

La posta elettronica certificata nelle Pubbliche Amministrazioni – II parte

SOMMARIO

- **La bozza delle regole tecniche relative alla posta elettronica certificata**
- **Gli standards di riferimento e la struttura dei messaggi**
- **I gestori di posta elettronica: caratteristiche e requisiti**

Le regole tecniche relative alla posta elettronica certificata saranno oggetto di un DPCM e includeranno tutti i requisiti tecnici per le piattaforme di posta elettronica certificata. Uno schema di decreto è stato pubblicato sul sito del CNIPA e a tale bozza del 12 maggio si fa d'ora in poi riferimento nella trattazione. Al termine del processo di notifica alla Commissione Europea ai sensi della direttiva 1998/48/EC il decreto sarà pubblicato in Gazzetta Ufficiale e, da tale momento, gli operatori che saranno in possesso dei requisiti previsti potranno svolgere la propria attività come gestori di posta elettronica certificata.

Il CNIPA avrà un ruolo di controllo e supporterà la P.A. nell'introduzione della posta elettronica certificata nei procedimenti amministrativi, dato il rilievo dato a tale strumento dal nuovo Codice dell'Amministrazione digitale.

Nella bozza per la creazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata, l'articolo 3 elenca una serie di standards che devono obbligatoriamente essere presi in considerazione.

Tali standards sono:

- a) RFC 1847 (Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted)
- b) RFC 1891 (SMTP Service Extension for Delivery Status Notification)
- 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)
- j) RFC 2849 (The LDAP Data Interchange Format (LDIF) – Technical Specification)
- k) RFC 3174 (US Secure Hash Algorithm 1 – SHA 1)
- l) RFC 3207 (SMTP Service Extension for Secure SMTP over Transport Layer Security)
- m) RFC 3280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List – CRL Profile)

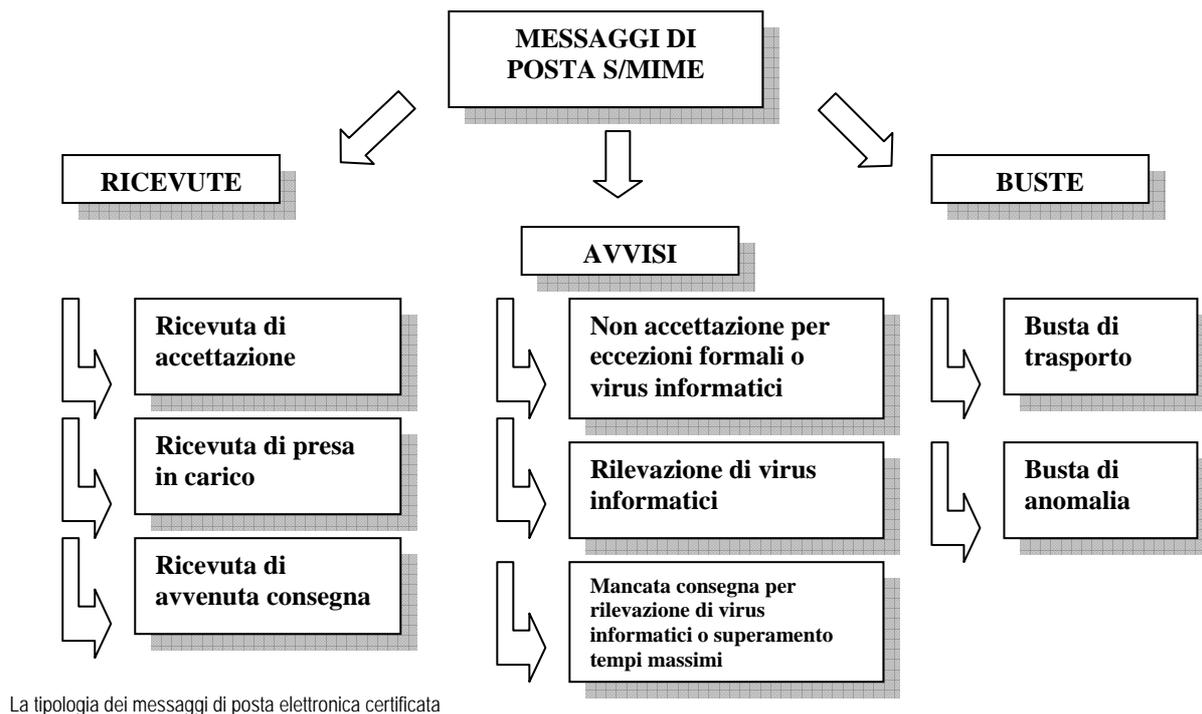
Uno dei compiti di CNIPA è verificare la coerenza operativa di tali standards in funzione dell'evoluzione tecnologica e pubblicare ogni cambiamento agli stessi sul proprio sito istituzionale (art. 4). La messa in opera dei servizi di posta elettronica certificata è condizionata dall'impiego di tali specifiche, che potrebbero limitare l'entrata di operatori del mercato che abbiano fatto scelte tecnologiche diverse, ma non necessariamente meno sicure. Si fa riferimento in particolare all'obbligo di utilizzazione dello standard internazionale S/MIME (RFC 2633) nella generazione dei messaggi, di cui all'art. 6 della bozza di decreto.

In base al decreto, i messaggi si suddividono in tre categorie: ricevute, avvisi, buste. La differenziazione tra gli stessi deve avvenire tramite la struttura *header* dello standard S/MIME.

I messaggi di ricevuta sono distinti in ricevuta di accettazione, ricevuta di presa in carico, ricevuta di avvenuta consegna completa, breve, sintetica.

Anche gli avvisi possono essere di diverso tenore: devono essere previsti avvisi di non accettazione per eccezioni formali o virus informatici, oppure avvisi di rilevazione di virus informatici o ancora avvisi di mancata consegna per rilevazione di virus informatici o superamento dei tempi massimi previsti per la consegna.

Le buste di trasporto sono a loro volta distinte tra buste di trasporto e buste di anomalia.



I messaggi generati dal sistema di posta elettronica certificata devono essere sottoscritti dai gestori mediante la firma elettronica avanzata del gestore di posta certificata. I certificati di firma saranno rilasciati dal CNIPA per un massimo di 10 certificati per ogni gestore, salvo casi eccezionali valutati da CNIPA in cui saranno concessi più certificati.

Ciascuna trasmissione è caratterizzata dall'apposizione di un riferimento temporale, generato con qualsiasi sistema che garantisca uno scarto non superiore al minuto rispetto al tempo UTC.

Entrando nel merito dei requisiti dei gestori di posta elettronica certificata, per le pubbliche Amministrazioni che intendano iscriversi all'elenco dei gestori di posta tenuto da CNIPA sono previsti i limiti di utilizzo previsti dall'articolo 15, ovvero la possibilità di gestire esclusivamente rapporti tra la P.A. e i privati. E' necessario che, al momento dell'iscrizione, la P.A. richiedente illustri in una relazione tecnica le misure adottate affinché tali limiti siano rispettati. Non è necessario che la stessa sia in possesso di una polizza assicurativa a copertura dei rischi (art. 16 comma 2).

Tutti i soggetti che intendano iscriversi all'elenco devono fornire a CNIPA una serie di documenti e informazioni: denominazione sociale, sede legale, sedi operative, rappresentante legale, piano per la sicurezza, manuale operativo, dichiarazione d'impegno al rispetto delle disposizioni del DPR 68/2005, dichiarazione di conformità alle regole tecniche, relazione sulla struttura organizzativa (art. 16).

Requisiti di qualità della struttura e di organizzazione e competenza del personale sono altresì previsti per garantirsi la permanenza nell'elenco dei gestori sottoposto alla vigilanza e al controllo di CNIPA.

Daniela Rocca

Studio Genghini & Associati