ARTICLE:

# THE ITALIAN CERTIFIED E-MAIL SYSTEM

WRITTEN BY:
**ROBERTA FALCIAI AND LAURA LIBERATI**

**E-mail has become the communication method par excellence. Correspondingly, the need for legal protection has started to press urgently during the last years. Trade operators, public administrations as well private citizens have experienced the increasing necessity, on the one hand, to intensify their electronic communications, and, on the other hand, to be assured that the communication effectively took place. Prior to February 2005, however, the traditional (paper) registered letter represented the only method which proved mail delivery to the actual addressee.**

The Italian Legislator was determined to remedy this defective scenario, and accordingly issued Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 (Presidential Decree No. 68 of February 11, 2005) (the Decree) and the relevant technical implementing measures provided for by Decreto del Ministro per l'Innovazione e le Tecnologie del 2 novembre 2005 (Ministerial Decree of 2 November, 2005) (the Technical Rules), which introduced and regulated the certified transmission and receipt of electronic documents between government offices, citizens and businesses under Italian law. The certified e-mail system aims at granting legal validity to the transmission and receipt of electronic messages between those senders and receivers who, through the certified e-mail providers (gestore del servizio, s2 of the Decree) (the CEP), make use of this system in their mutual relationships. In particular, according to section 6 of the Decree, the sender will receive both an "acceptance receipt" from its CEP and a "delivery receipt" from that of the recipient: these receipts,[1] duly signed by the relevant CEP with an electronic advanced signature, will "certify" the main phases (i.e. the sending and delivery) of the transmission process and ensure its legal validity.

## How the certified e-mail system works

In detail, the transmission process of certified e-mail proceeds as follows:

1. The sender transmits the message to its CEP.
2. If both the sender and the recipient have the same CEP, the CEP forwards it directly to the recipient's mailbox.
3. Alternatively, the CEP forwards it directly to the recipient's CEP. The recipient's CEP will deliver it to the recipient's mailbox.
4. The CEP sends an "acceptance receipt" to the sender.[2] The acceptance receipt contains the "certification data" (such as the date and time of sending, the identity of the sender and recipient) and provides documentary evidence that the certified e-mail has been sent. This certification data, together with the original message of the sender, are contained in the "transport envelope", which is a file created by the sender's CEP and signed by the latter with an advanced electronic signature.
5. Once the certified e-mail is delivered to the recipient's mailbox, the recipient's CEP provides the sender with a "delivery receipt" (or, as the case may be, a receipt of delivery failure), which proves that the original e-mail message has been (or not) effectively delivered. The delivery receipt provides the date and time of delivery, and thereby grants the transmission of the certified e-mail with a date certain at law, regardless of whether the recipient has read the e-mail message.[3]

Consequently, in accordance with Section 3 of the Decree, the electronic document (and the relevant attachments, if any) shall be considered to have been legally "sent", if it is transmitted to the sender's CEP and "delivered" if it has been conveyed to the recipient's mailbox with the relevant CEP. Moreover, as for standard registered mail, the certified e-mail shall

[1] *Section 9 of the Decree.*

[2] *Sections 5 and 6 of the Decree.*

[3] *Please note that the delivery receipt is issued exclusively against the delivery to the recipient's CEP of a transportation envelope validly created pursuant to the requirement provided for the Technical Rules.*

be considered to have been “received” by the recipient at the time of delivery, as certified by the delivery receipt.

In the light of the brief description of how the certified e-mail system works, both receipts issued by the CEPs and the transport envelope are signed by an advanced electronic signature and, therefore, the certified e-mail system, as well as the registered mail, aims at guaranteeing the integrity of the transmission process, but does not guarantee the identity of the sender of the certified e-mail message.[4] Indeed, such advanced electronic signature,[5] which is automatically generated by the e-mail system and based on a pair of asymmetrical keys (one public and one private), is appended exclusively to the receipts described above. Therefore the advanced electronic signature, being uniquely linked to the CEP and capable of identifying it during the transmission process, guarantees the origin, integrity and authenticity of the original message during the sending and delivery phases.[6]

## The role of the certified e-mail provider

The effectiveness of the whole certified e-mail system lies with the crucial role of the CEP. Indeed, according to Section 2(c) of the Decree, the CEP is the sole subject, either public or private, entitled to supply certified e-mail services and to manage the certified e-mail domains.[7] In order to recognize the legal validity of the transmission of certified e-mails as transmitted, the CEP is required to meet specific requirements to be admitted in the register of the National Centre for Information Technology in the Public Administration (CNIPA), which is a precondition for supplying such services. Section 14 of the Decree lists a number of mandatory and strict requirements, which the applicants shall have to comply with to serving as a CEP pursuant to the Decree:

“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 societa' 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

[4] *Indeed, in order to recognize the legal validity of the message, the sender shall sign it with digital signature, although even the use of a digital signature does not provide proof that the sender caused the digital signature to be affixed to the message.*

[5] *In this respect, please note that the difference between the advanced electronic signature and the digital one lies with the hardware used.*

[6] *Section 9 of the Decree expressively provides that the origin, integrity and authenticity of both the receipts and the transport envelope are granted by the advanced electronic signature.*

[7] *Section 2(c) of the Decree states that one of the subjects of certified e-mail service is: “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” (The service provider, i.e. the subject, either public or private, which supplies certified e-mail services and manages the certified e-mail domains).*

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'attivita' 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 e' comunicata al CNIPA entro il quindicesimo giorno.
12. Il venire meno di uno o più requisiti tra quelli indicati al presente articolo e' 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”.

(English unofficial translation) Section 14 – List of certified e-mail providers

1. Any sender or recipient wishing to make use of the certified e-mail system shall choose a provider recorded in a public list according to the regulation of this section.
2. Public administrations and individuals wishing to serve as a certified e-mail provider shall submit to CNIPA an application for admission to the list of certified e-mail providers.
3. Any applicant for admission to the list of certified e-mail providers other than public administrations shall have legal form of a stock corporation and its wholly paid-up corporate capital shall not be lower than one million euro.
4. Certified e-mail providers or, in the case of legal entities, their legal representatives or any person with managing functions shall meet specific standing requirements which apply to persons with directorial, managerial and supervisory responsibilities within banking institutes pursuant to Section 26 of the banking law act, namely the Legislative Decree of 1st September 1993, no. 385, and any subsequent amendments.
5. No person will be allowed to act as legal representative, member of the Board of Directors or the Board of Statutory Auditors or be entrusted with managing powers by the private provider if they are subject to precautionary measures by order of the criminal Court pursuant to Law no. 1423 of 27 December 1956, and Law no. 575 of 31 May 1965, and any subsequent amendments, or they have been sentenced to imprisonment by final judgment, unless exempted under the rehabilitation of offenders act, for more than one year for offences against IT systems, public administration, public belief, property, public economy or tax laws.
6. The applicant shall also:
   - a. prove to have the level of organizational and technical effectiveness required to provide certified e-mail services;
   - b. recruit highly skilled staff with broad expertise for the provision of services, specifically good management skills, specific knowledge of e-mail technology and familiarity with the relevant safety

procedures;

c. comply with the provisions set forth herein and the technical rules provided for by Section 17;

d. apply the relevant procedures and methods for the administration and management as well as the established practices;

e. in accordance with Section 9 and for the purposes of the electronic signature, use systems ensuring that information is treated as confidential and provided in compliance with established European and international standards;

f. take all necessary measures to ensure integrity and safety of the certified e-mail services;

g. establish emergency procedures that ensure, in any event, the effective transmission;

h. submit, within the next twelve months from the application for admission to the list of certified e-mail providers, a statement of compliance of the quality system with ISO 9000, any subsequent amendments or equivalent rules, as to the supply of certified e-mail services;

i. submit a copy of the insurance policy to cover risks and damages caused to third parties.

7. If ninety days have elapsed from the date of the submission and you have not received a notice of rejection by CNIPA, the application shall be deemed as accepted.

8. The time limits set forth in Section 7 may be interrupted only once, exclusively with a reasoned request for discovery of any documents that will complete the information provided, where they are not available to CNIPA or cannot be gathered on its own initiative. In such event, the time limits shall run again from the date of receipt of the additional documentation.

9. The application process for admission to the list of certified e-mail providers may be suspended if the applicant is being criminally prosecuted for offences against IT systems according to this Section.

10. Any person included within the scope of paragraph 1 shall submit, in accordance with the technical rules set forth in Section 17, the data required to apply for admission to the list of providers.

11. Any change to either the management organization or the technical rules regarding the provider or the certified e-mail services shall be notified to CNIPA within the fifteenth day.

12. Subsequent failure to comply with one or more requirements set forth herein will cause to be struck off.

13. The CNIPA has functions of surveillance and control of the activity carried out by the subjects enrolled in the list referred under paragraph 1.

As can be seen from the provisions of article 14, the CEPs shall, amongst other things:

- be a stock corporation having a wholly paid-up corporate capital of, at least, one million Euro, unless it is a public administration;
- ensure that its legal representatives have the same standing as required to those with directorial, managerial and supervisory responsibilities within banking institutes; either legal representatives or top managers shall not be subject to criminal proceedings concerning, amongst others things, offences against IT systems;
- ensure maximum organizational and technical reliability, highly skilled staff, the adequacy of security and emergency measures,[8] as well as the compliance with the ISO 9000 provisions;
- obtain an insurance policy to cover risks and damages caused to third parties.

The CNIPA shall verify, within 90 days from the submission of the request, whether the subject meets all the subjective and objective requirements. Oddly enough, the CNIPA does not release an express acceptance notice to the applicant, but the request for registration is automatically accepted when the 90-days period elapses. This system, known as “silenzio-assenso” (implied acceptance), seems to be unsatisfactory in light of the strict requirements for providers wishing to act as CEPs. It would probably have been more appropriate to set forth a method of providing for a higher degree of certainty that the CNIPA will strictly monitor compliance with the requirements.

However, it must be pointed out that the CNIPA has to deliver a certificate to the applicant provider to enable the latter to become operative. This certificate implies that the CNIPA has already verified the provider’s compliance with the above requirements, and, indirectly, it also implies that the CNIPA communicates to the applicant the outcome of the acceptance process, even if the Decree does not provide for express notice of acceptance. Moreover, the CNIPA acts as a supervisory and controlling body after the acceptance process of the provider is completed.

[8] *The expression “emergency measures” is referred to the ability of the CEP to ensure the completion of the transmission process also in case of service malfunctioning of any nature (e.g. disaster recovery measures in case of blackouts).*

*In this scenario, the transmission of certified e-mail involves two CEPs, as the CEP of the sender has to transmit the e-mail to the CEP of the recipient, rather than delivering the e-mail directly to the latter.*

Indeed, the CNIPA is empowered to cancel a CEP from the public list, albeit regularly registered, whenever it finds that the latter does not comply with the requirements above mentioned. CNIPA's role as permanent control body probably balances and justifies the above apparent incongruence of the "implied acceptance".

## Interoperability among CEPs and service levels

As a matter of fact, senders and recipients will most likely have different CEPs, as each user may freely choose a CEP from the public list managed and updated by the CNIPA. In this scenario, the transmission of certified e-mail involves two CEPs, as the CEP of the sender has to transmit the e-mail to the CEP of the recipient, rather than delivering the e-mail directly to the latter. Within such a basic framework, the Decree provides that the CEP of the recipient gives certification to the CEP of the sender through a sort of "bill of lading" of the e-mail.[9] According to this system, the two CEPs must guarantee a necessary interoperability in order to grant that the certified e-mail system does not experience any interruption or malfunctioning for the transition of the e-mail message between the two CEPs. Indeed, the annex of the Technical Rules provides for technical levels of interoperability, which all the CEPs registered in the CNIPA's list are required to comply with.

Moreover, Section 12 of the Technical Rules provides for a minimum service level, which the CEP shall ensure, such as the maximum number of recipients for each e-mail sent and the maximum size of the e-mail. Each CEP is entitled to establish a maximum service level, provided that it meets at least the minimum level required by the Technical Rules (i.e. at least 50 recipients, no more than 30 MB for each e-mail). Rather predictably, the technical service levels granted by each provider over the minimum ones required by the Technical Rules will most likely represent the key aspect for the users' choice of a CEP.

*Roberta Falciai is a lawyer at the Milan office of Macchi di Cellere Gangemi, and specialises in mergers and acquisitions, corporate reorganisations, e-commerce, intellectual property, telecommunications and media law. Education: University of Siena, J.D., magna cum laude; University College London (UCL), LL.M. degree.*

**r.falciai@macchi-gangemi.com**

*Laura Liberati is a lawyer at Rome office of Macchi di Cellere Gangemi, and specialises in telecommunications and media, intellectual property, corporate governance and entertainment law. Education: University of Rome "La Sapienza", J.D., magna cum laude; University of Alicante, Master in Intellectual Property and Information Society Law.*

**l.liberati@macchi-gangemi.com**
**http://www.macchi-gangemi.com**

[9] *In case the sender and the recipient have the same CEP, the latter will be undoubtedly held liable for the failure to deliver the e-mail. It is not clear, instead, which of the two CEPs is liable in case the e-mail has to be delivered to the recipient by a different CEP from that of the sender. Indeed, the Decree does not explicitly establish which of the two CEPs is to be held liable vis-à-vis the sender for the possible malfunctioning of the system once the e-mail message has been transferred to the recipient's CEP (e.g. a right of action is time-barred). This issue arises from the consideration that the sender enters into the certified e-mail service agreement with his CEP only and has no relationship whatsoever with the CEP of the recipient, which does not release the "bill of lading" to the sender but to his CEP. The release of this "bill of lading" seems to discharge the CEP of the sender from any liability where the system malfunctions during the delivery of the message (from the CEP of the recipient to the recipient's mailbox). The question is actually whether this "bill of lading" discharges the sender's CEP vis-à-vis the sender himself or it only forms the basis for the CEP of the sender claim to recover any costs incurred from the CEP of the recipient. The last solution would be the most appropriate; indeed, if the first solution were adopted, the sender would have to face a shift of the burden of proof, as the recipient's CEP would be held liable in tort, not in contract.*