Questo documento riporta delle note integrative ai documenti di riferimento della Posta Elettronica Certificata (PEC). Nello specifico le seguenti note fanno riferimento a:

- Decreto del Presidente della Repubblica 11 febbraio 2005, n.68 "*Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3. [G.U. n. 97 del 28-4-2005]*";
- Decreto Ministeriale 2 novembre 2005 "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata" [G.U. del 14 novembre 2005, n. 265]";
- Allegato al Decreto Ministeriale 2 novembre 2005, "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata" [G.U. del 14 novembre 2005, n. 265], nel seguito indicato RT.

Le seguenti note integrative sono fornite al fine di migliorare la comprensione di alcuni temi che potenzialmente possono presentare criticità interpretative.

Le note sono elencate dalla più recente alla meno recente.

[05/05/2008 NOTA 11]

Questa nota definisce quali sono le informazioni di cui un gestore deve tenere traccia nei log PEC, al fine di rispettare quanto previsto dall'articolo 6, comma 7 del DPR

La posta elettronica certificata consente l'invio di messaggi la cui trasmissione è valida agli effetti di legge. Come previsto dall'art. 4, comma 6, del DPR, 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'art 6 dello stesso DPR.
Più in dettaglio, il mittente, a seconda dell'esito dell'invio, riceverà delle ricevute o degli avvisi, secondo quanto previsto dall'art. 6 del DM 2 novembre 2005.
Le possibili ricevute ed avvisi che un sistema di posta elettronica certificata rilascia ad un mittente sono:

a) ricevuta di accettazione;
b) avviso di non accettazione per eccezioni formali ovvero per virus informatici;
c) ricevuta di avvenuta consegna, che può essere completa, breve o sintetica;
d) avviso di mancata consegna per superamento dei tempi massimi previsti ovvero per rilevazione di virus informatici;
e) avviso di mancata consegna.

Nel caso in cui un mittente non disponga più dei precedenti avvisi e/o ricevute le tracce delle operazioni svolte, conservate dai gestori su un apposito log dei messaggi, sono opponibili a terzi ai sensi dell'articolo 6, comma 7 del DPR.

Le regole tecniche allegate al DM 2 novembre 2005 definiscono le finalità del log dei messaggi ed individuano i dati significativi che devono essere detenuti dal gestore per ogni evento che si verifica sul sistema PEC presso i punti di accesso, ricezione e consegna.

In relazione a quanto detto, un gestore deve essere in grado di fornire, dietro richiesta di un titolare di una casella PEC, le informazioni associate ad un invio di un messaggio di posta elettronica certificata. La seguente tabella identifica tali informazioni in funzione dell'evento considerato e delle possibili ricevute/avvisi associati.

EVENTO	RICEVUTE/AVVISI ASSOCIATE ALL'EVENTO	INFORMAZIONI DA REGISTRARE NEL LOG									
		messagge-ID messaggio originale	data	ora	mittente	destinatari	oggetto	tipo evento	gestore mittente	tipologia destinatari	descrizione
		O	O	O	O	O	O	O	O	R	R
Invio	ricevuta di accettazione	X	X	X	X	X	X	X	X	X	
	avviso di non accettazione per eccezioni formali	X	X	X	X	X	X	X	X		X
	avviso di non accettazione per virus informatico	X	X	X	X	X	X	X	X		X
Ricezione	ricevuta completa di avvenuta consegna	X	X	X	X	X	X	X	X		
	ricevuta breve di avvenuta consegna	X	X	X	X	X	X	X	X		
	ricevuta sintetica di avvenuta consegna	X	X	X	X	X	X	X	X		
	avviso di mancata consegna per superamento dei tempi massimi previsti	X	X	X	X	X	X	X	X		X
	avviso di mancata consegna per rilevazione virus informatico	X	X	X	X	X	X	X	X		X
	avviso di mancata consegna	X	X	X	X	X	X	X	X		X

Legenda della tipologia delle informazioni: O = obbligatorio, R = raccomandato

Il paragrafo 6.2 delle RT dispone la memorizzazione nel log di un'informazione non presente nella precedente tabella e relativa al message-ID dei messaggi correlati generati. Questa

informazione, di tipo "O", è necessaria per associare tutte le ricevute/avvisi relativi ad un invio ad una ricevuta di accettazione.

Nella tabella sono inserite le colonne "tipologia destinatari" e "descrizione" che sono informazioni non comprese tra quelle elencate al punto 6.2 delle RT, ma presenti nella parte testuale di alcuni avvisi e ricevute. Per poter riproporre le stesse informazioni contenute negli avvisi e nelle ricevute originali, si raccomanda comunque la memorizzazione, all'interno dei log, anche di queste due informazioni.

La colonna "tipologia destinatari", di tipo "R", indica che il gestore deve memorizzare le categorie di destinatari (posta ordinaria o posta certificata), previste nella ricevuta di accettazione.

La colonna "descrizione", di tipo "R", indica che il gestore deve memorizzare:

- per l'avviso di non accettazione per virus informatico, quanto previsto dal campo "identificativo del tipo di contenuto rilevato" relativo al paragrafo 6.4.3.1 delle RT;
- per l'avviso di non accettazione per eccezioni formali, quanto previsto dal campo "descrizione errore" relativo al paragrafo 6.3.2 delle RT;
- per l'avviso di mancata consegna per superamento dei tempi massimi, a seconda delle circostanze, una indicazione che faccia riferimento alla mancata consegna nelle prime 12 ore oppure alla mancata consegna nelle successive 12 ore (ad es. "superamento tempi massimi, 12 ore" oppure "superamento tempi massimi, 24 ore");
- per l'avviso di mancata consegna per rilevazione virus, quanto previsto dal campo "identificativo del tipo di contenuto rilevato" relativo al paragrafo 6.4.3.3 delle RT;
- per l'avviso di mancata consegna, quanto previsto dal campo "errore sintetico" relativo al paragrafo 6.5.3 delle RT.

E' opportuno ricordare che tutte le informazioni, sia obbligatorie che raccomandate, sono presenti nel file XML allegato ad ogni ricevuta/avviso PEC.

Se il gestore memorizza anche le informazioni previste nelle colonne "tipologia destinatari" e "descrizione", di tipo "R", deve estrarle dal log insieme alle informazioni di tipo "O".

Infine, quando il gestore restituisce al titolare della casella le informazioni presenti nel log, è opportuno che il formato di presentazione di tali informazioni sia adeguatamente strutturato e quanto più possibile analogo ad una ricevuta/avviso di posta elettronica certificata rilasciato abitualmente dal gestore stesso.

[23/01/2008 NOTA 10]

Questa nota definisce il comportamento del gestore in relazione alle indisponibilità del servizio, in presenza di indisponibilità minori di cinque minuti.

Per evitare ai gestori l'onere di dover comunicare formalmente non disponibilità di durata limitata, si ritiene tollerabile l'assenza di comunicazioni per eventi che non superino i cinque minuti.

La scelta deriva dall'aver rilevato che, frequentemente, le indisponibilità di durata non superiore ai cinque minuti possono essere indotte dalle caratteristiche proprie dei sistemi di monitoraggio.
Rimane comunque l'obbligo di indicare la durata di tali eventi nei report quadrimestrali.

I precedenti contenuti si devono considerare un'integrazione alla nota 5 del 16/11/2007 nella quale è specificato che: "*Ogni evento di indisponibilità deve essere comunicato al Cnipa, utilizzando il modulo per la segnalazione dei malfunzionamenti gravi disponibile sul sito web.*"

[05/12/2007 NOTA 9]

Questa nota riporta alcune spiegazioni per facilitare la corretta interpretazione circa l'avviso di mancata consegna per superamento dei tempi massimi previsti, par 6.3.5 dell'allegato al Decreto Ministeriale 2 novembre 2005.

PARAGRAFO 6.3.5 – PRIME 12 ORE

"*Qualora il gestore mittente non abbia ricevuto dal gestore del destinatario, nelle 12 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 effettuare la consegna del messaggio.*"

E' sufficiente che il gestore, nelle prime 12 ore, abbia ricevuto almeno una delle due ricevute per non emettere l'avviso di mancata consegna relativo alle prime 12 ore.

Ad esempio:
il gestore mittente al momento dell'invio del messaggio avvia il timer per calcolare quando emettere eventualmente l'avviso di mancata consegna relativo alle 12 ore.

a) Se entro le prime 12 ore il gestore mittente riceve solo la ricevuta di presa in carico allora non emette l'avviso di mancata consegna relativo alle prime 12 ore;
b) Se entro le prime 12 ore riceve solo la ricevuta di avvenuta consegna, pur non ricevendo quella di presa in carico, la transazione si considera conclusa correttamente dal punto di vista del mittente, poiché c'è l'evidenza dell'avvenuta consegna.
   L'assenza di presa in carico non pregiudica quindi la corretta conclusione della trasmissione. In questo caso, tuttavia, il gestore mittente non avrà a disposizione l'evidenza del passaggio di consegne con il gestore destinatario.
   In altre parole si è presentata un anomalia nella trasmissione che ha causato l'assenza della ricevuta di presa in carico, ma non la corretta conclusione del processo di invio del messaggio.

PARAGRAFO 6.3.5 – SUCCESSIVE 12 ORE

"Qualora, entro ulteriori 12 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 e non prima delle 22 ore successive all'invio"

E' sufficiente che il gestore non riceva, nelle ulteriori successive 12 ore, la ricevuta di avvenuta consegna, per emettere l'avviso di mancata consegna per superamento dei tempi massimi previsti

La seguente tabella mostra i possibili scenari e i corretti comportamenti da parte del gestore mittente:

ricezione della ricevuta di **presa in carico entro le 12 ore**	Ricezione della ricevuta di **avvenuta consegna entro le 12 ore**	Ricezione della ricevuta di **avvenuta consegna dopo le 12 ore ed entro le 24 ore**	Emissione avviso di mancata consegna per superamento dei tempi massimi previsti
X	X		NO
X		X	NO
X			SI (24 ore)
	X		NO
		X	SI (12 ore)
			SI (12 ore e 24 ore)

[05/12/2007 NOTA 8]

Questa nota riporta alcuni aspetti circa la ricevuta di avvenuta consegna breve nel caso il messaggio originale sia in formato S/MIME.

In primo luogo si rammenta che la ricevuta di avvenuta consegna breve inserisce al suo interno il messaggio originale, sostituendone gli allegati con i relativi hash crittografici al fine di ridurre le dimensioni della ricevuta.

Nel caso di messaggi originali in formato S/MIME è necessario non alterare l'integrità della struttura del messaggio modificando la parte MIME che contiene i dati di firma, cioè la parte MIME "application/pkcs7-signature" oppure "application/x-pkcs7-signature".

Un messaggio S/MIME con MIME type multipart/signed (come da RFC 1847) è formato da due parti MIME:

1. la prima parte, costituisce il messaggio composto dal mittente prima della sua firma; ad esempio, questa parte può essere di tipo "multipart/mixed" ed essere composta a sua volta, da una parte di tipo "text/plain" (ad esempio, il corpo del messaggio) e da una parte di tipo "application/vnd.ms-excel" (ad esempio, un attach di tipo excel);

2. la seconda parte (generalmente di tipo "application/pkcs7-signature" oppure "application/x-pkcs7-signature"), contiene i dati di firma, cioè i dati aggiunti durante la fase di firma del messaggio e deve essere lasciata inalterata per non compromettere la struttura complessiva del messaggio.

Pertanto, nel caso di emissione della ricevuta breve di avvenuta consegna, il gestore destinatario dovrà:

1. individuare e estrarre tutti gli allegati dalla sezione di cui al precedente punto 1;
2. effettuare l'hash di tutti file allegati dal mittente al messaggio originale;
3. inserire, al posto degli originali, i rispettivi hash.

In generale, la copia del messaggio contenuta all'interno della ricevuta di avvenuta consegna breve avrà le seguenti caratteristiche:

- se il messaggio originale è firmato, la struttura S/MIME ed i relativi dati di firma resteranno inalterati. Il messaggio genererà un errore in un'eventuale fase di verifica dell'integrità della firma, in seguito alla sostituzione degli allegati con i relativi hash;

- se il messaggio originale è crittografato gli allegati contenuti nel messaggio non saranno sostituiti dagli hash data l'impossibilità di identificarli all'interno del blocco crittografico. Il contenuto della ricevuta di avvenuta consegna breve coinciderà quindi con quello di una normale ricevuta di avvenuta consegna.

[05/12/2007 NOTA 7]

Questa nota tratta l'avviso di rilevazione virus informatico.

Quando un sistema PEC riceve un messaggio contenente un virus informatico deve, dopo aver emesso la ricevuta di presa in carico (come specificato nella seguente NOTA 4), emettere un avviso di rilevazione virus informatico per ogni destinatario del messaggio originale. Il numero di avvisi di rilevazione virus informatico, emessi dal gestore destinatario, deve essere pari al numero di destinatari del messaggio originale di competenza del gestore destinatario.

Per quanto riguarda lo schema dei dati di certificazione, definito nel suddetto Allegato al Decreto Ministeriale 2 novembre 2005, si precisa che anche nel caso di avviso di rilevazione virus deve essere correttamente valorizzato l'elemento XML "consegna".

Si rammenta che l'elemento XML "ricezione" è dedicato, invece, alle sole ricevute di presa in carico, come definito nello schema dei dati di certificazione.

[16/11/2007 NOTA 6]

Questa nota riporta alcune raccomandazioni in caso di cessazione dell'attività da parte di un gestore.

Il dPR 11 febbraio 2005, n. 68, prevede, all'art. 14 comma 11, che "ogni variazione organizzativa o tecnica concernente il gestore o il servizio di posta elettronica certificata è comunicata al CNIPA entro il quindicesimo giorno".

Pertanto, in caso di cessazione dell'attività, il gestore è tenuto a comunicarlo al CNIPA a cessazione avvenuta, qualora non sia stato diversamente indicato nel manuale operativo.

E' fortemente raccomandato che la data della cessazione dell'attività del gestore venga comunicata al CNIPA prima della effettiva cessazione, in modo che sia possibile aggiornare prontamente l'elenco pubblico dei gestori di posta elettronica certificata, pubblicato sul sito web.

Inoltre il gestore dovrà:

- rendere disponibile, nell'istante successivo alla cessazione, il file LDIF eliminando tutti i domini gestiti in precedenza. Il file LDIF dovrà essere reso disponibile per 5 giorni lavorativi alla medesima URL utilizzata in esercizio.
- sincronizzarsi con l'eventuale gestore che prenderà in carico i domini da lui precedentemente gestiti, in modo che nei rispettivi LDIF non compaia, nello stesso istante, un medesimo dominio.

Si rammenta che l'obbligo di conservazione del registro dei log delle operazioni svolte, di cui all'articolo 11 comma 2 del dPR 11 febbraio 2005, n. 68, rimane valido per i 30 mesi successivi alla data di cessazione dell'attività da parte di un gestore.

[16/11/2007 NOTA 5]

Questa nota è relativa alla disponibilità del servizio (art. 12 DM 2 novembre 2005).

La disponibilità del servizio è la possibilità di accedere ai sistemi del gestore ed usufruire di tutte le funzionalità del servizio di posta elettronica certificata.
Pertanto, ai fini del computo della disponibilità del servizio di posta elettronica certificata prendono parte i fermi servizio, sia programmati che non.

Ogni evento di indisponibilità deve essere comunicato al Cnipa, utilizzando il modulo per la segnalazione dei malfunzionamenti gravi disponibile sul sito web.

All'interno del modulo è presente un campo di testo libero nel quale è possibile specificare che l'indisponibilità del servizio non è derivata da un malfunzionamento grave bensì fa un fermo servizio, di cui il gestore deve fornire indicazioni relative alle circostanze che lo hanno determinato.

[04/10/2007 NOTA 4]

Questa nota riporta alcuni aspetti circa l'emissione della ricevuta di presa in carico da parte del gestore destinatario nel caso riscontrasse la presenza di un virus informatico all'interno di una busta di trasporto.

A fronte dell'invio di un messaggio da parte del gestore mittente, il gestore destinatario deve sempre emettere una o più ricevute di presa in carico.

Il testo del paragrafo 6.4.1 delle RT recita:

> *"Allo scambio di messaggi di posta certificata corretti tra differenti gestori di posta certificata, il gestore ricevente emette una ricevuta di presa in carico nei confronti del gestore mittente".*
>
> *…*
>
> *"In generale, a fronte di una busta di trasporto, ogni gestore destinatario dovrà emettere una o più ricevute di presa in carico per i destinatari di propria competenza. L'insieme di tali ricevute coprirà, in assenza di errori di trasporto, il complessivo dei destinatari del messaggio".*

Una busta di trasporto, seppur contenente virus informatico, è considerata corretta ed integra quando supera i controlli di cui al paragrafo 6.4.1 delle suddette RT.
Nella fattispecie i controlli effettuati sono:

- Controllo dell'esistenza della firma;
- Controllo che la firma sia stata emessa da un gestore di posta certificata;
- Controllo della validità della firma;
- Correttezza formale.

Quanto indicato nel paragrafo 6.4.1 è avvalorato dall'illustrazione presente nell'appendice A delle RT paragrafo 9.1.1.3. Il punto 2b prevede recita:

> "*il PdR verifica la BdT e crea una ricevuta di presa in carico (RdPiC) che viene inoltrata al PdR del Gestore mittente*"

Solo in un secondo momento, il punto di ricezione verifica il contenuto della busta di trasporto, ne rileva la potenziale pericolosità e non inoltra il messaggio al destinatario, emettendo un avviso di mancata consegna per virus informatico.

Si evince quindi che, anche in presenza di virus informatico all'interno della busta di trasporto, il gestore è tenuto a generare la ricevuta di presa in carico a favore del gestore mittente.

[29/08/2007 NOTA 3]

Questa nota specifica alcuni aspetti dello schema dei dati di certificazione relativo al file XML, contenente i dati di certificazione, da allegare alle ricevute, agli avvisi ed ai messaggi di PEC. In particolare indica la giusta interpretazione dello schema e l'obbligatorietà del campo "*consegna*" in alcuni tipi di messaggi di PEC.

Le indicazioni fornite con la presente nota si riferiscono al paragrafo 7.4 "*Schema dei dati di certificazione*" delle RT.

Nelle RT viene indicato il DTD relativo al file XML da utilizzare, come prevede la norma, per l'eventuale elaborazione automatica dei dati di certificazione associati alle ricevute, agli avvisi ed ai messaggi di PEC.

Di seguito viene mostrato un estratto del suddetto DTD che contiene le parti di interesse trattate in questa nota:

```
…
<!--Dati del messaggio di posta certificata-->
<!ELEMENT dati (
gestore-emittente,
data,
identificativo,
msgid?,
ricevuta?,
consegna?,
ricezione*,
errore-esteso?
)>
…
```

Nello specifico si vuole sottolineare che il "?" indica che non tutte le tipologie di messaggi del sistema PEC prevedono il campo "*consegna*". Il "?" alla fine del campo "*consegna*" quindi, non deve essere interpretato come libertà di inserire o meno tale campo.

E' necessario evidenziare che le ricevute di avvenuta consegna e gli avvisi di mancata consegna prevedono la presenza di tale campo, che quindi risulta **obbligatorio**.

L'elaborazione del file XML dovrà perciò prevedere la presenza del campo "*consegna*" così come specificato nei commenti presenti all'interno del suddetto DTD:

```
…
<!--Per le ricevute di consegna, gli avvisi di mancata consegna e-->
<!--di mancata consegna per virus informatico-->
<!--Destinatario a cui e' stata effettuata/tentata la consegna-->
<!ELEMENT consegna (#PCDATA)>
…
```

Quanto detto ha valore anche per altri campi presenti nel DTD, come ad esempio "*ricevuta*" e "*ricezione*", per i quali devono essere seguite le indicazioni date nei commenti e quindi, se previsti, considerati **obbligatori**.

[06/07/2007 NOTA 2]

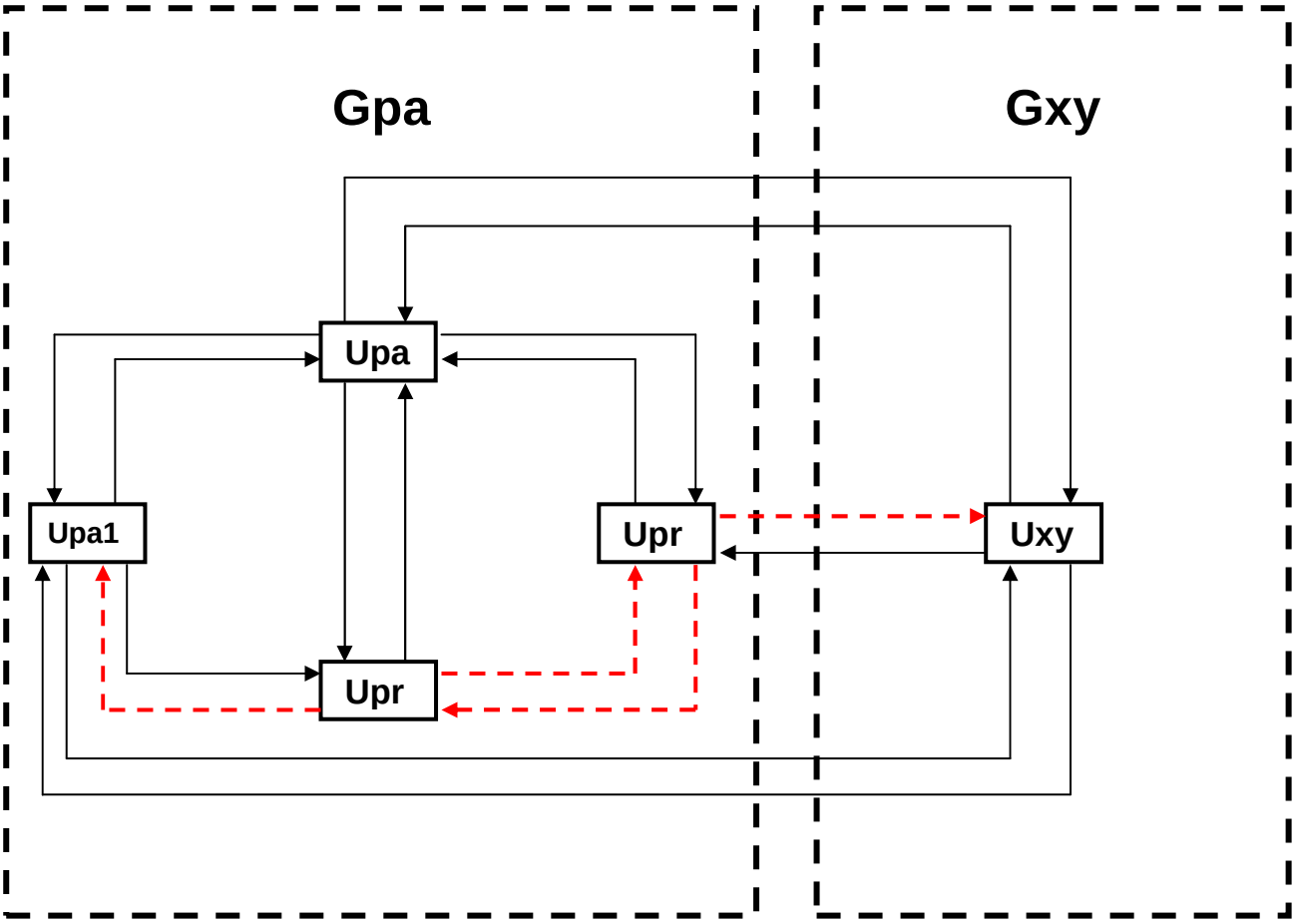
Questa nota riporta alcune spiegazioni per facilitare la corretta interpretazione delle previsioni contenute nel comma 2 dell'art. 16 "*Disposizioni per le pubbliche amministrazioni*" del DPR.

Il testo del comma 2 del predetto art. 16, recita:

> *"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."*

Pertanto lo scenario previsto nel comma 2 prevede: un Gestore di PEC che sia una PA (**Gpa**), degli utenti (**Upa**) che appartengono alla stessa PA e dei privati (**Upr**) che hanno in uso il servizio reso disponibile da **Gpa**.
Per completare il quadro, rendendolo coerente ad una possibile situazione reale, è opportuno considerare anche: gli utenti (**Upa1**), del servizio reso disponibile da **Gpa,** che facciano riferimento a delle PA distinte da quella del Gestore, un ulteriore generico Gestore di PEC (**Gxy**) e gli utenti di tale Gestore (**Uxy**).

Tale scenario può essere rappresentato graficamente come segue:



Le linee rosse tratteggiate evidenziano gli scambi di messaggi non ammessi dal comma 2.

Quindi, in sintesi, valgono le seguenti affermazioni:

1. **Upr** può ricevere da qualsiasi soggetto ma può inviare unicamente ad **Upa;**
2. **Upa**, **Upa1** e **Uxy** possono scambiarsi, tra loro, messaggi senza vincoli.

Facendo riferimento a precedente schema interpretativo del comma 2, il sistema di PEC utilizzato dal generico Gestore **Gpa** deve essere in grado di fornire queste ulteriori specifiche funzionalità:

1. gestire almeno tre distinti insiemi di utenti: **U_{pa}**, **U_{pa1}** e **U_{pr}**;
2. nel caso in cui il mittente appartenga all'insieme **U_{pr}**, il sistema deve produrre la ricevuta di accettazione solo se il destinatario appartiene all'insieme **U_{pa}** altrimenti, per destinatari appartenenti agli insiemi **U_{pa1}** e **U_{pr}**, produrrà un avviso di non accettazione.

[24/04/2006 NOTA 1]

Questa nota tratta l'*identificativo unico del messaggio* ed il *Message-ID*. In particolare, verrà descritto il loro impiego nella determinazione dell'header di un messaggio PEC e nei dati di certificazioni allegati alle ricevute e alla busta di trasporto.

L'univocità dei messaggi originali gestiti dal sistema PEC, al fine di consentirne una corretta tracciatura, è garantita dall'utilizzo dell'identificativo del messaggio così come descritto nel par.6.3 delle RT. Tale identificativo del messaggio, denominato *identificativo unico*, deve rispettare il seguente formato:

[identificativo unico] = [stringa alfanumerica]@[dominio_di_posta_gestore]

ovvero:

[identificativo unico] = [stringa alfanumerica]@[FQDN_server_di_posta]

L'identificativo unico viene utilizzato, nel messaggio originale e nella corrispondente busta di trasporto, nell'header:

Message-ID: **<**[identificativo unico]**>**

Da notare, nel formato del Message-ID, l'impiego dei delimitatori "**<**" e "**>**", così come stabilito in RFC2822, § 3.6.4.

Qualora il client di posta elettronica, utilizzato per inviare un messaggio PEC, avesse già inserito un Message-ID all'interno del messaggio originale, quest'ultimo andrà sostituito con l'identificativo unico appena descritto; l'eventuale Message-ID originario dovrà essere inserito nel messaggio originale, nelle relative ricevute, avvisi e busta di trasporto, utilizzando il seguente campo header:

X-Riferimento-Message-ID: [Message-ID originale]

In accordo, quindi, al citato RFC2822 i delimitatori "**<**" e "**>**" vanno utilizzati nella composizione dei due header appena considerati.

Per quanto riguarda i dati di certificazione, prodotti in formato XML, il par. 7.4 delle RT, prevede l'utilizzo sia dell'identificativo unico del messaggio sia del Message-ID del messaggio originale, prima della modifica da parte del sistema di PEC:

```
…
<!—Identificativo unico del messaggio-->
<!ELEMENT identificativo (#PCDATA)>

<!—Message-ID del messaggio originale prima della modifica-->
<!ELEMENT msgid (#PCDATA)>
…
```

Ove, come riportato nei commenti presenti nel DTD, **identificativo** è l'identificativo unico del messaggio e **msgid** è il Message-ID del messaggio originale (prima della sostituzione da parte del sistema PEC). Quindi, il solo campo **msgid** prevederà la presenza dei caratteri "**<**" e "**>**".