento.
4. Il periodo temporale di riferimento, per il calcolo della disponibilità del servizio di posta elettronica certificata, è pari ad un quadrimestre.
5. La durata massima di ogni evento di indisponibilità del servizio di posta elettronica certificata deve essere minore, o uguale, al 50% del totale previsto per l'intervallo di tempo di riferimento.
6. Nell'ambito dell'intervallo di disponibilità di cui al comma 3, la ricevuta di accettazione deve essere fornita al mittente entro un termine, da concordarsi tra gestore e titolare, da calcolare a partire dall'inoltro del messaggio, non considerando i tempi relativi alla trasmissione.
7. Al fine di assicurare in ogni caso il completamento della trasmissione ed il rilascio delle ricevute, il gestore di posta elettronica certificata descrive nel manuale operativo, di cui all'art. 23, le soluzioni tecniche ed organizzative che realizzano i servizi di emergenza, ai sensi di quanto previsto dall'art. 11, comma 4, del decreto del Presidente della Repubblica n. 68 del 2005, e consentano il rispetto dei vincoli definiti nei commi 4 e 5 del presente articolo.

Articolo 13**Avvisi di mancata consegna**

1. Qualora il gestore del mittente non abbia ricevuto dal gestore del destinatario, nelle dodici ore successive all'inoltro del messaggio, la ricevuta di presa in carico o di avvenuta consegna del messaggio inviato, comunica al mittente che il gestore del destinatario potrebbe non essere in grado di realizzare la consegna del messaggio.
2. Qualora, entro ulteriori dodici ore, il gestore del mittente non abbia ricevuto 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, così come previsto dal decreto del Presidente della Repubblica n. 68 del 2005

Articolo 14**Norme di garanzia sulla natura della posta elettronica ricevuta**

1. Il gestore di posta elettronica certificata del destinatario ha l'obbligo di segnalare a quest'ultimo se la posta elettronica in arrivo non è qualificabile come posta elettronica certificata, secondo quanto prescritto dal decreto del Presidente della Repubblica n. 68 del 2005, nonché dal presente decreto e relativo allegato.
2. I messaggi relativi all'invio e alla consegna di documenti attraverso la posta elettronica certificata sono rilasciati indipendentemente dalle caratteristiche e dal valore giuridico dei documenti trasmessi.

Articolo 15**Limiti di utilizzo**

1. La pubblica amministrazione che intende iscriversi all'elenco dei gestori di posta elettronica certificata, di cui all'art. 14 del decreto del Presidente della Repubblica n. 68 del 2005, è tenuta a presentare a DigitPA una relazione tecnica che illustri le misure adottate affinché l'utilizzo di caselle di posta elettronica rilasciate a privati dall'amministrazione medesima:
 - a) costituisca invio valido ai sensi dell'art. 16, comma 2, del decreto del Presidente della Repubblica n. 68 del 2005;
 - b) avvenga limitatamente ai rapporti di cui al medesimo art. 16, comma 2.

Articolo 16**Modalità di iscrizione all'elenco dei gestori di posta elettronica certificata**

1. I soggetti che presentano domanda di iscrizione all'elenco pubblico, di cui all'art. 14 del decreto del Presidente della Repubblica n. 68 del 2005, forniscono

inoltre a DigitPA le informazioni e i documenti di seguito indicati, anche su supporto elettronico, ad eccezione del documento di cui alla lettera e):

- a) denominazione sociale;
- b) sede legale;
- c) sedi presso le quali è erogato il servizio;
- d) rappresentante legale;
- e) piano per la sicurezza, contenuto in busta sigillata;
- f) manuale operativo di cui all'art. 23;
- g) dichiarazione di impegno al rispetto delle disposizioni del decreto del Presidente della Repubblica n. 68 del 2005;
- h) dichiarazione di conformità ai requisiti previsti nel presente decreto e suo allegato;
- i) relazione sulla struttura organizzativa.

2. I soggetti che rivestono natura giuridica privata trasmettono, inoltre, copia cartacea di una polizza assicurativa o di un certificato provvisorio impegnativo di copertura dei rischi dell'attività e dei danni causati a terzi, rilasciata da una società di assicurazioni abilitata ad esercitare nel campo dei rischi industriali, a norma delle vigenti disposizioni.

Articolo 17

Equivalenza dei requisiti dei gestori stranieri

1. Il gestore di posta elettronica certificata stabilito in altri Stati membri dell'Unione europea che si trovi nelle condizioni di cui all'art. 15 del decreto del Presidente della Repubblica n. 68 del 2005 ed intenda esercitare il servizio di posta elettronica certificata in Italia, comunica in via preventiva a DigitPA tale intenzione ed ogni notizia utile al fine della verifica di cui al citato art. 15. La comunicazione costituisce domanda di iscrizione nell'elenco di gestori di posta elettronica certificata; sono applicabili le disposizioni procedurali di cui all'art. 14 del decreto del Presidente della Repubblica n. 68 del 2005.

Articolo 18

Indice ed elenco pubblico dei gestori di posta elettronica certificata

1. I gestori di posta elettronica certificata si attengono alle regole riportate nell'allegato per accedere all'indice dei gestori di posta elettronica certificata..

2. Il certificato elettronico, da utilizzare per la funzione di accesso di cui al comma 1, è rilasciato da DigitPA al gestore al momento dell'iscrizione nell'elenco pubblico di cui all'art. 14 del decreto del Presidente della Repubblica n. 68 del 2005.

3. L'elenco pubblico dei gestori di posta elettronica certificata tenuto da DigitPA contiene, per ogni gestore, le seguenti indicazioni:

- a) denominazione sociale;
- b) sede legale;
- c) rappresentante legale;
- d) indirizzo internet;
- e) data di iscrizione all'elenco;
- f) data di cessazione ed eventuale gestore sostitutivo.

4. L'elenco pubblico è sottoscritto con firma digitale di DigitPA, che lo rende disponibile per via telematica.

Articolo 19

Disciplina dei compiti di DigitPA

1. DigitPA definisce con circolari le modalità di inoltro della domanda e le modalità dell'esercizio dei compiti di vigilanza e controllo di cui all'art. 14 del decreto del Presidente della Repubblica n. 68 del 2005.

Articolo 20

Sistema di qualità del gestore

1. Entro un anno dall'iscrizione del gestore all'elenco pubblico di cui all'art. 14 del decreto del Presidente della Repubblica n. 68 del 2005, il gestore medesimo fornisce copia della certificazione di conformità del proprio sistema di qualità alle norme UNI EN ISO 9001:2000 e successive evoluzioni relativamente a tutti i processi connessi al servizio di posta elettronica certificata.

2. Il manuale della qualità è depositato presso DigitPA e reso disponibile presso il gestore.

Articolo 21

Organizzazione e funzioni del personale del certificatore

1. L'organizzazione del personale addetto al servizio di posta elettronica certificata prevede almeno la presenza di responsabili preposti allo svolgimento delle seguenti attività e funzioni:

- a) registrazione dei titolari;
- b) servizi tecnici;
- c) verifiche e ispezioni (auditing);
- d) sicurezza;
- e) sicurezza dei log dei messaggi;
- f) sistema di riferimento temporale.

2. È possibile attribuire al medesimo soggetto più responsabilità tra quelle previste dalle lettere d), e) ed f).

Articolo 22

Requisiti di competenza ed esperienza del personale

1. Il personale cui sono attribuite le funzioni previste dall'art. 21 deve aver maturato un'esperienza almeno quinquennale nelle attività di analisi, progettazione, commercializzazione e conduzione di sistemi informatici.
2. Per ogni aggiornamento apportato al sistema di posta elettronica certificata, il gestore eroga, alle figure professionali interessate, apposita attività di addestramento.

Articolo 23

Manuale operativo

1. Il manuale operativo definisce e descrive le procedure applicate dal gestore di posta elettronica certificata nello svolgimento della propria attività.
2. Il manuale operativo è depositato presso DigitPA.
3. Il manuale contiene:
 - a) i dati identificativi del gestore;
 - b) i dati identificativi della versione del manuale operativo;
 - c) l'indicazione del responsabile del manuale operativo;
 - d) l'individuazione, l'indicazione e la definizione degli obblighi del gestore di posta elettronica certificata e dei titolari;
 - e) la definizione delle responsabilità e delle eventuali limitazioni agli indennizzi;
 - f) l'indirizzo del sito web del gestore ove sono pubblicate le informazioni relative ai servizi offerti;
 - g) le modalità di protezione della riservatezza dei dati;
 - h) le modalità per l'apposizione e la definizione del riferimento temporale.

Decreto legge del 29 novembre 2008, n. 185, recante “misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale”, convertito in legge, con modificazioni, con la Legge 28 del gennaio 2009, n. 2

(pubblicata in Gazzetta Ufficiale n. 22 del 28 gennaio 2009 - supplemento ordinario)

[...]

Articolo 16

Riduzione dei costi amministrativi a carico delle imprese

6. Le imprese costituite in forma societaria sono tenute a indicare il proprio indirizzo di posta elettronica certificata nella domanda di iscrizione al registro delle imprese o analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità del contenuto delle stesse, garantendo l'interoperabilità con analoghi sistemi internazionali. Entro tre anni dalla data di entrata in vigore del presente decreto tutte le imprese, già costituite in forma societaria alla medesima data di entrata in vigore, comunicano al registro delle imprese l'indirizzo di posta elettronica certificata. L'iscrizione dell'indirizzo di posta elettronica certificata nel registro delle imprese e le sue successive eventuali variazioni sono esenti dall'imposta di bollo e dai diritti di segreteria.
7. I professionisti iscritti in albi ed elenchi istituiti con legge dello Stato comunicano ai rispettivi ordini o collegi il proprio indirizzo di posta elettronica certificata o analogo indirizzo di posta elettronica di cui al comma 6 entro un anno dalla data di entrata in vigore del presente decreto. Gli ordini e i collegi pubblicano in un elenco riservato, consultabile in via telematica esclusivamente dalle pubbliche amministrazioni, i dati identificativi degli iscritti con il relativo indirizzo di posta elettronica certificata.
8. Le amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni, qualora non abbiano provveduto ai sensi dell'articolo 47, comma 3, lettera a), del Codice dell'Amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, istituiscono una casella di posta certificata o analogo indirizzo di posta elettronica di cui al comma 6 per ciascun registro di protocollo e ne danno comunicazione al Centro nazionale per l'informatica nella pubblica

amministrazione, che provvede alla pubblicazione di tali caselle in un elenco consultabile per via telematica. Dall'attuazione del presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e si deve provvedere nell'ambito delle risorse disponibili.

9. Salvo quanto stabilito dall'articolo 47, commi 1 e 2, del codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, le comunicazioni tra i soggetti di cui ai commi 6, 7 e 8 del presente articolo, che abbiano provveduto agli adempimenti ivi previsti, possono essere inviate attraverso la posta elettronica certificata o analogo indirizzo di posta elettronica di cui al comma 6, senza che il destinatario debba dichiarare la propria disponibilità ad accettarne l'utilizzo.

10. La consultazione per via telematica dei singoli indirizzi di posta elettronica certificata o analoghi indirizzi di posta elettronica di cui al comma 6, nel registro delle imprese o negli albi o elenchi costituiti ai sensi del presente articolo avviene liberamente e senza oneri. L'estrazione di elenchi di indirizzi è consentita alle sole pubbliche amministrazioni per le comunicazioni relative agli adempimenti amministrativi di loro competenza.

[...]

Articolo 16-bis

Misure di semplificazione per le famiglie e per le imprese

[...]

5. Per favorire la realizzazione degli obiettivi di massima diffusione delle tecnologie telematiche nelle comunicazioni, previsti dal codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai cittadini che ne fanno richiesta è attribuita una casella di posta elettronica certificata.

L'utilizzo della posta elettronica certificata avviene ai sensi degli articoli 6 e 48 del citato codice di cui al decreto legislativo n. 82 del 2005, con effetto equivalente, ove necessario, alla notificazione per mezzo della posta. Le comunicazioni che transitano per la predetta casella di posta elettronica certificata sono senza oneri.

6. Per i medesimi fini di cui al comma 5, ogni amministrazione pubblica utilizza unicamente la posta elettronica certificata, ai sensi dei citati articoli 6 e 48 del codice di cui al decreto legislativo n. 82 del 2005, con effetto equivalente, ove necessario, alla notificazione per mezzo della posta, per le comunicazioni e le notificazioni aventi come destinatari dipendenti della stessa o di altra amministrazione pubblica.

7. Con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro per la pubblica amministrazione e l'innovazione, da emanare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, previa intesa in sede di Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, e successive modificazioni, sono definite le modalità di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini ai sensi del comma 5 del presente articolo, con particolare riguardo alle categorie a rischio di esclusione ai sensi dell'articolo 8 del citato codice di cui al decreto legislativo n. 82 del 2005, nonché le modalità di attivazione del servizio mediante procedure di evidenza pubblica, anche utilizzando strumenti di finanza di progetto. Con il medesimo decreto sono stabilite le modalità di attuazione di quanto previsto nel comma 6, cui le amministrazioni pubbliche provvedono nell'ambito degli ordinari stanziamenti di bilancio.

[...]

DPCM 6 maggio 2009**“Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini”****(pubblicato in Gazzetta Ufficiale n. 119 del 25 maggio 2009)****Art. 1****Oggetto**

1. Il presente decreto definisce le modalità di rilascio e di utilizzo della casella di posta elettronica certificata assegnata ai cittadini ai sensi dell'art. 16-bis, commi 5 e 6, del decreto-legge 29 novembre 2008, n. 185, di seguito: «PEC», con particolare riguardo alle categorie a rischio di esclusione ai sensi dell'art. 8 del codice dell'amministrazione digitale, di cui al decreto legislativo n. 82 del 2005, nonché le modalità di attivazione del servizio mediante procedure di evidenza pubblica, anche utilizzando strumenti di finanza di progetto.

Articolo 2

Modalità di attivazione e rilascio casella di PEC al cittadino

1. Al cittadino che ne fa richiesta la Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie, direttamente o tramite l'affidatario del servizio, assegna un indirizzo di PEC.
2. L'attivazione della PEC e le comunicazioni che transitano per la predetta casella di PEC sono senza oneri per il cittadino.
3. Le modalità di richiesta, di attivazione, di utilizzo e di recesso dal servizio di PEC sono definite nell'allegato A che costituisce parte integrante del presente decreto.

Articolo 3

Utilizzo della PEC per il cittadino

1. La PEC consente l'invio di documenti informatici per via telematica la cui trasmissione avviene ai sensi degli articoli 6 e 48 del citato codice di cui al decreto legislativo n. 82 del 2005, con gli effetti di cui all'art. 16-bis, comma 5, del decreto-legge 29 novembre 2008, n. 185.
2. Per i cittadini che utilizzano il servizio di PEC, l'indirizzo valido ad ogni effetto giuridico, ai fini dei rapporti con le pubbliche amministrazioni, è quello espressamente rilasciato ai sensi dell'art. 2, comma 3. Le modalità e le procedure tecniche relative alla conoscibilità dell'atto saranno precisate

nell'ambito delle specifiche del servizio.

4. La volontà del cittadino espressa ai sensi dell'art. 2, comma 1, rappresenta la esplicita accettazione dell'invio, tramite PEC, da parte delle pubbliche amministrazioni di tutti i provvedimenti e gli atti che lo riguardano.

Articolo 4

Modalità di attivazione della PEC per le pubbliche amministrazioni

1. Le pubbliche amministrazioni, di cui all'art. 1, comma 2 del decreto legislativo 30 marzo 2001, n. 165, istituiscono una casella di PEC per ogni registro di protocollo e ne danno comunicazione a DigitPA che provvede alla pubblicazione in rete consultabile per via telematica.
2. Le pubbliche amministrazioni, nell'adempire a quanto previsto dall'art. 57, comma 1, del decreto legislativo 7 marzo 2005, n. 82, includono gli estremi di eventuali pagamenti per ogni singolo procedimento.
3. Ai sensi dell'art. 54, comma 1, del decreto legislativo 7 marzo 2005, n. 82, le pubbliche amministrazioni rendono disponibili sul loro sito istituzionale, per ciascun procedimento, ogni tipo di informazione idonea a consentire l'inoltro di istanze da parte dei cittadini titolari di PEC, inclusi i tempi previsti per l'espletamento della procedura.
4. Le pubbliche amministrazioni accettano le istanze dei cittadini inviate tramite PEC nel rispetto dell'art. 65, comma 1, lettera c), del decreto legislativo n. 82 del 2005. L'invio tramite PEC costituisce sottoscrizione elettronica ai sensi dell'art. 21, comma 1, del decreto legislativo n. 82 del 2005; le pubbliche amministrazioni richiedono la sottoscrizione mediante firma digitale ai sensi dell'art. 65, comma 2, del citato decreto legislativo.

Articolo 5

Procedura di scelta dell'affidatario

1. Per l'individuazione dell'affidatario, anche costituito in associazione temporanea d'impresa o consorzio, del servizio di PEC ai cittadini, la Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie avvia le procedure di evidenza pubblica, anche utilizzando gli strumenti di finanza di progetto ai sensi del decreto legislativo 12 aprile 2006, n. 163, recante «Codice dei contratti pubblici relativi a lavori, servizi e forniture in attuazione delle direttive 2004/17/CE e 2004/18/CE».
2. Nella procedura di cui al comma 1, la Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie definisce le caratteristiche tecniche del servizio, i livelli di servizio garantiti, gli obblighi, anche informativi, dell'affidatario nonché gli ulteriori servizi da mettere a

disposizione, anche con specifico riferimento alle categorie a rischio di esclusione ai sensi dell'art. 8 del decreto legislativo n. 82 del 2005.

Articolo 6

Monitoraggio del servizio PEC

1. L'affidatario del servizio fornisce alla Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie e alle pubbliche amministrazioni, per quanto di competenza di ciascuna di esse, elementi quantitativi e qualitativi relativi alle pubbliche amministrazioni adempienti ed a quelle non adempienti, nonché ogni altro elemento atto a verificare l'effettiva funzionalità, anche con riferimento ai tempi di espletamento delle procedure del servizio di PEC.
2. Tali elementi sono presi in considerazione ai fini della valutazione dei risultati conseguiti dalle pubbliche amministrazioni in base alle norme vigenti in materia.

Articolo 7

Accessibilità degli indirizzi di PEC ai cittadini

1. L'affidatario del servizio di PEC ai cittadini di cui all'art. 6, comma 1, rende consultabili alle pubbliche amministrazioni, in via telematica, gli indirizzi di PEC di cui al presente decreto, nel rispetto dei criteri di qualità e sicurezza ed interoperabilità definiti da DigitPA e nel rispetto della disciplina in materia di tutela dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.

Articolo 8

Diffusione e pubblicità dell'iniziativa

1. La Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie cura la realizzazione di campagne di comunicazione volte a diffondere e pubblicizzare i contenuti dell'iniziativa e le modalità di rilascio e di uso della casella di PEC ai cittadini, con particolare riguardo alle categorie a rischio di esclusione ai sensi dell'art. 8 del decreto legislativo n. 82 del 2005.

Art. 9

Comunicazioni tra pubbliche amministrazioni e dipendenti

1. I pubblici dipendenti, all'atto dell'assegnazione di una casella di PEC da parte dell'amministrazione di appartenenza, possono optare per l'utilizzo della stessa ai fini di cui all'art. 16-bis, comma 6, del decreto-legge 29 novembre 2008, n. 185.
2. Per adempire alle finalità di cui all'art. 16-bis, comma 6, del decreto-legge

29 novembre 2008, n. 185, le pubbliche amministrazioni ovvero altri soggetti pubblici da loro delegati o le loro associazioni rappresentative, mediante convenzione stipulata direttamente con la Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie o con l'affidatario del servizio, definiscono le modalità, nel rispetto della normativa vigente, con le quali viene attribuita la casella di PEC ai propri dipendenti.

ALLEGATO A

Modalità per la richiesta, l'attivazione, l'utilizzo e il recesso del servizio di posta elettronica certificata per i cittadini

Modalità di richiesta del servizio.

Qualunque cittadino italiano maggiorenne, compresi i cittadini residenti all'estero, può chiedere l'attivazione di un'utenza personale di posta elettronica certificata accedendo al sito dedicato al servizio di posta elettronica certificata per i cittadini (di seguito sito).

Sul sito sono evidenziate:

- le regole per l'attivazione e l'utilizzo del servizio da parte del cittadino;
- i requisiti tecnici per l'accesso al servizio;
- le buone prassi per l'utilizzo del servizio in condizioni di massima sicurezza;
- i manuali d'uso di riferimento.

Sul sito è altresì disponibile tutta la documentazione inerente le caratteristiche del servizio reso, gli obblighi contrattuali dell'affidatario del servizio e la normativa di riferimento.

Per effettuare la richiesta il cittadino inserisce in appositi campi i propri dati anagrafici comprensivi del codice fiscale; deve inoltre scegliere la password ovvero idonei sistemi di accesso sicuro al servizio. Il sistema verifica la coerenza dei dati, sulla base delle informazioni fornite.

La richiesta si perfeziona con l'attivazione mediante esplicita operazione con cui il cittadino dichiara di avere preso visione delle condizioni indicate e di averle espressamente accettate. La registrazione di tale operazione, confermata dalla successiva attivazione dell'utenza, costituisce evidenza, valida ai fini di legge, della volontà del cittadino di aderire alle condizioni d'uso del servizio di posta elettronica certificata.

La fase di richiesta si conclude con la comunicazione del suo esito e, se positivo, con l'indicazione delle modalità di attivazione.

Attivazione del servizio.

L'attivazione dell'utenza di posta elettronica certificata per i cittadini ha luogo presso uffici pubblici o aperti al pubblico largamente diffusi sul territorio e dotati di connessione telematica, la cui tipologia e localizzazione è resa pubblica attraverso mezzi di comunicazione di massa. L'elenco di tali uffici è inoltre reperibile sul sito di richiesta del servizio.

I cittadini possono recarsi presso gli uffici abilitati all'attivazione a partire dalla data comunicata dal sito all'atto della registrazione entro e non oltre tre mesi a partire da tale data, muniti di un documento di riconoscimento valido

e del documento recante il codice fiscale.

L'ufficio abilitato effettua la verifica della correttezza dei dati identificativi collegandosi al sito e, nel caso di verifica positiva, provvede alla stampa della richiesta che viene firmata dal richiedente dando così luogo all'attivazione del servizio, anche tramite la consegna delle credenziali di accesso al medesimo. L'ufficio abilitato provvede inoltre ad informare il richiedente, in modo compiuto e chiaro, sulle condizioni d'uso del servizio.

Utilizzo del servizio.

Il cittadino deve utilizzare il servizio attenendosi alle modalità operative ed alle regole indicate sul sito.

L'uso del servizio è personale e riservato. Non è consentito accedere ad un'utenza per conto di terzi o cedere la propria utenza a terzi. La password per l'accesso al servizio deve essere mantenuta segreta e modificata periodicamente seguendo le regole pubblicate sul sito.

Il cittadino può richiedere, attraverso funzioni rese disponibili dal sito, la notifica dell'avvenuta ricezione di un messaggio di posta elettronica certificata, mediante comunicazione verso un altro indirizzo di posta elettronica da lui prescelto.

L'affidatario del servizio può rendere disponibili, secondo regole predefinite, funzionalità aggiuntive utili per la gestione della corrispondenza, quali la notifica tramite sms, l'invio di comunicazioni in formato cartaceo, l'inoltro dei messaggi verso altre caselle di posta elettronica, la conservazione delle email a lungo periodo, ecc.

All'indirizzo di posta elettronica certificata del cittadino possono essere associati uno o più recapiti a cui inviare le comunicazioni in forma cartacea, nei casi previsti, nonché numeri di telefono sia fissi che mobili, numeri di fax, indirizzi di posta elettronica ed ogni altro strumento utile per comunicazioni inerenti il servizio. In caso di variazione, è compito e responsabilità del cittadino aggiornare tali riferimenti, anche utilizzando gli appositi servizi telematici di gestione del suo profilo personale.

Possono altresì essere resi disponibili servizi di gestione del fascicolo individuale digitale concernente gli atti amministrativi relativi al rapporto tra il cittadino e la pubblica amministrazione, nonché altri servizi idonei ad assicurare una migliore funzionalità della PEC. L'affidatario deve altresì assicurare la gestione degli elenchi degli indirizzi di posta elettronica certificata rendendone disponibile la consultazione alle pubbliche amministrazioni.

L'affidatario deve mantenere traccia delle operazioni svolte sulla casella elettronica certificata ed adotta inoltre le opportune soluzioni tecniche

organizzative che garantiscono la riservatezza, la sicurezza e l'integrità nel tempo delle informazioni.

Recesso dal servizio

In qualunque momento il cittadino può comunicare la sua volontà di recedere dal servizio di posta elettronica certificata. La comunicazione è effettuata, previa autenticazione, tramite un'apposita funzione del sito.

Il recesso comporta la cessazione del servizio e la conseguente cancellazione dagli elenchi contenenti gli indirizzi di posta elettronica certificata dei cittadini entro ventiquattro ore dall'avvenuta comunicazione del recesso.

In conseguenza del recesso, le comunicazioni tra il cittadino e la pubblica amministrazione si realizzano secondo le procedure tradizionali.