Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

LINEE GUIDA PER LA VIGILANZA SUI GESTORI DI

POSTA ELETTRONICA CERTIFICATA

(Art. 14 comma 13 Decreto Presidente della Repubblica

11 FEBBRAIO 2005, N. 68)

V 1.0

22 febbraio 2008

Area "Architetture, standard e infrastrutture"
Agenzia per l'Italia digitale

SOMMARIO

Capitolo 1

Introduzione

1.1 Premessa

L'art. 48 del decreto legislativo del 7 luglio 2005, n. 82, recante, "Codice dell'amministrazione digitale", dispone: "*La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68*."

Il citato DPR n. 68 del 2005, all'articolo 14, comma 13, recita: "*Il CNIPA svolge funzioni di vigilanza e controllo sull'attività esercitata dagli iscritti all'elenco di cui al comma 1*."

Pertanto il Centro nazionale per l'informatica nella pubblica amministrazione – CNIPA – esplica la funzione di vigilare sul rispetto, da parte dei gestori del servizio di Posta Elettronica Certificata – PEC, di quanto disposto dal citato decreto del Presidente della Repubblica, dalle relative regole tecniche recate dal decreto del Ministro per l'innovazione e le tecnologie del 2 novembre 2005 e dai provvedimenti emanati dallo stesso CNIPA. Questi ultimi sono, alla data di pubblicazione delle presenti Linee Guida, le Circolari CNIPA n. 49 del 24 novembre 2005 e n. 51 del 7 dicembre 2006.

In aggiunta al doveroso rispetto degli obblighi normativi, la vigilanza e il controllo su tali gestori da parte del CNIPA sono fondamentali per assicurare agli utenti di Posta Elettronica Certificata la necessaria fiducia nella correttezza e imparzialità, e quindi affidabilità, dei gestori iscritti nell'Elenco di cui all'art. 14 comma 1 del citato decreto del Presidente della Repubblica n. 68 del 2005. Garantendo, infatti, tale affidabilità si agevola il passaggio allo eGovernment, obiettivo per il raggiungimento del quale la Commissione Europea e la pubblica amministrazione italiana stanno dedicando un notevole impegno.

Si ritiene infine utile segnalare, a tale riguardo, la pubblicazione nella seconda metà dell'anno 2008 da parte dello European Telecommunications Standards Institute – ETSI – di un insieme di standard volti a costituire una base tecnica comune per la realizzazione di servizi di PEC (denominata in tali standard "Registered E-Mail" – REM) interoperabili tra i gestori che volessero adottare detti standard.

1.2 Obiettivi del documento

I gestori di PEC possono ottemperare alla normativa in materia con soluzioni tecniche differenti tra loro. Questa situazione, unitamente alla doverosa "neutralità tecnologica" delle norme giuridiche che correttamente non specificano tutti i requisiti tecnici nei minimi dettagli, rende necessario stabilire una base comune di valutazione su cui fondare le operazioni di vigilanza onde raggiungere una equanimità nelle valutazioni sul rispetto delle norme da parte dei gestori.

Il presente documento ha l'obiettivo di predefinire, in via generale, le modalità con cui le operazioni di vigilanza vengono svolte da parte del CNIPA tramite verifiche e ispezioni effettuate da propri incaricati, nel presente documento denominati "valutatori" e le attività di supporto a questi ultimi che i gestori devono fornire nel corso di tali operazioni. In particolare si indicano:

a. al Gestore di PEC gli adempimenti da svolgere in dettaglio durante l'esercizio della propria attività e in occasione di ispezioni da parte del CNIPA, onde poter esibire evidenza di aver ottemperato ai requisiti normativi;

b. al personale ispettivo del CNIPA (i "Valutatori") le operazioni che essi devono in dettaglio svolgere per raggiungere gli scopi dell'ispezione.

1.3 Struttura del documento

Nell'impostazione delle presenti Linee Guida si è fatto riferimento anche alle specifiche indicate negli standard ISO/IEC comunemente adottati nel campo della sicurezza dei sistemi informatici. In particolare si è tenuto conto delle misure di sicurezza definite nello ISO/IEC 27002:2007, che nello ISO/IEC 27001:2005 sono indicate come "Best practices", con cui attuare i controlli specificati nello Annex A di quest'ultimo.

Il documento, dopo alcuni capitoli introduttivi che riportano il quadro giuridico e tecnico di riferimento e le principali modalità di impostazione delle verifiche, entra nel dettaglio degli specifici aspetti tecnico-giuridici dell'attività di gestione della Posta Elettronica Certificata, dedicando a ognuno di essi un capitolo, suddiviso in tre paragrafi:

1. il primo paragrafo indica i provvedimenti normativi che specificamente riguardano l'argomento o gli argomenti a cui il capitolo stesso si rivolge;
2. il secondo indica le attività operative e di supporto che il Gestore deve svolgere per rendere possibili le operazioni di vigilanza;
3. il terzo indica le attività principali sulle quali il Valutatore si può basare nell'operare.

Il documento si conclude con un capitolo che riporta la normativa afferente la Posta Elettronica Certificata e che quindi è rilevante ai fini della vigilanza sulle attività di gestione di PEC. Ai singoli punti, articoli e commi dei dispositivi ivi riportati fanno riferimento le citazioni riportate nel primo paragrafo di cui sopra.

1.4 Termini chiave

In queste Linee Guida vengono utilizzati i seguenti termini chiave con significato analogo a quello indicato al punto 10.3 dell'Allegato al Decreto del Ministro per l'innovazione e le tecnologie del 2 novembre 2005.

Le parole chiave "DEVE", "DEVONO", "NON DEVE", "NON DEVONO", "E' RICHIESTO", "DOVREBBE", "NON DOVREBBE", "RACCOMANDATO", "NON RACCOMANDATO" "PUO'" e "OPZIONALE" nel testo del documento debbono essere interpretate come descritto nel seguito, in conformità alle corrispondenti traduzioni contenute nel documento IETF RFC 2119 [1].

Le parole chiave "DEVE" o "DEVONO" o "E' RICHIESTO" stanno a significare che l'oggetto in questione è un requisito assoluto. Le parole chiave "NON DEVE" o "NON DEVONO" stanno a significare che l'oggetto in questione è un divieto assoluto.

Le parole chiave "DOVREBBE" o "RACCOMANDATO" stanno a significare che, in particolari circostanze, possono esistere valide motivazioni per ignorare la particolare specifica, ma le complete implicazioni di tale scelta debbono essere comprese e pesate con cautela prima di optare per un'altra soluzione.

Le parole chiave "NON DOVREBBE" o "NON RACCOMANDATO" stanno a significare che, in particolari circostanze, possono esistere valide motivazioni perché la specifica sia accettabile o anche utile, ma le complete implicazioni debbono essere comprese e pesate con cautela prima di optare per una soluzione corrispondente.

Le parole chiave "PUO'" o "OPZIONALE" stanno a significare che una specifica è puramente opzionale. Un soggetto può scegliere di avvalersene, mentre è possibile che un altro soggetto la ometta.

Nota: Lo standard ISO/IEC 27001 usa il verbo DEVE (SHALL) per i requisiti in esso indicati. Si è pertanto ritenuto opportuno in queste Linee Guida utilizzare tale verbo (SHALL/DEVE) anche per le misure riprese dallo ISO/IEC 27002 che attuano tali requisiti dello ISO/IEC 27001, in quanto ritenute di per sé necessarie. Lo ISO/IEC 27001/27002 è solo citato a conferma della opportunità delle misure stesse.

Capitolo 2

La normativa giuridico-tecnica

Anche nel campo della Posta Elettronica Certificata l'Italia vanta, e non solo in Europa, il primato cronologico di aver assicurato il riconoscimento giuridico "erga omnes" a messaggi di posta elettronica emessi nel rispetto di determinate norme, mediante il citato decreto legislativo n. 82 del 7 marzo 2005 che all'art. 48, come detto, stabilisce:

> "*1. La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.*
>
> *2. La trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta.*
>
> *3. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso mediante posta elettronica certificata sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche.*"

La emanazione di tale decreto legislativo ha seguito di pochi giorni quella del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, a cui fa riferimento, che fu emanato dopo un periodo di circa due anni di sperimentazione "sul campo" regolamentata dai seguenti documenti CNIPA:

- Linee guida del servizio di trasmissione di documenti informatici mediante posta elettronica certificata, del 3 febbraio 2003;
- Allegato tecnico alle linee guida del servizio di trasmissione di documenti informatici mediante posta elettronica certificata, del 3 febbraio 2003;
- Guida ai servizi di Indice delle amministrazioni pubbliche e delle aree organizzative omogenee, del 18 dicembre 2002.

Questa sperimentazione si basava sull'esecuzione di un insieme di casi di prova, elencato nel documento "Prove per la verifica dell'interoperabilità fra servizi di Posta Elettronica Certificata", del 13 febbraio 2003.

Le regole tecniche attuative di quanto disposto dal DPR 68/2005 furono emanate dal Ministro per l'innovazione e la tecnologia con il richiamato decreto del 2 novembre 2005 che reca all'art. 19 la "Disciplina dei compiti del CNIPA":

> "*Il CNIPA definisce con circolari le modalità di inoltro della domanda e le modalità dell'esercizio dei compiti di vigilanza e controllo di cui all'Articolo 14 del D.P.R. n. 68 del 2005.*"

Il CNIPA ha quindi definito:

1. le modalità di inoltro della domanda di iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata con la Circolare 24 novembre 2005, n. 49, recante "*Modalità per la presentazione delle domande di iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata (PEC), di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.*"
2. le modalità dell'esercizio dei compiti di vigilanza e controllo con la Circolare 7 dicembre 2006, n. 51:

   "*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, «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. 296 del 21 dicembre 2006)

Quanto sopra è stato integrato dal CNIPA con ulteriori documenti dei quali i principali sono i seguenti, meglio descritti al Capitolo 5:

a. Linee Guida Iscrizione PEC – Raccomandazioni in merito alla predisposizione della documentazione prevista per l'iscrizione nell'Elenco pubblico dei gestori di Posta Elettronica Certificata – 13 febbraio 2006;

b. FAQ - Circolare 51 Vigilanza PEC – Versione 1.1 del 4 maggio 2007.

Le presenti Linee Guida si basano sui provvedimenti sopra elencati nell'indicare, come dettagliato al paragrafo 1.2, gli adempimenti che il Gestore PEC deve svolgere, le evidenze che esso deve esibire al personale ispettivo del CNIPA e le operazioni previste a cura di quest'ultimo.

E' interessante notare quanto recita l'Allegato tecnico al citato decreto ministeriale del 2 novembre 2005, all'art. 8.1: "*La chiave privata e le operazioni di firma devono essere gestite utilizzando un dispositivo hardware dedicato, in grado di garantirne la sicurezza in conformità a criteri riconosciuti in ambito europeo o internazionale.*". In sostanza non viene disposta la certificazione del dispositivo di firma, il cui uso è comunque reso obbligatorio, bensì ne è accettata la conformità a qualsiasi criterio di sicurezza, purché la sua validità sia riconosciuta in ambito europeo o internazionale. Nel Capitolo 3 sono indicati gli standard più comuni per la certificazione dei dispositivi hardware di firma.

Capitolo 3

Gli standard di riferimento

Si riportano di seguito gli standard tecnici a cui si fa riferimento nelle presenti Linee Guida. Ad alcuni di essi fa anche riferimento l'allegato tecnico al richiamato Decreto del Ministro per l'innovazione e le tecnologie del 2 novembre 2005. Quelli indicati espressamente da tale allegato sono segnalati chiaramente.

3.1 Standard ISO/IEC

3.1.1 Serie di standard ISO/IEC 9594

Lo standard ISO/IEC citato dall'Allegato tecnico al Decreto del Ministro per l'innovazione e le tecnologie del 2 novembre 2005 è lo ISO/IEC 9594-8:2001 Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks.

Si tratta dello standard ISO/IEC che costituisce la base di riferimento per la firma digitale, ed è uno di quelli comunemente noti come appartenenti alla serie X.500 relativa alla gestione della Directory. Essi sono dapprima emessi come raccomandazioni dallo ITU-T (International Telecommunication Union - Telecommunication Standardization Sector), che è l'agenzia delle Nazioni Unite relativa alle telecomunicazioni, e successivamente recepiti come veri e propri standard dallo ISO/IEC. Quest'ultimo li pubblica con propri identificativi nell'ambito della famiglia degli standard ISO/IEC 9594 il cui titolo generale è: "Information technology — Open Systems Interconnection — The Directory".

I componenti della famiglia 9594 sono attualmente i seguenti:

— Part 1: Overview of concepts, models and services

— Part 2: Models

— Part 3: Abstract service definition

— Part 4: Procedures for distributed operation

— Part 5: Protocol specifications

— Part 6: Selected attribute types

— Part 7: Selected object classes

— Part 8: Public-key and attribute certificate frameworks

— Part 9: Replication

— Part 10: Use of systems management for administration of the Directory

Va notato che dopo la promulgazione del più volte citato decreto ministeriale, e precisamente il 15 dicembre 2005, è stata pubblicata la nuova edizione dello ISO/IEC 9594-8:2005, ma le differenze principali rispetto all'edizione del 2001, a parte alcuni "errata corrige" che peraltro erano già automaticamente entrati a far parte dell'edizione del 2001, riguardano i certificati di attributo, di dubbio interesse per la posta elettronica. Pertanto non vi sono controindicazioni sostanziali all'uso di uno standard che è solo formalmente obsoleto.

3.1.2 ISO/IEC 27001 e 27002

Al British Standards Institution – BSI – va riconosciuto il merito di avere, molto tempo fa, avvertito l'esigenza di definire una "paradigma" di sicurezza per i sistemi informativi e di aver consolidato tale sensibilità in quello che è poi diventato uno standard, prima de facto e poi de jure: il BS 7799.

Nel 1995 ne fu pubblicata la prima versione che, sia pure impostata sulla normativa giuridica britannica, dava indicazioni su come costituire quello che ormai è noto come Information Security Management System – ISMS.

Una volta fornite tali indicazioni era necessario realizzare uno strumento che consentisse una uniformità di valutazione del loro livello di realizzazione. Nel febbraio 1998 il BSI pubblicò quello che divenne il BS 7799-2, cioè la guida alla valutazione (e anche alla certificazione formale) dello ISMS di un'organizzazione o di una sua parte. Il BS 7799-2, infatti, indicava i requisiti in base ai quali realizzare e valutare le misure di sicurezza di un Information Security Management System.

Da allora queste due parti del BS 7799 si sono evolute. La parte 1 è stata formalizzata nel 2000 come standard ISO/IEC 17799 ed è stata poi aggiornata nel 2005. Essa è stata infine inserita nel 2007 nella famiglia degli standard di sicurezza ISO/IEC 27000 con il numero ISO/IEC 27002. La parte 2 è stata recepita nel 2005 come standard ISO/IEC 27001. La famiglia degli standard ISO/IEC 27000 comprende o prevede altri documenti, per lo più ancora in fase di sviluppo alla data della redazione delle presenti Linee Guida. Tra questi ultimi si citano, a titolo di esempio:

- ISO/IEC 27003: Information technology - Security techniques – Information security management system implementation guidance,
- ISO/IEC 27004: Information technology - Security techniques - Information security metrics and measurements,
- ISO/IEC 27005: Information technology -- Security techniques -- Information security risk management.

Si può quindi affermare che dai due originali documenti del BSI si sia ormai sviluppata una famiglia di standard di sicurezza per realizzare prima e misurare poi un ISMS, rendendone possibile anche la certificazione di conformità agli standard.

Per tale motivo le presenti Linee Guida sono state redatte facendo riferimento in particolare alle misure di sicurezza indicate nello ISO/IEC 27002, in quanto la realizzazione di un ISMS conforme con esse costituisce una sana pratica. Non si è ritenuto invece rifarsi allo ISO/IEC 27001 perché attinente a una certificazione di sicurezza che non è prescritta da alcuna norma.

Nota: poiché lo standard ISO/IEC 27002 è identico allo standard ISO/IEC 17799:2005, essendovi soltanto stata cambiata la sigla, si fa riferimento allo standard ISO/IEC 27002:2007 anche se esso, nominalmente, è stato pubblicato soltanto il 1 luglio 2007.

3.1.3 Altri standard ISO/IEC

Altri standard ISO/IEC, di interesse per la PEC, sono i seguenti:

ISO/IEC 9000:2005 - Quality management systems -- Fundamentals and vocabulary

ISO/IEC 13335:2004 - Information technology – Guidelines for the management of IT Security – Part 1: Concepts and models for information and communications technology security management

ISO/IEC 10118 - Information technology -- Security techniques -- Hash-functions, di cui esistono 4 parti emesse in varie date dal 2000 al 2004, con correzioni nel 2006 e nel 2007.

ISO/IEC 15408:2006 - Common Criteria for Information Technology Security Evaluation

Nota: Questo standard è citato espressamente dalla Circolare CNIPA No 49 del 24 novembre 2005, con l'indicazione del livello di valutazione EAL4, come uno dei possibili criteri di valutazione dei dispositivi di firma dei gestori.

ISO/IEC 19790:2006 - Information technology -- Security techniques -- Security requirements for cryptographic modules

Una annotazione merita lo ISO/IEC 19790. Esso infatti è, come espressamente dichiarato nel suo capitolo Introduction: "derived from NIST Federal Information Processing Standard (FIPS) PUB 140-2". Se si associa a questa asserzione quanto disposto dalla richiamata Circolare CNIPA n. CR/49/2005 alla lettera r) " … Sono altresì ammessi:" e al punto 2. indica: "i livelli di valutazione internazionalmente riconosciuti", si deduce che sono utilizzabili da un Gestore PEC anche dispositivi di firma certificati FIPS 140-2. E' evidente che le caratteristiche di riservatezza del dispositivo di firma sono da ritenere soddisfatte solo se il loro livello di sicurezza (Security level) è almeno 3.

3.2 IETF

La Internet Engineering Task Force si auto definisce: "un'ampia e aperta comunità internazionale di progettisti, operatori, fornitori e ricercatori nel campo delle reti.".

Essa si articola in numerosissimi gruppi di lavoro (Working Group) organizzati in otto aree di interesse. In una di esse (Security Area) opera il Working Group (WG) di maggior interesse per lo smime – S/MIME Mail Security.

Un elenco completo degli RFC prodotti da questo WG sarebbe eccessivamente lungo, ci si limita pertanto ad elencare di seguito quelli citati espressamente dall'Allegato tecnico al decreto ministeriale 2 novembre 2005.

Nota: l'elenco completo degli RFC emessi, comprendente i collegamenti ipertestuali ai singoli RFC, si può reperire all'indirizzo internet: http://www.rfc-editor.org/rfc-index.html.

3.2.1 Working Group S/MIME Mail Security

[1]. RFC 1847 Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted

[2]. RFC 1891 SMTP Service Extension for Delivery Status Notifications

[3]. RFC 1912 Common DNS Operational and Configuration Errors

[4]. RFC 2045 Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies

[5]. RFC 2049 Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples

[6]. RFC 2252 Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions

[7]. RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5

[8]. RFC 2633 S/MIME Version 3 Message Specification

[9]. RFC 2821 Simple Mail Transfer Protocol

[10]. RFC 2822 Internet Message Format

[11]. RFC 2849 The LDAP Data Interchange Format (LDIF) - Technical Specification

[12]. RFC 3174 US Secure Hash Algorithm 1 (SHA1)

[13]. RFC 3207 SMTP Service Extension for Secure SMTP over Transport Layer Security

[14]. RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Riguardo allo RFC 2633 va notato che esso è stato reso obsoleto dallo RFC 3851, ma la differenza sostanziale tra il nuovo e il vecchio RFC consiste, a parte l'introduzione "preferenziale", ma non obbligatoria, dello AES come algoritmo di cifra simmetrico e l'obbligatorietà sull'uso di RSA in vari casi quali la firma, nell'introduzione della possibilità (MAY) di proteggere gli RFC822 header con un message/rfc822 wrapper. A parte il fatto che anche lo RFC 3851 presumibilmente dovrà essere aggiornato rapidamente, se non altro a causa delle risultanze della criptoanalisi che hanno dimostrato l'indebolimento dello SHA-1, l'uso dello RFC 2633 si ritiene ancora adeguato, almeno per adesso, in quanto in pratica gli algoritmi che sono diventati obbligatori con lo RFC 3851 sono già da tempo di uso comune e la protezione dello RFC822 header, come detto, è una possibilità e non un obbligo. Pertanto, anche in questo caso, non vi sono controindicazioni sostanziali all'uso di uno standard formalmente obsoleto.

3.3 EESSI

Alla fine del 1998, mentre era ancora in gestazione quella che poi diventò la Direttiva 1999/93/CE sulla firma elettronica, la Commissione Europea chiese allo ICTSB (Information and Communications Technologies Standards Board) di valutare se gli standard allora esistenti fornivano alla imminente Direttiva una adeguata base tecnologica, tale da assicurarne l'effettiva applicabilità.

Il 24 febbraio 1999 venne lanciata la European Electronic Signature Standardisation Initiative, che, dopo una iniziale disamina dello stato dell'arte, raccomandò lo sviluppo di standard integrativi a quelli prodotti da ISO e IETF allo scopo precipuo di soddisfare i requisiti posti dalla Direttiva stessa.

Lo ICTSB quindi designò lo ETSI (European Telecomunications Standards Institute) e il CEN (Comité Européen de Normalisation) a sviluppare tali standard integrativi. Nell'ottobre 2004, avendo lo EESSI adempiuto al proprio mandato, fu chiuso.

Il 14 luglio 2003 la Commissione europea decise che alcuni degli standard sviluppati in seno allo EESSI, e cioè quelli relativi ai dispositivi di firma e alle caratteristiche di affidabilità dei sistemi utilizzati dai certificatori, andassero indicati come "norme generalmente riconosciute relative a prodotti di firma elettronica conformemente alla direttiva 1999/93/CE del Parlamento europeo e del Consiglio." Questa Decisione fu pubblicata il 15 luglio 2003 nella Gazzetta ufficiale della Comunità europea.

Il Gruppo di lavoro E-sign del CEN terminò la sua attività nel 2003, come pianificato, ma altri Technical Committee del CEN curano sia la manutenzione dei documenti da esso prodotti sia il prosieguo di alcuni di essi verso l'acquisizione dello status di European Norm (EN).

Il Technical Body (TC) Electronic Signature and Infrastructures (ESI) dello ETSI invece prosegue tuttora nello sviluppo di ulteriori specifiche che si stanno adesso orientando verso la parte applicativa della firma elettronica, tra cui la Registered E-Mail (Posta Elettronica Certificata), come anticipato nel paragrafo 1.1 Premessa.

Anche in questo caso l'elenco di tutti i documenti prodotti dallo EESSI e successivamente dallo ETSI ESI sarebbe eccessivamente lungo. Se ne elencano, quindi, di seguito i principali ai fini della PEC.

3.3.1 CEN E-sign WS

CWA 14167-2: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)

CWA 14167-3: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)

CWA 14167-4: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP

CWA 14169: Secure Signature-creation devices "EAL 4+"

Il CWA 14169 è indicato espressamente dalla Circolare CNIPA No 49 del 24 novembre 2005 tra i criteri di valutazione dei dispositivi di firma riconosciuti.

Circa i CWA 14167-2 e CWA 14167-4 va chiarito un punto. Ambedue questi CWA recitano al capitolo 2. "TOE description":

> "The Protection Profile's primary scope is for signing qualified certificates. Still components evaluated against this standard may be applied for other signature-creation tasks carried out by a certificate service provider (CSP) such as time-stamping, signing certificate revocation lists (CRLs) or issuing online certificate status protocol (OCSP) messages."

Vi sono due considerazioni da fare a questo riguardo:

1. che il periodo citato parla correttamente di "other signature-creation tasks carried out by a certificate service provider (CSP)" e che fa solo alcuni esempi, non esclusivi, di possibile utilizzo.
2. che la sigla CSP, ivi indicata, è espansa (certificat***e*** service provider) in maniera incorretta, come peraltro nel resto del CWA, mentre è definita correttamente nel capitolo "Terminology" dello stesso CWA:

   > "Certificat***ion***-service-provider (CSP) means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures (defined in the Directive [1], article 2.11)".

   Si ricorda che neppure la citata Direttiva si limita agli esempi indicati nella frase del capitolo 2. "TOE description" del CWA sopra riportata, ma, anzi, ne estende la casistica. E' pertanto lecito utilizzare da parte di un Gestore ai fini della PEC un dispositivo di firma certificato secondo uno dei due protection profiles sopra indicati, purché, ovviamente, siano attuate le condizioni organizzative previste nel medesimo capitolo 2 "TOE Description".

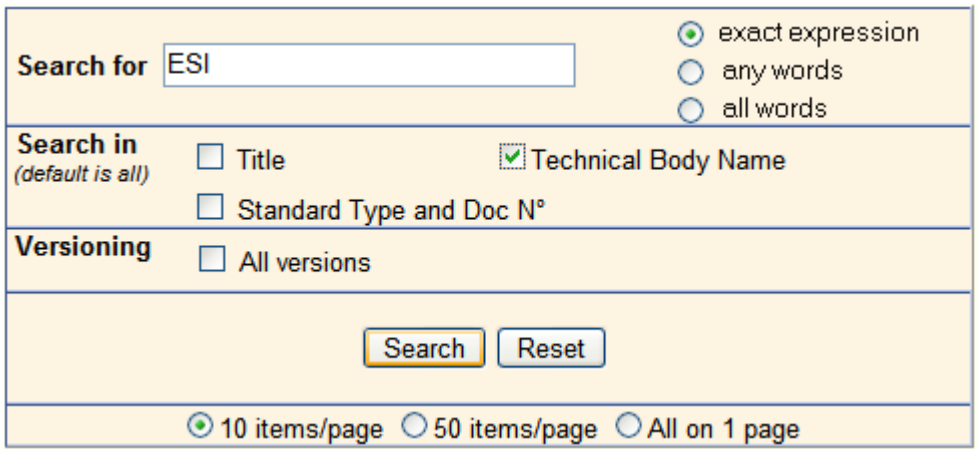
L'elenco completo delle pubblicazioni prodotte da questo Workshop si può ottenere all'indirizzo internet: http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/cwa/electronic+signatures.asp.

3.3.2 ETSI ESI

ETSI TS 102 176-1: Algorithms and Parameters for Secure Electronic Signatures;Part 1: Hash functions and asymmetric algorithms

ETSI TS 102 176-2: Algorithms and Parameters for Secure Electronic Signatures;Part 2: Secure channel protocols and algorithms for signature creation devices

L'elenco completo delle pubblicazioni prodotte da questo Technical Body si può ottenere all'indirizzo internet: http://pda.etsi.org/pda/queryform.asp, indicando "ESI" nel campo "Search for" e selezionando la scelta Technical Body Name nell'opzione "Search in…", come indicato nella figura seguente.



3.4 ITSEC

Il Consiglio dell'Unione Europea nella riunione del 7 aprile 1995 raccomandò:

> "*1) che siano applicati, per un periodo iniziale di due anni, i criteri per la valutazione della sicurezza delle tecnologie dell'informazione (ITSEC) nell'ambito delle procedure di valutazione e certificazione, legate alla commercializzazione e dell'utilizzo di prodotti, servizi e sistemi in materia di tecnologia dell'informazione;*
>
> *… omissis*"

Questa raccomandazione dette impulso all'adozione della certificazione sulla sicurezza delle informazioni in base ai criteri Information Technology Security Evaluation Criteria (ITSEC) il cui uso è andato ben oltre i due anni inizialmente previsti.

Questo insieme di criteri di sicurezza denominato ITSEC era stato inizialmente sviluppato nel 1990 congiuntamente da Francia, Germania, Olanda e Regno Unito, ma il suo uso e riconoscimento si diffusero poi presso gli altri paesi della Unione Europea, anche a seguito della citata raccomandazione.

Successivamente, i paesi europei e quelli nord-americani, presso i quali ultimi erano in uso altri criteri aventi scopi analoghi, denominati TCSEC, onde superare ostacoli al mutuo riconoscimento di prodotti per la sicurezza informatica, concordarono lo sviluppo di quelli che furono chiamati Common Criteria, proprio per il comune accordo tra i paesi interessati a riconoscerne le relative certificazioni. Questi Common Criteria divennero poi nel 2000 lo standard ISO/IEC 15408 di cui si è parlato al paragrafo 3.1.3 "Altri standard ISO/IEC".

La principale caratteristica dei Common Criteria, che ne costituisce una basilare differenziazione con lo ITSEC, è che un oggetto può essere certificato solo in conformità con un Profilo (detto Protection Profile) a sua volta precedentemente certificato il quale, in sintesi, definisca le caratteristiche di sicurezza atte ad assicurare l'ottenimento di specifici livelli di sicurezza.

La normativa italiana cominciò a fare riferimento alla certificazione ITSEC per i dispositivi di firma già con il DPCM 8 febbraio 1999 che stabiliva le regole tecniche per la firma digitale. Da allora la certificazione di un dispositivo di tale tipo effettuata in base allo ITSEC è accettata dalle norme italiane sia per la firma digitale, sia per la PEC.

Nel caso della PEC la Circolare CNIPA n. 49/2005 stabilisce i livelli minimi di sicurezza secondo i quali i dispositivi di firma dei gestori devono essere certificati, nel caso si usino i citati criteri di valutazione ITSEC e Common Criteria:

- ITSEC: livello E3, robustezza (Strength Of Functions) High
- Common Criteria – ISO/IEC 15408: livello di valutazione (Evaluation Assurance Level) EAL 4.

Capitolo 4

Definizioni e Abbreviazioni

Si riportano di seguito definizioni e abbreviazioni integrative rispetto a quelle indicate nei provvedimenti normativi di cui al Capitolo 5.

4.1 Definizioni

Asset	Risorse materiali e immateriali del Gestore correlate con la fornitura dei suoi servizi.

	Nota 1: Esempi di asset materiali sono i locali, i sistemi, i dispositivi sicuri di firma. Esempi di asset immateriali sono le informazioni e l'immagine aziendale.
	Nota 2: La presente definizione è più dettagliata rispetto a quella datane dallo standard ISO 13335: 2004, "anything that has value to the organization", in quanto è più focalizzata alle attività del Gestore.
Audit	Ispezione formale sulle modalità con cui vengono gestiti processi, sistemi, documenti, ecc., condotta allo scopo di verificare se le modalità di gestione sono conformi con quanto previsto dalle relative procedure. Tale ispezione è condotta da organismi, indipendenti dai reparti cui fa capo quanto è oggetto dell'ispezione, i quali possono far parte della stessa organizzazione dei reparti soggetti all'ispezione (*audit interno*) oppure possono appartenere a organizzazioni esterne (a*udit esterno*). Ove non specificato altrimenti il termine "audit" fa riferimento indifferentemente a audit interni ed esterni.
Autenticazione forte	Autenticazione, ossia verifica mediante mezzi informatici dell'identità di un utente, realizzata con strumenti e metodi adeguatamente affidabili. Nota: sono da ritenere adeguatamente affidabili dispositivi hardware, di tipo OTP (One Time Password) o crittografico, oppure PIN e password di composizione complessa immesse mediante modalità sicure (tastiera fisica non soggetta a intercettazione, tastiera presentata sullo schermo con disposizione dei tasti casuale e sempre diversa, ecc.). In questi ultimi casi è però necessario che l'utente adotti misure atte a proteggere PIN e password da acquisizione da parte di persone non autorizzate, quali: conservazione in modo sicuro, protezione dalla lettura furtiva, ecc.
Certificatore	il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime (Dlgs 82/2005, art. 1, comma 1, lettera g)
Datakey	Dispositivi crittografici (usualmente smart card o dispositivi USB) contenenti le chiavi o loro parti (in questo secondo caso normalmente determinate con modalità di secret sharing come definito da Blakley o da Shamir – vedi Bibliografia) con cui attivare un dispositivo crittografico.
Dual Control	Esecuzione di procedure da parte di almeno due addetti adeguatamente competenti, per aumentare il livello di fiducia sulla corretta esecuzione della procedura. Nota 1: questo requisito è suffragato da quanto indicato nello standard ISO/IEC 27002 al capitolo "10.1.3 Segregation of duties" ("Separazione dei compiti") laddove recita: "Care should be taken that no single person can access, modify or use assets without authorization or detection." ("Dovrebbe essere prestata attenzione a che nessuna persona possa da sola accedere, modificare o utilizzare un asset senza essere autorizzata o senza che un tale accesso sia rilevato"). Al citato capitolo si legge inoltre: "The possibility of collusion should be considered in designing the controls." ("Nel definire le misure si dovrebbe valutare la possibilità di collusione"). Si ritiene quindi necessario che almeno nei casi più delicati, in cui perfino il "dual control" o il monitoraggio potrebbero non essere ritenuti sufficienti, non sia concessa l'autorizzazione a operare da soli di cui al capoverso precedente. Nota 2: il rispetto del dual control mediante misure organizzative, ove non sia possibile attuarlo con misure tecniche, è da ritenersi adeguato.
Incidente di sicurezza	Un singolo evento inatteso o indesiderato, o una serie di tali eventi, correlato con la sicurezza delle informazioni che abbia una non trascurabile probabilità di compromettere le operazioni di business e di minacciare la sicurezza delle informazioni [ISO/IEC TR 18044:2004]
Information Security	

Management System	La parte dell'intero sistema di gestione che, in base a una valutazione dei rischi, definisca, realizzi, renda operativa, controlli, sottoponga a revisione, mantenga aggiornata e migliori la sicurezza delle informazioni. Nota: il sistema di gestione comprende strutture organizzative, norme, attività di pianificazione, responsabilità, modalità operative, procedure, processi e risorse. (Traduzione informale dallo ISO/IEC 27001:2005.)
Malware	Vedi "Virus (informatico)"
Time Stamping Authority	Ente affidabile che emette TST avvalendosi di sistemi appositi detti TSS
Time Stamp Server	Sistema di cui si avvale un certificatore, operante come TSA, per emettere TST
Time Stamp Token	Marca temporale
Time Stamping Unit	Insieme di hardware e software, facente parte di un Time Stamp Server e da esso gestito in maniera esclusiva per firmare TST, che dispone di un solo dispositivo di firma il quale utilizza una sola coppia di chiavi di firma per volta
Valutatore	Il team CNIPA di valutazione nel suo complesso o i suoi singoli componenti.
Verbale	Qualsiasi evidenza, anche elettronica, che documenti l'avvenuta effettuazione di procedure, attività, ispezioni, ecc.
Virus (informatico)	Qualsiasi tipo di codice (software) avente lo scopo, una volta che sia installato in un sistema di elaborazione dati, di causare danni o di raccogliere arbitrariamente informazioni. Comunemente detto anche "malware".
Vulnerabilità	Un punto debole di un asset o di un gruppo di asset che può essere sfruttato da una o più minacce (ISO/IEC 13335-1:2004)

4.2 Abbreviazioni

All. DM 2/11/2005	Allegato al DM 2 novembre 2005
CAD	Codice Amministrazione Digitale (Dlgs 82/2005)
CNIPA/CR/49	Circolare CNIPA 24 novembre 2005, n. 49 [56]
CNIPA/CR/51	Circolare CNIPA 7 dicembre 2006, n. 51
CNIPA	Centro nazionale per l'informatica nella pubblica amministrazione
Del. CNIPA 11/2004	Deliberazione CNIPA n. 11 del 19 febbraio 2004
IGPEC	Indice dei Gestori di PEC
ISMS	Information Security Management System
TSA	Time Stamping Authority
TSS	Time Stamp Server
TST	Time Stamp Token

Capitolo 5

Riferimenti normativi

CNIPA/CR/49	Circolare CNIPA 24 novembre 2005, n. 49 – Modalità per la presentazione delle domande di iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata (PEC), di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.
CNIPA/CR/51	Circolare CNIPA 7 dicembre 2006, n. 51 – Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell'elenco dei gestori di po-sta elettronica certificata (PEC), di cui all'articolo 14 del decreto del Presiden-te della Repubblica 11 febbraio 2005, n. 68, «Regolamento recante disposi-zioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3». G.U. n. 296 del 12 dicembre 2006.
Codice Amministrazione Digitale	Si veda: "Dlgs 82/2005"
DPR 68/2005	Decreto del Presidente della Repubblica 11 febbraio 2005, n.68 – Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3, pubblicato sulla G.U Gazzetta Ufficiale del 28 aprile 2005, n. 97.
DM 2/11/2005	Decreto del Ministro per l'innovazione e le tecnologie del 2 novembre 2005, pubblicato sulla Gazzetta Ufficiale del 15 novembre 2005, n. 266.
Deliberazione CNIPA 11/2004	Deliberazione n. 11 del 19 febbraio 2004 – Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali - Art. 6, commi 1 e 2, del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.
Dlgs 196/2003	Decreto Legislativo 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali"
Dlgs 82/2005	Decreto Legislativo 7 marzo 2005, n. 82 recante "Codice dell'amministrazione digitale", come modificato dal Decreto legislativo 4 aprile 2006, n. 159;.
DPR 445/2000	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 recante "Testo unico delle disposizioni legislative e regolamentari in materia di do-cumentazione amministrativa"
FAQ – CNIPA/CR/51	Frequently Asked Questions sulla Circolare CNIPA/CR/51
Legge 241/90	Legge 7 agosto 1990, n. 241 recante "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi"
LL GG Iscrizione PEC	Raccomandazioni in merito alla predisposizione della documentazione prevista per l'iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata
MO Certificati Server	Manuale Operativo per il Servizio "Cnipa Certificati Server" – Certificate Practice Statement –Manuale Operativo – ver. 1.1 Gennaio 2008
Racc. iscrizione IGPEC	Vedi: LLGG Iscrizione PEC
Testo Unico	Si veda: "DPR 445/2000"

Capitolo 6

Le modalità di verifica

6.1 Il Gestore

Per dimostrare la conformità della propria attività ai requisiti di legge, il Gestore, su richiesta del Valutatore, esibisce i documenti comprovanti il sussistere delle condizioni richieste dal DPR 68/2005. In particolare esibisce anche le parti del Piano per la sicurezza necessarie per il controllo.

Inoltre, il Gestore esibisce quanto indicato di seguito.

Documentazione (ivi inclusi i log dei messaggi di PEC, i messaggi nei quali sia stata riscontrata la presenza di virus informatici almeno negli ultimi trenta mesi e, ove del caso, i log di sistema e delle applicazioni) volta a dimostrare il rispetto dei requisiti di legge e di altri requisiti di sicurezza, in conformità con gli standard comunemente adottati, in particolare con gli standard prodotti da ISO/IEC (si veda al Capitolo 3 "Gli standard di riferimento"). Per la maggior parte di essi le modalità specifiche di esibizione della documentazione sono indicate nei singoli capitoli delle presenti Linee Guida.

I verbali di verifiche e ispezioni effettuate a cura del Gestore con cadenza almeno semestrale in conformità con quanto indicato nella CNIPA/CR/51 al punto 8.1. Esse, come indicato dal citato punto: "devono riguardare, in particolare, le componenti tecniche ed organizzative del sistema di PEC, il sistema di raccolta dei livelli di servizio e le tipologie di contratti di vendita dei servizi di PEC".

Più in dettaglio il Gestore esibisce verbali di verifiche e ispezioni riguardanti il rispetto delle proprie procedure interne, eseguite presso le sedi proprie e dei propri fornitori, da cui risulti il rispetto almeno di quanto segue.

- conservazione del log di PEC e dei messaggi contenenti virus in conformità con quanto previsto dalla normativa;
- conservazione del log dei sistemi, con modalità che ne assicurino l'integrità, da cui risultino le informazioni sulle sessioni, in particolare i dati di inizio e fine e gli estremi di chi vi ha acceduto
- esattezza dell'inventario dei dispositivi di firma e dei loro eventuali accessori crittografici;
- corrispondenza della effettiva configurazione dei sistemi (HW e SW, di PEC e di rete quali: firewall, IDS, ecc.) con quanto formalizzato e custodito dalla funzione aziendale a ciò deputata;
- utilizzo della documentazione contrattuale relativa alle caselle di posta o ai loro domini così come è stata predisposta dal Gestore;
- conformità alle procedure delle prassi utilizzate dagli addetti per quanto riguarda le operazioni di:
  - controllo accessi fisici ove non siano utilizzati dispositivi che li registrino automaticamente;
  - conservazione della documentazione contrattuale relativa alla concessione e alla cessazione di caselle di posta e loro domini;
  - predisposizione dello LDIF di input per il CNIPA e regolare scarico giornaliero di quello predisposto dal CNIPA;
  - rispetto delle misure di sicurezza imposte dal Dlgs 196/2003 e successive modificazioni e integrazioni;
  - congruenza tra i dati presenti nella sede principale e in quelle di disaster recovery o di conservazione delle copie di sicurezza;
- costante disponibilità della procedura di disaster recovery, ove prevista, e suo tempestivo aggiornamento;

- esistenza e rispetto delle procedure di rilevazione dei livelli di servizio previsti dal DM 2/11/2005 all'art. 12, come richiesto dalla CNIPA/CR/51 al punto 4.1 lettera c);
- rispetto delle altre procedure utilizzate nell'attività di gestione PEC.

Esibisce, a richiesta, verbali di prove di restart dei sistemi di PEC, anche simulando situazioni di disastro che richiedano, per esempio e ove del caso, l'attivazione del sito di disaster recovery, e del recupero di dati dai siti di back up.

Esibisce, a richiesta, evidenza che a fronte di situazioni riscontrate non in rispondenza con quanto atteso siano state intraprese azioni correttive atte a evitare per il futuro il ripetersi delle medesime o di analoghe situazioni.

Qualora da ispezioni effettuate presso fornitori di servizi affidati in outsourcing siano risultate situazioni non in rispondenza con le condizioni contrattuali, esibisce evidenza che sono state intraprese nei confronti dei fornitori le azioni correttive previste dagli accordi stessi atte a evitare per il futuro il ripetersi delle medesime o di analoghe situazioni.

Conformemente con la "*dichiarazione di piena disponibilità a consentire l'accesso di incaricati del CNIPA presso le strutture dedicate all'erogazione del servizio di posta elettronica certificata, al fine di poter verificare la rispondenza delle stesse ai requisiti tecnici, organizzativi e funzionali di cui alla documentazione allegata alla domanda*", depositata presso il CNIPA come previsto dalla CNIPA/CR/49 al punto 1 lettera q), garantisce al team CNIPA di valutazione l'accesso, nel rispetto delle misure di sicurezza indicate nel Piano per la Sicurezza, ai sistemi e locali utilizzati per la fornitura dei servizi di PEC, anche se di pertinenza di suoi fornitori.

Su richiesta del Valutatore esegue specifiche procedure e operazioni.

Mette a disposizione del Valutatore un numero sufficiente di adeguate postazioni di lavoro dotate dei necessari servizi: accesso a internet, alimentazione elettrica, ecc.

6.2 Il Valutatore

Nell'analisi delle misure di sicurezza e delle procedure operative adottate dal Gestore il Valutatore presumerà che esse siano state impostate in base allo standard ISO/IEC 27002. Qualora il Gestore abbia adottato criteri diversi, sarà sua cura informarne il CNIPA entro l'inizio della visita ispettiva.

Il team di valutazione nel suo complesso:

1. anteriormente all'ispezione:
    a. prende visione della documentazione depositata dal Gestore presso CNIPA all'atto della richiesta di accreditamento in conformità con la CNIPA/CR/49 del 2005, o di eventuali suoi aggiornamenti depositati successivamente;
    b. verifica che il Manuale Operativo pubblicato presso il sito del Gestore corrisponda alla versione approvata dal CNIPA;
    c. acquisisce conoscenza di quali siano altre sedi eventualmente utilizzate dal Gestore come sedi di conservazione delle copie di scorta, come sedi di disaster recovery, o per la erogazione dei servizi di PEC;
    d. nel caso in cui il Gestore si avvalga di fornitori esterni per tutti i servizi di PEC o per loro parte acquisisce dal Gestore stesso evidenza che detti fornitori siano adeguatamente formati sulle attività loro demandate.
2. durante l'ispezione, in base a quanto indicato in queste Linee Guida:
    a. verifica a campione:
        i. l'esistenza della documentazione indicata nei vari paragrafi e, sempre eventualmente a campione, la sua rispondenza ai relativi obiettivi;
        ii. che dai verbali di esecuzione delle procedure risulti il rispetto delle medesime;

iii. che i verbali delle ispezioni più recenti effettuate dal Gestore nel rispetto delle proprie procedure, sia al proprio interno sia presso eventuali fornitori, non si riferiscano a ispezioni effettuate al di là del periodo previsto dalle procedure stesse; in particolare i verbali relativi alle ispezioni indicate al precedente paragrafo 6.1 devono non essere anteriori ai sei mesi precedenti l'ispezione di vigilanza;

iv. che, ove dai citati verbali delle ispezioni risultino situazioni di non conformità con le procedure, siano state prese azioni correttive atte a evitare per il futuro il ripetersi delle medesime, o analoghe, situazioni;

b. verifica, eventualmente a campione, le risultanze dei verbali di auditing formale, interno o esterno, e, nel caso in cui in tali verbali segnalino problemi, vulnerabilità, mancato rispetto delle procedure, ecc., verifica se a tali segnalazioni siano seguiti interventi correttivi;

c. effettua, eventualmente a campione, i sopralluoghi e gli altri controlli indicati in queste Linee Guida;

d. può effettuare altri sopralluoghi e controlli, oltre a quelli indicati nelle presenti Linee Guida, che a suo giudizio siano utili ai fini della valutazione;

e. può richiedere, onde effettuare le verifiche ritenute necessarie, l'esecuzione delle procedure relative al rilascio e alla successiva gestione di caselle di PEC. Queste ultime possono essere utilizzati ai soli fini dell'ispezione e al termine della stessa saranno definitivamente disattivate;

f. può chiedere l'esecuzione sotto la sua vigilanza di operazioni atte a consentire il controllo dell'attività del Gestore.

Nota 1: Le valutazioni delle verifiche, indicate nelle presenti Linee Guida, sulle misure di sicurezza e operative, sulla consistenza e preparazione del personale, sui dispositivi di sicurezza impiegati, saranno fatte esclusivamente sulla base dei documenti in vigore depositati presso il CNIPA, anche nel caso in cui il Gestore ne esibisca versioni più recenti in occasione dell'ispezione di vigilanza.

Nota 2: L'attività di vigilanza sui Gestori si limita a verificare l'esistenza e l'applicazione delle procedure volte al rispetto delle norme di cui al Dlgs 196/2003, senza che questo comporti una valutazione sull'adeguatezza di tali procedure.

6.3 Modalità dell'ispezione

La data di inizio dell'ispezione viene comunicata da parte del CNIPA al Gestore nella persona del Responsabile del servizio, indicato dal Gestore stesso in occasione della sua domanda di iscrizione nell'Elenco Pubblico dei Gestori, e nella persona del Responsabile delle verifiche e ispezioni, come individuato dal DM 2 novembre 2005, art. 21 comma 1 lettera c). Tale comunicazione viene anche inviata per conoscenza al legale rappresentante del Gestore.

Il momento dell'inizio dell'ispezione viene ufficializzato in un incontro del Valutatore almeno con il citato Responsabile delle verifiche e ispezioni del Gestore, o con diversa persona formalmente incaricata dal legale rappresentante del Gestore, e con la Direzione Aziendale.

La conclusione dell'ispezione può essere ufficializzata dal Valutatore sia in un analogo incontro con il medesimo Responsabile delle verifiche e ispezioni, o con persona formalmente incaricata dal legale rappresentante del Gestore, sia con una comunicazione del Valutatore allo stesso Responsabile, inoltrata per posta ordinaria o, preferibilmente, per Posta Elettronica Certificata. In quest'ultimo caso il verbale è firmato digitalmente.

Il momento dell'inizio e quello di fine sono indicati dal Valutatore nel verbale dell'ispezione.

Il verbale è controfirmato dal citato Responsabile delle verifiche e ispezioni o da persona formalmente incaricata dal legale rappresentante del Gestore. Nel caso in cui il verbale sia stato inviato in formato elettronico, e quindi firmato digitalmente, il Gestore è tenuto a restituirlo controfirmato digitalmente al CNIPA.

Il Valutatore baserà le proprie ispezioni sulla verifica, eventualmente a campione e in base ai verbali di auditing, del rispetto di quanto indicato nel Manuale Operativo, nel Piano per la Sicurezza del Gestore, e sulle altre disposizioni indicate nelle presenti Linee Guida.

Altri documenti di riferimento per la conduzione delle valutazioni sono i seguenti documenti citati al Capitolo 5 – Riferimenti

- ISO/IEC 27001
- ISO/IEC 27002.

6.4 Procedure e documentazione del Gestore

Le procedure e la documentazione del Gestore cui si fa riferimento in queste Linee Guida devono essere predisposte in conformità con quanto indicato ai paragrafi "Normativa" delle varie sezioni. Ove in uno di essi non siano indicate specifiche norme giuridiche, vengono comunque fornite precise indicazioni da rispettare nelle procedure in questione.

Tali procedure e tale documentazione possono essere conservate con modalità informatica nel rispetto della normativa vigente in materia. In tal caso il Valutatore prende atto della dichiarazione del Gestore sul fatto che sono rispettate le norme per la conservazione sostitutiva.

6.5 Verbali

6.5.1 Verbali di esecuzione di procedure

Il Gestore esibisce verbali di esecuzione di specifiche procedure per attestare che esse sono state eseguite secondo i piani.

6.5.2 Verbali di auditing

Il Gestore esibisce i verbali di auditing interno ed esterno di verifiche effettuate per attestare che specifiche procedure/operazioni:

- sono, o sono state, eseguite correttamente;
- sono conformi con i requisiti di legge o di standard tecnici o con normative interne;
- soddisfano requisiti non altrimenti verbalizzabili..

Il Valutatore prende atto dell'esistenza di tali verbali, ne visiona il contenuto dal quale può trarre spunto per ulteriori verifiche. Il Valutatore può verificare a campione l'effettiva esecuzione dell'attività di auditing verbalizzata.

6.6 Dotazione dei valutatori

Il Valutatore dispone di propri strumenti, messi a disposizione dal CNIPA, per la verifica del contenuto dei dati di certificazione, delle firme apposte su Ricevute, Avvisi e Buste di trasporto, ecc.

Capitolo 7

Gestione chiavi, certificati, LDIF del Sistema di PEC

7.1 Dispositivi di firma del Gestore

Finalità: i dispositivi di firma del Gestore devono essere conformi a criteri di sicurezza atti ad assicurare la riservatezza della chiave privata, l'accesso esclusivo ad essa e il suo utilizzo esclusivo da parte solo di utenti identificati e autorizzati, la immodificabilità dell'impronta oggetto di cifra.

7.1.1 Normativa

DPR 68/2005

Art. 14., comma 6, lettera e)

All. DM 2/11/2005

8.1 Firma

CNIPA/CR/49

1, [lettera r) dell'elenco degli allegati alla domanda di iscrizione nell'elenco dei gestori di posta elettronica certificata]

2.2 Piano per la sicurezza, lettera b).

7.1.2 Il Gestore

1. Esibisce documentazione comprovante la corrispondenza dei dispositivi di firma alla descrizione datane nel Piano per la sicurezza, come previsto dalla CNIPA/CR/49, al punto 2.2, lettera b).
2. Esibisce documentazione comprovante la rispondenza dei dispositivi di firma alle caratteristiche di sicurezza richieste dalla CNIPA/CR/49, al punto 1, lettera r).

7.1.3 Il Valutatore

1. Verifica l'esistenza della documentazione comprovante la corrispondenza dei dispositivi di firma alla descrizione datane nel Piano per la sicurezza.
2. Verifica dalla documentazione che i dispositivi di firma utilizzati siano corrispondenti a quanto comunicato al CNIPA.

7.2 Generazione delle chiavi del Gestore

Finalità: il Gestore deve garantire che le chiavi di PEC siano generate sotto adeguato controllo che ne assicuri la sicurezza e nel rispetto della normativa.

7.2.1 Normativa

CNIPA/CR/49

2.1 Manuale operativo, lettera e)

MO Certificati Server

9.2 Obblighi del Richiedente

10.2 Registrazione del Server, punto 3

7.2.2 Il Gestore

1. Esibisce la procedura prevista per la generazione della coppia di chiavi di PEC da cui risulti l'adozione di misure finalizzate ad "evitare danni, alterazioni o usi non autorizzati della stessa", come richiesto al punto 9.2 "Obblighi del Richiedente" del MO Certificati Server.

   Tra le misure ritenute adeguate a tale scopo, in aggiunta al requisito del MO Certificati server al punto 10.2 punto 3 di fare generare le coppie di chiavi sotto la responsabilità del Responsabile del Server, si indicano le seguenti:

   a. Generazione effettuata, a cura del Responsabile del Server, in situazione di dual control, stante l'estrema delicatezza dell'operazione (si veda la nota alla definizione del termine "dual control");

   b. Conservazione e utilizzo dei dispositivi di firma in ambienti ad accesso fisico o logico limitato e controllato.

2. Esibisce evidenza che le funzioni della procedura di cui al punto 1 assicurino il rispetto delle politiche di sicurezza previste dall'Obiettivo di sicurezza (Security Target) o dal Protection Profile del dispositivo di firma, con particolare attenzione al rispetto della procedura di installazione del dispositivo e di generazione delle chiavi, alla riservatezza delle chiavi generate e dei dati per l'autenticazione degli addetti al dispositivo stesso.
3. Esibisce i verbali di esecuzione della procedura di cui al precedente punto 1.
4. Esibisce verbali di audit che attestino quanto previsto al precedente punto 2.

7.2.3 Il Valutatore

1. Verifica che la procedura di generazione della coppia di chiavi di PEC di cui al punto 1 del paragrafo 7.2.2 risponda ai requisiti ivi indicati circa l'adozione di misure finalizzate all'ivi citato obiettivo di "evitare danni, alterazioni o usi non autorizzati della" coppia di chiavi.
2. Può verificare l'autenticità della documentazione di cui ai punti 2 (Security Target o Protection Profile) del paragrafo 7.2.2.
3. Verifica l'esistenza dei verbali di esecuzione di cui al punto 3 del paragrafo 7.2.2.
4. Verifica che dai verbali di audit di cui al punto 4 risulti che la procedura citata al punto 1 del paragrafo 7.2.2 rispetta le politiche di sicurezza previste dall'Obiettivo di sicurezza (Security Target) o dal Protection Profile del dispositivo di firma.

7.3 Richiesta dei certificati delle chiavi del Gestore

Finalità: il Gestore deve formulare la richiesta di certificati al CNIPA secondo le modalità previste nel MO Certificati Server.

7.3.1 Normativa

All. DM 2/11/2005

10.4 Certificato S/MIME

10.5 Certificato S/MIME

10.5.1 Informazioni relative al Gestore (subject)

10.5.2 Estensioni del certificato

MO Certificati Server

10.2 Registrazione del Server

7.3.2 Il Gestore

1. Esibisce la propria procedura interna per la richiesta di certificati Server PEC conforme con quanto indicato al punto 10.2 del MO Certificati Server; in essa devono essere indicate anche le modalità per la verifica delle correttezza dei certificati entro il periodo di tempo previsto al punto 10.6 del MO Certificati Server, per la richiesta della loro revoca ove tali dati siano errati, e per la loro installazione nei corrispondenti server.
2. Esibisce i verbali di esecuzione della procedura di cui al precedente punto 1.

7.3.3 Il Valutatore

1. Verifica che le caratteristiche della procedura interna del Gestore per la richiesta di certificati Server PEC sia conforme con quanto previsto al punto 10.2 del MO Certificati Server e che in essa sia previsto quanto indicato al punto 1 del paragrafo 7.3.2.
2. Verifica l'esistenza dei verbali di cui al punto 2 del paragrafo 7.3.2.

7.4 Sostituzione delle chiavi del Gestore

Finalità: il Gestore deve garantire che le sue chiavi di firma siano sostituite con tempestività tale da consentire il rispetto da parte del proprio sistema di PEC dei livelli di servizio previsti.

Nota: una sostituzione tardiva comporterebbe l'attesa del periodo di tempo previsto nel MO Certificati Server per la generazione del certificato a partire dal ricevimento da parte del CNIPA della Richiesta di emissione certificato

7.4.1 Normativa

DM 2/11/2005

Articolo 12 - Livelli di servizio, commi 3, 4 e 5

All. DM 2/11/2005

7.5

MO Certificati Server

9.2 Obblighi del Richiedente

10.2 Registrazione del Server

10.10 Riemissione del certificato

10.12 Livelli di servizio

7.4.2 Il Gestore

1. Esibisce la procedura operativa per la:
    a. generazione di una nuova coppia di chiavi, in situazione di emergenza o in caso di normale sostituzione all'approssimarsi della scadenza di un certificato server;
    b. formulazione della richiesta del certificato relativo, in ottemperanza alla "Procedura per la richiesta di emissione certificato" di cui al punto 10.2, punto 4 del MO Certificati Server;

c. aggiornamento del file LDIF.

Tale procedura deve essere organizzata tenendo conto dei tempi previsti nel MO Certificati Server, punto 10.12 "Livelli di servizio", in modo da essere eseguita con tempistica e modalità tali da evitare che vi sia un'interruzione del servizio di PEC per un periodo più lungo di quanto previsto all'art. 12 del DM 2/11/2005.

2. Qualora tale sostituzione di certificato sia stata già effettuata esibisce i relativi verbali anche di audit.

7.4.3 Il Valutatore

1. Verifica l'esistenza della procedura prevista al punto 1 del paragrafo 7.4.2 e che essa corrisponda ai requisiti ivi indicati
2. Qualora la sostituzione del certificato sia già avvenuta verifica l'esistenza dei verbali di esecuzione della procedura
3. Qualora la procedura di sostituzione del certificato sia già avvenuta verifica che i relativi verbali di audit ne mostrino il rispetto.

7.5 Conservazione e gestione delle chiavi del Gestore e dei dati per attivarle

Finalità: il Gestore deve assicurare che le chiavi private di PEC rimangano riservate e conservino la loro integrità.

Nota: per quanto riguarda il ritiro dall'operatività di tali chiavi veder anche il capitolo 7.8.

7.5.1 Normativa

Dlgs 82/2005

Art. 32. Obblighi del titolare e del certificatore, commi 1 e 2.

All. DM 2/11/2005

8.1 Firma

CNIPA/CR/49

1, lettere p), r)

2.1 Manuale operativo, lettera e)

MO Certificati Server

9.2 Obblighi del Richiedente

7.5.2 Il Gestore

1. Esibisce procedure operative da cui emerga che esso gestisce i dispositivi di firma in conformità con le Security Policy e con i Profili di Protezione a cui i dispositivi stessi sono stati dichiarati conformi, in particolare che la chiave privata del Gestore sia custodita in modo sicuro all'interno del relativo dispositivo di firma e che i dati per l'attivazione delle chiavi stesse siano conservati in modo sicuro.

   Nota: per quanto riguarda le copie di sicurezza della chiave privata di firma del Gestore si veda il paragrafo 7.6.

2. Esibisce procedure operative da cui emerga che esso informa tempestivamente il CNIPA nel caso in cui ritenga che la sicurezza del server su cui è stato installato il certificato possa essere compromessa, richiedendo la revoca del certificato stesso; analoga informativa deve essere attuata anche nel caso in cui risulti compromessa la riservatezza della chiave privata, o di sue copie, e/o dei relativi dati di attivazione.

3. Esibisce verbali di audit da cui risulti che le procedure di cui ai punti precedenti sono state rispettate, ivi incluso la loro esecuzione da parte del personale a cui la mansione di gestione delle chiavi di firma sia stata indicata nella "Relazione sulla struttura organizzativa" a suo tempo depositata presso il CNIPA.

7.5.3 Il Valutatore

1. Verifica l'esistenza delle procedure previste al paragrafo 7.5.2 e la rispondenza di quelle di cui al relativo punto 1 con quanto previsto nella misure di sicurezza alle quali il dispositivo è stato dichiarato conforme e con le attribuzioni indicate nella Relazione sulla struttura organizzativa, di cui al punto p) della CNIPA/49/2005.
2. Verifica l'esistenza delle procedure previste al punto 2 del paragrafo 7.5.2 circa le azioni da svolgere in caso di compromissione della sicurezza del server, della chiave o dei relativi dati di attivazione.
3. Verifica che dai verbali di cui al punto 3 del paragrafo 7.5.2 emerga il rispetto delle procedure relative.

   Nota: Per le procedure per la esportazione delle chiavi private di PEC si veda il paragrafo 7.6.

7.6 Copie per backup e recovery delle chiavi del Gestore

Finalità: il Gestore deve assicurare che le chiavi private di PEC e le loro copie rimangano riservate e conservino la loro integrità.

Nota: le disposizioni in questo paragrafo si applicano ai casi in cui il Gestore preveda la creazione di copie di sicurezza delle proprie chiavi private di firma. Questa è una misura altamente raccomandata, purché ciò sia consentito dal Security Target o dal Protection Profile del dispositivo di firma, in quanto nel caso non sia possibile effettuare tali copie di sicurezza la compromissione o la distruzione di una chiave di firma comporterebbe la necessità di richiedere al CNIPA i certificati per una nuova coppia di chiavi e di attenderne il rilascio per poi pubblicarli nel file LDIF messo a disposizione del CNIPA almeno 48 ore prima della loro entrata in esercizio. Questo sarebbe incompatibile con i requisiti di livello di servizio previsti dalla norma e comporterebbe inevitabilmente la dichiarazione dello stato di Disastro.

7.6.1 Normativa

All. DM 2/11/2005

8.1 Firma

CNIPA/CR/49

1, lettere p) ed r)

2.1 Manuale operativo, lettera e)

MO Certificati Server

9.2 Obblighi del Richiedente

7.6.2 Il Gestore

1. Ove il Gestore esegua copie di sicurezza delle chiavi private di PEC, esibisce la procedura operativa che deve rispettare i requisiti di sicurezza di cui agli obblighi del Richiedente indicati nel MO Certificati server, ivi inclusa la sua esecuzione da parte delle persone appositamente incaricate, come dalla Relazione sulla struttura organizzativa di cui alla lettera p) del punto 1 della CNIPA/CR/49. Si ritiene auspicabile, in base a considerazioni di sicurezza e affidabilità, che tale copia, anche se ciò non è esplicitamente previsto dalla normativa, sia eseguita in condizioni di dual control.

   Nota 1: normalmente, laddove i dispositivi di firma utilizzati per i sistemi di PEC prevedano l'effettuazione di tali copie di sicurezza, sono previste dal costruttore anche le procedure da eseguire per backup e restore, anch'esse oggetto di valutazione di conformità;

Nota 2: laddove le copie di sicurezza siano protette mediante cifra, la Special Publication 800-57 Part 1 del NIST indica gli anni fino ai quali si ritiene possano resistere algoritmi e lunghezze di chiavi.

2. Ove il Gestore esegua il ripristino delle chiavi private di PEC esibisce la procedura operativa che deve rispettare i requisiti di sicurezza di cui agli obblighi del Richiedente indicati nel MO Certificati server, in conformità con le indicazioni del costruttore, e deve essere eseguita da parte delle persone appositamente incaricate, come dalla Relazione sulla struttura organizzativa di cui alla lettera p) del punto 1 della CNIPA/CR/49. Si ritiene auspicabile, in base a considerazioni di sicurezza e affidabilità, che tale ripristino, anche se ciò non è esplicitamente prevista dalla normativa, sia eseguito in condizioni di dual control.
3. Esibisce evidenza che il personale preposto all'esecuzione delle procedure in questione è compreso tra quello indicato agli articoli 21 e 22 del DM 2/11/2005, o quanto meno ricade sotto la responsabilità delle figure ivi indicate.
4. In aggiunta alle procedure previste dalle Security Policy dei dispositivi di firma utilizzati per i sistemi di PEC, valutati secondo uno dei criteri di sicurezza conformi con quanto previsto alla lettera r) del punto 1 della CNIPA/CR/49, il Gestore esibisce procedure che assicurino che le copie delle chiavi di PEC o di loro elementi, così come le informazioni atte ad attivarle, siano custodite e accedute secondo modalità che rispettino le indicazioni del costruttore conformi con i criteri di valutazione. Da tale procedura deve risultare l'adozione di misure adeguate ad "evitare danni, alterazioni o usi non autorizzati" delle copie delle chiavi di PEC o di loro elementi, così come le informazioni atte ad attivarle, come richiesto al punto 9.2 "Obblighi del Richiedente" del MO Certificati Server.
5. Esibisce procedure operative da cui emerga che esso informa tempestivamente il CNIPA nel caso in cui ritenga che la sicurezza delle copie delle chiavi possa essere compromessa, ivi compresa anche la compromissione dei dati di attivazione delle copie stesse, richiedendo la revoca del certificato relativo;
6. Esibisce verbali, anche di audit, dell'esecuzione delle procedure di esecuzione delle copie di sicurezza e della loro conservazione.
7. Ove sia stato già effettuato il ripristino delle chiavi di PEC, il Gestore esibisce i relativi verbali, anche di audit.

7.6.3 Il Valutatore

1. Verifica l'esistenza delle procedure previste al paragrafo 7.6.2 e la rispondenza di quelle indicate ai punti 1 e 2 del medesimo paragrafo (creazione delle copie di sicurezza e ripristino delle chiavi di firma) sia con quanto previsto nella certificazione del dispositivo, ove ivi indicata, sia con la opportunità di eseguire queste operazioni in situazione di dual control.
2. Verifica l'esistenza delle procedure di segnalazione al CNIPA di eventuale compromissione delle copie delle chiavi di firma previste al punto 5 del paragrafo 7.6.2.
3. Verifica l'esistenza della evidenza che il personale preposto all'esecuzione delle procedure in questione sia compreso tra quello indicato agli articoli 21 e 22 del DM 2/11/2005, o che quanto meno ricada sotto la responsabilità delle figure ivi indicate.
4. Verifica la conformità delle procedure di cui ai punti 4 e 5 del paragrafo 7.6.2 con quanto indicato al riguardo nel Piano per la sicurezza o nel Manuale operativo.
5. Verifica che dai verbali previsti al punto n. 6 del precedente paragrafo 7.6.2 emerga evidenza dell'esecuzione delle procedure indicate nel Piano per la sicurezza o nel Manuale operativo.
6. Ove sia stato già effettuato il ripristino delle chiavi di PEC, verifica l'esistenza del relativo verbale, anche di audit.

7.7 Gestione dello LDIF

Finalità: il Gestore deve assicurare:

1. che i certificati per la firma del Gestore, in occasione della messa in esercizio delle corrispondenti coppie di chiavi, siano tempestivamente messi a disposizione del CNIPA mediante il loro inserimento nel file LDIF previsto nell'Allegato al DM 2/11/2005 almeno 48 ore prima della loro entrata in esercizio.
2. la acquisizione da parte del Gestore del contenuto dello IGPEC gestito dal CNIPA con la cadenza prevista al punto 7.5 dell'All. DM 2/11/2005, e la sua conservazione in una cache interrogata dai propri server.

7.7.1 Normativa

All. DM 2/11/2005

7.5 Schema indice dei gestori di posta certificata

8.5 Indice dei gestori di posta elettronica certificata

LL GG Iscrizione PEC

4 Raccomandazioni generali

7.7.2 Il Gestore

1. Esibisce documentazione che mostri che l'inizio dell'effettiva disponibilità del proprio file LDIF (Light-weight Directory Interchange Format) ha realmente avuto luogo alla data a suo tempo comunicata al CNIPA con l'anticipo, rispetto alla data di attivazione del servizio, previsto dal punto 4 delle LLGG Iscrizione PEC.
2. Esibisce documentazione (anche sotto forma di procedura informatica) che mostri che ha inserito i dati di ogni proprio ambiente operativo nel proprio file LDIF.
3. Esibisce procedura che mostri come il file LDIF pubblicato dal CNIPA sia scaricato tempestivamente almeno una volta ogni 24 ore, onde consentire ai propri sistemi di verificare celermente la validità dei certificati di firma degli altri gestori PEC in esso riportati.
4. Esibisce verbali, anche di audit, che attestino l'effettiva corretta esecuzione delle procedure di cui ai punti precedenti

7.7.3 Il Valutatore

1. Verifica l'esistenza della documentazione di cui al punto 1 del paragrafo 7.7.2 che mostri l'attivazione del proprio servizio e di eventuali nuovi certificati di firma ha realmente avuto luogo alla data a suo tempo comunicata al CNIPA con l'anticipo, rispetto alla data di attivazione del servizio, previsto dal punto 4 delle LLGG Iscrizione PEC
2. Verifica l'esistenza di documentazione attestante che il file LDIF del Gestore riporta i record di tutti i suoi ambienti operativi.
3. Verifica che la procedura che scarica il file IGPEC aggiornato dal CNIPA, conservandolo in un'area a cui accedano i sistemi di PEC del Gestore, mostri come il file LDIF pubblicato dal CNIPA sia scaricato tempestivamente almeno una volta ogni 24 ore.
4. Verifica l'esistenza dei verbali, anche di audit, di cui al punto 4 del paragrafo 7.7.2.

7.8 Cessazione di una coppia di chiavi del Gestore

Finalità: le chiavi di firma del Gestore non devono essere utilizzate oltre il momento del loro ritiro dall'impiego operativo, mentre i relativi certificati devono essere conservati sul file LDIF.

7.8.1 Normativa

La normativa non presenta disposizioni che riguardino esplicitamente come gestire le chiavi di firma del Gestore ritirate dall'attività o perché il loro certificato è scaduto, o perché esse sono compromesse direttamente o indirettamente (caso, quest'ultimo, che si verifica quando non si ritengano più affidabili l'algoritmo di firma utilizzato o la lunghezza delle chiavi stesse), o perché il Gestore cessa la propria attività, o per qualsiasi altro motivo. Tuttavia è necessario che al verificarsi di un evento che ne richieda il ritiro dall'impiego operativo tali chiavi siano rese definitivamente inutilizzabili così come le loro eventuali copie.

Nota: l'utilizzo abusivo di una chiave di firma afferente a un Gestore, anche scaduta, potrebbe originare falsi messaggi di PEC dei quali il Gestore stesso potrebbe essere chiamato a rispondere. In particolare, con una chiave utilizzata in modo abusivo potrebbe essere creato un falso messaggio di PEC che riporti un riferimento temporale arbitrario, tale da far ritenere che esso sia stato generato dal Gestore durante il periodo di validità del certificato corrispondente alla chiave utilizzata.

7.8.2 Il Gestore

1. Esibisce una procedura dettagliata che preveda che le chiavi e le eventuali rispettive copie siano rese definitivamente inutilizzabili oppure, ove ciò non sia possibile, siano resi definitivamente inutilizzabili i dispositivi che le contengono.

   Tale procedura dovrà essere documentata e basata sulle specifiche di sicurezza alle quali il dispositivo è stato riconosciuto conforme.

   Nota: Si veda paragrafo 9.2.6 "Secure disposal or re-use of equipment" dello ISO/IEC 27002: "Devices containing sensitive information should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function." (I dispositivi contenenti informazioni delicate dovrebbero essere distrutti fisicamente oppure le informazioni dovrebbero essere distrutte, cancellate o soprascritte usando tecniche che rendano l'informazione originale non recuperabile, piuttosto che utilizzare le funzioni standard di cancellazione o formattazione del dispositivo")

2. Qualora tale procedura sia stata già eseguita, ne esibisce i verbali di esecuzione e i verbali di audit che ne attestino il rispetto.

7.8.3 Il Valutatore

1. Verifica che la procedura di cui al punto 1 del paragrafo 7.8.2:
   a. corrisponda a quanto previsto nelle Security Policy del dispositivo,
   b. oppure sia sufficientemente dettagliata da spiegare chiaramente come essa ottenga l'obiettivo di rendere effettivamente inutilizzabili le chiavi oppure i dispositivi che le contengono.
2. Nel caso in cui la procedura di cui al punto 1 del paragrafo 7.8.2 sia stata eseguita, verifica l'esistenza dei relativi verbali
3. Nel caso in cui la procedura di cui al punto 1 del paragrafo 7.8.2 sia stata eseguita, verifica che i verbali di cui al punto 2 del medesimo paragrafo ne mostrino il rispetto.

7.9 Gestione del ciclo di vita dei dispositivi di firma del Gestore

Finalità: il Gestore garantisce la sicurezza dei dispositivi di firma per tutto il loro ciclo di vita

7.9.1 Normativa

La normativa non presenta disposizioni che riguardino esplicitamente come gestire i dispositivi di firma del Gestore. Tuttavia è necessario che essi siano gestiti in modo da garantirne la sicurezza.

Normalmente le Security Policy di questi dispositivi prevedono esplicitamente tali misure.

7.9.2 Il Gestore

1. Mostra procedure che prevedano per questi dispositivi:
    a. i controlli da effettuare alla consegna per accertare che essi non siano stati manomessi durante il trasporto;
    b. le misure da attuare per evitare che essi siano manomessi durante la loro conservazione anteriormente all'attivazione e i controlli relativi;
    c. le operazioni da eseguire, prima di metterli in esercizio, per accertarne il corretto funzionamento;
    d. la loro distruzione all'atto del loro ritiro dall'operatività, oppure la garanzia che il loro contenuto sia definitivamente cancellato in maniera che non ne sia possibile la ricostruzione;

       Nota: si vedano le Note ai paragrafi 7.8.1 e 7.8.2.
    e. l'aderenza a quant'altro descritto nel Piano della Sicurezza.

   Tali procedure dovranno essere basate sulle specifiche di sicurezza alle quali il dispositivo è stato riconosciuto conforme, ove applicabile.
2. Qualora tali procedure siano state già eseguite, ne esibisce i verbali di esecuzione.
3. Qualora tali procedure siano state già eseguite, esibisce i verbali di audit che mostrino che la loro effettuazione è stata condotta come previsto.

7.9.3 Il Valutatore

1. Verifica l'esistenza delle procedure di cui al punto 1 del paragrafo 7.9.2 e verifica che esse
    a. corrispondano a quanto previsto nelle Security Policy del dispositivo,
    b. oppure siano sufficientemente dettagliate da spiegare chiaramente come esse portino effettivamente al rispetto dei requisiti indicati al medesimo punto 1 del paragrafo 7.9.2.
2. Nel caso in cui le procedure di cui al punto 1 del paragrafo 7.9.2 siano state eseguite, verifica l'esistenza dei verbali di effettuazione.
3. Nel caso in cui le procedure di cui al punto 1 del paragrafo 7.9.2 siano state eseguite, verifica l'esistenza di verbali di audit che mostrino che la loro effettuazione è stata condotta come previsto.

7.10 Algoritmi

Finalità: gli algoritmi che il Gestore utilizza direttamente devono essere conformi alla normativa; esso inoltre deve indicare ai titolari di proprie caselle di PEC quali algoritmi e quali lunghezze minime di chiavi essi devono utilizzare nelle loro applicazioni di verifica della firma apposta sui messaggi di PEC.

7.10.1 Normativa

MO Certificati Server

11.3 Sicurezza del modulo crittografico

7.10.2 Il Gestore

1. Esibisce evidenza dell'utilizzo dell'algoritmo di crittografia asimmetrica RSA e che le chiavi di firma dei server siano generate con lunghezza massima pari a 1024 bit, come disposto dal punto 11.3 del "MO Certificati Server".

   Nota: Nella specifica pubblica ETSI TS 102 176-1, section 6.2.2.1, si evidenzia che "si può usare un esponente basso (per esempio = 3) qualora le esigenze di prestazione siano critiche, altrimenti si RACCOMANDA e $\geq 2^{16}+1$"[1]. Inoltre, sia in considerazione degli studi nell'ambito della criptoanalisi sia per analogia con le specifiche tecniche del tachigrafo[2], si RACCOMANDA di usare esponenti che rispettino anche $e \leq 2^{64}-1$.

2. Esibisce evidenza della informativa data ai titolari, come indicato al punto 2.d del § 8.3.2, di quali algoritmi e di quali lunghezze minime di chiavi devono utilizzare nelle loro applicazioni di verifica della firma apposta sui messaggi di PEC.

7.10.3 Il Valutatore

1. Verifica che dalla documentazione di cui al paragrafo 7.10.2 risulti che sono utilizzati algoritmi e chiavi di firma come dal punto 11.3 Sicurezza del modulo crittografico del "MO Certificati Server".
2. Verifica l'esistenza dell'evidenza dell'informativa ai titolari, di cui al punto 2.d del § 8.3.2, di quali algoritmi e di quali lunghezze minime di chiavi utilizzare.

Capitolo 8

Gestione caselle di PEC

8.1 Servizio di Registrazione dei titolari

Finalità: il Gestore verifica in modo affidabile l'identità dei titolari all'atto della registrazione e ne conserva i dati in modo sicuro.

8.1.1 Normativa

Dlgs 82/2005

Art. 2, comma 5

DPR 68/2005

Art. 1, Lettera l)

DM 2/11/2005

Art. 1, Lettera t)

[1] "A small public exponent (e.g. e = 3) MAY be used if performance is critical, otherwise e $\geq 2^{16}+1$ is RECOMMENDED."

[2] EUROPEAN COMMISSION JOINT RESEARCH CENTRE – Digital Tachograph System European Root Policy – http://dtc.jrc.it/docs/SPI0416.pdf

Articolo 21 - Organizzazione e funzioni del personale del certificatore, comma 1, lettera a)

Articolo 22 - Requisiti di competenza ed esperienza del personale

CNIPA/CR/49

1. Modalità di presentazione delle domande., lettera p)

8.1.2 Il Gestore

1. Esibisce documentazione che dimostri che al responsabile della registrazione dei titolari, di cui verifica la corrispondenza con quanto dichiarato al CNIPA, sia stato erogato adeguato addestramento, a fronte degli aggiornamenti tecnici e organizzativi di cui all'articolo 22 del DM 2/11/2005, al fine di mantenerne le caratteristiche di esperienza.
2. Esibisce procedure operative e relativa documentazione (quali verbali, anche di audit, dichiarazioni sottoscritte dai richiedenti, ecc.) che mostrino che in fase di registrazione il Gestore, o chi da esso delegato, opera in conformità con quanto indicato nel Manuale operativo relativamente a quanto afferisce l'identificazione del richiedente.
3. Esibisce procedure e verbali anche di audit che mostrino che esso conserva le informazioni e i dati relativi agli accordi di servizio stipulati con i clienti secondo la vigente normativa..
4. Esibisce procedure e verbali, anche di audit, che mostrino che esso informa tempestivamente i richiedenti sulle caratteristiche del servizio reso, sui reciproci obblighi e su quant'altro riguarda la fornitura del servizio di PEC.

   Nota: ulteriori approfondimenti su questo argomento si possono trovare al paragrafo 8.3.2.
5. Qualora si avvalga di servizi di registrazione effettuati da terze parti, esibisce gli accordi che impegnano queste ultime a seguire procedure analoghe a quelle indicate ai punti precedenti.
6. Esibisce verbali di audit effettuati presso terze parti eventualmente incaricate di eseguire il servizio di registrazione.
7. Su richiesta del valutatore organizza specifiche ispezioni presso terze parti eventualmente incaricate di eseguire il servizio di registrazione, alle quali può partecipare anche il valutatore.

8.1.3 Il Valutatore

1. Verifica che dalla documentazione esibita risulti che il Responsabile della registrazione dei titolari corrisponda con quanto dichiarato dal Gestore al CNIPA e che ad esso sia stato erogato adeguato addestramento, a fronte degli aggiornamenti tecnici e organizzativi di cui all'articolo 22 del DM 2/11/2005, al fine di mantenerne le caratteristiche di esperienza. (Vedere punto 2 del paragrafo 12.6.3).
2. Verifica l'esistenza delle procedure e della documentazione di cui al paragrafo 8.1.2, sull'identificazione dei richiedenti le caselle di PEC, e che in esse sia prevista l'attuazione delle misure ivi indicate.
3. Nel caso in cui le procedure di cui al paragrafo 8.1.2 siano già state eseguite, verifica che i verbali anche di audit e gli analoghi documenti di cui allo stesso paragrafo ne attestino il rispetto e, ove invece sia stato riscontrato il mancato rispetto di tali procedure, che siano state intraprese dal Gestore le opportune azioni correttive
4. Verifica, ove del caso, l'esistenza degli accordi previsti al punto 5 del paragrafo 8.1.2 .
5. Verifica, ove del caso, l'esistenza di verbali di audit effettuati presso terze parti eventualmente incaricate di eseguire il servizio di registrazione.
6. Può richiedere al Gestore di organizzare specifiche ispezioni presso terze parti eventualmente incaricate di eseguire il servizio di registrazione, alle quali può partecipare anche il valutatore stesso, onde verificare il rispetto di quanto previsto al paragrafo 8.1.2.

8.2 Assegnazione caselle di PEC

Finalità: il Gestore assegna le caselle di PEC in base ad accordi sottoscritti con le persone fisiche o giuridiche, i quali possono prevedere anche la definizione di domini specifici, conservando i dati relativi in ottemperanza al Dlgs 196/2003.

8.2.1 Normativa

Dlgs 82/2005

Art. 54, comma 1, lettera b)

DM 2/11/2005

Art. 1 Oggetto e definizioni, lettere s), t), u), z)

CNIPA/CR/51

1.2 (Superamento test di interoperabilità)

FAQ - Circolare 51 Vigilanza PEC 1.1

Quali sono le modalità di commercializzazione dei servizi di PEC?

8.2.2 Il Gestore

1. Esibisce gli accordi con clienti e, ove del caso, con canali commerciali in base ai quali è eventualmente prevista anche la definizione di diversi domini di PEC e la loro assegnazione ai richiedenti.
2. Esibisce procedure e verbali di audit, inclusi verbali di audit effettuati presso canali commerciali, che mostrino il rispetto di quanto dichiarato nel Manuale Operativo riguardo alle modalità di assegnazione delle caselle e dei domini di PEC.

8.2.3 Il Valutatore

1. Verifica l'esistenza della documentazione di cui al paragrafo 8.2.2:
    a. Accordi con organizzazioni clienti
    b. Accordi con canali commerciali
    c. Procedure sul rispetto delle modalità di assegnazioni di caselle e domini di PEC e i relativi verbali di audit
    d. Verbali di ispezioni presso i canali commerciali.

8.3 Termini e condizioni

Finalità: il Gestore fornisce una tempestiva, duratura e comprensibile informazione ai clienti sui termini e sulle condizioni contrattuali.

8.3.1 Normativa

DM 2/11/2005

Articolo 18 - Indice ed elenco pubblico dei gestori di posta elettronica certificata, comma 3. lettera f)

Articolo 23 - Manuale operativo, commi 1, 2, 3 lettera f)

All. DM 2/11/2005

9.2 Requisiti tecnico funzionali di un client di un sistema di PEC

CNIPA/CR/49

2.1, lettere dalla g) in poi.

CNIPA/CR/51

7.2

LL GG Iscrizione PEC

4.3

8.3.2 Il Gestore

1. Esibisce procedure operative e relativi verbali anche di audit che mostrino che esso fornisce a coloro che richiedono il suo servizio di PEC il proprio Manuale Operativo, onde informarli con tempestività, chiaramente e compiutamente sui termini e sulle condizioni relative a tale servizio. Alternativamente il Gestore può invitare formalmente i richiedenti ad accedere al proprio sito, di cui fornisce l'indirizzo internet, ove tale Manuale Operativo sia pubblicato. Laddove le politiche relative alla gestione dei messaggi di posta elettronica non certificata in arrivo e sull'invio di messaggi di PEC a indirizzi di posta elettronica non certificata non siano indicate nel Manuale Operativo, il Gestore fornisce adeguata informazione ai propri titolari.
2. Esibisce procedure operative e relativi verbali anche di audit che mostrino che esso fornisce su mezzi di comunicazione durevoli ai soggetti che richiedono la fornitura del servizio di PEC le informazioni relative ai loro obblighi; tra cui quello che il Titolare:
    a. informi le persone abilitate a utilizzare le caselle di posta sulle tematiche di sicurezza concernenti il loro uso: custodia degli strumenti di accesso alle caselle onde evitarne un uso non autorizzato da parte altrui, eventuali norme deontologiche, ecc.;
    b. adotti misure atte a evitare l'inserimento nei messaggi di codici eseguibili dannosi (ad es. virus).
    c. rispetti eventuali ulteriori obblighi indicati nello specifico accordo tra l'organizzazione di appartenenza del Terzo interessato e il Gestore;
    d. si avvalga nelle applicazioni di verifica della firma apposta sui messaggi di PEC di algoritmi e di lunghezze minime di chiavi come a lui indicato dal Gestore.
3. Esibisce procedure operative e relativi verbali anche di audit che mostrino che esso richiede ai titolari di prendere conoscenza del Manuale Operativo.

    Nota: il Manuale Operativo comprende anche le informazioni relative agli obblighi del Gestore stesso e le fornisce ai soggetti che richiedono la fornitura del servizio di PEC.

8.3.3 Il Valutatore

1. Verifica l'esistenza delle procedure e dei relativi verbali di cui al precedente paragrafo 8.3.2 riguardanti la informazione fornita ai Titolari riguardo a:
    a. termini e condizioni contrattuali, ivi inclusa la gestione di messaggi non di PEC ove del caso;
    b. obblighi dei Titolari;
    c. obblighi del Gestore stesso.

8.4 Gestione delle disattivazioni di caselle o domini

Finalità: Elaborare tempestivamente, previa adeguata autenticazione del richiedente, le richieste relative alle disattivazioni di caselle e/o domini di PEC.

8.4.1 Normativa

La normativa vigente non dà disposizioni al riguardo, ma si ritiene pratica corretta che, su richiesta di persona fisica o giuridica abilitata, le caselle e i domini di PEC possano essere disattivate come indicato nel Manuale Operativo o convenuto in apposito accordo.

8.4.2 Il Gestore

1. Esibisce documentazione, ivi inclusi log di sistema, procedure operative e verbali di audit che mostrino che, ove previsto nel Manuale Operativo:
    a. le richieste di disattivazione delle caselle di PEC vengono elaborate, entro l'orario di servizio indicato nel Manuale operativo, non appena ricevute;
    b. prima di elaborare una richiesta di disattivazione delle caselle di PEC viene verificato, secondo quanto indicato nel Manuale operativo, che essa provenga effettivamente da una persona autorizzata dal titolare o da un'autorità competente;
    c. prevedano la comunicazione al titolare di una casella di PEC di avvenute disattivazioni;
    d. le richieste di disattivazione delle caselle di PEC siano conservate per il periodo previsto nel Manuale Operativo o in appositi accordi.
2. Su richiesta del Valutatore effettua la disattivazione delle caselle assegnate al CNIPA a fronte di quanto indicato al punto 2 del paragrafo 8.2.2.

Nota 1: queste caselle di PEC devono essere utilizzate esclusivamente ai fini ispettivi e sono disattivate d'autorità dal Gestore, qualora non lo siano state prima, dopo la fine dell'ispezione.

8.4.3 Il Valutatore

1. Verifica l'esistenza dei documenti, delle procedure e dei verbali di audit di cui al paragrafo 8.4.2, compreso il contenuto dei log dei sistemi. In particolare, ma non esclusivamente, verifica l'esistenza di procedure che prevedano:
    a. l'elaborazione delle richieste di disattivazione delle caselle di PEC, entro l'orario di servizio indicato nel Manuale operativo, non appena sono ricevute;
    b. l'effettiva autenticazione del richiedente di una disattivazione delle caselle di PEC ove previsto dal Manuale Operativo;
    c. le comunicazioni al titolare di una casella di PEC relative ad avvenute disattivazioni;
    d. la conservazione delle richieste di disattivazione delle caselle di PEC per il periodo previsto nel Manuale Operativo o in specifici accordi.
2. Può utilizzare le caselle di PEC assegnate al CNIPA dal Gestore per effettuare le verifiche previste, ivi inclusa la disattivazione delle medesime.
3. Verifica esistenza e congruità dei verbali di cui al paragrafo 8.4.2.

Capitolo 9

Gestione del processo di PEC

9.1 Log di PEC

Finalità: assicurare la creazione con le modalità previste dalla normativa, del log di PEC la sua estrazione, marcatura temporale e inoltro alla conservazione sostitutiva. Assicurarne l'esibizione a richiedenti autorizzati del contenuto del Log di PEC.

Nota: per quanto riguarda la conservazione del Log di PEC vedere il capitolo 12.14.

9.1.1 Normativa

Dlgs 82/2005

Art. 45 Valore giuridico della trasmissione

DPR 68/2005

Articolo 6

Articolo 10, comma 2

Articolo 11, commi 2 e 3.

DM 2/11/2005

Articolo 10 - Conservazione dei log dei messaggi

Articolo 21 - Organizzazione e funzioni del personale del certificatore, comma 1, lettera e) e comma 2

Articolo 22 - Requisiti di competenza ed esperienza del personale

All. DM 2/11/2005

6.2 Log

CNIPA/CR/49

1. Modalità di presentazione delle domande, lettere p), q).

2.1 Manuale operativo, lettera h)

2.2 Piano per la sicurezza, lettere a), l), m).

9.1.2 Il Gestore

1. Esibisce documentazione che dimostri che al responsabile della sicurezza del Log, di cui verifica la corrispondenza con quanto dichiarato al CNIPA, sia stato erogato adeguato addestramento, a fronte degli aggiornamenti tecnici e organizzativi di cui all'articolo 22 del DM 2/11/2005, al fine di mantenerne le caratteristiche di esperienza.
2. Esibisce procedure e documentazione relative a:
    a. contenuto delle registrazioni di Log;
    b. estrazione del Log registrato durante l'intervallo temporale, come indicato nel Piano per la sicurezza, orientativamente al termine dell'intervallo stesso;
    c. apposizione di una marca temporale al Log estratto;

   d. inoltro del Log estratto e marcato temporalmente al soggetto incaricato della conservazione sostitutiva.

3. Esibisce procedure e documentazione relative alle modalità di reperimento e di presentazione delle informazioni presenti nei Log dei messaggi a richiesta dei titolari o di altre persone autorizzate (addetti del Gestore, autorità, ecc.).

   Nota 1: Tali procedure devono gestire ambedue i casi in cui il Log cercato:

      a. sia ancora presente nel sistema di PEC,

      b. sia presente solo nel sistema di conservazione sostitutiva.

4. Su richiesta del Valutatore esibisce i Log da lui richiesti adottando le procedure di cui al punto 3.
5. Su richiesta del Valutatore consente al medesimo di assistere all'estrazione del Log il cui intervallo di conservazione cada durante il periodo dell'ispezione.
6. Esibisce verbali di esecuzione delle procedure di cui ai punti 2 e 3 a fronte di richieste di esibizione dei Log, ivi incluso quello relativo alla esibizione di cui al punto 4.
7. Esibisce verbali di audit che attestino la correttezza della documentazione e dei verbali di cui ai punti 2 e 3 e al punto 6.

9.1.3 Il Valutatore

1. Verifica che dalla documentazione esibita risulti che il Responsabile della sicurezza del Log dei messaggi corrisponda con quanto dichiarato dal Gestore al CNIPA e che ad esso sia stato erogato adeguato addestramento, a fronte degli aggiornamenti tecnici e organizzativi di cui all'articolo 22 del DM 2/11/2005, al fine di mantenerne le caratteristiche di esperienza. (Vedere punto 2 del paragrafo 12.6.3).
2. Verifica l'esistenza dei documenti e delle procedure di cui al paragrafo 9.1.2.
3. Verifica l'esistenza e la congruità dei verbali di cui ai punti 6 e 7 del paragrafo 9.1.2.
4. Richiede l'esibizione di Log di PEC relativi a transazioni effettuate negli ultimi trenta mesi:

   a. da altri utenti;

   b. dalle caselle assegnate al CNIPA dal Gestore come previsto al punto 1.2 della CNIPA/CR/51, anche utilizzate dal valutatore stesso come indicato al punto 4 del paragrafo 9.5.3.3.

5. Per i Log di cui al precedente punto 4 verifica che essi contengano i dati indicati al punto 6.2 dell'All. al DM 2/11/2005.
6. Può assistere all'estrazione del Log il cui intervallo di conservazione cada durante il periodo dell'ispezione, per verificare la rispondenza della procedura eseguita con quella prevista.

9.2 Autenticazione dei titolari

Finalità: il Gestore assicura che i titolari possano avere il controllo esclusivo della casella di PEC loro assegnata, ove lo vogliano.

9.2.1 Normativa

All. DM 2/11/2005

8.2 Autenticazione

CNIPA/CR/49

21 Manuale operativo, lettera j)

9.2.2 Il Gestore

1. Esibisce procedure e documentazione che mostrino che esso associa a ogni casella di PEC almeno un codice identificativo di titolare abbinato a un sistema di autenticazione conforme con quanto indicato al punto 8.2 dell'All. DM 2/11/2005. Questi codici identificativi, insieme con le misure di protezione del colloquio tra titolare e Gestore di cui al paragrafo 9.3, devono poter consentire al titolare di assicurare il controllo della casella di PEC alle persone autorizzate ad accedervi.
2. Esibisce documentazione e procedure che mostrino che, ove previsto dal Manuale operativo o concordato con il cliente, il titolare può avvalersi di strumenti di autenticazione forte, quali la Carta d'Identità Elettronica, la Carta Nazionale dei Servizi o altri sistemi.
3. Esibisce verbali di audit che attestino che alle caselle di PEC sia possibile accedere soltanto mediante identificazione del titolare e, ove del caso, l'effettiva possibilità per i titolari a cui si applichi il punto 2 di avvalersi dei sistemi di autenticazione forte previsti nel Manuale operativo o in specifici accordi.

9.2.3 Il Valutatore

1. Verifica l'esistenza di procedure, documentazione e verbali di audit che mostrino che alle caselle di PEC si può accedere solo dietro identificazione conforme con quanto indicato al punto 8.2 dell'All. DM 2/11/2005, anche tramite l'utilizzo di protocolli sicuri quali quelli indicati al paragrafo 9.3, potendo così consentire al titolare di assicurare il controllo esclusivo della casella di PEC alle persone autorizzate ad accedervi.
2. Verifica l'esistenza di procedure e accordi con i clienti che mostrino che, ove previsto nel Manuale Operativo o concordato con il cliente, il titolare può avvalersi di strumenti di autenticazione forte.
3. Verifica l'esistenza di verbali di audit che attestino che alle caselle di PEC sia possibile accedere soltanto mediante identificazione del titolare e, ove del caso, l'effettiva possibilità per i titolari di avvalersi dei sistemi di autenticazione forte previsti nel Manuale operativo o in specifici accordi.

9.3 Colloquio sicuro del Gestore con il titolare e con gli altri Gestori

Finalità: assicurare che il colloquio del Gestore con il titolare e con gli altri Gestori sia riservato e che né i dati di autenticazione né altri dati scambiati tra queste due parti possano essere intercettati o alterati.

9.3.1 Normativa

DM 2/11/2005

Articolo 21 - Organizzazione e funzioni del personale del certificatore, comma 1, lettera d)

Articolo 23 - Manuale operativo, comma 3, lettera f)

All. DM 2/11/2005

8.3 Colloquio sicuro

CNIPA/CR/49

2.2 Piano per la sicurezza, lettera o).

9.3.2 Il Gestore

1. Esibisce documentazione che dimostri che al Responsabile della sicurezza, di cui verifica la corrispondenza con quanto dichiarato al CNIPA, sia stato erogato adeguato addestramento, a fronte degli aggiornamenti tecnici e organizzativi di cui all'articolo 22 del DM 2/11/2005, al fine di mantenerne le caratteristiche di esperienza.

2. Esibisce documentazione e procedure che mostrino la protezione della riservatezza del colloquio del Gestore con i titolare e con gli altri gestori di PEC con l'effettivo utilizzo per la connessione di protocolli sicuri, quali ad esempio quelli indicati nell'All. al DM 2/11/2005, al punto 8.3.

   Nota: la CA CNIPA non fornisce certificati per realizzare le connessioni protette tra Gestori, per cui ogni Gestore è responsabile di acquisirli autonomamente.

3. Esibisce verbali di audit che mostrino che le misure di sicurezza predisposte per assicurare la riservatezza dei messaggi di PEC, come indicate nel Manuale operativo e nel Piano per la sicurezza, sono realmente attuate e che raggiungono lo scopo di proteggere la riservatezza dei messaggi nel il colloquio del Gestore con i titolari e con gli altri Gestori.

9.3.3 Il Valutatore

1. Verifica che dalla documentazione esibita risulti che il Responsabile della sicurezza corrisponda con quanto dichiarato dal Gestore al CNIPA e che ad esso sia stato erogato adeguato addestramento, a fronte degli aggiornamenti tecnici e organizzativi di cui all'articolo 22 del DM 2/11/2005, al fine di mantenerne le caratteristiche di esperienza. (Vedere punto 2 del paragrafo 12.6.3).
2. Verifica l'esistenza di documentazione e procedure che mostrino che è assicurata la riservatezza del colloquio del Gestore con il titolare e con gli altri Gestori, essendo realizzate con protocolli affidabili, quali quelli indicati nell'All. al DM 2/11/2005 al punto 8.3.
3. Verifica l'esistenza dei verbali di audit attestanti la riservatezza della connessione tra Gestore e titolare della casella di cui al punto 3 del paragrafo 9.3.2.

9.4 Protezione della segretezza della corrispondenza

Finalità: assicurare la riservatezza dei messaggi di PEC durante la loro permanenza sul sistema del Gestore.

9.4.1 Normativa

D.lgs. n. 82/2005

Art. 49 Segretezza della corrispondenza trasmessa per via telematica

Art. 51 Sicurezza dei dati

DM 2/11/2005

Articolo 21 - Organizzazione e funzioni del personale del certificatore, comma 1, lettera d)

Articolo 23 - Manuale operativo, comma 3, lettera g)

All. DM 2/11/2005

8.3 Colloquio sicuro

CNIPA/CR/49

1. Modalità di presentazione delle domande, lettera p).

2.1 Manuale operativo, lettera e)

2.2 Piano per la sicurezza, lettera o).

9.4.2 Il Gestore

1. Esibisce documentazione, inclusi i verbali di audit, che dimostri che al Responsabile della sicurezza, di cui verifica la corrispondenza con quanto dichiarato al CNIPA, sia stato erogato adeguato addestramento, a fronte degli aggiornamenti tecnici e organizzativi di cui all'articolo 22 del DM 2/11/2005, al fine di mantenerne le caratteristiche di esperienza.

2. Esibisce documentazione, inclusi i verbali di audit, e procedure che mostrino che i messaggi di PEC durante il periodo di permanenza nel sistema del Gestore sono protetti da qualsiasi tipo di accesso non autorizzato al loro contenuto.
3. Vedere punto 3 del § 9.3.2.

9.4.3 Il Valutatore

1. Vedere il punto 1 del paragrafo 9.3.3 per quanto riguarda le verifiche riguardanti il Responsabile della sicurezza.
2. Verifica l'esistenza della documentazione, inclusi i verbali di audit, e delle procedure di cui al punto 1 del paragrafo 9.4.2 che assicurino la riservatezza dei messaggi di PEC sul sistema.
3. Vedere punto 3 del § 9.3.3.

9.5 Gestore mittente – Mansioni specifiche

9.5.1 Determinazione del Message Identifier

Finalità: il message identifier dei messaggi di PEC deve rispondere al formato previsto al punto 6.3 dell'All. al DM 2/11/2005 onde garantirne l'univocità nel complesso dell'infrastruttura di posta certificata e quindi consentire una corretta tracciatura dei messaggi e delle relative ricevute.

9.5.1.1 Normativa

All. DM 2/11/2005

6.3 Punto di accesso

CNIPA/CR/51

1.2 (Superamento test di interoperabilità)

9.5.1.2 Il Gestore

1. Esibisce documentazione, procedure operative e verbali di audit che mostrino che le modalità con cui viene ottenuta la composizione del message identifier dei messaggi di PEC assicurano l'univocità dell'identificativo e la correttezza formale come previsto al punto 6.3 dell'All. al DM 2/11/2005.

9.5.1.3 Il Valutatore

1. Verifica l'esistenza della documentazione, delle procedure e dei verbali di audit di cui al paragrafo 9.5.1.2.
2. PUO' inviare da una casella di PEC, assegnata al CNIPA dal Gestore come previsto al punto 1.2 della CNIPA/CR/51, messaggi a utenze PEC e non PEC. Nel caso di destinatari utenti PEC PUO' utilizzare come destinatario la medesima casella di PEC utilizzata per inviare i messaggi, o altra assegnata al CNIPA.

9.5.2 Verifiche sui messaggi in spedizione

Finalità: assicurare la correttezza formale dei messaggi immessi nel sistema di PEC e impedire l'introduzione di virus o altro codice nocivo.

9.5.2.1 Normativa

DPR 68/2005

Articolo 12 - Virus informatici, comma 1

All. DM 2/11/2005

6.3 Punto di accesso

6.3.1 Controlli formali sui messaggi in ingresso

CNIPA/CR/51

1.2 (Superamento test di interoperabilità)

9.5.2.2 Il Gestore

1. Esibisce documentazione e procedure che mostrino che per ogni messaggio inviato dai titolari il Gestore stesso verifica che:
   a. nel messaggio siano assenti virus; a tale proposito esso cura il regolare funzionamento dei programmi antivirus, e in generale contro i vari tipi di malware, a tale scopo installati e che essi siano costantemente aggiornati;
   b. nel corpo del messaggio esista un campo "From" riportante un indirizzo email conforme alle specifiche di cui al § 3.4.1 dello RFC 2822;
   c. nel corpo del messaggio esista un campo "To" riportante uno o più indirizzi email conformi alle specifiche di cui al § 3.4.1 dello RFC 2822;
   d. l'indirizzo del mittente del messaggio specificato nei dati di instradamento (reverse path) coincida con quanto specificato nel campo "From" del messaggio;
   e. gli indirizzi dei destinatari del messaggio specificati nei dati di instradamento (forward path) coincidano con quelli presenti nei campi "To" o "Cc" del messaggio;
   f. nel campo "Ccn" del messaggio non siano presenti indirizzi di destinatari.

   Qualora il Gestore preveda di inoltrare messaggi anche a indirizzi di posta elettronica non certificata effettua i controlli di cui sopra anche per essi. In caso contrario si veda la Nota al § 9.5.3.2; lettera b.
2. Esibisce verbali, anche di audit, che mostrino l'effettiva esecuzione delle verifiche e delle azioni di cui al punto precedente ivi incluso il regolare aggiornamento dei programmi di tipo antivirus.
3. Per le azioni svolte dal Gestore a fronte di destinatari i cui domini di posta appartengano o non al circuito PEC si veda il paragrafo 9.5.3.2.

9.5.2.3 Il Valutatore

1. Verifica l'esistenza della documentazione e dei verbali, anche di audit, relativi alle verifiche sui messaggi inviati dai titolari, di cui al paragrafo 9.5.2.2.
2. Allo scopo di verificare il comportamento del sistema di PEC del Gestore, il Valutatore PUO' inviare da una casella di PEC assegnata al CNIPA messaggi:
   a. contenenti virus; in questo caso la casella del destinatario DEVE essere o la medesima utilizzata per l'invio o altra casella di PEC assegnata al CNIPA; ne deve conseguire la creazione di un "Avviso di non accettazione per virus informatico" e il Valutatore deve verificare che il messaggio sia gestito come indicato al paragrafo 9.5.2.2;
   b. i cui campi mittente e destinatari non siano conformi con quanto indicato alle lettere da "b" a "e" del punto 1 del paragrafo 9.5.2.2; ne deve conseguire la creazione di un "Avviso di non accettazione per eccezioni formali" e il messaggio non deve essere inoltrato;
   c. in cui siano indicati anche destinatari nel campo "Ccn" o equivalenti; ne deve conseguire la creazione di un "Avviso di non accettazione per eccezioni formali" e il messaggio non deve essere inoltrato;
   d. in cui siano indicati come destinatari anche utenti non di PEC; anche tali destinatari devono ricevere ugualmente la Busta di trasporto contenente il messaggio inviato.
3. L'esame da parte del Valutatore di quanto prodotto dal Gestore a fronte dei messaggi errati di cui al punto precedente è indicato al paragrafo 9.5.3.3.

4. Sulle azioni svolte dal Valutatore per verificare il comportamento del Gestore nel caso di destinatari i cui domini di posta appartengano o non al circuito PEC si veda il paragrafo 9.5.3.3.

9.5.3 Creazione Ricevute, Avvisi, Buste di trasporto

Finalità: assicurare la tracciabilità del flusso di messaggi di posta elettronica certificata nel rispetto dei requisiti di servizio previsti, e cioè:

1. assicurando l'invio di un messaggio di PEC almeno a 50 destinatari, entro una dimensione massima di 30 megabytes ottenuta moltiplicando il numero dei destinatari per la dimensione del messaggio,
2. dando al mittente una corretta comunicazione su accettazione o non accettazione del messaggio spedito e sul tipo di destinatario riconosciuto (utente di PEC o non di PEC),
3. predisponendo correttamente la busta di trasporto,
4. dando corretta comunicazione al mittente di una eventuale mancata consegna per superamento dei tempi massimi previsti nel caso in cui il Gestore del destinatario non restituisca entro i tempi previsti una Ricevuta di avvenuta consegna o un Avviso di mancata consegna.

9.5.3.1 Normativa

Dlgs 82/2005

Art. 45 Valore giuridico della trasmissione, commi 2 e 3

Art. 48 Posta elettronica certificata

DPR 68/2005

Articolo 4, comma 6

Articolo 6 - Ricevuta di accettazione e di avvenuta consegna, comma 1

Articolo 11 - Sicurezza della trasmissione, commi 1 e 4

DM 2/11/2005

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

Articolo 12 - Livelli di servizio, commi 1 e 2,

Articolo 13 - Avvisi di mancata consegna

Articolo 14 - Norme di garanzia sulla natura della posta elettronica ricevuta, comma 2

All. DM 2/11/2005

6.1 Formato dei messaggi generati dal sistema

6.3 Punto di accesso

6.3.2 Avviso di non accettazione per eccezioni formali

6.3.3 Ricevuta di accettazione

6.3.4 Busta di trasporto

6.3.5 Avviso di mancata consegna per superamento dei tempi massimi previsti

6.4.3 Avvisi relativi alla rilevazione di virus informatici

6.4.3.1 Avviso di non accettazione per virus informatico

6.4.3.3 Avviso di mancata consegna per virus informatico

6.5.2.1 Ricevuta completa di avvenuta consegna

6.5.2.2 Ricevuta di avvenuta consegna breve

6.5.2.3 Ricevuta sintetica di avvenuta consegna

7.3 Specifiche degli allegati

7.3.1 Corpo del messaggio

7.3.2 Messaggio originale

7.3.3 Dati di certificazione

7.4 Schema dei dati di certificazione

8.4 Virus

CNIPA/CR/51

1.2 (Superamento test di interoperabilità)

7. (Sospensione del servizio.)

7.1 (Autosospensione del servizio)

7.2 (Sospensione del servizio disposta dal CNIPA)

7.4 (Autosospensione producendo «avviso di non accettazione per eccezioni formali» e non producendo la «ricevuta di presa in carico»)

7.5 (Sospensione del servizio disposta dal CNIPA con le medesime modalità previste per l'autosospensione)

9.5.3.2 Il Gestore

1. Esibisce documentazione e procedure che mostrino che esso:
    a. consenta a un mittente di optare per uno dei tre tipi di ricevute di avvenuta consegna: completa, breve, sintetica, come previsto dal Manuale operativo.
    b. genera le ricevute di accettazione e gli avvisi di non accettazione a fronte degli esiti delle verifiche di cui al paragrafo 9.5.2.2;

        Nota: gli avvisi di non accettazione sono generati anche nel caso in cui i messaggi siano inviati a indirizzi di posta elettronica non certificata e il Gestore non ne preveda la gestione;
    c. opera nel rispetto dei requisiti minimi di servizio:
        i. definiti all'art. 12, commi 1 e 2 del DM 2/11/2005, per quanto riguarda il numero di destinatari e il complessivo volume di messaggi trasmessi,
        ii. o concordati con i clienti;
    d. genera le buste di trasporto in conformità con il punto 6.3.4 "Busta di trasporto" dell'All. al DM 2/11/2005, ivi inclusa la possibilità di optare per uno dei tre tipi di ricevuta: completa, breve, sintetica, con le modalità indicate nel Manuale operativo;
    e. genera gli avvisi di mancata consegna per superamento dei tempi massimi previsti a fronte di mancata ricezione di ricevuta di presa in carico da parte del Gestore destinatario entro i tempi previsti dalla norma;
    f. all'arrivo di un avviso di rilevazione di virus informatico proveniente dal Gestore destinatario, emette un avviso di mancata consegna da restituire al mittente.
2. Laddove il Gestore abbia già ricevuto un Avviso di rilevazione di virus informatico proveniente dal Gestore destinatario, esibisce documentazione che mostri che esso ha emesso nei confronti del mittente un Avviso di mancata consegna per virus (si veda anche il paragrafo 9.7.2).
3. Laddove le condizioni di mancata consegna per superamento dei tempi massimi previsti si siano già verificate esibisce documentazione attestante che, a fronte della mancata ricezione della Ricevuta di presa in carico o di avvenuta consegna del messaggio inviato, ha rilasciato ai titolari il previsto "Avviso di mancata consegna per superamento dei tempi massimi previsti".
4. Laddove le condizioni che prevedono la sospensione del servizio, di cui ai punti 7.1 e 7.2 della CNIPA/CR/51, si siano già verificate esibisce documentazione attestante che, a seguito dell'esecuzione dell'autosospensione (punto 7.1) o della sospensione disposta dal CNIPA (punto 7.2), sono stati effettivamente rilasciati ai titolari "Avvisi di non accettazione per eccezioni formali".

5. Esibisce documentazione e procedure che mostrino che laddove le verifiche di cui al paragrafo 9.5.2.2 diano esito favorevole esso produce correttamente buste di trasporto conformi con quanto previsto al punto 6.3.4 dell'All. DM 2/11/2005.
6. Esibisce verbali di audit che attestino la corretta esecuzione di quanto sopra.

Nota: la documentazione di cui ai punti dall'1 al 5 può essere costituita dal contenuto del log.

9.5.3.3 Il Valutatore

1. Verifica l'esistenza di procedure, documentazione e verbali di audit, come al paragrafo 9.5.3.2, da cui risulti la corretta produzione di avvisi, ricevute e buste di trasporto al verificarsi dei casi relativi. Verifica che sia possibile per un mittente optare per uno dei tre tipi di ricevute di avvenuta consegna: completa, breve, sintetica, come previsto dal Manuale operativo.
2. Per verificare la correttezza del comportamento del Gestore qualora, in base alle informazioni in possesso del CNIPA, si siano già verificati i casi di cui ai punti 2, 3 e 4 del paragrafo 9.5.3.2, il Valutatore PUO' chiedere al personale del Gestore che gli siano esibiti i file di log, anche quelli per i quali sia già stata effettuata la conservazione sostitutiva.
3. Esamina quanto prodotto dal Gestore a fronte dei messaggi che il Valutatore stesso ha inviato, come indicato al punto 2 del paragrafo 9.5.2.3 onde verificare la corretta preparazione di avvisi, ricevute, buste di trasporto.
4. PUO'inviare messaggi di PEC a uno o più destinatari con i quali abbia preso preventivi accordi in tal senso, oppure alle caselle di PEC messe a disposizione del CNIPA come da punto 1.2 della CNIPA/CR/51, per verificare se:
    a. il Gestore opera nel rispetto dei requisiti minimi di servizio di cui alla lettera 1.c del paragrafo 9.5.3.2 e se dà al mittente la possibilità di scegliere tra i tre tipi diversi di ricevuta di avvenuta consegna, come previsto dal Manuale operativo;
    b. il formato dei messaggi (ricevute, avvisi e buste) è conforme con quanto previsto al punto 6.1 dell'All. al DM 2/11/2005.

Nota: ai fini delle verifiche di cui ai punti 3 e 4 può avvalersi del log di PEC.

9.5.4 Gestione di Avvisi, Ricevute provenienti da altri gestori

Finalità: assicurare la tracciabilità dei messaggi di PEC e fornire ai mittenti documentazione con validità legale dell'avvenuta consegna o mancata consegna di messaggi di PEC, evitando che la ricezione di Avvisi e Ricevute generi ulteriori comunicazioni.

9.5.4.1 Normativa

All. DM 2/11/2005

6.4 Punto di ricezione

9.5.4.2 Il Gestore

1. Esibisce documentazione, procedure e verbali di audit che mostrino che se ricevute o avvisi di PEC, con l'esclusione delle ricevute di presa in carico:
    a. sono corretti ed integri, li inoltra al loro destinatario;
    b. non rispondono ai requisiti previsti, ma provengono da un Gestore di posta certificata e superano le verifiche di esistenza, provenienza e validità della firma, li imbusta in una busta di anomalia che inoltra al loro destinatario.
2. Poiché i destinatari di questi tipi di messaggio, avvisi e ricevute, sono gli originali mittenti di messaggi a cui tali avvisi e ricevute fanno riferimento, a fronte della loro ricezione non deve produrre né ricevute né avvisi. Il Gestore esibisce evidenza che a ciò sia ottemperato.

Nota 1: La documentazione di cui sopra può essere costituita o integrata dal log di PEC.

9.5.4.3 Il Valutatore

1. Verifica l'esistenza di documentazione, procedure e verbali di audit, di cui al paragrafo 9.5.4.2, relativamente alla gestione di avvisi e ricevute indirizzate a un titolare di casella di PEC che abbia precedentemente inviato un messaggio di PEC ad altro titolare di casella di PEC.

   Nota: questa documentazione può essere costituita o integrata dal log di PEC.

2. PUO' inviare messaggi dalle caselle di PEC fattesi attivare come da punto **Errore. L'origine riferimento non è stata trovata.** del paragrafo 8.2.2, o a quelle messe a disposizione del CNIPA come da punto. 1.2 della CNIPA/CR/51, per verificare la correttezza della gestione di cui al punto 1 precedente.

9.6 Gestore destinatario – Mansioni specifiche

9.6.1 Verifiche sui messaggi in entrata

Finalità: prevenire l'entrata o la permanenza nel circuito PEC di messaggi contenenti virus; verificare la conformità alle norme di interoperabilità e di sicurezza dei messaggi in arrivo al Gestore, provengano essi dal circuito PEC o dall'esterno del circuito stesso.

9.6.1.1 Normativa

DPR 68/2005

Articolo 7 - Ricevuta di presa in carico

Articolo 12 - Virus informatici, comma 2

All. DM 2/11/2005

6.4 Punto di ricezione

6.4.1 Ricevuta di presa in carico

6.4.2 Busta di anomalia

6.5 Punto di consegna

6.5.1 Verifiche sui messaggi in ingresso

8.4 Virus

9.6.1.2 Il Gestore

1. Esibisce documentazione e procedure che mostrino che esso, alla ricezione di messaggi da parte del Gestore di un mittente:

   a. effettua sui messaggi i controlli previsti dall'All. DM 2/11/2005 al punto 6.4[3];

   b. svolge le azioni derivanti da tali controlli previste dall'All. DM 2/11/2005 al punto 6.4[4] provvedendo come previsto dalla normativa (si veda il paragrafo 9.6.3) a creare Ricevute, Avvisi, e Buste di anomalia e a curarne l'inoltro al Gestore del mittente e al destinatario.

---

[3] "Al ricevimento di un messaggio presso il punto di ricezione, il sistema compie i seguenti controlli, per verificare che la busta di trasporto/ricevuta/avviso sia corretta/integra:

- Controllo dell'esistenza della firma [omissis];
- Controllo che la firma sia stata emessa da un Gestore di posta certificata [omissis]
- Controllo della validità della firma [omissis]
- Correttezza formale [omissis]."

[4] "Il punto di ricezione, a fronte dell'arrivo di un messaggio, effettua la seguente serie di controlli ed operazioni:

- verifica la correttezza/natura del messaggio in ingresso;
- se il messaggio in ingresso è una busta di trasporto corretta ed integra:
  - emette una ricevuta di presa in carico verso il Gestore mittente;

2. Esibisce documentazione e procedure che mostrino che, qualora il punto di ricezione del Gestore riceva un messaggio di posta elettronica non certificata, e il Gestore stesso abbia come propria politica di inoltrare tali messaggi al destinatario, esso controlla la presenza di virus informatici e, in caso di loro assenza, lo inserisce in una busta di anomalia. Nel caso sia riscontrata la presenza di virus il messaggio è scartato dal punto di ricezione.
3. Esibisce verbali di audit che attestino la corretta esecuzione dei controlli e delle azioni di cui al punto 6.4 dell'All. DM 2/11/2005 (vedi punti 1 e 2 di questo paragrafo).

Nota: il log di PEC può essere utilizzato per fornire le informazioni di cui ai punti precedenti.

9.6.1.3 Il Valutatore

1. Verifica l'esistenza di procedure, documentazione e verbali di audit che mostrino che il Gestore effettua i controlli e svolge le operazioni previste al punto 6.4 dell'All DM 2/11/2005 come indicato al paragrafo 9.6.1.2.
2. Ove il Gestore abbia come propria politica di inoltrare al destinatario messaggi di posta elettronica non certificata, PUO', avvalendosi di un'utenza di posta non certificata, inviare messaggi a una o più caselle di PEC assegnate al CNIPA dal Gestore come da punto 1.2 della CNIPA/CR/51, per verificare la corretta gestione degli stessi.
3. PUO' inserire un virus in alcuni dei messaggi di cui al punto 2 per verificare che essi vengano rifiutati.

Nota: in base alla Nota del paragrafo 9.6.1.2 il Valutatore PUO' effettuare ricerche sui log, inclusi quelli già sottoposti a conservazione sostitutiva.

9.6.2 Deposito in casella destinatario

Finalità: assicurare la tracciabilità dei messaggi di PEC, anche informando il destinatario, ove del caso, della eventuale non conformità alle norme di interoperabilità e di sicurezza di messaggi a lui indirizzati, provengano essi dal circuito PEC o dall'esterno del circuito stesso.

9.6.2.1 Normativa

Dlgs 82/2005

Art. 45. Valore giuridico della trasmissione, commi 1 e 2.

Art. 48. Posta elettronica certificata.

DPR 68/2005

Articolo 5 - Modalità della trasmissione e interoperabilità

Articolo 11 - Sicurezza della trasmissione, comma 1

DM 2/11/2005

Articolo 1 - Definizioni, comma 1, lettera o)

- inoltra la busta di trasporto verso il punto di consegna;

- se il messaggio in ingresso è una ricevuta corretta ed integra o un avviso di posta certificata corretto ed integro:
  - inoltra la ricevuta/avviso verso il punto di consegna;
- se il messaggio in ingresso non risponde ai requisiti per una busta di trasporto o per una ricevuta/avviso corretto ed integro, ma risulta proveniente da un Gestore di posta certificata, quindi supera le verifiche di esistenza, provenienza e validità della firma, il messaggio deve essere propagato verso il destinatario, quindi:
  - imbusta il messaggio in arrivo in una busta di anomalia;
  - inoltra la busta di anomalia verso il punto di consegna.
- se il messaggio in ingresso non proviene da un sistema di posta certificata, quindi non supera le verifiche di esistenza, provenienza e validità della firma, viene considerato di posta ordinaria, quindi, se propagato verso il destinatario:
  - imbusta il messaggio in arrivo in una busta di anomalia;
  - inoltra la busta di anomalia verso il punto di consegna."

Articolo 6 - Caratteristiche dei messaggi gestiti dai sistemi di posta elettronica certificata, comma 5

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

All. DM 2/11/2005

6.5.1 Verifiche sui messaggi in ingresso

9.6.2.2 Il Gestore

1. Esibisce procedure, documentazione e verbali di audit che mostrino che esso:
    a. a seguito di verifiche favorevoli sul contenuto delle buste di trasporto in arrivo effettua il tentativo di depositarle nella casella di PEC del destinatario;
    b. a seguito di verifiche favorevoli sul contenuto dei messaggi in arrivo da posta ordinaria effettua il tentativo di depositare nella casella di PEC del destinatario le buste di anomalia in cui li ha inseriti (si veda punto 1.b del paragrafo 9.6.1.2)
    c. se una busta di trasporto in ingresso non risponde ai relativi requisiti di correttezza e integrità, ma risulta proveniente da un Gestore di posta certificata, e supera le verifiche di esistenza, provenienza e validità della firma, la inserisce in una busta di anomalia ed effettua il tentativo di depositarla nella casella di PEC del destinatario.

Nota: il log di PEC può essere utilizzato per fornire le informazioni precedenti.

9.6.2.3 Il Valutatore

1. Verifica l'esistenza di documentazione, procedure e verbali di audit che mostrino il corretto deposito di buste di trasporto o di anomalia nella casella di PEC del destinatario.
2. PUO' verificare l'esito della consegna dei messaggi inviati da una propria casella di PEC, come indicato al punto 2 del paragrafo 9.6.1.3.

Nota: il log di PEC può essere utilizzato per verificare le informazioni precedenti.

9.6.3 Creazione Ricevute, Avvisi, Buste

Finalità: assicurare la tracciabilità dei messaggi di PEC informando il mittente dell'avvenuta consegna di un messaggio da esso inviato, mediante la creazione e l'inoltro verso lo stesso mittente di uno dei tre tipi previsti di Ricevute di consegna, o della impossibilità di consegnarlo qualora si tratti di destinatario appartenente al circuito PEC.

9.6.3.1 Normativa

Dlgs 82/2005

Art. 45. Valore giuridico della trasmissione, commi 1 e 2.

Art. 48. Posta elettronica certificata.

DPR 68/2005

Articolo 6 - Ricevuta di accettazione e di avvenuta consegna, commi dal 2 al 6

Articolo 8 - Avviso di mancata consegna

Articolo 11 - Sicurezza della trasmissione, comma 4

DM 2/11/2005

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

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

All. DM 2/11/2005

5 Definizioni

6.1 Formato dei messaggi generati dal sistema

6.4 Punto di ricezione

6.4.2 Busta di anomalia

6.5.2 Ricevuta di avvenuta consegna

6.5.2.1 Ricevuta completa di avvenuta consegna

6.5.2.2 Ricevuta di avvenuta consegna breve

6.5.2.3 Ricevuta sintetica di avvenuta consegna

6.5.3 Avviso di mancata consegna

7.3 Specifiche degli allegati

7.3.1 Corpo del messaggio

7.3.2 Messaggio originale

7.3.3 Dati di certificazione

7.4 Schema dei dati di certificazione

8.4 Virus

CNIPA/CR/51

1.2 (Superamento test di interoperabilità)

9.6.3.2 Il Gestore

1. Esibisce documentazione, procedure e verbali di audit che mostrino che:
    a. al ricevimento di una busta di trasporto genera regolarmente una Ricevuta di presa in carico che invia al Gestore del mittente;
    b. qualora il deposito di una busta di trasporto avvenga regolarmente, esso genera una Ricevuta di avvenuta consegna che invia al Gestore del mittente; tale ricevuta deve essere del tipo specificato nella Busta di trasporto: completa, breve, sintetica;
    c. qualora non sia possibile depositare una busta di trasporto, il Gestore genera un Avviso di mancata consegna che invia verso il Gestore del mittente;
    d. a fronte di esito positivo o negativo del tentativo di deposito di una Busta di anomalia generata come indicato al punto 1.b del § 9.6.2.2 non genera né ricevute di avvenuta consegna né avvisi di mancata consegna.

9.6.3.3 Il Valutatore

1. Verifica l'esistenza di procedure, documentazione e verbali di audit che attestino la regolare creazione di ricevute e avvisi in base all'effettiva consegna o mancata consegna di messaggi nella casella di PEC dei destinatari, come indicato al paragrafo 9.6.3.2.
2. Qualora, come indicato al punto 4 del paragrafo 9.5.3.3, abbia inviato messaggi di PEC da caselle assegnate dal Gestore al C NIPA come da CNIPA/CR/51 al punto 1.2, verifica che:
    a. le ricevute di avvenuta consegna siano del tipo indicato nella rispettiva Busta di trasporto: completa, breve, sintetica
    b. il formato dei messaggi (ricevute, avvisi e buste) sia conforme con quanto previsto al punto 6.1 dell'All. DM 2/11/2005.

9.7 Gestione virus

Finalità: escludere dal circuito PEC i messaggi immessi dai titolari di caselle di PEC da esso rilasciate, o ricevuti da altri gestori, nei quali il Gestore abbia riscontrato virus e assicurare la possibilità di esibirli alle persone autorizzate durante l'arco di tempo previsto dalla normativa. I messaggi contenenti virus ricevuti da gestori estranei al circuito di PEC devono essere scartati.

Nota: per quanto riguarda la conservazione dei messaggi contenenti virus vedere il capitolo 12.14.

9.7.1 Normativa

DPR 68/2005

Articolo 12 - Virus informatici, comma 1

DM 2/11/2005

Articolo 11 - Conservazione dei messaggi contenenti virus e relativa informativa al mittente, commi 2 e 3

All. DM 2/11/2005

6.4 Punto di ricezione

6.4.3 Avvisi relativi alla rilevazione di virus informatici

6.4.3.1 Avviso di non accettazione per virus informatico

6.4.3.2 Avviso di rilevazione virus informatico

6.4.3.3 Avviso di mancata consegna per virus informatico

8.4 Virus

9.7.2 Il Gestore

1. Esibisce documentazione, procedure e verbali di audit che mostrino che:
    a. i messaggi contenenti virus inviati dai titolari non vengono inoltrati ai destinatari, ma vengono conservati per almeno trenta mesi;
    b. i mittenti di tali messaggi sono informati dell'evento con Avvisi di non accettazione per virus informatico (si veda il punto 1 del paragrafo 9.5.3.2)
    c. le buste di trasporto nelle quali rilevi virus non vengono inoltrate al destinatario e che in tal caso viene emesso un Avviso di rilevazione di virus informatico verso il Gestore mittente;
    d. le buste di trasporto contenenti virus sono sottoposti a conservazione sostitutiva per almeno trenta mesi;
    e. le buste di trasporto contenenti virus sono esibiti ove ciò sia richiesto da persona fisica o giuridica autorizzata;
    f. qualora riceva un Avviso di rilevazione di virus informatico proveniente dal Gestore di un destinatario, oltre ad emettere nei confronti del mittente un Avviso di mancata consegna per virus (si veda anche il punto 2 del paragrafo 9.5.3.2), agisce prontamente per individuare la causa per la quale il messaggio contenente tale virus sia sfuggito al controllo da esso effettuato in fase di accettazione e quindi per eliminarla.
2. Esibisce documentazione, procedure e verbali di audit che mostrino che mantiene attivo e prontamente aggiornato un sistema di protezione contro virus.

9.7.3 Il Valutatore

1. Verifica l'esistenza di documentazione, procedure, verbali di audit che mostrino la corretta gestione di messaggi e buste di trasporto contenenti virus, come indicato al paragrafo 9.7.2.

2. Ove abbia operato come indicato al punto 2 lettera a del paragrafo 9.5.2.3, riscontra l'esattezza della gestione dei messaggi contenenti virus da lui generati come ivi indicato.

9.8 Gestione sospensioni del servizio

Finalità: il Gestore deve essere preparato a reagire con immediatezza al verificarsi dei casi per i quali sia previsto dalla norma di sospendere il servizio.

Nota: vedere anche i capitoli 9.5.3 e 14.2.

9.8.1 Normativa

DM 2/11/2005

Art. 12 - Livelli di servizio, comma 7

CR/CNIPA/51

7. Sospensione del servizio.

9.8.2 Il Gestore

1. Esibisce documentazione e procedure tecniche e organizzative che mostrino di essere in grado di:
    a. sospendere con immediatezza il servizio, su propria iniziativa o su richiesta del CNIPA, pur ottemperando al requisito di "assicurare in ogni caso il completamento della trasmissione ed il rilascio delle ricevute" previsto dall'art. 12, comma 7, del DM 2/11/2005;
    b. fornire adeguata e tempestiva informativa ai propri utenti ed agli altri gestori in caso di sospensione del servizio.

    Nota: vedere anche il § 14.2.2 e il punto 5 del § 9.5.3.2.
2. Esibisce verbali di audit che mostrino l'esistenza e la funzionalità delle procedure tecniche e organizzative di cui al precedente punto 1.

9.8.3 Il Valutatore

1. Verifica l'esistenza della documentazione e delle procedure tecniche e organizzative di cui al punto 1 del § 9.8.2.

    Nota: vedere anche il § 14.2.3 e il punto 4 del § 9.5.3.3
2. Verifica l'esistenza di verbali di audit che mostrino l'esistenza e la funzionalità delle procedure tecniche e organizzative di cui al punto 1 del § 9.8.2.

Capitolo 10

Firme di ricevute, avvisi, buste, IGPEC

10.1 Formato delle firma

Finalità: assicurare che ricevute, avvisi, buste siano firmate con la firma del Gestore con le modalità previste.

10.1.1 Normativa

DPR 68/2005

Articolo 9 - Firma elettronica delle ricevute e della busta di trasporto

DM 2/11/2005

Art. 1 Definizioni, lettera d)

Art. 7 - Firma elettronica dei messaggi di posta elettronica certificata

All. DM 2/11/2005

6.1 Formato dei messaggi generati dal sistema

8.1 Firma

8.3 Colloquio sicuro

10.1.2 Il Gestore

1. Esibisce procedure, documentazione e verbali di audit che mostrino che i messaggi sono firmati dal Gestore in modo da ottenere il formato "multipart/signed" (formato .p7s) così come descritto nello RFC 2633 §3.4.3.

   Nota: tale documentazione può essere integrata dal contenuto del log.

10.1.3 Il Valutatore

1. Verifica l'esistenza della documentazione di cui al paragrafo 10.1.2.

10.2 Creazione della firma

Finalità: assicurare che l'applicazione di creazione della firma del Gestore possa essere attivata esclusivamente da personale autorizzato e che, una volta attivata, essa abbia il controllo esclusivo delle chiavi di firma del Gestore contenute nei dispositivi di firma, in conformità con le valutazioni di sicurezza di questi ultimi.

10.2.1 Normativa

In aggiunta ai requisiti indicati di seguito, che fanno sostanzialmente riferimento ai dispositivi di firma, è RACCOMANDATO che l'attivazione del dispositivo di firma avvenga in situazione di dual control.

DPR 68/2005

Art. 9 - Riferimento temporale

DM 2/11/2005

Articolo 7 - Firma elettronica dei messaggi di posta elettronica certificata, comma 1

All. DM /2/11/2005

6.1 Formato dei messaggi generati dal sistema

8.1 Firma

8.3 Colloquio sicuro

CNIPA/CR/49

1. Modalità di presentazione delle domande, lettera r).

10.2.2 Il Gestore

1. Esibisce documentazione, procedure operative e verbali di audit che mostrino che:
    a. l'applicazione di firma può essere attivata soltanto da personale autorizzato in situazioni almeno di "dual control";

        Nota: anche se non è prescritto dalla normativa, le normali misure di sicurezza prevedono che la gestione di procedure relative ad attività critiche siano eseguite in regime di almeno dual control (si veda Nota alla definizione del termine "Dual control");

    b. le specifiche procedure tecniche od organizzative che consentono di aggirare i vincoli del "dual control" sono utilizzate esclusivamente in emergenza e ove sia strettamente necessario; tali procedure devono assicurare la registrazione e il successivo riscontro della gestione dell'evento eccezionale;

    c. la chiave di firma custodita nel dispositivo di firma può essere utilizzata soltanto dall'applicazione, una volta attivata;

    d. quanto indicato ai precedenti punti è applicabile al sistema di PEC presente sia nel sito principale sia in quello di disaster recovery, ove previsto.

10.2.3 Il Valutatore

1. Verifica l'esistenza della documentazione di cui al paragrafo 10.2.2 relativa all'attivazione dell'applicazione di firma da parte di personale autorizzato in regime almeno di dual control, e del controllo esclusivo della chiave privata di firma da parte di quest'applicazione, anche nel sito di disaster recovery, ove previsto.

Nota: si tenga presente la Nota della lettera a del punto 1 del paragrafo 10.2.2.

10.3 Verifica firma

Finalità: assicurare che la validità delle firme apposte sui messaggi di PEC e sullo IGPEC possa essere verificata dall'applicazione PEC del Gestore e dai client dei suoi titolari attuando le misure previste dalla norma.

10.3.1 Normativa

All. DM 2/11/2005

6.4 Punto di ricezione

6.5.2.1 Ricevuta completa di avvenuta consegna

6.5.2.2 Ricevuta di avvenuta consegna breve

6.5.2.3 Ricevuta sintetica di avvenuta consegna

9.2 Requisiti tecnico funzionali di un client di un sistema di PEC

10.3.2 Il Gestore

1. Esibisce documentazione, procedure e verbali di audit che mostrino che:
    a. la applicazione di PEC utilizzata verifica le firma S/MIME versione 3, come da RFC 2633, dei messaggi di PEC:
        i. controllando che la firma sia stata emessa da un Gestore di posta certificata: per far questo estrae il certificato usato per la firma del messaggio in ingresso;
        ii. verificando la validità temporale del certificato di firma;
        iii. accedendo alla CRL, verificandone la validità e verificando la validità del certificato di firma;

        Nota: qualora le CRL siano conservate localmente esse devono essere scaricate con una tempestività tale da garantire di far uso di CRL in vigore.
    b. informa i titolari sui client di posta che rispondono ai requisiti di verifica delle firme del Gestore come da punto 9.2 dell'All. al DM 2/11/2005.

10.3.3 Il Valutatore

1. Verifica l'esistenza della documentazione di cui al paragrafo 10.3.2 sull'informativa fornita dal Gestore ai titolari sui client di posta da utilizzare e sulle modalità con cui esso stesso verifica le firme sui messaggi di PEC.

Capitolo 11

Commercializzazione dei servizi di PEC tramite canali esterni

Finalità: assicurare che il soggetto terzo che commercializza i servizi di PEC forniti dal Gestore operi in conformità con le prescrizioni di legge, e che il rapporto contrattuale sia posto in essere tra il titolare e il Gestore.

11.1.1 Normativa

CNIPA/CR/51

3 – Modalità di vendita dei servizi di PEC attraverso canali commerciali.

3.1

4. Struttura informativa dei gestori.

4.2, lettera b)

FAQ a CNIPA/CR/51 - 3. Modalità di vendita dei servizi di PEC attraverso canali commerciali – Punto 3 della circolare 7 dicembre 2006, n. 51.

11.1.2 Il Gestore

1. Ove la commercializzazione delle caselle di PEC sia effettuata attraverso canali commerciali di terzi, esibisce gli specifici accordi con detti terzi e i verbali di audit relativi a ispezioni presso di essi da cui risulti:
    a. "che le modalità di vendita siano conformi alle prescrizioni di legge e che il rapporto contrattuale sia sempre posto in essere tra il titolare di cui all'art. 1, lettera t) del decreto ministeriale" (punto. 3.1 di CNIPA/CR/51)
    b. "che il titolare della casella di PEC sottoscriva un apposito modulo avente valore di disciplina contrattuale, dal quale risulti che il servizio di PEC è erogato dal Gestore" (FAQ - Circolare 51 Vigilanza PEC 1.1).
2. Esibisce lo schema di contratto utilizzato dal soggetto terzo per la commercializzazione dei servizi PEC del Gestore dal quale risulti:
    a. che il rapporto contrattuale di servizio sia posto in essere tra il cliente e il Gestore;
    b. che in esso siano riportate, direttamente o per il tramite di documenti a cui fa riferimento, esaurienti indicazioni su come usare il servizio di PEC.

Nota 1: Nel caso in cui non sia possibile esibire lo schema di contratto, l'evidenza in questione può essere fornita da copie di contratti effettivamente stipulati nelle quali siano resi illeggibili i nominativi dei clienti.

Nota 2: Si veda anche quanto indicato ai paragrafi 8.1.2 e 8.3.2.

3. Esibisce verbali di audit effettuati presso i soggetti terzi che effettuano la commercializzazione dei servizi PEC del Gestore dal quale risulti il rispetto degli accordi riportati nei contratti.
4. Dietro richiesta del valutatore organizza specifiche ispezioni presso le sedi di soggetto terzo, che effettua la commercializzazione dei suoi servizi PEC, alle quali può partecipare anche il valutatore.

11.1.3 Il Valutatore

1. Verifica che la documentazione contrattuale, ivi incluso lo schema di contratto, fornisca evidenza che, anche nel caso di commercializzazione effettuata mediante soggetti terzi:
    a. le modalità di commercializzazione siano conformi alle prescrizioni di legge;
    b. siano date esaurienti indicazioni su come usare il servizio di PEC;
    c. il rapporto contrattuale sia sempre posto in essere tra il titolare e il Gestore.
2. Verifica l'esistenza di verbali di audit effettuati presso i soggetti terzi che effettuano la commercializzazione dei servizi PEC del Gestore dai quali risulti il rispetto degli accordi riportati nei contratti.
3. Può richiedere al gestore di organizzare specifiche ispezioni presso le sedi di soggetto terzo, che effettua la commercializzazione dei suoi servizi PEC, alle quali può partecipare anche il valutatore.

Capitolo 12

Gestione e operatività del Gestore

12.1 Misure globali di sicurezza

Finalità: Applicare procedure e metodi amministrativi e di gestione adeguati e corrispondenti a norme riconosciute, tra cui gli standard di sicurezza emessi da organismi internazionali.

Nota: Le misure indicate nello standard ISO/IEC 27002 consentono di ottenere una adeguata sicurezza dei sistemi informativi. Sono pertanto ritenute soddisfacenti le misure ad esso conformi.

12.1.1 Normativa

DPR 68/2005

Articolo 14 - Elenco dei gestori di posta elettronica certificata, comma 6, lettere a) ed f).

DM 2/11/2005

Articolo 21 - Organizzazione e funzioni del personale del certificatore, comma 1, lettera d).

CNIPA/CR/49

1. Modalità di presentazione delle domande., lettere p) e q).

2.1 Manuale operativo, lettera e)

2.2 Piano per la sicurezza., lettere a), f), g), h)

12.1.2 Il Gestore

1. Esibisce documentazione che dimostri che al Responsabile della sicurezza, di cui verifica la corrispondenza con quanto dichiarato al CNIPA, sia stato erogato adeguato addestramento, a fronte degli aggiornamenti tecnici e organizzativi di cui all'articolo 22 del DM 2/11/2005, al fine di mantenerne le caratteristiche di esperienza.
2. In base a quanto indicato nel Piano per la sicurezza depositato in CNIPA, relativamente a risultanze di Risk Assessment, contromisure, controlli aggiornati e procedure interne coerentemente adottate, DOVREBBE esibire ICT Security Policy aziendali e di sistema (ISO/IEC 13335:2004 – capitolo 4.2 / ISO/IEC 27002:2007 – capitolo 5), approvate dal Management e rese note al personale interessato. Ove alcuni rischi siano stati accettati dal Gestore, DEVE esserne esibita la formale accettazione integrata dalla relativa motivazione.

   Nota 1: il Risk Assessment DEVE essere periodicamente rivisto sotto la responsabilità del Responsabile della sicurezza, in base all'evoluzione della tecnologia, ai risultati degli audit di sicurezza interni ed esterni, agli incidenti di sicurezza, all'evoluzione degli attacchi e alle vulnerabilità individuate (vedere capitolo 4.1 di ISO/IEC 27002). Le Security Policy, ove esistenti, DEVONO essere aggiornate di conseguenza, in aggiunta alle loro revisioni periodiche previste dallo ISO/IEC 27002 al capitolo 5.1.2.

Nota 2: è buona norma disporre di un "portafoglio" di security policy elementari, anch'esse approvate dal Management, che indichino le singole misure da adottare nei vari casi; in tal modo è più agevole ottenere coerenza tra le varie security policy di sistema.

3. Ove il Valutatore lo richieda, consente a quest'ultimo l'accesso, debitamente controllato e registrato, se necessario utilizzando le funzionalità previste per gli auditor e gli ispettori, a funzioni, servizi, sistemi, locali, ecc. Ove del caso gli consente, con pari modalità, anche l'accesso alle sedi di fornitori esterni che svolgono mansioni per conto del Gestore.

   Nota 3: Per quanto riguarda la sicurezza fisica e altri aspetti specifici del sistema di PEC fare riferimento anche agli altri paragrafi di questo Capitolo 12.

4. Esibisce verbali di audit che mostrino che le procedure esibite dal Gestore sono conformi con quanto indicato nel Piano per la sicurezza.

   Nota 4: le norme tecniche indicate dallo ISO/IEC 27002 prevedono che almeno le attività più delicate siano svolte in regime di "dual control" (vedere la Nota alla definizione del termine "dual control").

12.1.3 Il Valutatore

1. Vedere il punto 1 del paragrafo 9.3.3 per quanto riguarda le verifiche riguardanti il Responsabile della sicurezza.
2. Verifica che i rischi individuati dal Risk Assessment, riflessi nelle contromisure e nei controlli indicati nel Piano per la sicurezza, siano adeguatamente gestiti nelle procedure, conformemente con le Security Policy in vigore approvate dal Management e rese note al personale interessato, oppure che il Management stesso abbia formalmente ed esplicitamente accettato di non porre in atto contromisure per contrastarli, nel qual caso verifica che le motivazioni di tale accettazione siano esposte chiaramente.
3. PUO' chiedere di accedere, con funzioni di auditor o ispettore, a funzioni, servizi, sistemi, locali, ecc., anche di fornitori del Gestore.

   Nota 1: Si veda anche la Nota 3:del paragrafo 12.1.2

4. Verifica l'esistenza di verbali di audit che mostrino che le procedure esibite dal Gestore sono conformi con quanto indicato nel Piano per la sicurezza.

12.2 Sicurezza fisica

Finalità: assicurare che i servizi critici del sistema di PEC siano gestiti in ambienti sicuri in modo da rendere minimi i rischi fisici per il personale e per gli asset.

12.2.1 Normativa

DPR 68/2005

Articolo 14 - Elenco dei gestori di posta elettronica certificata, comma 6, lettere a) f).

DM 2/11/12005

Articolo 21 - Organizzazione e funzioni del personale del certificatore, comma 1, lettera d)

CNIPA/CR/49

1. Modalità di presentazione delle domande., lettere p), q).

2.2 Piano per la sicurezza, lettere f), g), i), j), k)

12.2.2 Il Gestore

1. Esibisce documentazione che dimostri che al Responsabile dei servizi tecnici, di cui verifica la corrispondenza con quanto dichiarato al CNIPA, sia stato erogato adeguato addestramento, a fronte degli aggiornamenti tecnici e organizzativi di cui all'articolo 22 del DM 2/11/2005, al fine di mantenerne le caratteristiche di esperienza.
2. Esibisce le procedure per l'accesso ai locali del sistema di PEC, e i relativi verbali anche di audit, da cui risultino l'attuazione delle misure indicate al proprio Piano per la Sicurezza alle voci: "g) descrizione delle procedure per la gestione dei rischi" e "i) l'indicazione della struttura generale e della struttura logistica dell'organizzazione e delle relative modalità operative". Esibisce anche la loro comunicazione agli interessati e l'elenco delle persone autorizzate ad accedervi.

   Per quanto concerne le seguenti Note vedere ISO/IEC 27002, capitolo 9.1.

   Nota 1: Anche se non esplicitamente richiesto dalla normativa della PEC è buona norma di sicurezza, alla quale pertanto il Gestore DOVREBBE attenersi, registrare gli accessi del personale ai locali dove sono installati i sistemi di PEC.

   Nota 2: Nel caso in cui i sistemi per i servizi di PEC siano collocati in locali adeguatamente protetti ma condivisi con altri sistemi destinati ad usi differenti, il Gestore DEVE provvedere a impedire accessi indebiti ai sistemi destinati ai servizi di PEC almeno con misure logiche, ma, ove necessario e possibile, anche mediante strutture fisiche; in tal caso l'accesso a queste strutture, le quali DEVONO poter ospitare contemporaneamente gli addetti previsti per ognuna delle varie funzioni, DEVE essere limitato alle sole persone autorizzate; sempre in tal caso almeno l'entrata e l'uscita da queste strutture DOVREBBERO essere registrate; l'alimentazione elettrica, le connessioni di rete, eventuali tubature, ecc. DEVONO essere protette, così come quanto utilizzato per il servizio di PEC; inoltre il Gestore DOVREBBE:

   a. prevedere che locali, sistemi e reti adibiti alla prestazione di servizi ad alto contenuto di sicurezza siano realizzati e collocati in modo tale da evitare:

      i. l'acquisizione indebita di informazioni mediante lettura, anche dall'esterno del locale, degli schermi di computer e dei display di unità varie,

      ii. l'acquisizione indebita di informazioni riservate captando le emanazioni magnetiche, di campo elettrico o simili; quest'ultimo aspetto DOVREBBE riguardare anche i cavedi ove transitano i collegamenti di rete.

   b. formalizzare e rendere operative security policy opportune che richiedano una verifica periodica e, ove necessario, estemporanea dell'integrità delle strutture fisiche di protezione dei sistemi di PEC;

   c. verbalizzare l'esecuzione delle procedure connesse ai servizi di PEC nel rispetto di tali security policy.

3. Esibisce documentazione, ivi inclusi verbali di audit, attestante l'adozione di misure di sicurezza per prevenire danni ai locali, alle persone che ivi operano e alle apparecchiature ivi allocate.

   Nota 3: le misure di sicurezza indicate nello ISO/IEC 27002, alle quali è auspicato che il Gestore si adegui, prevedono, tra l'altro, che:

   a. siano attuate misure preventive contro eventi quali "*incendi, allagamenti, terremoti, esplosioni, rivolte, altri disastri naturali o provocati dall'uomo*"[5];

[5] ISO/IEC 27002 capitolo 9.1.4

   b. locali, sistemi e reti adibiti alla prestazione di servizi ad alto contenuto di sicurezza siano realizzati e collocati in modo tale da evitare condizioni ambientali sfavorevoli sia per le persone sia per le attrezzature,
   c. esistano misure per ovviare a inconvenienti quali prolungata mancanza di acqua o di energia elettrica o di riscaldamento o condizionamento.

4. Esibisce documentazione che riporti le autorizzazioni del personale ad accedere ai locali ove sono installati i sistemi di PEC e ad operarvi, in conformità con le contromisure indicate nel Piano per la sicurezza (si veda precedente Nota 2:).
5. DOVREBBE esibire le registrazioni dell'accesso del personale ai locali o alle strutture ove sono installati i sistemi di PEC (si vedano precedenti Nota 1: e Nota 2:).
6. Consente l'accesso ai locali o alle strutture del sistema di PEC al Valutatore accompagnato da personale autorizzato, nel rispetto delle misure di sicurezza indicate nel Piano per la sicurezza.
7. Consente al Valutatore l'esame in sola lettura del registro dal quale possano rilevarsi gli accessi ai locali del sistema di PEC, ivi compreso anche l'accesso del Valutatore stesso.

12.2.3 Il Valutatore

1. Verifica che dalla documentazione esibita risulti che il Responsabile dei servizi tecnici corrisponda con quanto dichiarato dal Gestore al CNIPA e che ad esso sia stato erogato adeguato addestramento, a fronte degli aggiornamenti tecnici e organizzativi di cui all'articolo 22 del DM 2/11/2005, al fine di mantenerne le caratteristiche di esperienza. (Vedere punto 2 del paragrafo 12.6.3).
2. Verifica che le persone che hanno acceduto ai locali in questione siano state debitamente e preventivamente autorizzate.

   Nota 1: si veda anche quanto indicato in Nota 1: e in Nota 2: del paragrafo 12.2.2.

   Nota 2: si veda anche quanto indicato in Nota 1: e in Nota 2: del paragrafo 12.2.2.
3. Verifica che nel registro degli accessi al locale o alle strutture ove sono installati i sistemi di PEC risultino le entrate e le uscite dai locali del personale autorizzato, tra cui anche quelle del Valutatore stesso.
4. Verifica di persona l'impossibilità di accedere a locali e strutture, sistemi e applicazioni in questione se non a seguito di esito positivo di controllo accessi fisici e/o logici.
5. Verifica che locali e strutture ove si trovano i sistemi di PEC presentino caratteristiche costruttive di base sicure, ad esempio che gli ingressi controllati non possano restare indefinitamente aperti senza allarme, che non sia possibile distinguere dall'esterno quanto viene presentato sugli schermi video, che vi siano impianti di sicurezza: antincendio, anti-allagamento, ecc.
6. Verifica l'esistenza della documentazione e dei verbali di audit di cui ai punti 2 e 3 del paragrafo 12.2.2.

12.3 Componenti HW e SW dei sistemi del Gestore

Finalità: verificare che il Gestore utilizzi effettivamente per fornire i servizi di PEC i componenti HW e SW dichiarati al CNIPA.

12.3.1 Normativa

CNIPA/CR/49

1, lettera t)

12.3.2 Il Gestore

1. Esibisce documentazione che mostri che la propria dotazione di HW e SW correlata alla fornitura dei servizi di PEC corrisponde a quanto dichiarato al CNIPA all'atto della domanda di iscrizione nello IGPEC.

   Nota: Non può essere considerato conforme a tale dichiarazione HW e SW che abbia subito aggiornamenti di versione tali da alterarne le caratteristiche principali.

12.3.3 Il Valutatore

1. Verifica l'esistenza di documentazione sulla dotazione HW e SW del Gestore, come da paragrafo 12.3.2.

12.4 Gestione accesso ai sistemi

Finalità: assicurare che ai sistemi del Gestore possano accedere sia fisicamente sia logicamente solo persone debitamente autorizzate.

12.4.1 Normativa

Dlgs 196/2003

Art. 31: "Obblighi di sicurezza"

1. *I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.*

Nel caso di soggetti pubblici si applica anche il seguente art. 22.3:

"*I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.*"

Dlgs 82/2005

Art. 48. Posta elettronica certificata, comma 3.

DPR 68/2005

Articolo 11 - Sicurezza della trasmissione, commi 2 e 3

Articolo 14 - Elenco dei gestori di posta elettronica certificata, comma 6, lettere a), c), f)

CNIPA/CR/49

2.2 Piano per la sicurezza, lettera a).

12.4.2 Il Gestore

1. Esibisce documentazione da cui emerga che la propria rete destinata alla fornitura dei servizi di PEC è adeguatamente protetta da accessi logici non autorizzati da parte di personale interno ed esterno (ad esempio: mediante identificazione e autenticazione, Firewall, IDP, IPS, utilizzo di secure channel per il personale autorizzato, cifratura per i dati personali sensibili, ecc.).
2. Esibisce procedure e verbali di audit da cui emerga che i sistemi utilizzati per l'erogazione dei propri servizi sono protetti da accessi logici non autorizzati.
3. Esibisce le procedure, e i relativi verbali di audit, per la registrazione, gestione e rimozione dei privilegi del personale all'accesso logici a sistemi e reti.
4. Esibisce l'elenco delle persone autorizzate ad accedere logicamente a sistemi, locali e reti.
5. Esibisce documentazione e i relativi verbali di audit da cui emerga che almeno le attività più delicate di gestione dei sistemi e della rete sono svolte in regime di "dual control" (si veda Nota alla definizione del termine "Dual control").
6. Ove del caso esibisce le regole per la composizione delle password e le misure per verificarne l'effettivo rispetto.
7. Esibisce procedure e relativi verbali di audit che prevedano una regolare ispezione dei log dei sistemi utilizzati e dei dispositivi messi a protezione della rete da intrusioni, da cui risultino gli accessi logici, i tentativi di accesso logico non autorizzato, i codici identificativi degli autori dell'accesso logico o dei tentativi di accesso, come anche le misure intraprese a seguito dei tentativi di intrusione e accesso logico non autorizzato. E' auspicabile che siano stati effettuati anche penetration test.
8. Esibisce verbali di auditing interno o esterno da cui emerga la corrispondenza con quanto conservato da apposta funzione della configurazione prevista per gli strumenti utilizzati per prevenire intrusioni logiche nella rete e l'effettiva periodica ispezione dei log e registri interessati.
9. Assiste il Valutatore nei tentativi di accesso logico non autorizzato che questo ritenesse utile effettuare.

12.4.3 Il Valutatore

1. Verifica l'esistenza di documentazione, procedure e verbali di audit come indicato al paragrafo 12.4.2 e che emerga il rispetto delle misure e delle procedure ivi indicate. E' auspicabile che l'auditor interno o esterno abbia effettuato anche penetration test.
2. Verifica alcune registrazioni del log allo scopo di controllare se persone non autorizzate dal Gestore abbiano avuto accesso logico a sistemi e reti, e che almeno le attività più delicate siano svolte in regime di "dual control" (si veda Nota alla definizione del termine "Dual control").
3. Può effettuare, con l'assistenza del personale del Gestore, tentativi di accesso logico a sistemi e reti per verificarne l'effettiva rispondenza della protezione a quanto dichiarato.

12.5 Gestione degli asset

Finalità: Assicurare che dati, informazioni e altri asset siano adeguatamente protetti.

12.5.1 Normativa

CNIPA/CR/49

1. Modalità di presentazione delle domande., lettera q)

2.2 Piano per la sicurezza, lettere a), f), g)

Nota: A integrazione della normativa, che per sua natura non può scendere troppo in dettaglio, si fornisce di seguito a titolo esemplificativo un elenco non esauriente di possibili "asset" relativi all'esercizio dei servizi di PEC, impostato sviluppando quanto indicato nello standard ISO/IEC 27002:

- Sale macchine e chiavi o codici per accedervi;
- Armadi, casseforti e chiavi o codici per accedervi;
- Sistemi e password o chiavi fisiche per accedere al BIOS;
- Sistemi operativi dei computer e account abilitati con i relativi livelli di sicurezza;
- Reti LAN e WAN, relativi dispositivi e installazioni fisiche (router, firewall, IDS, IPS, cavedi, ecc.);
- Software di PEC e vari tipi di utenza.
- Dispositivi crittografici e datakey, chiavi fisiche;
- Codici PIN e password dei dispositivi crittografici.
- Supporti mobili e altre apparecchiature.
- Vari tipi di dati:
    - database e file, contratti, accordi, documentazione di sistema;
    - documentazioni contrattuali, manuali utente, procedure operative o di supporto;
    - Business Continuity Plan, accordi ad esso relativi;
    - Dati di audit;
    - Tool di sviluppo, programmi di utilità.

12.5.2 Il Gestore

1. Anche se non è previsto esplicitamente dalla normativa, il Gestore, per operare con misure conformi con quanto indicato nello standard ISO/IEC 27002, DEVE:
    a. attribuire a ogni asset il corretto livello di criticità, in base alle sue finalità (Confidentiality, Integrity, Availability) e al suo livello di importanza; (ISO/IEC 27002 Capitolo 7.2)
    b. "*individuare chiaramente tutti gli "asset" di rilievo e redigerne un inventario che mantiene aggiornato*" (ISO/IEC 27002 Capitolo 7.1); questo inventario, redatto e tenuto aggiornato tenendo conto della classificazione di cui al punto precedente, dovrebbe elencare gli asset tenendo conto di quanto indicato nella Nota del paragrafo precedente;
    c. contraddistinguere ciascun asset di rilievo con un codice identificativo in base a criteri e a procedure stabiliti che ne attribuiscano le relative responsabilità (si veda punto seguente d); ad esempio: gli asset materiali con un'etichetta o un contrassegno ad essi applicati ove possibile, quelli immateriali, come ad esempio le informazioni, con un contrassegno applicato al supporto che le contiene e che faccia riferimento al contenuto;
    d. attribuire la responsabilità di ogni elemento inventariato a una persona o a una funzione (ISO/IEC 27002 Capitolo 7.2), in questo secondo caso il responsabile della funzione diventa automaticamente responsabile dell'asset;
    e. ove del caso, agli elementi inventariati DOVREBBERO applicarsi specifiche misure di sicurezza.

2. L'inventario e quant'altro descritto al precedente punto 1 DOVREBBE essere attuato almeno per i dispositivi di sicurezza la cui descrizione è richiesta nel Piano per la sicurezza.
3. Per quegli asset per i quali esistano Security Policy specifiche, esibisce procedure e, ove del caso, i relativi verbali di audit, che ne assicurino l'ottemperanza.
4. Consente al Valutatore di effettuare le verifiche del caso in situ.
5. Ove tali asset siano situati presso le sedi di fornitori esterni assicura al Valutatore la possibilità di accedervi.

12.5.3 Il Valutatore

1. Verifica l'esistenza dell'inventario degli asset, come indicato al punto 1 del paragrafo 12.5.2, con i relativi codici identificativi e assegnatari, in particolar modo per i dispositivi di sicurezza la cui descrizione è richiesta nel Piano per la sicurezza.
2. Per quegli asset per i quali esistano Security Policy specifiche verifica l'esistenza di procedure che ne assicurino l'ottemperanza, verificando, ove del caso, i relativi verbali di audit.
3. Effettua, ove del caso, verifiche in situ, eventualmente anche presso i fornitori del Gestore, sugli asset onde verificare che le procedure che li riguardano siano rispettate.

12.6 Gestione del personale

Finalità: impiegare personale dotato delle conoscenze specifiche, dell'esperienza e delle qualifiche necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della posta elettronica e della dimestichezza con appropriate procedure di sicurezza; avvalersi, inoltre, di personale affidabile e pienamente consapevole dei propri compiti e responsabilità.

Nota: quanto segue si applica al personale, esecutivo e manageriale, sia del Gestore sia di eventuali suoi fornitori di servizi strumentali all'esercizio dell'attività di PEC.

12.6.1 Normativa

DPR 68/2005

Articolo 14 - Elenco dei gestori di posta elettronica certificata, comma 6, lettera b)

DM 2/11/2005

Articolo 16 - Modalità di iscrizione all'elenco dei gestori di posta elettronica certificata, comma 1, lettera i)

Articolo 21 - Organizzazione e funzioni del personale del Gestore

Articolo 22 - Requisiti di competenza ed esperienza del personale

CNIPA/CR/49

1, lettera p)

12.6.2 Il Gestore

1. Esibisce documentazione da cui risulti che al personale indicato nella Relazione sulla struttura organizzativa, di cui verifica la corrispondenza con quanto dichiarato al CNIPA, siano state formalmente assegnate le responsabilità previste dall'art. 21 del DM 2/11/2005.
2. Per ciascuna persona esibisce documentazione da cui emerga che essa ha preso formalmente conoscenza delle proprie mansioni e responsabilità coerenti con le Security Policy in essere. In particolare, ove del caso e per ruoli specifici, tra le responsabilità DEVONO essere indicati il vincolo alla riservatezza e le eventuali modalità con cui esso deve essere assicurato anche dopo la cessazione dall'incarico.
3. Anche se non è chiaramente indicato in nessuna norma, è RACCOMANDATO che una persona non sia incaricata di svolgere operazioni all'interno dei servizi di PEC in situazione di conflitto di interesse con altre mansioni da lui rivestite.
4. Esibisce documentazione relativa a un'adeguata informativa al personale interno, e a una analoga clausola degli accordi con i fornitori esterni, sul fatto che violazioni delle disposizioni operative e di sicurezza possono essere sanzionate in base alle normative vigenti.
5. Esibisce documentazione volta a mostrare l'effettivo possesso da parte del personale dei requisiti di competenza, esperienza, anche nel campo della sicurezza, previsti dalla normativa vigente.
6. Esibisce documentazione volta a mostrare l'erogazione al personale in questione di opportuno e aggiornato addestramento sulla parte di rispettiva competenza, ivi inclusi gli aspetti relativi alla sicurezza.
7. Esibisce procedure che indichino le misure da adottare quando una persona addetta ai servizi di PEC lascia l'incarico, in maniera pianificata o imprevista, con particolare attenzione al caso della cessazione conflittuale del rapporto di lavoro. Esse dovrebbero prevedere almeno che, con tempestività, abbia luogo la restituzione del materiale affidato in relazione all'erogazione dei servizi di PEC, l'eliminazione dei relativi account o, ove del caso, almeno la disattivazione dei privilegi relativi. Esibisce, ove del caso, documentazione comprovante l'avvenuta esecuzione di tali procedure.
8. Laddove le procedure previste per quando una persona addetta ai servizi di PEC lascia l'incarico siano state già eseguite, esibisce documentazione, inclusi i verbali di audit, che ne mostri il rispetto.
9. Ove richiesto dal Valutatore, consente l'esecuzione di procedure documentate per verificarne la dimestichezza da parte del personale a ciò deputato.

12.6.3 Il Valutatore

1. Verifica che al personale indicato nella Relazione sulla struttura organizzativa, di cui verifica, eventualmente a campione, la corrispondenza con quanto dichiarato al CNIPA, le responsabilità previste dall'art. 21 del DM 2/11/2005 siano state formalmente assegnate.
2. Verifica che dalla documentazione esibita dal Gestore non risultino evidenti situazioni di conflitto di interesse tra incarichi differenti ricoperti da una stessa persona.
3. Verifica che la documentazione esibita dia evidenza:
    a) che ogni persona interessata, ove del caso anche di fornitori esterni, sia stata messa a conoscenza delle proprie responsabilità connesse con lo specifico incarico coerenti con le Security Policy in essere e del fatto che in caso di violazione di disposizioni operative e di sicurezza possono essere applicate le sanzioni previste dalla normativa vigente;
    b) In particolare, ove del caso e per ruoli specifici, tra le responsabilità DEVONO essere indicati il vincolo alla riservatezza e le eventuali modalità con cui esso deve essere assicurato anche dopo la cessazione dall'incarico.

c) del possesso da parte di ogni persona interessata dei requisiti di competenza ed esperienza previsti dalla normativa in vigore;

d) dell'erogazione al personale del necessario addestramento;

e) della gestione della cessazione dagli incarichi.

4. Verifica ove del caso, dalla documentazione esibita e da altre evidenze, inclusi i verbali di audi, che le procedure previste per la cessazione di una persona da incarichi connessi con il servizio di PEC siano state effettivamente eseguite.
5. Può richiedere l'esecuzione di procedure documentate per verificarne la dimestichezza da parte del personale a ciò deputato.

12.7 Sicurezza supporti informatici

Finalità: assicurare che i supporti informatici del sistema di PEC siano gestiti in sicurezza onde evitare violazione di riservatezza.

12.7.1 Normativa

CNIPA/CR/49

2.2 Piano per la sicurezza., lettere a), f), g)

12.7.2 Il Gestore

1. Esibisce le procedure di gestione dei supporti informatici, deputati a contenere informazioni relative alle attività di PEC, volte a proteggere gli stessi e in particolare il loro contenuto da accessi non autorizzati (nel caso in cui essi vengano eliminati si deve procedere a sanitisation – capitolo 9.2.6 dello ISO/IEC 27002) e da incidenti quali: mancanza improvvisa di tensione elettrica, blocco del sistema di aria condizionata, allagamenti, ecc..
2. Esibisce le procedure in vigore per la gestione dei supporti informatici, deputati a contenere informazioni relative alle attività di PEC, quali la informazioni sui titolari, il Log e i messaggi contenenti virus, che comprendano anche verifiche sul loro livello di degrado e prevenzione della loro obsolescenza tecnica.

   Qualora la conservazione sostitutiva (come da Del. CNIPA 11/2004) si eseguita a cura di terzi, il Gestore esercita la necessaria diligente vigilanza sull'operato del fornitore.

   Nota: questo si applica anche al caso in cui informazioni e dati relativi alla fornitura del servizio di PEC, non inclusi nel Log di PEC, siano conservati su supporto informatico.
3. Esibisce gli inventari dei supporti informatici in questione.
4. Esibisce i verbali di esecuzione delle procedure di gestione dei supporti informatici in questione.
5. Esibisce verbali di auditing interno ed esterno attestanti la corretta gestione dei supporti informatici.

12.7.3 Il Valutatore

1. Verifica l'esistenza di evidenze, ivi inclusi verbali di audit, dell'esecuzione delle procedure di gestione dei supporti informatici di cui al paragrafo 12.7.2 destinati a contenere informazioni relative alle attività di PEC.

2. Verifica, se del caso a campione, la rispondenza degli inventari dei supporti informatici in questione alla situazione reale.

12.8 Altri aspetti della gestione operativa

Finalità: assicurare che i sistemi di erogazione dei servizi di PEC siano protetti da attacchi provenienti sia dall'esterno sia dall'interno e che dispongano di capacità elaborativa utile a fornire con continuità il servizio richiesto rendendo minimo il rischio di interruzioni di servizio anche in caso di incidente, sottoponendo il tutto a verifiche di auditing..

12.8.1 Normativa

DM 2/11/2005

Articolo 23 - Manuale operativo, commi 1, 2, 3 lettera g)

CNIPA/CR/49

2.1 Manuale operativo, lettera m)

2.2 Piano per la sicurezza, lettere a), f), g).

12.8.2 Il Gestore

1. Esibisce documentazione da cui emerga che gli aspetti di sicurezza indicati al capitolo 12.8.1 sono formalmente assegnati a Responsabili individuati tra quelli indicati nella Relazione sulla Struttura organizzativa consegnata al CNIPA.
2. Esibisce la documentazione, custodita da apposita funzione, delle configurazioni dei sistemi e dei dispositivi di rete utilizzati per la fornitura dei servizi di PEC (vedere ISO/IEC 27002, capitolo 12.4.1, lettera d): "*a configuration control system should be used to keep control of all implemented software as well as the system documentation*") che mostri l'adozione di misure di contrasto a codice dannoso e ad attacchi provenienti sia dall'esterno sia dall'interno; in particolare dovrebbe emergere una procedura che preveda una tempestiva applicazione delle "patch" di sicurezza rilasciate dai produttori del SW utilizzato, dopo attenta valutazione della loro applicabilità e previa fase di collaudo (vedere ISO/IEC 27002, capitolo 15.5.3, lettera d).
3. Esibisce le procedure in vigore, inclusa l'assegnazione delle specifiche responsabilità, atte a tenere i responsabili prontamente aggiornati su problemi concernenti la sicurezza: mailing list, contatti con Computer Emergency Response Team, ecc.
4. Esibisce le procedure in vigore per la revisione almeno periodica della capacità elaborativa.
5. Esibisce verbali di auditing interno e/o esterno da cui risulti la effettiva corrispondenza delle configurazioni operative con quelle descritte nella documentazione di cui al punto 2.
6. Esibisce verbali da cui emergano l'effettivo adeguamento della capacità elaborativa a seguito delle procedure di revisione di cui al punto 4 e il rispetto delle procedure per la gestione dei supporti informatici.

Nota: per quanto è applicabile, le attività relative alle misure di sicurezza devono essere coerenti con il Risk Assessment indicato nel Piano per la sicurezza. Per un maggior dettaglio circa le modalità di effettuazione e gestione del Risk Assessment e la gestione degli incidenti e dei disastri vedere il paragrafo 12.12.

12.8.3 Il Valutatore

1. Verifica l'esistenza delle procedure e della documentazione di cui al paragrafo 12.8.2; in particolare, ma non esclusivamente, verifica l'esistenza di procedure atte a mantenere aggiornato il personale sui problemi di sicurezza.
2. Verifica che dai verbali prodotti risulti:
    a. che le configurazioni esibite per sistemi e reti sono effettivamente corrispondenti a quelle operative (verbali di audit); può effettuare personalmente verifiche in sito a tale scopo;
    b. l'effettiva esecuzione delle procedure di revisione, e conseguente adeguamento, della capacità elaborativa e il rispetto delle procedure per la gestione dei supporti informatici; può effettuare personalmente verifiche per controllare l'effettivo adeguamento delle configurazioni.

12.9 Domini di PEC

Finalità: I messaggi di PEC assicurano le caratteristiche di tracciabilità e di opponibilità a terzi della trasmissione e ricezione fintantoché scambiati tra domini di posta elettronica rispondenti ai requisiti di legge.

12.9.1 Normativa

Dlgs 82/2005

Art. 48 Posta elettronica certificata

All DM 2/11/2005

5 Definizioni

8.3 Colloquio sicuro

12.9.2 Il Gestore

1. Esibisce documentazione e procedure che mostrino che i propri domini di PEC sono composti da sistemi totalmente sotto il controllo del Gestore e che a ogni dominio di PEC è associato un record di tipo "MX" definito all'interno del sistema di risoluzione dei nomi secondo le raccomandazioni della RFC 1912.
2. Esibisce verbali di audit che attestino la rispondenza dei domini di PEC ai requisiti di cui al punto 1.

12.9.3 Il Valutatore

1. Verifica l'esistenza di documentazione e procedure sulle caratteristiche dei domini di PEC del Gestore, come da paragrafo 12.9.2.
2. Verifica l'esistenza di verbali di audit che attestino la rispondenza dei domini di PEC ai requisiti di cui al punto 1 del paragrafo 12.9.2.

12.10 Utilizzo e manutenzione dei sistemi del Gestore

Finalità: utilizzare sistemi affidabili e prodotti protetti da alterazioni e che forniscano sicurezza ai procedimenti a cui afferiscono.

12.10.1 Normativa

DPR 68/2005

Articolo 14 - Elenco dei gestori di posta elettronica certificata, comma 6, lettere a) e d).

12.10.2 Il Gestore

1. Esibisce le procedure di "hardening" dei sistemi e, ove del caso, dei dispositivi utilizzati.
2. Esibisce le procedure di change management di sistemi, dispositivi e reti, che assicurino la valutazione, il collaudo e l'accettazione dei medesimi, o delle modifiche ad essi apportate, prima che essi o le relative modifiche divengano operative (vedere ISO/IEC 27002, capitolo 12.5.1).
3. Esibisce verbali di installazione di sistemi, dispositivi e reti da cui risulti sia un'adeguata fase di prova e collaudo prima dell'attivazione in ambiente operativo, sia, ove del caso, l'esecuzione delle procedure di hardening.
4. Esibisce verbali di auditing che confermino la corretta esecuzione delle procedure di cui ai punti precedenti e, ove del caso, la verifica di assenza di funzioni non necessarie da sistemi e dispositivi.
5. Esegue su incarico del Valutatore accessi ai sistemi, nel rispetto delle procedure di sicurezza, per verificarne la rispondenza alle misure di hardening.

Nota: anche se non previsto esplicitamente dalla normativa, le normali misure di sicurezza (si veda ISO/IEC 27002) richiedono l'uso di ambienti elaborativi separati per lo sviluppo e test, per il collaudo e per la produzione.

12.10.3 Il Valutatore

1. Verifica l'esistenza della documentazione e delle procedure indicate al capitolo 12.10.2.
2. Verifica l'esistenza dei verbali di installazione di cui al punto 3 del paragrafo 12.10.2.
3. Verifica l'esistenza dei verbali di auditing di cui al punto 4 del paragrafo 12.10.2.
4. Può far effettuare in sua presenza verifiche sull'assenza dai sistemi di funzioni non necessarie, in conformità con la procedura di hardening esibita dal Gestore.

12.11 Livelli minimi di servizio

Finalità: Assicurare il livelli minimi di servizio previsti dalla normativa.

12.11.1 Normativa

DPR 68/2005

Articolo 11 - Sicurezza della trasmissione, comma 4

Articolo 13 - Livelli minimi di servizio, comma 1

Articolo 14 - Elenco dei gestori di posta elettronica certificata, comma 6, lettera g)

DM 2/11/2005

Articolo 12 - Livelli di servizio

CNIPA/CR/49

2.1 Manuale operativo

CNIPA/CR/51

5.1 (Invio al CNIPA delle informazioni sulla propria operatività)

12.11.2 Il Gestore

1. Esibisce documentazione e procedure che mostrino che esso misura con continuità il livello di servizio erogato e che ne tiene traccia al duplice scopo di:
    a. rispettare i livelli minimi previsti dal DM 2/11/2005 all'art. 12;
    b. comunicarne i dati al CNIPA con la frequenza prevista al punto 5.1 della CNIPA/CR/51.
2. Esibisce verbali di audit che attestino la regolare rilevazione dei livelli di servizio e la corretta elaborazione dei dati acquisiti.
3. Esegue le operazioni richieste dal Valutatore atte a consentire la misurazione dei livelli di servizio.

12.11.3 Il Valutatore

1. Verifica l'esistenza della documentazione, delle procedure e dei verbali di audit di cui al paragrafo 12.11.2.
2. PUO' chiedere l'esecuzione sotto la sua vigilanza di operazioni atte a consentire la misurazione dei livelli di servizio.

12.12 Gestione incidenti

Finalità: assicurare che ogni incidente sia prontamente segnalato secondo procedure formali, affrontato e gestito in modo da assicurare quanto meno il completamento della trasmissione ed il rilascio delle ricevute.

Nota 1: in questo capitolo viene trattato solo quanto riguarda incidenti di sicurezza che non abbiano conseguenze tali da dover ricorrere alle risorse presenti presso la sede di Disaster Recovery, ove prevista nel Manuale Operativo. Per questo aspetto vedere il paragrafo 2.

Nota 2: La compromissione della chiave privata di firma del Gestore è comunque a priori da considerare un "disastro" in quanto i termini per la revoca e l'emissione dei certificati indicati nel MO Certificati Server potrebbero rendere impossibile il rispetto dei livelli di servizio in questione.

12.12.1 Normativa

DPR 68/2005

Articolo 11 - Sicurezza della trasmissione, comma 4

Articolo 14 - Elenco dei gestori di posta elettronica certificata, comma 6, lettera g)

CNIPA/CR/49 punto 2.2 Piano per la sicurezza

MO Certificati Server punto 9.2 Obblighi del Richiedente

12.12.2 Il Gestore

1. Esibisce le procedure in vigore per la organizzazione della gestione degli incidenti dalle quali emerga che la loro gravità viene tempestivamente valutata da parte di una funzione specifica[6]. Questa documentazione può essere, ove del caso, depurata degli aspetti più riservati, purché sia consentito al Valutatore di effettuare le necessarie verifiche sulla reale operatività delle procedure.

   Tali procedure devono indicare chiaramente almeno:

   a. il piano di addestramento erogato al personale che mostri che il personale medesimo è adeguatamente addestrato e che viene tenuto aggiornato tempestivamente anche sulle procedure di gestione degli incidenti al variare delle soluzioni tecnologiche e organizzative adottate;

   b. le responsabilità assegnate al riguardo a ogni singolo individuo;

   c. le informazioni da riportare sui singoli tipi di incidente e punti deboli del sistema di sicurezza, da chiunque riscontrati;

   d. la periodicità massima entro la quale le procedure stesse devono essere riviste.

2. Esibisce le procedure in vigore per la gestione degli incidenti, o delle vulnerabilità potenzialmente causa di incidenti, dalle quali emerga che vi sono indicate chiaramente le misure da attuare per il ripristino dell'operatività, tali da assicurare il completamento della trasmissione e del rilascio delle ricevute.

3. Esibisce, ove del caso, i verbali sulla registrazione e gestione di incidenti già verificatisi, o di vulnerabilità già segnalate, da cui risulti che essi siano stati gestiti come previsto dalle rispettive procedure.

   Nota 1: Conformemente con la raccomandazione indicata nella Nota del capitolo 12.1 è auspicabile che gli incidenti di sicurezza, attuali o potenziali, siano gestiti come indicato al capitolo 13 dello ISO/IEC 27002 (paragrafo 3.1.2).

4. Esibisce, ove sia trascorso un tempo tale da richiedere l'effettuazione della revisione della procedura di gestione incidenti, i relativi verbali. Qualora nel periodo di tempo interessato si siano verificati incidenti di sicurezza da questi verbali devono emergere la loro gestione e, ove del caso, la conseguente richiesta di adeguamento delle misure di sicurezza. Conseguentemente esibisce documentazione da cui emerga che le misure di sicurezza sono state effettivamente adeguate.

5. Esibisce verbali di auditing interno o esterno che mostrino l'effettiva aderenza dell'organizzazione del Gestore alle proprie procedure di gestione incidenti.

12.12.3 Il Valutatore

1. Il Valutatore verifica la esistenza di documentazione e procedure che mostrino:

   a. l'esistenza delle procedure di gestione degli incidenti e della segnalazione di un loro possibile rischio, ivi compresa l'assegnazione delle responsabilità a singoli individui e l'indicazione puntuale delle informazioni da riportare;

   b. l'addestramento del personale ai fini della gestione degli incidenti;

[6] Si veda anche quanto indicato al paragrafo 14.2.2

c. che tali procedure sono state rispettate nel caso di incidenti o di individuazione di possibili rischi, in particolare che sia stata rispettata la loro tempestiva e formale segnalazione onde consentirne la valutazione da parte della funzione a ciò incaricata;

d. che periodicamente, e al verificarsi di incidenti, o di individuazione di possibili rischi, le procedure di gestione incidenti sono riviste anche in base all'esperienza acquisita con quanto segnalato.

2. Il Valutatore verifica la esistenza di procedure per la gestione degli incidenti, o delle vulnerabilità potenzialmente causa di incidenti, dalle quali emerga che vi sono indicate chiaramente le misure da attuare per il ripristino dell'operatività, tali da assicurare il completamento della trasmissione e del rilascio delle ricevute.

3. Il Valutatore verifica la esistenza, ove del caso, di verbali sulla registrazione e gestione di incidenti già verificatisi, o di vulnerabilità potenzialmente causa di incidenti già segnalate, da cui risulti che le rispettive procedure siano state eseguite.

4. Il Valutatore, ove sia trascorso un tempo tale da richiedere l'effettuazione della revisione della procedura di gestione incidenti, verifica la esistenza dei relativi verbali. Qualora nel periodo di tempo interessato si siano verificati incidenti di sicurezza, da questi verbali devono emergere la loro gestione e, ove del caso, la conseguente richiesta di adeguamento delle misure di sicurezza. Conseguentemente esibisce documentazione da cui emerga che le misure di sicurezza sono state effettivamente adeguate.

5. Il Valutatore verifica la esistenza di verbali di auditing interno o esterno che mostrino l'effettiva aderenza dell'organizzazione del Gestore alle proprie procedure di gestione incidenti.

12.13 Business Continuity management

Premessa: questo capitolo si applica ai Gestori che abbiano indicato nella documentazione consegnata al CNIPA, ai fini del proprio inserimento nell'Elenco dei Gestori di PEC, l'adozione di un piano di gestione dei disastri.

Nota 1: la particolare rilevanza giuridica data alla PEC dalla normativa italiana[7] richiede che il Gestore abbia in essere almeno un sistema che assicuri "la riservatezza, la sicurezza, l'integrità e l'inalterabilità nel tempo delle informazioni" contenute nel log di PEC, come previsto dal DPR 68/2005, art. 6, comma 3. Questo comporta non solo la necessità di conservare in ogni caso il contenuto del log per almeno il periodo di 30 mesi previsto al comma 2 del citato articolo, ma anche quella di poter esibire tale contenuto durante questo periodo. Ne consegue che DEVE esistere un piano per garantire la continuità almeno di questo sia pur limitato servizio del Gestore.

Considerando, inoltre, la responsabilità che grava sui Gestori a seguito dell'art. 48, comma 2 del CAD[8], è da ritenersi quanto meno altamente RACCOMANDABILE l'adozione di un Business Coninuity Plan che, almeno nei casi ai quali sia applicabile tale comma, assicuri agli utenti un servizio affidabile nel suo insieme.

[7] Opponibilità ai terzi di data e ora "di trasmissione e di ricezione di un documento informatico trasmesso mediante posta elettronica certificata" (CAD art. 48, comma 3), prova che un messaggio di posta è stato effettivamente consegnato al destinatario, se utente di PEC (DPR 68/2005, art. 6, comma 3), opponibilità ai terzi del log di PEC (DPR 68/2005, art. 6, comma 7).

[8] "La trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta"

Finalità: assicurare che in caso di disastro le operazioni siano riprese entro i termini dichiarati nel Piano per la sicurezza; la compromissione della chiave privata di firma del Gestore deve essere trattata alla stregua di un disastro tenendo conto di quanto indicato nel MO Certificati Server, relativamente ai tempi di revoca e di emissione di un certificato.

Nota 2: in questo capitolo viene trattato solo quanto riguarda incidenti di sicurezza che abbiano conseguenze tali da dover ricorrere alle risorse presenti presso la sede di Disaster Recovery, ove ciò sia previsto. Per incidenti che non abbiamo tali conseguenze vedere il paragrafo 12.12.

12.13.1 Normativa

Dlgs 82/2005

Art. 48 – comma 2

DPR 68/2005

Articolo 11 - Sicurezza della trasmissione, commi 2 e 4

CNIPA/CR/49

2.2 Piano per la sicurezza, lettere d), e), f), g), h).

12.13.2 Il Gestore

1. Esibisce, ove del caso depurandolo dagli aspetti più riservati purché sia consentito al Valutatore di effettuare le necessarie verifiche, il piano di gestione dei disastri approvato dal management, ove tale piano sia indicato nei documenti consegnati al CNIPA.

   Tale piano DOVREBBE indicare tutte le attività a partire dalla dichiarazione dello stato di Disastro fino alla sua risoluzione e DOVREBBE riguardare le attività del Gestore e dei suoi fornitori relative alla PEC e alla conservazione della relativa documentazione.

   Da tale piano, comprensivo ed eventualmente integrativo di quanto indicato nel Piano per la sicurezza, DOVREBBE emergere quanto segue:

   a. la metodologia di risk assessment adottata relativamente alle attività di PEC;
   b. il criterio di definizione dei livelli di rischio accettabili e come individuarli;
   c. l'individuazione dei rischi di interruzione del servizio correlati ai vari asset (minacce, vulnerabilità e conseguenze sui servizi – impact analysis);
   d. la valutazione del rischio (probabilità che si verifichi, livello, valutazione della possibilità di accettare o di trasferire il rischio).
   e. il tempo massimo previsto per il restart a seconda dei tipi di disastro;
   f. le misure adottate (piano di manutenzione HW e SW, duplicazione di attrezzature elaborative, di dati, reti e servizi ausiliari, ecc.) per assicurare la ripresa del servizio quando necessario ed entro i tempi previsti;
   g. la configurazione dei siti di eventuale disaster recovery e/o di storage backup e i relativi controlli, previsti in modo congruo con le esigenze di sicurezza e con quella di far ripartire il servizio nel più breve tempo possibile;
   h. gli incarichi affidati inequivocabilmente al personale e l'addestramento al riguardo, ivi inclusa l'attribuzione dei privilegi di accesso e attivazione in maniera adeguata a consentire un ritorno all'operatività entro i tempi dichiarati a CNIPA;

i. modalità e frequenza delle prove di restart dei vari aspetti del piano, dal semplice ripristino dei dati a partire dalle copie di back up fino all'attivazione in emergenza delle sedi di disaster recovery;

j. modalità e tempificazione per la revisione del piano stesso.

2. Esibisce documentazione da cui risulti che il contenuto del Business Continuity Plan, ove applicabile, è conforme con quanto indicato nel Piano per la sicurezza.
3. Esibisce, ove sia trascorso un tempo adeguato da richiedere l'effettuazione delle prove di gestione del restart di cui al punto 1.i, i relativi verbali.
4. Esibisce, ove sia trascorso un tempo adeguato da richiedere l'effettuazione della revisioni del piano di gestione incidenti e disastri di cui al precedente punto 1.j, i relativi verbali.
5. Esibisce verbali di auditing interno o esterno che mostrino l'effettiva aderenza dell'organizzazione del Gestore al piano di gestione di incidenti e disastri.
6. Ove richiesto dal Valutatore, gli fornisce assistenza nel verificare l'effettiva esistenza e predisposizione delle misure previste dal piano nel sito principale e nei siti di Disaster Recovery e di storage backup, ivi incluse le procedure esecutive di dettaglio.

12.13.3 Il Valutatore

1. Verifica che esistano documentazione e procedure che mostrino l'esistenza e attuazione del piano di gestione incidenti e disastri, in conformità con quanto indicato al CNIPA nel Piano per la sicurezza, ove applicabile, ivi incluse le risultanze del Risk Assessment, come specificato al riguardo nel paragrafo 12.13.2.
2. Ove applicabile, verifica che dalla documentazione risulti che il contenuto del Business Continuity Plan è conforme con quanto indicato nel Piano per la sicurezza.
3. Verifica, ove applicabile, che le procedure previste per la ripresa delle operazioni siano sviluppate in previsione dei tempi eventualmente comunicati a CNIPA per i casi di disastro, come previsto alla lettera "e" del punto 2.2 (Piano della sicurezza) della CNIPA/CR/49.
4. Verifica, ove applicabile e ove sia trascorso un tempo adeguato da richiedere l'effettuazione delle prove di gestione del restart di cui al precedente punto 1.i del § 12.13.2, i relativi verbali.
5. Verifica, ove applicabile e ove sia trascorso un tempo adeguato da richiedere l'effettuazione della revisioni del piano di gestione incidenti e disastri di cui al precedente punto 1.j del § 12.13.2, l'esistenza dei relativi verbali.
6. Verifica l'esistenza di verbali di auditing interno o esterno che mostrino, ove applicabile, l'effettiva aderenza dell'organizzazione del Gestore al piano di gestione di incidenti e disastri.
7. Può verificare l'effettiva esistenza e predisposizione delle misure previste dal piano nel sito principale e nei siti di Disaster Recovery e di storage backup, ove applicabile, ivi incluse le procedure esecutive di dettaglio.

12.14 Conservazione ed esibizione del log e dei messaggi con virus

Finalità: assicurare la conservazione, per il periodo e con le modalità previste dalla normativa, dei messaggi contenenti virus e del log di PEC.

Nota: per quanto riguarda altri aspetti relativi al log di PEC rifarsi anche al capitolo 9.1, per quanto riguarda altri aspetti relativi ai messaggi contenenti virus rifarsi anche al capitolo 9.7.

12.14.1 Normativa

Dlgs 82/2005

Art. 44 Requisiti per la conservazione dei documenti informatici

DPR 68/2006

Art. 6 - Ricevuta di accettazione e di avvenuta consegna, comma 7

Art 11 - Sicurezza della trasmissione, commi 2, 3).

Articolo 12 - Virus informatici

DM 2/11/2005

Articolo 10 - Conservazione dei log dei messaggi

Articolo 11 - Conservazione dei messaggi contenenti virus e relativa informativa al mittente, commi 1), 3)

All. DM 2/11/2005

6.2 Log

6.4 Punto di ricezione

CNIPA/CR/49

2.1 Manuale operativo., lettera h)

2.2 Piano per la sicurezza, lettere l, m).

CNIPA/CR/51

1.2 (Superamento test di interoperabilità)

12.14.2 Il Gestore

1. Esibisce procedure e documentazione che mostrino le modalità di conservazione e protezione dei record di Log di PEC da accessi non autorizzati prima e dopo il loro processo di estrazione e di marcatura temporale fino alla loro trasmissione al servizio di conservazione sostitutiva, come da Deliberazione CNIPA 11/2004 e sue successive integrazioni o modificazioni.
2. Esibisce procedure e documentazione che mostrino le modalità di conservazione e protezione da accessi non autorizzati dei messaggi contenenti virus fino alla loro trasmissione al servizio di conservazione sostitutiva, come da Deliberazione CNIPA 11/2004 e sue successive integrazioni o modificazioni.
3. Esibisce documentazione che attesti che la conservazione sostitutiva dei record di Log di PEC e dei messaggi contenenti virus avviene secondo la Deliberazione CNIPA 11/2004, se è il Gestore stesso ad eseguirlo. Nel caso in cui tale servizio sia affidato a un fornitore esterno, o ad altro reparto della medesima organizzazione, fornisce documentazione comprovante l'impegno di tale fornitore o diverso reparto a rispettare la predetta norma.
4. Esibisce procedure e documentazione che diano garanzia della possibilità di conservare ed esibire Log di PEC e messaggi contenenti virus per i trenta mesi di cui all'art. 11, comma 3, del DM 2/11/2005 e dell'art. 11, comma 2, del DPR 68/2005, anche in caso di disastro. Ne è elemento indispensabile la replica di tali dati presso siti diversi da quello principale, opportunamente scelti e attrezzati. Ove tale servizio sia fornito da entità esterna esibisce il relativo accordo che assicuri analoghe misure.

Nota: la Deliberazione 11/2004 al comma 1 dell'art. 6 "Obbligo di esibizione" recita: "Il documento conservato deve essere reso leggibile in qualunque momento presso il sistema di conservazione sostitutiva e disponibile, a richiesta, su supporto cartaceo." Ne deriva che tale esibizione deve essere garantita in ogni caso, compreso quello di disastro. E' pertanto necessario che il Gestore, o chi gli fornisce il servizio di Conservazione Sostitutiva, disponga quanto meno di un sito di back-up ove custodire copia di quanto sottoposto a conservazione.

5. Esibisce documentazione e procedure che assicurino l'esibizione dei log e dei messaggi contenenti virus a persone autorizzate.
6. Su richiesta del Valutatore esibisce messaggi contenenti virus, eventualmente inviati dallo stesso Valutatore, come indicato al punto 2 lettera a del paragrafo 9.5.2.3, così come del Log di PEC.
7. Esibisce verbali da cui risulti l'esecuzione delle procedure di cui ai punti precedenti.
8. Esibisce verbali di audit che comprovino la conformità delle procedure relative al punto 2 con la Deliberazione CNIPA 11/2004.

12.14.3 Il Valutatore

1. Verifica l'esistenza di procedure e documentazione che mostrino le modalità di conservazione e protezione dei record di Log di PEC da accessi non autorizzati prima e dopo il loro processo di estrazione e di marcatura temporale fino alla loro trasmissione al servizio di conservazione sostitutiva, come da Deliberazione CNIPA 11/2004 e sue successive integrazioni o modificazioni.
2. Verifica l'esistenza di procedure e documentazione che mostrino le modalità di conservazione e protezione dei messaggi contenenti virus fino alla loro tramissione al servizio di conservazione sostitutiva, come da Deliberazione CNIPA 11/2004 e sue successive integrazioni o modificazioni.
3. Verifica l'esistenza di documentazione e procedure per l'estrazione e marcatura temporale del Log e all'estrazione dei messaggi contenenti virus e per il loro inoltro alla conservazione sostitutiva.
4. Verifica l'esistenza di documentazione attestante l'esistenza di procedure concernenti il Log di PEC e i messaggi contenenti virus atte ad assicurarne, anche in caso di disastro:
    a. la conservazione sostitutiva per almeno i trenta mesi previsti dalla normativa;
    b. la esibizione per il citato periodo di trenta mesi.

    Ove tale conservazione sostitutiva sia affidata dal Gestore a entità esterna, verifica che gli accordi del Gestore con tale entità prevedano quanto sopra indicato.
5. Verifica l'esistenza di documentazione e procedure che assicurino l'esibizione a persone autorizzate dei log e dei messaggi contenenti virus.
6. Può richiedere l'esibizione di messaggi contenenti virus, eventualmente da esso stesso inviati come indicato al punto 2 lettera a del paragrafo 9.5.2.3, così come anche l'esibizione del Log di PEC.
7. Verifica l'esistenza dei verbali di esecuzione delle procedure di cui al capitolo 12.14.2.
8. Verifica l'esistenza di verbali di audit comprovino la conformità delle procedure di conservazione di Log e messaggi contenenti virus con la Deliberazione CNIPA 11/2004 e sue successive integrazioni o modificazioni.

12.15 Pubbliche Amministrazione operanti come Gestori di PEC

Finalità: assicurare che le caselle di PEC attribuite da Pubbliche Amministrazioni a privati siano utilizzate limitatamente ai rapporti intrattenuti tra questi ultimi le citate amministrazioni.

12.15.1 Normativa

Dlgs 82/2005

64. Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni.

DPR 68/2005

Articolo 16 - Disposizioni per le pubbliche amministrazioni, comma 2.

DM 2/11/2005

Articolo 15 - Limiti di utilizzo

CNIPA/CR/49

1, lettera t)

CNIPA/CR/51

1.2 (Superamento test di interoperabilità)

12.15.2 Il Gestore

1. Esibisce procedure, documentazione e verbali di audit che mostrino il rispetto di quanto da esso descritto nella Relazione tecnica prevista dall'art. 15 comma 1 del DM/2/11/2005, lettera b) relativamente:
    a. alle modalità con cui assicurare che le caselle assegnate dal Gestore stesso possano essere utilizzate solo per i rapporti intercorrenti tra i titolari e l'Amministrazione interessata;
    b. alle modalità di autenticazione dei titolari privati delle caselle di PEC nel rispetto di quanto indicato nel Dlgs 82/2005 all'art. 64.
2. Esibisce al Valutatore la documentazione relativa all'utilizzo di caselle assegnate dal Gestore a utenti non appartenenti alla medesima Amministrazione.

12.15.3 Il Valutatore

1. Verifica l'esistenza di documentazione, procedure e verbali di audit che mostrino il rispetto di quanto indicato nella Relazione tecnica prevista dall'art. 15 comma 1 del DM/2/11/2005, lettera b).
2. Da una casella di PEC assegnata al CNIPA dal Gestore come previsto al punto 1.2 della CNIPA/CR/51, invia messaggi a destinatari non appartenenti alla medesima PA da cui la casella gli sia stata assegnata, a fronte del cui invio può chiedere al Gestore la documentazione relativa.
3. Verifica l'esistenza della documentazione relativa all'utilizzo di caselle assegnate dal Gestore a utenti non appartenenti alla medesima Amministrazione.

Capitolo 13

Riferimenti temporali

13.1 Sistema affidabile di acquisizione del tempo

Finalità: il Gestore deve disporre di un sistema di acquisizione del tempo di cui è responsabile, che garantisca che i riferimenti temporali da esso apposti nei messaggi di cui al comma 1 dell'art. 6 del DM 2/11/2005 siano affidabili.

Il Gestore di PEC deve inoltre disporre di un servizio di emissione di marche temporali conforme con la normativa vigente, tramite il quale ottenere le marche temporali da apporre almeno una volta al giorno a quanto estratto dal log di PEC.

13.1.1 Normativa

Dlgs 82/2005

Art. 48 - Posta elettronica certificata, comma 3

DPR 68/2005

Articolo 10 - Riferimento temporale

DM 2/11/2005

Articolo 9 - Riferimento temporale

Articolo 21 - Organizzazione e funzioni del personale del certificatore, comma 1, lettera f)

Articolo 21 - Organizzazione e funzioni del personale del certificatore, comma 1, lettera f)

Articolo 23 - Manuale operativo, commi 1), 2), 3) lettera h)

All. DM 2/11/2005

7.1 Riferimento temporale

7.2 Formato data/ora utente

CNIPA/CR/49

1, lettera p)

2.2 Piano per la sicurezza, lettera n).

13.1.2 Il Gestore

1. Esibisce documentazione che dimostri che al Responsabile del sistema di riferimento temporale, di cui verifica la corrispondenza con quanto dichiarato al CNIPA, sia stato erogato adeguato addestramento, a fronte degli aggiornamenti tecnici e organizzativi di cui all'articolo 22 del DM 2/11/2005, al fine di mantenerne le caratteristiche di esperienza.
2. Esibisce procedure, documentazione e verbali di audit che mostrino l'affidabilità del proprio sistema di riferimento temporale. Tale documentazione deve tra l'altro:
    a. fornire evidenza del corretto funzionamento delle procedure che garantiscono la conformità del riferimento temporale alle norme in vigore,
    b. indicare le modalità di protezione del sistema di acquisizione del tempo,

c. indicare le modalità di verifica della correttezza del tempo acquisito (ad esempio mediante sistemi ridondati),

d. indicare le misure di protezione del sistema di trasmissione ai sistemi di PEC di tale tempo acquisito,

e. indicare i meccanismi di allarme in caso di incidente di sicurezza e le contromisure attuate.

3. Consente al verificatore, sotto la supervisione di proprio personale addetto e nel rispetto delle norme indicate nel Piano della Sicurezza, l'accesso ai locali e ai sistemi dove sono installate le apparecchiature relative al proprio sistema di riferimento temporale.
4. Esibisce la documentazione contrattuale con la TSA e le modalità di acquisizione delle marche temporali da apporre al Log di PEC all'atto della sua estrazione, prima di sottoporlo a conservazione sostitutiva. In aggiunta alle istruzioni consegnate dalla TSA il Gestore deve esibire le proprie procedure operative che indichino in dettaglio le responsabilità e le operazioni da svolgere.
5. Su richiesta del Valutatore fa eseguire, in sicurezza, al personale alcune operazioni sul sistema di riferimento temporale.

13.1.3 Il Valutatore

1. Verifica che dalla documentazione esibita risulti che il Responsabile del sistema di riferimento temporale corrisponda con quanto dichiarato dal Gestore al CNIPA e che ad esso sia stato erogato adeguato addestramento, a fronte degli aggiornamenti tecnici e organizzativi di cui all'articolo 22 del DM 2/11/2005, al fine di mantenerne le caratteristiche di esperienza. (Vedere punto 2 del paragrafo 12.6.3).
2. Verifica l'esistenza della documentazione di cui al punto 2 del paragrafo 13.1.2
3. Accede, sotto la supervisione del personale addetto, e in particolare del Responsabile del sistema di riferimento temporale, e nel rispetto delle norme indicate nel Piano della Sicurezza, ai locali e ai sistemi dove sono installate le apparecchiature relative al sistema di riferimento temporale, onde verificare la esistenza di misure di protezione e di allarme di cui al punto 2 del paragrafo 13.1.2.
4. PUO' far eseguire, in sicurezza, al personale alcune operazioni sul sistema di riferimento temporale, allo scopo di verificarne la familiarità con tale gestione.
5. PUO' verificare l'esistenza della documentazione contrattuale con la TSA e della procedura circa le modalità di acquisizione delle marche temporali.

Capitolo 14

Monitoraggio interoperabilità e livello di servizio

14.1 Test di Interoperabilità (Casella PEC Cnipa)

Finalità: Assicurare l'interoperabilità tra i sistemi dei vari gestori onde garantire che lo scambio di messaggi di PEC avvenga senza soluzione di continuità.

14.1.1 Normativa

DPR 68/2005

Articolo 5, comma 2

CNIPA/CR/51

1.2 (Superamento test di interoperabilità)

1.3 (Obbligatorietà dei test di interoperabilità)

1.4 (Verifiche CNIPA)

14.1.2 Il Gestore

1. Come disposto dalla CNIPA/CR/51 al punto 1.2, mette a disposizione del CNIPA una casella di PEC per tutta la durata della propria attività con la quale il CNIPA può effettuare le verifiche del caso.
2. Esibisce le procedure da attivare qualora i test di interoperabilità sulla propria piattaforma non abbiamo esito positivo.
3. Ove il valutatore lo richieda, esegue, in tutto o in parte, i test previsti dalle prove di interoperabilità

14.1.3 Il Valutatore

1. Verifica che le procedure predisposte dal gestore siano tali da rendere sollecite e risolutive le azioni correttive che il gestore dovrà intraprendere qualora i test di interoperabilità abbiano esito negativo.
2. Può eseguire, in tutto o in parte, la serie di test di interoperabilità

14.2 Comunicazioni a CNIPA – Monitoraggio livello di servizio e Gestione disservizi

Finalità: Assicurare un regolare flusso delle informazioni relative al livello di servizio e ai disservizi che il Gestore deve fornire al CNIPA in base alla normativa.

14.2.1 Normativa

CNIPA/CR/51

3. Modalità di vendita dei servizi di PEC attraverso canali commerciali.

3.1 (Monitoraggio CNIPA)

4. Struttura informativa dei gestori.

4.1 (Obbligo per i Gestori di organizzare una struttura per raccogliere le informazioni sul proprio servizio)

4.2 (Ulteriori richieste CNIPA)

4.3 (Registrazione disservizi)

5. Tempi e modalità delle comunicazioni dirette al CNIPA.

5.1 (Invio al CNIPA delle informazioni sulla propria operatività)

5.2 (Superamento test di interoperabilità)

6. Segnalazioni urgenti al CNIPA di malfunzionamenti gravi.

6.1 (Obbligo di comunicare al CNIPA i disservizi)

6.2 (Obbligo di comunicare i disservizi al CNIPA entro 30 minuti)

7.2 (Sospensione disposta dal CNIPA)

7.3 (Comunicazione al CNIPA della ripresa del servizio e di informazioni sulle cause del disservizio)

FAQ CNIPA/CR/51

6. Segnalazioni urgenti al CNIPA di malfunzionamenti gravi – Punto 6 della circolare 7 dicembre 2006, n. 51.

Quali possono essere esempi di eventi riconducibili alla classificazione riportata nella "Tabella A" allegata alla circolare?

Da quando decorre il termine massimo di trenta minuti previsto al punto 6.2 della circolare?

14.2.2 Il Gestore

1. Esibisce documentazione che mostri che esso dispone di un sistema per la regolare raccolta delle informazioni di cui al punto 5.1 della CNIPA/CR/51, in particolare: "- i livelli di servizio erogati, con riferimento a quelli previsti dal decreto ministeriale".
2. Esibisce documentazione e verbali di audit che mostrino che, nell'ambito delle procedure di rilevazione e gestione degli incidenti (di cui al paragrafo 12.12), vengono gestiti anche gli eventi contraddistinti da uno dei codici 1A, 1B, 2A, 2B, 3A, 3B, secondo quanto riportato nella tabella «A» della CNIPA/CR/51. Questi ultimi in particolare devono dare luogo alle seguenti azioni:
    a. "informare il CNIPA dell'evento occorso, entro trenta minuti dalla rilevazione dell'evento stesso, utilizzando i recapiti e l'apposito modulo indicati nel sito del CNIPA medesimo. La comunicazione deve fornire anche una prima valutazione dell'incidente e le eventuali misure adottate al riguardo." (punto 6.2 della CNIPA/CR/51)
    b. attivare l'autospensione nei casi 1A, 1B
    c. predisporsi per attuare tempestivamente una sospensione su eventuale disposizione del CNIPA per i casi 2A e 2B.

    Nota: nei casi precedenti il Gestore deve fornire "adeguata e tempestiva informativa ai propri utenti ed agli altri gestori", per cui nell'ambito della documentazione esibita, deve mostrare di avere anche predisposto procedure atte a ottemperare a questo requisito.

    Nel caso dei casi 3A e 3B, ovviamente, non è necessario provvedere all'autosospensione, ma è buona norma, laddove il Gestore disponga di un Contact Center, che esso sia tempestivamente tenuto informato, in modo che esso possa trasmettere le informazioni agli utenti che dovessero contattarlo. Anche se questo aspetto riguarda prevalentemente il rapporto commerciale di un Gestore con i propri utenti, è altamente raccomandato provvedere a una esauriente informazione verso l'utenza, in un momento in cui vengono complessivamente espletati sforzi per promuovere la dematerializzazione.
3. Esibisce documentazione e verbali di audit che mostrino che, nell'ambito delle procedure di rilevazione e gestione degli incidenti è organizzato in modo da essere in grado, non appena ripristinata l'operatività, di comunicare al CNIPA l'avvenuta rimozione e fornire parimenti al CNIPA entro una settimana una circostanziata relazione tecnica sull'accaduto e sui provvedimenti adottati in conseguenza.
4. Esibisce documentazione che mostri se i provvedimenti adottati in conseguenza ai malfunzionamenti, e comunicati al CNIPA come da CNIPA/CR/51 – punto 7.3, sono tuttora operativi o se sia stato ritenuto opportuno aggiornarli, documentando la eventuale decisione.
5. Qualora si siano già verificati casi di autosospensione o di sospensione disposta dal CNIPA, esibisce verbali di audit che attestino che tali misure sono state eseguite secondo procedure predisposte e che, qualora si siano verificate anomalie nell'attuarle, sono state riviste le procedure in modo da evitare il ripetersi dei malfunzionamenti.

14.2.3 Il Valutatore

1. Verifica l'esistenza di documentazione che mostri che il Gestore dispone di un sistema per la regolare raccolta delle informazioni di cui al punto 5.1 della CNIPA/CR/51, in particolare: "- i livelli di servizio erogati, con riferimento a quelli previsti dal decreto ministeriale".

2. Verifica l'esistenza di documentazione, procedure, verbali di auditing relativi alla gestione di comportamenti anomali e di malfunzionamenti, ivi compresa la sospensione, come indicato agli altri punti del paragrafo 14.2.2.
3. Verifica la corrispondenza tra i provvedimenti comunicati dal Gestore al CNIPA a seguito di malfunzionamenti, come da CNIPA/CR/51 – punto 7.3, e quelli in essere e, nel caso, verifica l'esistenza di documentazione che spieghi la eventuale decisione di modificarli.
4. Qualora si siano già verificati casi di autosospensione o di sospensione disposta dal CNIPA, verifica l'esistenza di verbali di audit che attestino che tali misure sono state eseguite secondo procedure predisposte e che, qualora si siano verificate anomalie nell'attuarle, sono state riviste le procedure in modo da evitare il ripetersi dei malfunzionamenti.

Capitolo 15

Auditing

Finalità: verificare, tramite ispezioni programmate e non, il rispetto dei requisiti tecnici e di legge che governano l'attività del Gestore.

15.1 Normativa

DM/2/11/2005

Articolo 21 - Organizzazione e funzioni del personale del certificatore, comma 1, lettera c), comma 2

CNIPA/CR/49

1, lettera p)

CNIPA/CR/51

8.1 (Verifiche semestrali da parte dei Gestori)

15.2 Il Gestore

Premessa: le ispezioni di audit periodiche o aperiodiche hanno l'obiettivo di verificare se le procedure che attuano misure tecniche e normative sono rispettate. Uno degli obiettivi di un'organizzazione è quello di ridurre i rischi e di evitare incidenti di tipo tecnico o violazioni delle norme. In aggiunta, pertanto, alle ispezioni previste dalla CNIPA/CR/51 è buona prassi, a cui è opportuno che i gestori si adeguino, esercitare, con personale interno specificamente competente, un costante controllo su quanto è in esercizio, indipendentemente dalle ispezioni formali.

1. Esibisce documentazione che dimostri che al Responsabile dell'auditing, di cui verifica la corrispondenza con quanto dichiarato al CNIPA, sia stato erogato adeguato addestramento, a fronte degli aggiornamenti tecnici e organizzativi di cui all'articolo 22 del DM 2/11/2005, al fine di mantenerne le caratteristiche di esperienza.
2. Esibisce piani e procedure che mostrino l'esecuzione almeno semestrale, e anche estemporanea, di ispezioni effettuate per verificare il rispetto delle procedure da parte:
   a. di personale interno ai singoli reparti operativi;

b. di personale del reparto aziendale preposto ai controlli di qualità e/o all'audit;

c. di enti esterni specializzati.

3. Esibisce verbali delle ispezioni da cui risulti la loro effettuazione almeno semestrale, come previsto dal punto 8.1 della CNIPA/CR/51, o estemporanea ove necessario, e le relative risultanze. A fronte di eccezioni e raccomandazioni sollevate dagli ispettori esibisce al Valutatore documentazione che attesti che sono state intraprese azioni per ovviarvi. In caso contrario esibisce documentazione che motivi le decisioni manageriali in tal senso.

   Nota: sulla necessità di documentare le decisioni manageriali circa l'accettazione dei rischi si rimanda allo ISO/IEC 27002, capitolo 4.2, che riprende al riguardo quanto disposto più in generale dallo ISO/IEC 27001 al capitolo 4.3.1.

4. Esibisce documentazione dalla quale risulti che gli strumenti eventualmente adoperati dagli ispettori per effettuare le verifiche sono protetti da accessi non autorizzati.

5. Consente al Valutatore di richiedere l'effettuazione di controlli e verifiche, anche sugli strumenti eventualmente utilizzati dagli auditor e ispettori.

15.3 Il Valutatore

1. Verifica che dalla documentazione esibita risulti che il Responsabile dell'auditing corrisponda con quanto dichiarato dal Gestore al CNIPA e che ad esso sia stato erogato adeguato addestramento, a fronte degli aggiornamenti tecnici e organizzativi di cui all'articolo 22 del DM 2/11/2005, al fine di mantenerne le caratteristiche di esperienza. (Vedere punto 2 del paragrafo 12.6.3).

2. Verifica l'esistenza di piani di ispezione che prevedano, e di verbali di audit che confermino, l'effettuazione di ispezioni almeno semestrali, come previsto dal punto 8.1 della CNIPA/CR/51, o anche estemporanee ove necessario.

3. Verifica che dalle eccezioni sollevate dagli ispettori siano derivate azioni correttive. In caso contrario verifica l'esistenza di documentazione che motivi le decisioni manageriali in tal senso.

4. Verifica che gli strumenti utilizzati ai fini delle verifiche di auditing siano protetti da accessi non autorizzati.

5. Può richiedere di effettuare controlli e verifiche sugli strumenti utilizzati dagli auditor o dagli ispettori interni onde verificare se non risultino macroscopiche violazioni alle procedure previste per proteggerli da accessi non autorizzati onde evitare manomissioni.

Capitolo 16

Norme sulla Posta Elettronica Certificata

Estratto dal Decreto legislativo 7 marzo 2005, n. 82 – Codice dell'amministrazione digitale, come modificato dal Decreto legislativo 4 aprile 2006, n. 159

Capo I

PRINCIPI GENERALI

Sezione I

Definizioni, finalità e ambito di applicazione

Art. 1. Definizioni.

1. Ai fini del presente codice si intende per:

b) autenticazione informatica: la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso;

c) carta d'identità elettronica: il documento d'identità munito di fotografia del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare;

d) carta nazionale dei servizi: il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni;e) certificati elettronici: gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche;

e) certificati elettronici: gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche;

[omissis]

g) Gestore: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;

h) chiave privata: l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;

i) chiave pubblica: l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche;

p) documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

q) firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;

[omissis]

z) pubbliche amministrazioni centrali: le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le istituzioni universitarie, gli enti pubblici non economici nazionali, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN), le agenzie di cui al decreto legislativo 30 luglio 1999, n. 300;

aa) titolare: la persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica;

bb) validazione temporale: il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.

Art. 2. Finalità e ambito di applicazione.

1. Lo Stato, le regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione.

2. Le disposizioni del presente codice si applicano alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, salvo che sia diversamente stabilito, nel rispetto della loro autonomia organizzativa e comunque nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione.

3. Le disposizioni di cui al capo II concernenti i documenti informatici, le firme elettroniche, i pagamenti informatici, i libri e le scritture, le disposizioni di cui al capo III, relative alla formazione, gestione, alla conservazione, nonché le disposizioni di cui al capo IV relative alla trasmissione dei documenti informatici si applicano anche ai privati ai sensi dell'articolo 3 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

4. Le disposizioni di cui al capo V, concernenti l'accesso ai documenti informatici, e la fruibilità delle informazioni digitali si applicano anche ai gestori di servizi pubblici ed agli organismi di diritto pubblico.

5. Le disposizioni del presente codice si applicano nel rispetto della disciplina rilevante in materia di trattamento dei dati personali e, in particolare, delle disposizioni del codice in materia di protezione dei dati personali approvato con decreto legislativo 30 giugno 2003, n. 196. I cittadini e le imprese hanno, comunque, diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.

6. Le disposizioni del presente codice non si applicano limitatamente all'esercizio delle attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, e consultazioni elettorali.

Art. 32. Obblighi del titolare e del certificatore.

1. Il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di firma e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma.

2. Il Gestore è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno a terzi.

Art. 43 Riproduzione e conservazione dei documenti

1. I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se la riproduzione sia effettuata in modo da garantire la conformità dei documenti agli originali e la loro conservazione nel tempo, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.

Art. 44 Requisiti per la conservazione dei documenti informatici

1. Il sistema di conservazione dei documenti informatici garantisce:

a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'articolo 50, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

b) l'integrità del documento;

c) la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi ì dati di registrazione e di classificazione originari;

d) il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in allegato B a tale decreto.

Art. 45 Valore giuridico della trasmissione

1. I documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, ivi compreso il fax, 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.

2. Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al pro-prio Gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiara-to, nella casella di posta elettronica del destinatario messa a disposizione dal Gestore.

3. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso mediante posta elettronica certificata sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche.

Art. 48 Posta elettronica certificata

1. La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Re-pubblica 11 febbraio 2005, n. 68.

2. La trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta.

3. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso mediante posta elettronica certificata sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presiden-te della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche.

Art. 49 Segretezza della corrispondenza trasmessa per via telematica

1. Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche.

2. Agli effetti del presente codice, gli atti, i dati e i documenti trasmessi per via telematica si considerano, nei confronti del Gestore del sistema di trasporto delle informazioni, di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario

Art. 51 Sicurezza dei dati

1. Le norme di sicurezza definite nelle regole tecniche di cui all'articolo 71 garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati.

Art. 54. Contenuto dei siti delle pubbliche amministrazioni

1. I siti delle pubbliche amministrazioni contengono necessariamente i seguenti dati pubblici:

[OMISSIS]

b) l'elenco delle tipologie di procedimento svolte da ciascun ufficio di livello dirigenziale non generale, il termine per la conclusione di ciascun procedimento ed ogni altro termine procedimentale, il nome del responsabile e l'unità organizzativa responsabile dell'istruttoria e di ogni altro adempimento procedimentale, nonché dell'adozione del provvedimento finale, come individuati ai sensi degli articoli 2, 4 e 5 della legge 7 agosto 1990, n. 241;

Art. 64. Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni.

1. La carta d'identità elettronica e la carta nazionale dei servizi costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'autenticazione informatica.

2. Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'autenticazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano di accertare l'identità del soggetto che richiede l'accesso. L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle mo-dalità di accesso predisposte dalle singole amministrazioni.

3. Ferma restando la disciplina riguardante le trasmissioni telematiche gestite dal Ministero dell'economia e delle finanze e dalle agenzie fiscali, con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica e d'intesa con la Conferenza unificata di cui all'art. 8 del decreto legislativo 28 agosto 1997, n. 281, è fissata la data, comunque non successiva al 31 dicembre 2007, a decorrere dalla quale non è più consentito l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni, con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi. È prorogato alla medesima data il termine relativo alla procedura di accertamento preventivo del possesso della Carta di identità elettronica (CIE), di cui all'articolo 8, comma 5, del decreto del Presidente della Repubblica 2 marzo 2004, n. 117, limitatamente alle richieste di emissione di Carte nazionali dei servizi (CNS) da parte dei cittadini non residenti nei comuni in cui è diffusa la CIE.

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. 28 aprile 2005, n. 97)

IL PRESIDENTE DELLA REPUBBLICA

- Visto l'articolo 87 della Costituzione;
- Visto l'articolo 15, comma 2, della legge 15 marzo 1997, n. 59;
- Visto l'articolo 27, commi 8, lettera e), e 9, della legge 16 gennaio 2003, n. 3;
- Visto l'articolo 17, comma 2, della legge 23 agosto 1988, n. 400;
- Visto l'articolo 14 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Vista la preliminare deliberazione del Consiglio dei Ministri, adottata nella riunione del 25 marzo 2004;

- Espletata la procedura di informazione di cui alla direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, modificata dalla direttiva 98/48/CE del Parlamento europeo e del Consiglio, del 20 luglio 1998, attuata con legge 21 giugno 1986, n. 317, cosi' come modificata dal decreto legislativo 23 novembre 2000, n. 427;
- Acquisito il parere della Conferenza unificata, ai sensi dell'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, espresso nella riunione del 20 maggio 2004;
- Vista la nota del 29 marzo 2004, con la quale e' stato richiesto il parere del Garante per la protezione dei dati personali;
- Udito il parere del Consiglio di Stato, espresso dalla Sezione consultiva per gli atti normativi nell'adunanza del 14 giugno 2004;
- Acquisito il parere delle competenti Commissioni della Camera dei deputati e del Senato della Repubblica;
- Vista la deliberazione del Consiglio dei Ministri, adottata nella riunione del 28 gennaio 2005;
- Sulla proposta del Ministro per la funzione pubblica e del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro dell'economia e delle finanze;

EMANA

il seguente regolamento:

Art. 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 e' 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, nonche' 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.

Art. 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.

Art. 3 - Trasmissione del documento informatico

1. Il comma 1 dell'articolo 14 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e' 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.».

Art. 4 - Utilizzo della posta elettronica certificata

1. La posta elettronica certificata consente l'invio di messaggi la cui trasmissione e' 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, e' 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. Le imprese, nei rapporti tra loro intercorrenti, possono dichiarare la esplicita volontà di accettare l'invio di posta elettronica certificata mediante indicazione nell'atto di iscrizione al registro delle imprese. Tale dichiarazione obbliga solo il dichiarante e può essere revocata nella stessa forma.

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 e' 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.

Art. 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.

Art. 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 e' 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 e' 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 e' 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'artico lo 14, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

Art. 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.

Art. 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.

Art. 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. 445, 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 e' 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.

Art. 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.

Art. 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.

Art. 12 - Virus informatici

1. Qualora il Gestore del mittente riceva messaggi con virus informatici e' 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 e' tenuto a non inoltrarli al destinatario, informando tempestivamente il Gestore del mittente, affinche' 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.

Art. 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.

Art. 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 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.

Art. 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. E' 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 3.

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.

Art. 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.

Art. 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 e' acquisito il concerto del Ministro delle comunicazioni.

Art. 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). Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

DM 2/11/2005 pubblicato sulla Gazzetta Ufficiale N. 266 del 15/11/2005

IL MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE

- Visto l'Articolo 17 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, concernente Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'Articolo 27 della legge 16 gennaio 2003, n. 3;
- Visti gli articoli 8, comma 2, e 14, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante Testo unico sulla documentazione amministrativa, e successive modificazioni;
- Visto il decreto del Presidente del Consiglio dei Ministri 6 maggio 2005, concernente delega di funzioni del Presidente del Consiglio dei Ministri in materia di innovazione e tecnologie al Ministro senza portafoglio, dott. Lucio Stanca;

- Espletata la procedura di notifica alla Commissione europea, di cui alla direttiva 98/34/CE del Parlamento europeo e del Consiglio del 22 giugno 1998, modificata dalla direttiva 98/48/CE del Parlamento europeo e del Consiglio del 20 luglio 1998, recepita nell'ordinamento italiano con il decreto legislativo 23 novembre 2000, n. 427;

- Sentito il Ministro per la funzione pubblica;

DECRETA

CAPO I

PRINCIPI GENERALI

Art. 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 del 27 aprile 2004, n. 98.

Art. 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 D.P.R. n. 68 del 2005.

Art. 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);

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

   k. RFC 3174 (US Secure Hash Algorithm 1 - SHA1);

   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).

Art. 4 - Compatibilità operativa degli standard

1. Il Centro nazionale per l'informatica nella pubblica amministrazione, di seguito denominato CNIPA, 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

Art. 5 - Comunicazione e variazione della disponibilità all'utilizzo della posta elettronica certificata

1. La dichiarazione di cui all'Art. 4, comma 4, del D.P.R. n. 68 del 2005[9], 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 D.P.R. 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.

[9] Art. 4.4: Le imprese, nei rapporti tra loro intercorrenti, possono dichiarare la esplicita volontà di accettare l'invio di posta elettronica certificata mediante indicazione nell'atto di iscrizione al registro delle imprese. Tale dichiarazione obbliga solo il dichiarante e può essere revocata nella stessa forma.

Art. 6 - Caratteristiche dei messaggi gestiti dai sistemi di posta elettronica certificata

1. I 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 immodificata nella casella di posta elettronica certificata di destinazione per permettere la verifica dei dati di certificazione da parte del ricevente.

Art. 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 dal CNIPA 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 al CNIPA documentando tale necessità. Il CNIPA, previa valutazione della richiesta, stabilisce se fornire o meno al Gestore ulteriori certificati di firma.

Art. 8 – Interoperabilità

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

Art. 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.

Art. 10 - Conservazione dei log dei messaggi

1. Al fine della conservazione dei log dei messaggi, di cui alle deliberazioni del CNIPA 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.

Art. 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 del CNIPA in materia di riproduzione e conservazione dei documenti su supporto ottico.

Art. 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 D.P.R. n. 68 del 2005, e consentano il rispetto dei vincoli definiti nei commi 4 e 5 del presente Art. .

Art. 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 D.P.R. n. 68 del 2005.

Art. 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 D.P.R. 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.

Art. 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 D.P.R. n. 68 del 2005, è tenuta a presentare al CNIPA 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 D.P.R. n. 68 del 2005;

   b. avvenga limitatamente ai rapporti di cui al medesimo Art. 16, comma 2.

Art. 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 D.P.R. n. 68 del 2005, forniscono inoltre al CNIPA 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 D.P.R. 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.

Art. 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 D.P.R. n. 68 del 2005 ed intenda esercitare il servizio di posta elettronica certificata in Italia, comunica in via preventiva al CNIPA 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 procedimentali di cui all'Art. 14 del D.P.R. n. 68 del 2005.

Art. 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 dal CNIPA al Gestore al momento dell'iscrizione nell'elenco pubblico di cui all'Art. 14 del D.P.R. n. 68 del 2005.

3. L'elenco pubblico dei gestori di posta elettronica certificata tenuto dal CNIPA 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 dal CNIPA, che lo rende disponibile per via telematica.

Art. 19 - Disciplina dei compiti del CNIPA

1. Il CNIPA 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 D.P.R. n. 68 del 2005.

Art. 20 - Sistema di qualità del Gestore

1. Entro un anno dall'iscrizione del Gestore all'elenco pubblico di cui all'Art. 14 del D.P.R 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 il CNIPA e reso disponibile presso il Gestore.

Art. 21 - Organizzazione e funzioni del personale del Gestore

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).

Art. 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.

Art. 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 il CNIPA.
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.

Il presente decreto è inviato ai competenti organi di controllo ed è pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana.

IL MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE

Allegato al DM 2/11/2005 (G. U. N. 266 del 15/11/2005) – Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata

[OMISSIS]

4 OBIETTIVI E CONTENUTI DEL DOCUMENTO

Il presente documento descrive le regole tecniche relative alle modalità di realizzazione e funzionamento della posta elettronica certificata.

5 DEFINIZIONI

Punto di accesso

È il punto 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*, di imbustamento del *messaggio originale* nella *busta di trasporto*.

Punto di ricezione

È il punto che riceve il messaggio all'interno di un *dominio di posta elettronica certificata*, effettua i controlli sulla provenienza/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 *busta di trasporto.*

Punto di consegna

È il punto che compie la consegna del messaggio nella casella di posta elettronica certificata del *titolare* destinatario. Verifica la provenienza/correttezza del messaggio, emette, a seconda dei casi, la *ricevuta di avvenuta consegna* o l'*avviso di mancata consegna*.

Ricevuta di accettazione

È la ricevuta, contenente i *dati di certificazione*, rilasciata al mittente dal *punto di accesso* a fronte dell'invio di un messaggio di posta elettronica certificata. La ricevuta di accettazione è firmata con la chiave del *Gestore di posta elettronica certificata* del mittente.

Avviso di non accettazione

E' l'avviso che viene emesso quando il Gestore mittente è impossibilitato ad accettare il messaggio in ingresso. La motivazione per cui non è possibile accettare il messaggio è inserita all'interno del testo della ricevuta che esplicita inoltre che il messaggio non potrà essere consegnato al destinatario. L'avviso di non accettazione è firmato con la chiave del *Gestore di posta elettronica certificata* del mittente.

Ricevuta di presa in carico

È emessa dal *punto di ricezione* verso il *Gestore di posta elettronica certificata* mittente per

attestare l'avvenuta presa in carico del messaggio da parte del *dominio di posta elettronica 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. La ricevuta di presa in carico è firmata con la chiave del *Gestore di posta elettronica certificata* del destinatario.

Ricevuta di avvenuta consegna

Il *punto di consegna* fornisce al mittente la ricevuta di avvenuta consegna nel momento in cui il messaggio è inserito nella *casella di posta elettronica certificata* del destinatario. È rilasciata una ricevuta di avvenuta consegna per ogni destinatario al quale il messaggio è consegnato. La ricevuta di avvenuta consegna è firmata con la chiave del *Gestore di posta elettronica certificata* del destinatario.

Ricevuta completa di avvenuta consegna

E' caratterizzata dal contenere in allegato i *dati di certificazione* ed il *messaggio originale*.

Ricevuta breve di avvenuta consegna

E' caratterizzata dal contenere in allegato i *dati di certificazione* ed un estratto del *messaggio originale*.

Ricevuta sintetica di avvenuta consegna

E' caratterizzata dal contenere in allegato i *dati di certificazione*.

Avviso di mancata consegna

Nel caso in cui il Gestore di posta elettronica certificata sia impossibilitato a consegnare il messaggio nella casella di posta elettronica certificata del destinatario, il sistema emette un avviso di mancata consegna per indicare l'anomalia al mittente del *messaggio originale.*

Messaggio originale

È il messaggio originale inviato da un *utente di posta elettronica certificata* prima del suo arrivo al *punto di accesso*. Il messaggio originale è consegnato al *titolare* destinatario per mezzo di una *busta di trasporto* che lo contiene.

Busta di trasporto

È il messaggio creato dal *punto di accesso*, all'interno del quale sono inseriti il *messaggio originale* inviato dall'*utente di posta elettronica certificata* ed i relativi *dati di certificazione*. La busta di trasporto è firmata con la chiave del *Gestore di posta elettronica certificata* mittente. La busta di trasporto è consegnata immodificata nella *casella di posta elettronica certificata* di destinazione per permettere la verifica dei *dati di certificazione* da parte del ricevente.

Busta di anomalia

Quando un messaggio errato/non di posta elettronica certificata deve essere consegnato ad un *titolare*, esso viene inserito in una busta di anomalia per evidenziare al destinatario detta anomalia. La busta di anomalia è firmata con la chiave del *Gestore di posta* elettronica *certificata* del destinatario.

Dati di certificazione

E' un insieme di dati che descrivono il *messaggio originale* e sono certificati dal *Gestore di posta elettronica certificata* del mittente. I dati di certificazione sono inseriti nelle varie ricevute e sono trasferiti al *titolare* destinatario insieme al *messaggio originale* per mezzo di una *busta di trasporto*. Tra i dati di certificazione sono compresi: data ed ora di invio, mittente, destinatario, oggetto, identificativo messaggio, ecc.

Gestore di posta elettronica certificata
È il soggetto che gestisce uno o più *domini di posta elettronica certificata* con i relativi *punti di accesso, ricezione e consegna*. È titolare della chiave usata per la firma delle ricevute e delle buste. Si interfaccia con altri gestori di posta elettronica certificata per l'interoperabilità con altri *titolari*.

Dominio di posta elettronica certificata
Corrisponde ad un dominio DNS dedicato alle caselle di posta elettronica dei *titolari*. All'interno di un dominio di posta elettronica certificata tutte le caselle di posta elettronica certificata devono appartenere a *titolari*. L'elaborazione dei messaggi di posta elettronica certificata (ricevute, buste di trasporto, ecc.) deve avvenire anche nel caso in cui il mittente ed il destinatario appartengano allo stesso dominio di posta elettronica certificata.

Indice dei gestori di posta elettronica certificata
Consiste in un server LDAP posizionato in un'area raggiungibile dai vari *gestori di posta elettronica certificata* che costituisce la struttura tecnica relativa all'elenco pubblico dei gestori di posta elettronica certificata. 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 e delle *buste di trasporto*.

Casella di posta elettronica certificata
È una casella di posta elettronica alla quale è associata una funzione che rilascia delle *ricevute di avvenuta consegna* al ricevimento di messaggi di posta elettronica certificata. Una casella di posta elettronica certificata può essere definita esclusivamente all'interno di un *dominio di posta elettronica certificata*.

Titolare
È il soggetto a cui è assegnata una *casella di posta elettronica certificata*.

Marca temporale
E' 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 del 27 aprile 2004, n. 98.

6 ELABORAZIONE DEI MESSAGGI

6.1 Formato dei messaggi generati dal sistema

Il sistema di PEC genera i messaggi (ricevute, avvisi e buste) in formato MIME. I messaggi sono composti da una parte di testo descrittivo, per l'utente, e da una serie di allegati (messaggio originale, dati di certificazione, ecc.) variabili a seconda della tipologia del messaggio.

Il messaggio (composto dall'insieme delle parti descritte nelle specifiche sezioni del presente allegato) è quindi inserito in una struttura S/MIME v3 in formato CMS, firmata con la chiave privata del Gestore di posta certificata. Il certificato associato alla chiave usata per la firma deve essere incluso in tale struttura. Il formato S/MIME usato per la firma dei messaggi generati dal sistema è il "multipart/signed" (formato .p7s) così come descritto nella RFC 2633 §3.4.3.

I messaggi sono trasferiti tra gestori usando una codifica a 7 bit sia per gli header sia per il corpo del messaggio e gli eventuali allegati.

Per garantire la possibilità di verifica delle firme presenti sui messaggi di posta certificata, sul più ampio numero di client di posta elettronica possibile, i certificati X.509v3 utilizzati dai sistemi di posta elettronica certificata dovranno rispettare il profilo proposto in APPENDICE B.

Per garantire la verificabilità della firma da parte del client di posta ricevente, il mittente del messaggio deve coincidere con quello specificato all'interno del certificato usato per la firma S/MIME. Questo meccanismo comporta che le buste di trasporto riportino nel campo "From" un indirizzo di posta mittente differente da quello del messaggio originale. Al fine di consentire una migliore fruibilità del messaggio da parte dell'utente finale, l'indirizzo di posta mittente del messaggio originale è inserito come "display name" mittente nel messaggio. Ad esempio, per un messaggio originale con il seguente campo "From":

```
From: "Mario Bianchi" <mario.bianchi@dominio.it>
```

la relativa busta di trasporto generata avrà un campo "From" del tipo:

```
From: "Per conto di: mario.bianchi@dominio.it" <posta-certificata@Ge-
store.it>
```

Per consentire che eventuali risposte alla busta di trasporto siano correttamente indirizzate verso il mittente originale, è necessario che l'indirizzo di quest'ultimo sia riportato nel campo "Reply-To" della busta di trasporto. Qualora tale campo non fosse esplicitamente specificato nel messaggio originale, il sistema che genera la busta di trasporto provvede a crearlo estraendolo dal campo "From" del messaggio originale.

Per l'invio delle ricevute, il sistema usa come destinatario esclusivamente il mittente del messaggio originale così come specificato nel dato di "reverse path" del protocollo SMTP. Le ricevute devono essere inviate alla casella di posta certificata del mittente senza tenere conto del campo "Reply-To" eventualmente presente nell'intestazione del messaggio.

Tutti i messaggi generati dal sistema di posta certificata sono identificabili per la presenza di un header specifico.

Ai fini della determinazione dei dati di certificazione fanno fede, per il sistema, gli elementi utilizzati per l'effettivo instradamento del messaggio verso i destinatari. Nelle fasi di colloquio mediante protocollo SMTP (ad esempio presso i punti di accesso e di ricezione) i dati di "reverse path" e "forward path" (comandi "MAIL FROM" e "RCPT TO") sono quindi considerati come dati di certificazione rispettivamente del mittente e dei destinatari. I dati di indirizzamento presenti nel corpo del messaggio (campi "To" e "Cc") sono usati esclusivamente per discriminare tra destinatari primari del messaggio e riceventi in copia, qualora necessario; i dati di indirizzamento presenti nel campo "Ccn" non sono considerati validi dal sistema.

6.2 Log

Durante le fasi di trattamento del messaggio presso i punti di accesso, ricezione e consegna, il sistema deve mantenere traccia delle operazioni svolte. Tutte le attività sono memorizzate su un registro riportante i dati significativi dell'operazione:

- il codice identificativo univoco assegnato al messaggio originale (Message-ID cfr. 6.3)
- la data e l'ora dell'evento
- il mittente del messaggio originale
- i destinatari del messaggio originale
- l'oggetto del messaggio originale
- il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.)
- il codice identificativo (Message-ID) dei messaggi correlati generati (ricevute, errori, ecc.)
- il Gestore mittente

Gli effettivi dati registrati sui singoli log dipendono dalla tipologia dell'operazione tracciata (ricezione di un messaggio, generazione ricevute, ecc.).

Deve essere garantita la possibilità di reperire, a richiesta, le informazioni contenute nei log.

6.3 Punto di accesso

Il punto di accesso consente ad un utente di accedere ai servizi di posta certificata resi disponibili dal proprio Gestore. La possibilità da parte di un utente di accedere ai servizi di PEC deve prevedere necessariamente l'autenticazione dello stesso da parte al sistema (cfr. 8.3). Alla ricezione di un messaggio originale, il punto di accesso:

- effettua dei controlli formali sul messaggio in ingresso;
- genera una ricevuta di accettazione;
- imbusta il messaggio originale in una busta di trasporto.

La ricevuta di accettazione indica al mittente che il suo messaggio è stato accettato dal sistema e certifica la data e l'ora dell'evento. All'interno della ricevuta è presente un testo leggibile dall'utente, un allegato XML con i dati di certificazione in formato elaborabile ed eventuali altri allegati per funzionalità aggiuntive offerte dal Gestore.

Il punto di accesso, utilizzando i dati dell'indice dei gestori di posta certificata (cfr. 7.5), effettua un controllo per ogni destinatario del messaggio originale per verificare se appartengono all'infrastruttura di posta certificata o sono utenti esterni (es. posta Internet). Tale controllo è realizzato verificando l'esistenza (mediante una ricerca "case insensitive") dei domini dei destinatari tra gli attributi "`managedDomains`" presenti all'interno dell'indice dei gestori. La ricevuta di accettazione (ed i relativi dati di certificazione) riporta quindi la tipologia dei vari destinatari per informare il mittente del differente flusso seguito dai due gruppi di messaggi (utenti di posta certificata, utenti esterni).

Deve essere garantita l'univocità dell'identificativo dei messaggi originali accettati nel complesso dell'infrastruttura di posta certificata per consentire una corretta tracciatura dei messaggi e delle relative ricevute. Il formato di tale identificativo è del tipo:

[stringa alfanumerica]@[dominio_di_posta_Gestore]

oppure:

[stringa alfanumerica]@[FQDN_server_di_posta]

Il messaggio originale e la corrispondente busta di trasporto dovranno quindi contenere il seguente campo di header:

`Message-ID: <`*[identificativo messaggio]*`>`

Qualora il client di posta elettronica che colloquia con il punto di accesso avesse già inserito un Message ID all'interno del messaggio originale da inviare, questo dovrà essere sostituito con l'identificativo sopra descritto. Al fine di consentire al mittente l'associazione tra il messaggio inviato e le corrispondenti ricevute, l'eventuale Message ID originariamente presente nel messaggio dovrà essere inserito nel messaggio originale e nelle relative ricevute, avvisi e busta di trasporto. Se presente, il Message ID originale dovrà essere reso disponibile nell'intestazione del messaggio mediante l'inserimento del seguente header:

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

che sarà poi incluso all'interno delle ricevute e della busta di trasporto e riportato nei dati di certificazione (cfr. 7.4).

6.3.1 Controlli formali sui messaggi in ingresso

Al momento dell'accettazione del messaggio il punto di accesso deve garantirne la correttezza formale verificando che:

- nel corpo del messaggio esista un campo "From" riportante un indirizzo email conforme alle specifiche RFC 2822 §3.4.1;
- nel corpo del messaggio esista un campo "To" riportante uno o più indirizzi email conformi alle specifiche RFC 2822 §3.4.1;
- l'indirizzo del mittente del messaggio specificato nei dati di instradamento (reverse path) coincida con quanto specificato nel campo "From" del messaggio;
- gli indirizzi dei destinatari del messaggio specificati nei dati di instradamento (forward path) coincidano con quelli presenti nei campi "To" o "Cc" del messaggio;
- non siano presenti indirizzi dei destinatari del messaggio specificati nel campo "Ccn" del messaggio.

Qualora il messaggio non superi i controlli, il punto di accesso non dovrà accettare il messaggio all'interno del sistema di posta certificata emettendo il relativo avviso di non accettazione.

6.3.2 Avviso di non accettazione per eccezioni formali

Qualora il punto di accesso non possa provvedere all'inoltro del messaggio, a causa del mancato superamento dei controlli formali, viene recapitato al mittente uno specifico avviso di non accettazione.

Per questo avviso di non accettazione gli header contengono i seguenti campi:

```
X-Ricevuta: non-accettazione
Date: [data di emissione ricevuta]
Subject: AVVISO DI NON ACCETTAZIONE: [subject originale]
```

```
From: posta-certificata@[dominio_di_posta]
To: [mittente originale]
X-Riferimento-Message-ID: [Message-ID messaggio originale]
```

Il corpo del messaggio di questa ricevuta è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile, secondo un modello che riporti i seguenti dati:

```
Errore nell'accettazione del messaggio
Il giorno [data] alle ore [ora] ([zona]) nel messaggio
"[subject]" proveniente da "[mittente originale]"
ed indirizzato a:
[destinatario1]
[destinatario2]
è stato rilevato un problema che ne impedisce l'accettazione
a causa di [descrizione errore].
Il messaggio non è stato accettato.
Identificativo messaggio: [identificativo]
```

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare alla ricevuta per permetterne una elaborazione automatica (cfr. 7.4). All'interno della ricevuta potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal Gestore di posta certificata; in nessun caso però potrà essere inserito il messaggio originale.

6.3.3 Ricevuta di accettazione

La ricevuta di accettazione è costituita da un messaggio di posta elettronica inviato al mittente e riportante data ed ora di accettazione, dati del mittente e del destinatario ed oggetto.

Negli header della ricevuta di accettazione sono inseriti i seguenti campi:

```
X-Ricevuta: accettazione
Date: [effettiva data di accettazione]
Subject: ACCETTAZIONE: [subject originale]
From: posta-certificata@[dominio_di_posta]
To: [mittente originale]
X-Riferimento-Message-ID: [Message-ID messaggio originale]
```

Il corpo del messaggio della ricevuta è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile, secondo un modello che riporta i seguenti dati:

```
Ricevuta di accettazione
Il giorno [data] alle ore [ora] ([zona]) il messaggio
"[subject]" proveniente da "[mittente originale]"
ed indirizzato a:
[destinatario1] (["posta certificata" | "posta ordinaria"])
[destinatario2] (["posta certificata" | "posta ordinaria"])
.
.
.
[destinatarion] (["posta certificata" | "posta ordinaria"])
è stato accettato dal sistema ed inoltrato.
Identificativo messaggio: [identificativo]
```

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare alla ricevuta per permetterne una elaborazione automatica. All'interno della ricevuta potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal Gestore di posta certificata.

6.3.4 Busta di trasporto

La busta di trasporto consiste in un messaggio generato dal punto di accesso e che contiene il messaggio originale ed i dati di certificazione.

La busta di trasporto eredita dal messaggio originale i seguenti header che dovranno quindi essere riportati immodificati:

- Received
- To

- Cc
- Return-Path
- Message-ID (così come descritto al punto 6.3)
- X-Riferimento-Message-ID (cfr. 6.3)
- X-TipoRicevuta

Dovranno invece essere modificati, od inseriti se necessario, gli header sotto elencati:

```
X-Trasporto: posta-certificata
Date: [effettiva data di accettazione]
Subject: POSTA CERTIFICATA: [subject originale]
From: "Per conto di: [mittente originale]" <posta-certificata@[domi-
nio_di_posta]>
Reply-To: [mittente originale (inserito solo se assente)]
```

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 un modello che riporti i seguenti dati di certificazione:

```
Messaggio di posta certificata
Il giorno [data] alle ore [ora] ([zona]) il messaggio
"[subject]" è stato inviato da "[mittente originale]"
indirizzato a:
[destinatario1]
[destinatario2]
.
.
.
[destinatarion]
Il messaggio originale è incluso in allegato.
Identificativo messaggio: [identificativo]
```

All'interno della busta di trasporto è inserito in allegato l'intero messaggio originale immodificato in formato conforme alla RFC 2822 (tranne per quanto detto a proposito del Message ID) completo di header, corpo ed eventuali allegati. Nella stessa busta di trasporto è inoltre incluso un allegato XML che specifica in formato elaborabile i dati di certificazione già riportati nel testo ed informazioni aggiuntive sul tipo di messaggio e tipo di ricevuta richiesta (cfr. 7.4). Alla busta di trasporto possono inoltre essere allegati ulteriori elementi opzionali per specifiche funzionalità fornite dal Gestore di posta certificata.

Anche se il campo "From" della busta di trasporto è modificato per consentire la verifica della firma da parte del destinatario, i dati di instradamento della busta di trasporto (forward path e reverse path del messaggio) rimangono immutati rispetto agli stessi dati del messaggio originale.

6.3.5 Avviso di mancata consegna per superamento dei tempi massimi previsti

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 effettuare la consegna del messaggio. Tale comunicazione è effettuata mediante un avviso di mancata consegna per superamento dei tempi massimi nel quale gli header contengono i seguenti campi:

```
X-Ricevuta: preavviso-errore-consegna
Date: [data di emissione ricevuta]
Subject: AVVISO DI MANCATA CONSEGNA PER SUP. TEMPO MASSIMO: [subject ori-
ginale]
From: posta-certificata@[dominio_di_posta]
To: [mittente originale]
X-Riferimento-Message-ID: [Message-ID messaggio originale]
```

Il corpo del messaggio del primo avviso di mancata consegna è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile secondo un modello che riporti i seguenti dati:

```
Avviso di mancata consegna
Il giorno [data] alle ore [ora] ([zona]) il messaggio
"[subject]" proveniente da "[mittente originale]"
e destinato all'utente "[destinatario]"
```

```
non e stato consegnato nelle prime dodici ore dal suo invio. Non esclu-
dendo 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.
Identificativo messaggio: [identificativo]
```

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare all'avviso per permetterne una elaborazione automatica (cfr. 7.4). All'interno all'avviso potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal Gestore di posta certificata; in nessun caso però potrà essere inserito il messaggio originale.

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 e non prima delle 22 ore successive all'invio.

Il corpo del messaggio di questo avviso di mancata consegna, ha gli stessi header del precedente avviso, ed è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile secondo un modello che riporti i seguenti dati:

```
Avviso di mancata consegna
Il giorno [data] alle ore [ora] ([zona]) il messaggio
"[subject]" proveniente da "[mittente originale]"
e destinato all'utente "[destinatario]"
non e stato consegnato nelle ventiquattro ore successive al suo invio. Si
ritiene che la spedizione debba considerarsi non andata a buon fine.
Identificativo messaggio: [identificativo]
```

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare all'avviso per permetterne una elaborazione automatica (cfr. 7.4). All'interno all'avviso potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal Gestore di posta certificata; in nessun caso però potrà essere inserito il messaggio originale.

6.4 Punto di ricezione

Il punto di ricezione permette lo scambio di messaggi di posta certificata tra diversi gestori di posta certificata. È inoltre il punto attraverso il quale messaggi di posta elettronica ordinaria possono essere inseriti nel circuito della posta certificata (cfr. schemi in Appendice A).

Lo scambio di messaggi tra diversi gestori avviene tramite una transazione basata sul protocollo SMTP come definito dalla RFC 2821. Eventuali errori verificatisi nel colloquio SMTP possono essere gestiti mediante i meccanismi standard di notifica degli errori propri del protocollo SMTP come previsto dalle RFC 2821 e RFC 1891. Tale sistema è adottato anche per la gestione di errori transitori in fase di trasmissione SMTP per i quali risulti un superamento del limite temporale di giacenza. Al fine di garantire al mittente una segnalazione dell'errore, coerentemente con le modalità definite nel paragrafo 6.3.5, i sistemi che gestiscono il traffico di posta certificata devono adottare come limite di tempo per la giacenza del messaggio un valore pari a 24 ore.

Il punto di ricezione, a fronte dell'arrivo di un messaggio, effettua la seguente serie di controlli ed operazioni:

- verifica la correttezza/natura del messaggio in ingresso;
- se il messaggio in ingresso è una busta di trasporto corretta ed integra:
  - emette una ricevuta di presa in carico verso il Gestore mittente (cfr. 6.4.1);
  - inoltra la busta di trasporto verso il punto di consegna (cfr. 6.5);
- se il messaggio in ingresso è una ricevuta corretta ed integra o un avviso di posta certificata corretto ed integro:
  - inoltra la ricevuta/avviso verso il punto di consegna;
- se il messaggio in ingresso non risponde ai requisiti per una busta di trasporto o per una ricevuta/avviso corretto ed integro, ma risulta proveniente da un Gestore di posta certificata, quindi supera le verifiche di esistenza, provenienza e validità della firma, il messaggio deve essere propagato verso il destinatario, quindi:
  - imbusta il messaggio in arrivo in una busta di anomalia (cfr. 6.4.2);
  - inoltra la busta di anomalia verso il punto di consegna.

- se il messaggio in ingresso non proviene da un sistema di posta certificata, quindi non supera le verifiche di esistenza, provenienza e validità della firma, viene considerato di posta ordinaria, quindi, se propagato verso il destinatario:
  - imbusta il messaggio in arrivo in una busta di anomalia (cfr. 6.4.2);
  - inoltra la busta di anomalia verso il punto di consegna.

La ricevuta di presa in carico è emessa dal Gestore ricevente il messaggio, nei confronti del Gestore mittente. Il suo fine è quello di consentire il tracciamento del messaggio nel passaggio tra un Gestore ed un altro.

Al ricevimento di un messaggio presso il punto di ricezione, il sistema compie i seguenti controlli, per verificare che la busta di trasporto/ricevuta/avviso sia corretta/integra:

- Controllo dell'esistenza della firma

  il sistema verifica la presenza della struttura S/MIME di firma all'interno del messaggio in ingresso;

- Controllo che la firma sia stata emessa da un Gestore di posta certificata

  il punto di ricezione estrae il certificato usato per la firma del messaggio in ingresso e ne verifica la presenza all'interno dell'indice dei gestori di posta certificata. Per facilitare il controllo, è possibile calcolare l'hash SHA1 del certificato estratto ed effettuare la ricerca "case insensitive" della sua rappresentazione esadecimale all'interno degli attributi "`providerCertificateHash`" presenti nell'indice. Questa operazione consente di individuare agevolmente il Gestore mittente per un successivo e necessario controllo della coincidenza del certificato estratto con quello presente nel record del Gestore;

- Controllo della validità della firma

  è verificata la correttezza della firma S/MIME del messaggio effettuando il ricalcolo degli algoritmi di firma,la verifica della CRL e la validità temporale del certificato. Nel caso di utilizzo di meccanismi di replica locale (cache) dei contenuti delle CRL, deve essere adottato un intervallo di aggiornamento tale da garantire l'attualità del dato, al fine di minimizzare il possibile ritardo tra pubblicazione della revoca da parte della CA ed il recepimento di questa variazione da parte del Gestore;

- Correttezza formale

  il Gestore effettua le verifiche sufficienti e necessarie a garantire gli aspetti di correttezza formale necessari per l'interoperabilità.

Nel caso di messaggi di posta ordinaria in ingresso al sistema di posta certificata, il Gestore deve effettuare un controllo sulla presenza di virus informatici al fine di impedire l'introduzione di messaggi di posta ordinaria potenzialmente pericolosi, nel circuito della posta certificata. Nel caso di presenza di virus informatici in un messaggio di posta ordinaria, questo potrà quindi essere scartato dal punto di ricezione prima dell'ingresso nel circuito della posta certificata, senza quindi un trattamento particolare dell'errore ma con una gestione conforme alle pratiche comunemente adottate per i messaggi sulla rete pubblica.

Quando in fase di ricezione viene rilevata la presenza di un virus all'interno di una busta di trasporto, il Gestore del destinatario emette un avviso di rilevazione virus informatico destinato al punto di consegna del Gestore mittente.

Il Gestore mittente, alla ricezione di un avviso di rilevazione virus informatico, di cui al paragrafo 6.4.3, dovrà :

1. controllare periodicamente quali tipologie di virus non sono state rilevate dal proprio sistema antivirus al fine di comprenderne le motivazioni e verificare l'opportunità di eventuali interventi,
2. inviare gli eventuali avvisi di mancata consegna per virus, destinati al mittente del messaggio.

6.4.1 Ricevuta di presa in carico

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. Le ricevute di presa in carico emesse sono relative ai destinatari ai quali è indirizzato il messaggio in ingresso, così come specificato nei dati di instradamento (forward path e reverse path) della transazione SMTP. All'interno dei dati di certificazione della singola ricevuta di presa in carico sono elencati i destinatari a cui la stessa fa riferimento. 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.

Gli header di una ricevuta di presa in carico contengono i seguenti campi:

```
X-Ricevuta: presa-in-carico
Date: [data di presa in carico]
Subject: PRESA IN CARICO: [subject originale]
From: posta-certificata@[dominio_di_posta]
To: [ricevute Gestore mittente]
X-Riferimento-Message-ID: [Message-ID messaggio originale]
```

L'indirizzo per l'invio delle ricevute al Gestore mittente è ricavato dall'indice dei gestori di posta certificata durante l'interrogazione necessaria per il controllo del soggetto che ha emesso la firma nella verifica del messaggio in ingresso.

Il corpo del messaggio di una ricevuta di presa in carico è composto secondo un modello riportante i seguenti dati:

```
Ricevuta di presa in carico
Il giorno [data] alle ore [ora] ([zona]) il messaggio
"[subject]" proveniente da "[mittente]"
ed indirizzato a:
[destinatario1]
[destinatario2]
.
.
.
[destinatarion]
è stato accettato dal sistema.
Identificativo messaggio: [identificativo]
```

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare alla ricevuta per permetterne una elaborazione automatica (cfr. 7.4). All'interno della ricevuta potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal Gestore di posta certificata.

6.4.2 Busta di anomalia

Nel caso in cui uno dei test evidenzi un errore nel messaggio in arrivo, oppure venga riconosciuto come un messaggio di posta ordinaria e il Gestore preveda la propagazione verso il destinatario, il sistema lo inserisce in una busta di anomalia. Prima della consegna, il messaggio pervenuto al punto di ricezione completo di header, testo ed allegati è inserito in formato conforme alla RFC 2822 come allegato all'interno di un nuovo messaggio che eredita dal messaggio in arrivo i seguenti header che dovranno quindi essere riportati immodificati:

- Received
- To
- Cc
- Return-Path
- Message-ID

Dovranno invece essere modificati, od inseriti se necessario, gli header sotto elencati:

```
X-Trasporto: errore
Date: [data di arrivo del messaggio]
Subject: ANOMALIA MESSAGGIO: [subject originale]
From: "Per conto di: [mittente originale]" <posta-certificata@[domi-
nio_di_posta]>
Reply-To: [mittente originale (inserito solo se assente)]
```

Il corpo della busta di anomalia è composto da un testo che costituisce la parte immediatamente leggibile dal destinatario del messaggio secondo un modello che riporti i seguenti dati:

```
Anomalia nel messaggio
Il giorno [data] alle ore [ora] ([zona]) è stato ricevuto
il messaggio "[subject]" proveniente da "[mittente originale]"
ed indirizzato a:
[destinatario1]
[destinatario2]
.
.
```

```
.
[destinatarion]
Tali dati non sono stati certificati per il seguente errore:
[descrizione sintetica errore riscontrato]
Il messaggio originale è incluso in allegato.
```

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.

Anche se il campo "From" della busta di anomalia è modificato per consentire la verifica della firma da parte del destinatario, i dati di instradamento della busta di anomalia (forward path e reverse path del messaggio) rimangono immutati rispetto agli stessi dati del messaggio originale. In questo modo è garantito sia l'inoltro del messaggio verso i destinatari originari sia il ritorno di eventuali notifiche di errore sul protocollo SMTP (come da RFC 2821 e RFC 1891) al mittente del messaggio.

6.4.3 Avvisi relativi alla rilevazione di virus informatici

6.4.3.1 Avviso di non accettazione per virus informatico

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.

Il punto di accesso deve compiere dei controlli sul contenuto del messaggio in ingresso e non accettarlo qualora all'interno di questo o di uno dei suoi eventuali allegati, fosse identificata la presenza di virus informatici. In questo caso deve essere emesso l'*avviso di non accettazione per virus informatico* per dare chiara comunicazione al mittente dei motivi che hanno portato al rifiuto del messaggio.

Per questo avviso di non accettazione gli header contengono i seguenti campi:

```
X-Ricevuta: non-accettazione
X-VerificaSicurezza: errore
Date: [data di emissione ricevuta]
Subject: AVVISO DI NON ACCETTAZIONE PER VIRUS: [subject originale]
From: posta-certificata@[dominio_di_posta]
To: [mittente originale]
X-Riferimento-Message-ID: [Message-ID messaggio originale]
```

Il corpo del messaggio di questa ricevuta è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile secondo un modello che riporti i seguenti dati:

```
Errore nell'accettazione del messaggio per presenza di virus
Il giorno [data] alle ore [ora] ([zona]) nel messaggio
"[subject]" proveniente da "[mittente originale]"
ed indirizzato a:
[destinatario1]
[destinatario2]
è stato rilevato un problema di sicurezza [identificativo del tipo di con-
tenuto rilevato].
Il messaggio non è stato accettato.
Identificativo messaggio: [identificativo]
```

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare alla ricevuta per permetterne una elaborazione automatica (cfr. 7.4). All'interno della ricevuta potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal Gestore di posta certificata; in nessun caso però potrà essere inserito il messaggio originale.

6.4.3.2 Avviso di rilevazione virus informatico

Qualora il Gestore del destinatario riceva messaggi di posta elettronica certificata con virus informatici è tenuto a non inoltrarli, informando tempestivamente il Gestore del mittente affinchè comunichi al mittente medesimo l'impossibilità di dar corso alla trasmissione.

Nel caso nella fase di ricezione si evidenzi la presenza di virus informatici nel messaggio di posta elettronica certificata la cui provenienza sia stata accertata dalle verifiche effettuate sulla firma del Gestore mittente, il sistema genera un avviso di rilevazione virus da restituire al Gestore mittente indicando come indirizzo quello specificato per le ricevute nell'Indice dei gestori di posta certificata, con l'indicazione dell'errore riscontrato.

Per questo avviso di rilevazione virus gli header contengono i seguenti campi:

```
X-Ricevuta: rilevazione-virus
X-Mittente: [mittente originale]
Date: [data di emissione ricevuta]
Subject: PROBLEMA DI SICUREZZA: [subject originale]
From: posta-certificata@[dominio_di_posta]
To: [ricevute Gestore mittente]
X-Riferimento-Message-ID: [Message-ID messaggio originale]
```

Il corpo del messaggio di questo avviso è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile, secondo un modello che riporti i seguenti dati:

```
Avviso di rilevazione virus informatico
Il giorno [data] alle ore [ora] ([zona]) nel messaggio
"[subject]" proveniente da "[mittente originale]"
e destinato all'utente "[destinatario]"
è stato rilevato un problema di sicurezza [identificativo del tipo di con-
tenuto rilevato].
Identificativo messaggio: [identificativo]
```

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare all'avviso, per permetterne un'elaborazione automatica (cfr. 7.4). All'interno all'avviso potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal Gestore di posta certificata; in nessun caso però potrà essere inserito il messaggio originale.

Nel corpo del messaggio deve essere specificato il motivo per il quale è stato impossibile dar corso alla trasmissione.

6.4.3.3 Avviso di mancata consegna per virus informatico

All'arrivo di un avviso di rilevazione di virus informatico proveniente dal Gestore destinatario, il Gestore del mittente emette un avviso di mancata consegna da restituire al mittente.

Per questo avviso di mancata consegna gli header contengono i seguenti campi:

```
X-Ricevuta: errore-consegna
X-VerificaSicurezza: errore
Date: [data di emissione ricevuta]
Subject: AVVISO DI MANCATA CONSEGNA PER VIRUS: [subject originale]
From: posta-certificata@[dominio_di_posta]
To: [mittente originale]
X-Riferimento-Message-ID: [Message-ID messaggio originale]
```

Il corpo del messaggio di questo avviso di mancata consegna è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile, secondo un modello che riporti i seguenti dati:

```
Avviso di mancata consegna per virus
Il giorno [data] alle ore [ora] ([zona]) nel messaggio
"[subject]" destinato all'utente "[destinatario]"
è stato rilevato un problema di sicurezza [identificativo del tipo di con-
tenuto rilevato].
Il messaggio non è stato consegnato.
Identificativo messaggio: [identificativo]
```

Tutte le informazioni necessarie per la costruzione di questo avviso derivano da quanto contenuto nel correlato avviso di rilevazione virus.

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare all'avviso per permetterne una elaborazione automatica (cfr. 7.4). All'interno dell'avviso potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal Gestore di posta certificata.

Nel corpo del messaggio deve essere specificato il motivo per il quale è stato impossibile dar corso alla trasmissione.

6.5 Punto di consegna

6.5.1 Verifiche sui messaggi in ingresso

All'arrivo del messaggio presso il punto di consegna, il sistema ne verifica la tipologia e stabilisce se deve inviare una ricevuta al mittente. La ricevuta di avvenuta consegna è emessa dopo che il messaggio è stato consegnato nella

casella di posta del destinatario ed esclusivamente a fronte della ricezione di una busta di trasporto valida, identificabile dalla presenza dell'header:

```
X-Trasporto: posta-certificata
```

In tutti gli altri casi (es. buste di anomalia, ricevute), la ricevuta di avvenuta consegna non è emessa. In ogni caso, il messaggio ricevuto dal punto di consegna deve essere consegnato immodificato alla casella di posta del destinatario.

La ricevuta di avvenuta consegna indica al mittente che il suo messaggio è stato effettivamente consegnato al destinatario specificato e certifica la data e l'ora dell'evento tramite un testo leggibile dall'utente ed un allegato XML con i dati di certificazione, oltre ad eventuali allegati per funzionalità aggiuntive offerte dal Gestore.

Se il messaggio pervenuto al punto di consegna non fosse recapitabile alla casella di destinazione, il punto di consegna emette un avviso di mancata consegna (cfr. 6.5.3). L'avviso di mancata consegna è generato, a fronte di un errore, relativo alla consegna di una busta di trasporto corretta.

6.5.2 Ricevuta di avvenuta consegna

6.5.2.1 Ricevuta completa di avvenuta consegna

Le ricevute di avvenuta consegna sono costituite da un messaggio di posta elettronica inviato al mittente che riporta la data e l'ora di avvenuta consegna, i dati del mittente e del destinatario e l'oggetto.

Negli header delle ricevute di avvenuta consegna sono inseriti i seguenti campi:

```
X-Ricevuta: avvenuta-consegna
Date: [data di consegna]
Subject: CONSEGNA: [subject originale]
From: posta-certificata@[dominio_di_posta]
To: [mittente originale]
X-Riferimento-Message-ID: [Message-ID messaggio originale]
```

Il corpo del messaggio di ricevuta è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile, secondo un modello che riporti i seguenti dati di certificazione:

```
Ricevuta di avvenuta consegna
Il giorno [data] alle ore [ora] ([zona]) il messaggio
"[subject]" proveniente da "[mittente originale]"
ed indirizzato a "[destinatario]"
è stato consegnato nella casella di destinazione.
Identificativo messaggio: [identificativo]
```

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare alla ricevuta (cfr. 7.4). All'interno della ricevuta potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal Gestore di posta certificata. La ricevuta di avvenuta consegna è emessa per ognuno dei destinatari a cui è consegnato il messaggio.

Nel rilascio delle ricevute di avvenuta consegna, il sistema distingue tra i messaggi consegnati ai destinatari primari ed i riceventi in copia. Tale verifica è effettuata mediante l'analisi dei campi "To" (destinatari primari) e "Cc" (riceventi in copia) del messaggio rispetto al destinatario oggetto della consegna. Esclusivamente per le consegne relative ai destinatari primari, all'interno della ricevuta di avvenuta consegna, oltre agli allegati descritti, è inserito il messaggio originale completo (header, testo ed eventuali allegati). Il sistema deve adottare una logica cautelativa nella valutazione della tipologia destinatario (primario o ricevente in copia) e nella conseguente decisione di non inserire il messaggio originale nella ricevuta di avvenuta consegna. Qualora il sistema che effettua la consegna non potesse determinare con certezza la natura del destinatario (primario od in copia) per problemi di ambiguità dei campi "To" e "Cc", la consegna dovrà essere considerata come indirizzata ad un destinatario primario ed includere il messaggio originale completo.

6.5.2.2 Ricevuta di avvenuta consegna breve

Al fine di consentire uno snellimento dei flussi, è possibile, per il mittente, richiedere la ricevuta di avvenuta consegna in formato breve. La ricevuta di avvenuta consegna breve inserisce al suo interno il messaggio originale, sostituendone gli allegati con i relativi hash crittografici per ridurre le dimensioni della ricevuta. Per permettere la verifica dei contenuti trasmessi è indispensabile che il mittente conservi gli originali immodificati degli allegati inseriti nel messaggio originale, a cui gli hash fanno riferimento.

Se all'interno della busta di trasporto è presente l'intestazione:

```
X-TipoRicevuta: breve
```

il punto di consegna emette, per i destinatari primari, una ricevuta di avvenuta consegna breve. L'assenza di tale intestazione o un valore diverso da 'breve' o 'sintetica' (cfr 6.5.2.3) comportano l'elaborazione della ricevuta di avvenuta consegna secondo le modalità già descritte al punto 6.5.2.1. Il valore dell'intestazione nella busta di trasporto deriva dal messaggio originale (cfr. 6.3.4) permettendo così al mittente di stabilire il formato delle ricevute di avvenuta consegna relative ai destinatari primari del messaggio originale. Per i destinatari riceventi in copia, le ricevute di avvenuta consegna seguono quanto descritto al punto 6.5.2.

Negli header delle ricevute brevi di avvenuta consegna sono inseriti i seguenti campi:

```
X-Ricevuta: avvenuta-consegna
Date: [data di consegna]
Subject: CONSEGNA: [subject originale]
From: posta-certificata@[dominio_di_posta]
To: [mittente originale]
X-Riferimento-Message-ID: [Message-ID messaggio originale]
```

Il corpo del messaggio di ricevuta è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile, secondo un modello che riporti i seguenti dati di certificazione:

```
Ricevuta breve di avvenuta consegna
Il giorno [data] alle ore [ora] ([zona]) il messaggio
"[subject]" proveniente da "[mittente originale]"
ed indirizzato a "[destinatario]"
è stato consegnato nella casella di destinazione.
Identificativo messaggio: [identificativo]
```

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare alla ricevuta (cfr. 7.4). All'interno della ricevuta potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal Gestore di posta certificata. La ricevuta di avvenuta consegna è emessa per ognuno dei destinatari a cui è consegnato il messaggio.

Alla ricevuta breve di avvenuta consegna è allegato il messaggio originale nel quale rimane inalterata la struttura MIME, ma i cui allegati sono sostituiti da altrettanti file di testo contenenti gli hash del file al quale si vanno a sostituire. Gli allegati sono identificati dalla presenza del parametro "`name`" nell'intestazione "`content-type`" oppure "`filename`" nell'intestazione "`content-disposition`" della parte MIME.

Nel caso di messaggi originali in formato S/MIME è necessario non alterare l'integrità della struttura del messaggio modificando le parti MIME proprie della costruzione S/MIME. La verifica della natura S/MIME del messaggio originale avviene controllando il MIME type dell'entità di livello più alto (coincidente con il messaggio stesso). Un messaggio S/MIME può avere i seguenti MIME type (come da RFC 2633):

- multipart/signed

  Il MIME type rappresenta un messaggio originale firmato dal mittente secondo la struttura descritta dalla RFC 1847. Il messaggio è formato da due parti MIME: la prima che costituisce il messaggio composto dal mittente prima della sua firma e la seconda che contiene i dati di firma. La seconda parte (generalmente di tipo "`application/pkcs7-signature`" oppure "`application/x-pkcs7-signature`") contiene i dati aggiunti durante la fase di firma del messaggio e deve essere lasciata inalterata per non compromettere la struttura complessiva del messaggio;

- `application/pkcs7-mime` oppure `application/x-pkcs7-mime`

  Questi MIME type sono generalmente associati a messaggi crittografati, anche se in alcune particolari implementazioni possono rappresentare messaggi firmati od altri oggetti crittografici. Il messaggio è composto da un unico oggetto CMS contenuto all'interno della parte MIME. Data l'impossibilità di distinguere gli allegati eventualmente presenti all'interno dell'oggetto CMS, la parte MIME viene lasciata intatta senza essere sostituita dal relativo hash, di fatto determinando l'emissione di una ricevuta di avvenuta consegna breve con gli stessi contenuti di una normale ricevuta di avvenuta consegna.

L'individuazione delle parti da non sottoporre alla sostituzione con i corrispondenti hash deve basarsi sul MIME type del messaggio (entità MIME di livello più alto) e sull'eventuale sottostruttura MIME interna. I MIME type

delle parti di livello inferiore così come i nomi dei file delle parti stesse non devono essere usati come elementi discriminanti per evitare ambiguità con allegati utente aventi stessi tipi od estensioni. Nel caso il messaggio originale contenga allegati il cui Content-Type risulti "message/rfc822", ossia contenga un messaggio di posta come allegato, l'intero messaggio allegato viene sostituito con il relativo hash.

In generale, nel caso di messaggi originali in formato S/MIME, 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 nel messaggio originale è presente il MIME Type :`application/pkcs7-mime` oppure `application/x-pkcs7-mime` : 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.

L'algoritmo utilizzato per il calcolo dell'hash è il Secure Hash Algorithm 1 (SHA1), così come descritto dalla RFC 3174 calcolato sull'intero contenuto dell'allegato. Per consentire di distinguere i file contenenti gli hash dai file a cui fanno riferimento, il suffisso "`.hash`" è aggiunto al termine del nome originale del file. L'hash è scritto all'interno del file con rappresentazione esadecimale come un'unica sequenza di 40 caratteri. Il MIME type di questi allegati è impostato a "`text/plain`" per evidenziare la loro natura testuale.

6.5.2.3 Ricevuta sintetica di avvenuta consegna

Se all'interno della busta di trasporto è presente l'intestazione:

```
X-TipoRicevuta: sintetica
```

il punto di consegna emette, sia per i destinatari primari sia per i riceventi in copia, una ricevuta di avvenuta consegna sintetica.

Negli header delle ricevute sintetiche di avvenuta consegna sono inseriti i seguenti campi:

```
X-Ricevuta: avvenuta-consegna
Date: [data di consegna]
Subject: CONSEGNA: [subject originale]
From: posta-certificata@[dominio_di_posta]
To: [mittente originale]
X-Riferimento-Message-ID: [Message-ID messaggio originale]
```

Il corpo del messaggio di ricevuta è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile, secondo un modello che riporti i seguenti dati di certificazione:

```
Ricevuta sintetica di avvenuta consegna
Il giorno [data] alle ore [ora] ([zona]) il messaggio
"[subject]" proveniente da "[mittente originale]"
ed indirizzato a "[destinatario]"
è stato consegnato nella casella di destinazione.
Identificativo messaggio: [identificativo]
```

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare alla ricevuta (cfr. 7.4). All'interno della ricevuta potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal Gestore di posta certificata. La ricevuta di avvenuta consegna è emessa per ognuno dei destinatari a cui è consegnato il messaggio.

Il valore dell'intestazione nella busta di trasporto deriva dal messaggio originale (cfr. 6.3.4) permettendo così al mittente di stabilire il formato delle ricevute di avvenuta consegna relative ai destinatari primari del messaggio originale.

La ricevuta sintetica di avvenuta consegna segue le medesime regole di emissione della ricevuta di avventa consegna; in allegato non contiene il messaggio originale ma contiene esclusivamente il file XML contenente i dati di certificazione descritti nella ricevuta di avvenuta consegna.

6.5.3 Avviso di mancata consegna

Nel caso si verifichi un errore nella fase di consegna del messaggio, il sistema genera un avviso di mancata consegna da restituire al mittente con l'indicazione dell'errore riscontrato.

Per un avviso di mancata consegna gli header contengono i seguenti campi:

```
X-Ricevuta: errore-consegna
Date: [data di emissione ricevuta]
Subject: AVVISO DI MANCATA CONSEGNA: [subject originale]
From: posta-certificata@[dominio_di_posta]
To: [mittente originale]
X-Riferimento-Message-ID: [Message-ID messaggio originale]
```

Il corpo del messaggio di un avviso di mancata consegna è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile secondo un modello che riporti i seguenti dati:

```
Avviso di mancata consegna
Il giorno [data] alle ore [ora] ([zona]) nel messaggio
"[subject]" proveniente da "[mittente originale]"
e destinato all'utente "[destinatario]"
è stato rilevato un errore [errore sintetico].
Il messaggio è stato rifiutato dal sistema.
Identificativo messaggio: [identificativo]
```

Gli stessi dati di certificazione sono inseriti all'interno di un file XML da allegare all'avviso per permetterne un'elaborazione automatica (cfr. 7.4). All'interno dell'avviso potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal Gestore di posta certificata.

7 FORMATI

7.1 Riferimento temporale

Per tutte le operazioni effettuate durante i processi di elaborazione dei messaggi, ricevute, log, ecc. svolte dai punti di accesso/ricezione/consegna è necessario disporre di un accurato riferimento temporale. Tutti gli eventi (generazione di ricevute, buste di trasporto, log, ecc.) che costituiscono la transazione di elaborazione del messaggio presso i punti di accesso, ricezione e consegna devono impiegare un unico valore temporale rilevato all'interno della transazione stessa. In questo modo l'indicazione dell'istante di elaborazione del messaggio è univoca all'interno dei log, delle ricevute, dei messaggi, ecc. generati dal server.

7.2 Formato data/ora utente

Le indicazioni temporali fornite dal servizio in formato leggibile dall'utente (testo delle ricevute, buste di trasporto, ecc.) sono fornite con riferimento all'ora legale vigente al momento indicato per l'operazione. Per la data il formato impiegato è "`gg/mm/aaaa`" mentre per l'indicazione oraria si utilizza "`hh:mm:ss`", dove *hh* è in formato 24 ore. Al dato temporale è fatta seguire tra parentesi la "zona" ossia la differenza (in ore e minuti) tra l'ora legale locale ed UTC. La rappresentazione di tale valore è in formato "`[+|-]hhmm`", dove il primo carattere indica una differenza positiva o negativa.

7.3 Specifiche degli allegati

Di seguito sono riportati i dati caratteristici delle varie componenti di messaggi e ricevute generati dal sistema di posta certificata. Nel caso in cui una delle parti del messaggio contenesse caratteri con valori al di fuori dell'intervallo 0÷127 (7-bit ASCII) la parte dovrà essere adeguatamente codificata in maniera tale da garantire che il messaggio finale sia compatibile con il trasporto a 7 bit previsto (es. quoted-printable, base64).

7.3.1 Corpo del messaggio

Set di caratteri: `ISO-8859-1 (Latin-1)`

MIME type: `text/plain` oppure `multipart/alternative`

Il MIME type `multipart/alternative` può essere utilizzato per aggiungere una versione in formato HTML del corpo dei messaggi generati dal sistema. In questo caso dovranno essere presenti due sotto-parti MIME: una di tipo `text/plain` ed un'altra `text/html`. La parte in formato HTML deve rispettare i seguenti vincoli:

- deve contenere le stesse informazioni riportate nella parte di testo;
- non deve contenere riferimenti ad elementi (es. immagini, suoni, font, style sheet) né interni al messaggio (parti MIME aggiuntive) né esterni (es. ospitati su server del Gestore);
- non deve avere contenuto attivo (es. Javascript, VBscript, Plug-in, ActiveX).

7.3.2 Messaggio originale

MIME type: message/rfc822

Nome allegato: `postacert.eml`

7.3.3 Dati di certificazione

Set di caratteri: UTF-8

MIME type: application/xml

Nome allegato: daticert.xml

7.4 Schema dei dati di certificazione

Di seguito viene indicato il DTD relativo al file XML che conterrà i dati di certificazione da allegare nelle ricevute.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Usare l'elemento "postacert" come radice-->
<!--"tipo" indica la tipologia del messaggio di posta certificata-->
<!--L'attributo "errore" può avere i seguenti valori-->
<!--"nessuno" = nessun errore-->
<!--"no-dest" (con tipo="errore-consegna") = destinatario errato-->
<!--"no-dominio" (con tipo="errore-consegna") = dominio errato-->
<!--"virus" (con tipo="errore-consegna") = virus informatico-->
<!--"virus" (con tipo="non-accettazione") = virus informatico-->
<!--"altro" = errore generico-->
<!ELEMENT postacert (intestazione, dati)>
<!ATTLIST postacert
      tipo (accettazione |
            non-accettazione |
            presa-in-carico |
            avvenuta-consegna |
            posta-certificata |
            errore-consegna |
            preavviso-errore-consegna |
            rilevazione-virus) #REQUIRED
      errore (nessuno |
              no-dest |
              no-dominio |
              virus |
              altro) "nessuno">

<!--Intestazione del messaggio originale-->
<!ELEMENT intestazione (mittente,
                        destinatari+,
                        risposte,
                        oggetto?)>

<!--Mittente (campo "From") del messaggio originale-->
<!ELEMENT mittente (#PCDATA)>

<!--Elenco completo dei destinatari (campi "To" e "Cc")-->
<!--del messaggio originale-->
<!--"tipo" indica la tipologia del destinatario-->
```

```
<!ELEMENT destinatari (#PCDATA)>
<!ATTLIST destinatari
      tipo (certificato | esterno) "certificato">

<!--Valore del campo "Reply-To" del messaggio originale-->
<!ELEMENT risposte (#PCDATA)>

<!--Valore del campo "Subject" del messaggio originale-->
<!ELEMENT oggetto (#PCDATA)>

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

<!--Stringa descrittiva del Gestore che certifica i dati-->
<!ELEMENT Gestore-emittente (#PCDATA)>

<!--Data/ora di elaborazione del messaggio-->
<!--"zona" e' la differenza tra ora legale locale ed UTC in-->
<!--formato "[+|-]hhmm"-->
<!ELEMENT data (giorno, ora)>
<!ATTLIST data
      zona CDATA #REQUIRED>

<!--Giorno in formato "gg/mm/aaaa"-->
<!ELEMENT giorno (#PCDATA)>

<!--Ora locale in formato "hh:mm:ss"-->
<!ELEMENT ora (#PCDATA)>

<!--Identificativo univoco del messaggio-->
<!ELEMENT identificativo (#PCDATA)>

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

<!--Per le buste di trasporto e le ricevute di consegna-->
<!--Indica il tipo di ricevuta richiesto dal mittente-->
<!ELEMENT ricevuta EMPTY>
<!ATTLIST ricevuta
      tipo (completa |
            breve   |
            sintetica ) #REQUIRED>

<!--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)>

<!--Per le ricevute di presa in carico-->
<!--Destinatari per i quali e' relativa la ricevuta-->
<!ELEMENT ricezione (#PCDATA)>

<!--In caso di errore-->
<!--Descrizione sintetica errore-->
<!ELEMENT errore-esteso (#PCDATA)>
```

7.5 Schema indice dei gestori di posta certificata

L'indice dei gestori di posta certificata è realizzato mediante un server LDAP centralizzato che contiene i dati dei gestori e dei relativi domini di posta certificata. La "base root" dell'indice è "`o=postacert`" ed i "DistinguishedName" dei singoli record sono del tipo "`providerName=<nome>,o=postacert`". La ricerca all'interno dell'indice avviene principalmente in modalità "case insensitive" usando gli attributi "`providerCertificateHash`" (in fase di verifica della firma delle buste) o "`managedDomains`" (in fase di accettazione del messaggio). All'interno del record di un singolo Gestore è possibile la presenza di più attributi "`providerCertificate`" e dei relativi "`providerCertificateHash`" per consentire la gestione dei rinnovi dei certificati in scadenza. Il Gestore deve provvedere, con un sufficiente anticipo rispetto alla scadenza del certificato, ad aggiornare il proprio record aggiungendo un nuovo certificato la cui validità può sovrapporsi con il certificato precedente. I precedenti certificati scaduti o revocati non devono essere rimossi dall'indice per consentire la verifica della firma dei messaggi in tempi successivi. L'attributo "LDIFLocationURL" deve puntare ad un oggetto HTTPS, messo a disposizione dal Gestore, che contiene un file in formato LDIF secondo RFC 2849. Per garantirne l'autenticità, tale file dovrà essere firmato dal Gestore per le operazioni proprie del servizio di posta certificata. Il file LDIF, la firma ed il certificato X.509v3, devono essere inseriti in una struttura PKCS#7 in formato binario ASN.1 DER come file con estensione "`.p7m`". Con cadenza giornaliera, il sistema LDAP centralizzato scarica tale file e, dopo le opportune verifiche sulla firma apposta, lo applica sul record relativo al Gestore. Il file LDIF che comprende i dati di tutti i gestori di posta certificata è disponibile, firmato con il metodo descritto per i singoli gestori, come oggetto HTTPS alla URL puntata dall'attributo "`LDIFLocationURL`" del record "`dn: o=postacert`". Mediante tale LDIF i singoli gestori dovranno replicare localmente, con cadenza giornaliera, il contenuto dell'indice al fine di migliorare i tempi di risposta del sistema evitando di effettuare richieste al sistema centrale per ogni fase di elaborazione del messaggio.

È possibile, per il Gestore, definire più record distinti per indicare diversi ambienti operativi secondari amministrati. Ogni record fa riferimento al singolo ambiente operativo secondario per il quale è possibile dichiarare specifici attributi, eventualmente distinti da quelli relativi agli altri ambienti e all'ambiente principale. Tutti i record devono riportare nell'attributo "`providerName`" il nome del Gestore, mentre l'attributo "`providerUnit`" è usato per identificare gli ambienti operativi secondari. I "DistinguishedName" dei record relativi agli ambienti operativi secondari sono del tipo

"`providerUnit=<ambiente>,providerName=<nome>,o=postacert`".

Ogni Gestore deve avere un record associato al proprio ambiente operativo principale distinguibile per l'assenza dell'attributo "`providerUnit`" all'interno del record e del DistinguishedName. I record per gli ambienti secondari non devono riportare l'attributo "`LDIFLocationURL`" che è ricavato, per tutti i record connessi al Gestore, dagli attributi dell'ambiente principale. Nel caso di presenza di ambienti secondari, il file LDIF indicato nel record dell'ambiente principale deve riportare il contenuto di tutti i record di pertinenza del Gestore.

Di seguito sono riportati gli attributi definiti per lo schema dell'indice dei gestori di posta certificata:

Nome attributo	Sintassi	Descrizione
`providerCertificateHash`	IA5 string	Rappresentazione esadecimale (40 caratteri) dell'hash in formato SHA1 del certificato usato dal Gestore per la firma delle ricevute e delle buste
`providerCertificate`	Certificate Binary transfer	Certificato/i usato/i dal Gestore per la firma delle ricevute e delle buste di trasporto
`providerName`	Directory string Single value	Nome del Gestore di posta certificata
`mailReceipt`	IA5 string	Indirizzo di posta elettronica a cui inviare le ricevute di presa in carico

	Single value	
managedDomains	IA5 string	Domini di posta certificata amministrati dal Gestore
LDIFLocationURL	Directory string Single value	URL HTTPS dove è mantenuta la definizione in formato LDIF del record relativo al Gestore (dell'intero indice per il record "dn: o=postacert")
providerUnit	Directory string Single value	Nome dell'ambiente operativo secondario (non presente per l'ambiente principale)

Quello che segue è lo schema LDAP per l'indice dei gestori di posta certificata secondo la sintassi descritta nella RFC 2252:

```
attributetype ( 16572.2.2.1
        NAME 'providerCertificateHash'
        DESC 'Hash SHA1 del certificato X.509 in formato esadecimale'
        EQUALITY caseIgnoreIA5Match
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{40} )

attributetype ( 16572.2.2.2
        NAME 'providerCertificate'
        DESC 'Certificato X.509 in formato binario ASN.1 DER'
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.8 )

attributetype ( 16572.2.2.3
        NAME 'providerName'
        DESC 'Nome del Gestore di posta certificata'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768}
        SINGLE-VALUE )

attributetype ( 16572.2.2.4
        NAME 'mailReceipt'
        DESC 'E-mail a cui inviare le ricevute di presa in carico'
        EQUALITY caseIgnoreIA5Match
        SUBSTR caseIgnoreIA5SubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{256}
        SINGLE-VALUE )

attributetype ( 16572.2.2.5
        NAME 'managedDomains'
        DESC 'Domini gestiti dal Gestore di posta certificata'
        EQUALITY caseIgnoreIA5Match
        SUBSTR caseIgnoreIA5SubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

attributetype ( 16572.2.2.6
        NAME 'LDIFLocationURL'
        DESC 'URL (HTTP) del file LDIF che definisce la entry'
        EQUALITY caseExactMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
        SINGLE-VALUE )

attributetype ( 16572.2.2.7
        NAME 'providerUnit'
```

```
        DESC 'Nome dell'ambiente operativo secondario'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768}
        SINGLE-VALUE )

objectclass ( 16572.2.1.1
        NAME 'LDIFLocationURLObject'
        DESC 'Classe per inserimento di un attributo LDIFLocationURL'
        MAY ( LDIFLocationURL )
        SUP top AUXILIARY )

objectclass ( 16572.2.1.2
        NAME 'provider'
        DESC 'Gestore di posta certificata'
        SUP top
        MUST    ( providerCertificateHash $
                  providerCertificate $
                  providerName $
                  mailReceipt $
                  managedDomains)
        MAY     ( description $
                  LDIFLocationURL $
                  providerUnit) )
```

Il seguente file LDIF rappresenta un esempio di indice dei gestori della posta certificata contenente una "base root" e due gestori fittizi. I certificati inseriti sono due certificati "self-signed" riportati a titolo di esempio:

```
dn: o=postacert
objectclass: top
objectclass: organization
objectClass: LDIFLocationURLObject
o: postacert
LDIFLocationURL: https://igpec.rupa.it/igpec.ldif.p7m
description: Base root per l'indice dei gestori di posta certificata

dn: providerName=Anonima Posta Certificata S.p.A.,o=postacert
objectclass: top
objectclass: provider
providerName: Anonima Posta Certificata S.p.A.
providerCertificateHash: 7E7AEF1059AE0F454F2643A95F69EC3556009239
providerCertificate;binary:: MIIDBjCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQ
 QFADBmMQswCQYDVQQGEwJJVDEpMCcGA1UEChMgQW5vbmltYSBQb3N0YSBDZXJ0aWZp
 Y2F0YSBTLnAuQS4xLDAqBgkqhkiG9w0BCQEWHXBvc3RhLWNlcnRpZmljYXRhQGFucG
 9jZXJ0Lml0MB4XDTAyMTIwOTE3MjQxNVoXDTAzMTIwOTE3MjQxNVowZjELMAkGA1UE
 BhMCSVQxKTAnBgNVBAoTIEFub25pbWEgUG9zdGEgQ2VydGlmaWNhdGEgUy5wLkEuMS
 wwKgYJKoZIhvcNAQkBFh1wb3N0YS1jZXJ0aWZpY2F0YUBhbnBvY2VydC5pdDCBnzAN
 BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAr8J+qKKdxV9LzDMPqwnEy0P8H/KwbI0Szs
 8p6UZajZdpeUK0Ncbrv1QyXZNNtSMC2uL09HDyx8agjgZWdhypnehguiSK3busha15
 RSpMGhiqxmz2b0HhOG73GfalZelqrwqmElna4MNUaLhbOvTd/sqPUS378w5IaIhWxz
 y34XcCAwEAAaOBwzCBwDAdBgNVHQ4EFgQUN8lC0znQWEs0xspZ/aBzsaGvRZMwgZAG
 A1UdIwSBiDCBhYAUN8lC0znQWEs0xspZ/aBzsaGvRZOhaqRoMGYxCzAJBgNVBAYTAk
 lUMSkwJwYDVQQKEyBBbm9uaW1hIFBvc3RhIENlcnRpZmljYXRhIFMucC5BLjEsMCoG
 CSqGSIb3DQEJARYdcG9zdGEtY2VydGlmaWNhdGFAYW5wb2NlcnQuaXSCAQAwDAYDVR
 0TBAUwAwEB/zANBgkqhkiG9w0BAQQFAAOBgQA58BZ+q1qSKpuffzTBpMtbeFkDIxMq
 Ma+ycnxdMNvcWgCm1A9ZiFJsvqYhDDqAXxfHjkrzXuSZkYq6WiQCsLp0aYVy40QCIw
 bOunhrvsxh3vsG5CgN76JzZ95Z/1OCFNhLfqf1VH2NSS8TaYCCi/VO7W1Q1KkcA2Vl
 xlQP7McSUw==
mailReceipt: ricevute@anpocert.it
LDIFLocationURL: https://www.anpocert.it/LDIF/anpocert.ldif.p7m
managedDomains: posta.anpocert.it
managedDomains: cert.azienda.it
managedDomains: costmec.it
```

```
description: Servizi di posta certificata per aziende

dn: providerName=Servizi Postali S.r.l.,o=postacert
objectclass: top
objectclass: provider
providerName: Servizi Postali S.r.l.
providerCertificateHash: e00fdd9d88be0e2cc766b893315caf93d5701a6a
providerCertificate;binary:: MIIDHjCCAoegAwIBAgIBADANBgkqhkiG9w0BAQ
 QFADBuMQswCQYDVQQGEwJJVDEfMB0GA1UEChMWU2Vydml6aSBQb3N0YWxpIFMuci5s
 LjEPMA0GA1UECxMGRC5DLkMuMS0wKwYJKoZIhvcNAQkBFh5wb3N0YS1jZXJ0aWZpY2
 F0YUBzZXJwb3N0YWwuaXQwHhcNMDIxMjA5MTczMjE2WhcNMDMxMjA5MTczMjE2WjBu
 MQswCQYDVQQGEwJJVDEfMB0GA1UEChMWU2Vydml6aSBQb3N0YWxpIFMuci5sLjEPMA
 0GA1UECxMGRC5DLkMuMS0wKwYJKoZIhvcNAQkBFh5wb3N0YS1jZXJ0aWZpY2F0YUBz
 ZXJwb3N0YWwuaXQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKoc7n6zA+sO8N
 ATMcfJ+U2aoDEsrj/cObG3QAN6Sr+lygWxYXLBZNfSDWqL1K4edLr4gCZIDFsq0PIE
 aYZhYRGjhbcuJ9H/ZdtWdXxcwEWN4mwFzlsASogsh5JeqS8db3A1JWkvhO9EUfaCYk
 8YMAkXYdCtLD9s9tCYZeTE2ut9AgMBAAGjgcswgcgwHQYDVR0OBBYEFHPw7VJIoIM3
 VYhuHaeAwpPF5leMMIGYBgNVHSMEgZAwgY2AFHPw7VJIoIM3VYhuHaeAwpPF5leMoX
 KkcDBuMQswCQYDVQQGEwJJVDEfMB0GA1UEChMWU2Vydml6aSBQb3N0YWxpIFMuci5s
 LjEPMA0GA1UECxMGRC5DLkMuMS0wKwYJKoZIhvcNAQkBFh5wb3N0YS1jZXJ0aWZpY2
 F0YUBzZXJwb3N0YWwuaXSCAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQQFAAOB
 gQApqeXvmOyEjwhMrXezPAXELMZwv4qqr5ri4XuxTq6sS9jRsEbZrS+NmbcJ7S7eFw
 NQMNxYFVJqdWoLh8qExsTLXnsKycPSnHbCfuphrKvXjQvR2da75U4zGSkroiyvJ2s9
 TtiCcT3lQtIjmvrFbaSBiyzj+za7foFUCQmxCLtDaA==
mailReceipt: presaincarico@serpostal.it
LDIFLocationURL: https://servizi.serpostal.it/ldif.txt.p7m
managedDomains: servizi-postali.it
managedDomains: postaricevuta.it
description: Servizi di posta certificata per il pubblico
```

Il seguente file LDIF rappresenta un esempio di indice dei gestori della posta certificata contenente una "base root" e due gestori fittizi, il primo dei quali gestisce anche un ambiente secondario. I certificati inseriti sono due certificati "self-signed" riportati a titolo di esempio:

```
dn: o=postacert
objectclass: top
objectclass: organization
objectClass: LDIFLocationURLObject
o: postacert
LDIFLocationURL: https://igpec.rupa.it/igpec.ldif.p7m
description: Base root per l'indice dei gestori di posta certificata

dn: providerName=Anonima Posta Certificata S.p.A.,o=postacert
objectclass: top
objectclass: provider
providerName: Anonima Posta Certificata S.p.A.
providerCertificateHash: 7E7AEF1059AE0F454F2643A95F69EC3556009239
providerCertificate;binary:: MIIDBjCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQ
 QFADBmMQswCQYDVQQGEwJJVDEpMCcGA1UEChMgQW5vbmltYSBQb3N0YSBDZXJ0aWZp
 Y2F0YSBTLnAuQS4xLDAqBgkqhkiG9w0BCQEWHXBvc3RhLWNlcnRpZmljYXRhQGFucG
 9jZXJ0Lml0MB4XDTAyMTIwOTE3MjQxNVoXDTAzMTIwOTE3MjQxNVowZjELMAkGA1UE
 BhMCSVQxKTAnBgNVBAoTIEFub25pbWEgUG9zdGEgQ2VydGlmaWNhdGEgUy5wLkEuMS
 wwKgYJKoZIhvcNAQkBFh1wb3N0YS1jZXJ0aWZpY2F0YUBhbnBvY2VydC5pdDCBnzAN
 BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAr8J+qKKdxV9LzDMPqwnEy0P8H/KwbI0Szs
 8p6UZajZdpeUK0Ncbrv1QyXZNNtSMC2uL09HDyx8agjgZWdhypnehguiSK3busha15
 RSpMGhiqxmz2b0HhOG73GfalZelqrwqmElna4MNUaLhbOvTd/sqPUS378w5IaIhWxz
 y34XcCAwEAAaOBwzCBwDAdBgNVHQ4EFgQUN8lC0znQWEs0xspZ/aBzsaGvRZMwgZAG
 A1UdIwSBiDCBhYAUN8lC0znQWEs0xspZ/aBzsaGvRZOhaqRoMGYxCzAJBgNVBAYTAk
 lUMSkwJwYDVQQKEyBBbm9uaW1hIFBvc3RhIENlcnRpZmljYXRhIFMucC5BLjEsMCoG
 CSqGSIb3DQEJARYdcG9zdGEtY2VydGlmaWNhdGFAYW5wb2NlcnQuaXSCAQAwDAYDVR
 0TBAUwAwEB/zANBgkqhkiG9w0BAQQFAAOBgQA58BZ+q1qSKpuffzTBpMtbeFkDIxMq
 Ma+ycnxdMNvcWgCm1A9ZiFJsvqYhDDqAXxfHjkrzXuSZkYq6WiQCsLp0aYVy40QCIw
 bOunhrvsxh3vsG5CgN76JzZ95Z/1OCFNhLfqf1VH2NSS8TaYCCi/VO7W1Q1KkcA2Vl
```

```
 xlQP7McSUw==
mailReceipt: ricevute@anpocert.it
LDIFLocationURL: http://www.anpocert.it/LDIF/anpocert.ldif.p7m
managedDomains: posta.anpocert.it
managedDomains: cert.azienda.it
managedDomains: costmec.it
description: Servizi di posta certificata per aziende

dn: providerUnit=Ambiente Secondario, providerName=Anonima Posta Ce
 rtificata S.p.A.,o=postacert
objectclass: top
objectclass: provider
providerName: Anonima Posta Certificata S.p.A.
providerUnit: Ambiente Secondario
providerCertificateHash: 7E7AEF1059AE0F454F2643A95F69EC3556009239
providerCertificate;binary:: MIIDBjCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQ
 QFADBmMQswCQYDVQQGEwJJVDEpMCcGA1UEChMgQW5vbmltYSBQb3N0YSBDZXJ0aWZp
 Y2F0YSBTLnAuQS4xLDAqBgkqhkiG9w0BCQEWHXBvc3RhLWNlcnRpZmljYXRhQGFucG
 9jZXJ0Lml0MB4XDTAyMTIwOTE3MjQxNVoXDTAzMTIwOTE3MjQxNVowZjELMAkGA1UE
 BhMCSVQxKTAnBgNVBAoTIEFub25pbWEgUG9zdGEgQ2VydGlmaWNhdGEgUy5wLkEuMS
 wwKgYJKoZIhvcNAQkBFh1wb3N0YS1jZXJ0aWZpY2F0YUBhbnBvY2VydC5pdDCBnzAN
 BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAr8J+qKKdxV9LzDMPqwnEy0P8H/KwbI0Szs
 8p6UZajZdpeUK0Ncbrv1QyXZNNtSMC2uL09HDyx8agjgZWdhypnehguiSK3busha15
 RSpMGhiqxmz2b0HhOG73GfalZelqrwqmElna4MNUaLhbOvTd/sqPUS378w5IaIhWxz
 y34XcCAwEAAaOBwzCBwDAdBgNVHQ4EFgQUN8lC0znQWEs0xspZ/aBzsaGvRZMwgZAG
 A1UdIwSBiDCBhYAUN8lC0znQWEs0xspZ/aBzsaGvRZOhaqRoMGYxCzAJBgNVBAYTAk
 lUMSkwJwYDVQQKEyBBbm9uaW1hIFBvc3RhIENlcnRpZmljYXRhIFMucC5BLjEsMCoG
 CSqGSIb3DQEJARYdcG9zdGEtY2VydGlmaWNhdGFAYW5wb2NlcnQuaXSCAQAwDAYDVR
 0TBAUwAwEB/zANBgkqhkiG9w0BAQQFAAOBgQA58BZ+q1qSKpuffzTBpMtbeFkDIxMq
 Ma+ycnxdMNvcWgCm1A9ZiFJsvqYhDDqAXxfHjkrzXuSZkYq6WiQCsLp0aYVy40QCIw
 bOunhrvsxh3vsG5CgN76JzZ95Z/1OCFNhLfqf1VH2NSS8TaYCCi/VO7W1Q1KkcA2Vl
 xlQP7McSUw==
mailReceipt: ricevute@secondario.anpocert.it
managedDomains: direzione.anpocert.it
managedDomains: personale.anpocert.it
description: Servizi interni aziendali

dn: providerName=Servizi Postali S.r.l.,o=postacert
objectclass: top
objectclass: provider
providerName: Servizi Postali S.r.l.
providerCertificateHash: e00fdd9d88be0e2cc766b893315caf93d5701a6a
providerCertificate;binary:: MIIDHjCCAoegAwIBAgIBADANBgkqhkiG9w0BAQ
 QFADBuMQswCQYDVQQGEwJJVDEfMB0GA1UEChMWU2Vydml6aSBQb3N0YWxpIFMuci5s
 LjEPMA0GA1UECxMGRC5DLkMuMS0wKwYJKoZIhvcNAQkBFh5wb3N0YS1jZXJ0aWZpY2
 F0YUBzZXJwb3N0YWwuaXQwHhcNMDIxMjA5MTczMjE2WhcNMDMxMjA5MTczMjE2WjBu
 MQswCQYDVQQGEwJJVDEfMB0GA1UEChMWU2Vydml6aSBQb3N0YWxpIFMuci5sLjEPMA
 0GA1UECxMGRC5DLkMuMS0wKwYJKoZIhvcNAQkBFh5wb3N0YS1jZXJ0aWZpY2F0YUBz
 ZXJwb3N0YWwuaXQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKoc7n6zA+sO8N
 ATMcfJ+U2aoDEsrj/cObG3QAN6Sr+lygWxYXLBZNfSDWqL1K4edLr4gCZIDFsq0PIE
 aYZhYRGjhbcuJ9H/ZdtWdXxcwEWN4mwFzlsASogsh5JeqS8db3A1JWkvhO9EUfaCYk
 8YMAkXYdCtLD9s9tCYZeTE2ut9AgMBAAGjgcswgcgwHQYDVR0OBBYEFHPw7VJIoIM3
 VYhuHaeAwpPF5leMMIGYBgNVHSMEgZAwgY2AFHPw7VJIoIM3VYhuHaeAwpPF5leMoX
 KkcDBuMQswCQYDVQQGEwJJVDEfMB0GA1UEChMWU2Vydml6aSBQb3N0YWxpIFMuci5s
 LjEPMA0GA1UECxMGRC5DLkMuMS0wKwYJKoZIhvcNAQkBFh5wb3N0YS1jZXJ0aWZpY2
 F0YUBzZXJwb3N0YWwuaXSCAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQQFAAOB
 gQApqeXvmOyEjwhMrXezPAXELMZwv4qqr5ri4XuxTq6sS9jRsEbZrS+NmbcJ7S7eFw
 NQMNxYFVJqdWoLh8qExsTLXnsKycPSnHbCfuphrKvXjQvR2da75U4zGSkroiyvJ2s9
 TtiCcT3lQtIjmvrFbaSBiyzj+za7foFUCQmxCLtDaA==
mailReceipt: presaincarico@serpostal.it
LDIFLocationURL: http://servizi.serpostal.it/ldif.txt.p7m
managedDomains: servizi-postali.it
```

```
managedDomains: postaricevuta.it
description: Servizi di posta certificata per il pubblico
```

8 ASPETTI RELATIVI ALLA SICUREZZA

Di seguito sono riportate le indicazioni che fanno riferimento agli aspetti della sicurezza del sistema di posta elettronica certificata.

8.1 Firma

La chiave privata e le operazioni di firma devono essere gestite utilizzando un dispositivo hardware dedicato, in grado di garantirne la sicurezza in conformità a criteri riconosciuti in ambito europeo o internazionale.

8.2 Autenticazione

La possibilità da parte di un utente di accedere ai servizi di PEC, tramite il punto di accesso, deve prevedere necessariamente l'autenticazione al sistema da parte dell'utente stesso. A titolo esemplificativo, e non esaustivo, le modalità di autenticazione possono prevedere, ad esempio, l'utilizzo di user-id e password o, se disponibili e ritenute modalità necessarie per il livello di servizio erogato, la carta d'identità elettronica o la carta nazionale dei servizi. La scelta della modalità con la quale realizzare l'autenticazione è lasciata al Gestore. L'autenticazione è necessaria per garantire che il messaggio sia inviato da un utente del servizio di posta certificata i cui dati di identificazione siano congruenti con il mittente specificato, al fine di evitare la falsificazione di quest'ultimo.

8.3 Colloquio sicuro

Al fine di garantire l'inalterabilità del messaggio originale spedito dal mittente si realizza l'imbustamento e la firma dei messaggi in uscita dal punto di accesso e la successiva verifica in ingresso al punto di ricezione. Il messaggio originale (completo di header, testo ed eventuali allegati) è inserito come allegato all'interno di una busta di trasporto. La busta di trasporto firmata dal Gestore mittente permette di verificare che il messaggio originale non sia stato modificato durante il suo percorso dal dominio mittente al dominio destinatario.

La sicurezza del colloquio tra mittente e destinatario prevede un meccanismo di protezione per tutte le connessioni previste dall'architettura di posta certificata (tra utente e punto di accesso, tra Gestore e Gestore, tra punto di consegna ed utente) attuato tramite l'impiego di canali sicuri.

L'integrità e la confidenzialità delle connessioni tra il Gestore di posta certificata e l'utente devono essere garantite mediante l'uso di protocolli sicuri. A titolo esemplificativo, e non esaustivo, dei protocolli accettabili per l'accesso figurano quelli basati su TLS (es. IMAPS, POP3S, HTTPS), quelli che prevedono l'attivazione di un colloquio sicuro durante la comunicazione (es. SMTP STARTTLS, POP3 STLS), quelli che realizzano un canale di trasporto sicuro sul quale veicolare protocolli non sicuri (es. IPSec).

Il colloquio tra i gestori deve avvenire con l'impiego del protocollo SMTP su trasporto TLS, come descritto nella RFC 3207. Il punto di ricezione deve prevedere ed annunciare il supporto per l'estensione STARTTLS ed accettare connessioni sia in chiaro (per la posta ordinaria) che su canale protetto. Riguardo il punto di accesso è invece possibile utilizzare unicamente connessioni su canale protetto.

Al fine di garantire la completa tracciabilità nel flusso di messaggi di posta certificata, questi non devono transitare su sistemi esterni al circuito di posta certificata. Nello scambio di messaggi tra gestori diversi, tutte le transazioni devono avvenire tra macchine appartenenti al circuito della posta certificata od a conduzione diretta del Gestore. Gli eventuali sistemi secondari di ricezione dei messaggi per il dominio di posta certificata devono essere sotto il controllo diretto del Gestore. Ad ogni dominio di posta certificata dovrà essere associato un record di tipo "MX" definito all'interno del sistema di risoluzione dei nomi secondo le raccomandazioni della RFC 1912.

8.4 Virus

Un altro aspetto rilevante di sicurezza, che riguarda l'intero sistema di posta elettronica certificata, è relativo all'architettura tecnico/funzionale che deve impedire che la presenza di virus possa compromettere la sicurezza di tutti i possibili messaggi gestiti; deve quindi essere prevista l'istallazione ed il costante aggiornamento di sistemi antivirus che impediscano quanto più possibile ogni infezione, senza però intervenire sul contenuto della posta certificata in accordo con quanto già definito.

8.5 Indice dei gestori di posta elettronica certificata

Il contenuto dell'indice dei gestori di posta elettronica certificata è interrogabile via HTTP su protocollo SSL esclusivamente dai gestori accreditati che disporranno di appositi certificati utente; tale modalità di accesso garantisce l'autenticità, l'integrità e la riservatezza dei dati.

9 APPENDICE A

[OMISSIS]

9.2 Requisiti tecnico funzionali di un client di un sistema di PEC

Nel seguito sono elencati i requisiti che devono essere rispettati da un client, per poter garantire ad un utente di un generico sistema di posta certificata, l'insieme minimo di funzionalità operative:

- gestione del colloquio con i punti di accesso e di consegna mediante l'utilizzo di canali sicuri;
- gestione dell'autenticazione dell'utente in fase di invio e di ricezione dei messaggi;
- supporto del formato MIME secondo RFC 2045 - RFC 2049;
- gestione del media type "`message/rfc822`";
- supporto del set di caratteri "`ISO-8859-1 (Latin-1)`";
- supporto dello standard S/MIME versione 3 come da RFC 2633 per la verifica delle firme delle buste e delle ricevute.

10 APPENDICE B

10.1 Profilo di certificato digitale per la firma elettronica dei messaggi di posta elettronica certificata

10.2 Riferimenti

I seguenti documenti contengono definizioni e indicazioni di riferimento che sono citate all'interno del testo e che costituiscono parte integrante della proposta.

> I riferimenti sono specifici (identificati dalla data di pubblicazione e/o numero di versione o dal numero di versione) oppure non specifici. Per i riferimenti specifici le revisioni successive non sono applicabili mentre lo sono per i riferimenti non specifici.

[1] RFC 2119, "Key words for use in RFCs to Indicate Requirement Levels", IETF, March 1997.
[2] RFC 2822, "Internet Message Format", IETF, April 2001 (rende obsoleto l'RFC 822).
[3] RFC 3280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", IETF, April 2002 (rende obsoleto l'RFC 2459).
[4] RFC 3850, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling", IETF, July 2004 (rende obsoleto l'RFC 2632).
[5] RFC 3851 - "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification" IETF, July 2004 (rende obsoleto l'RFC 2633).

10.3 Introduzione

Le parole chiave "*DEVE*", "*DEVONO*", "*NON DEVE*", "*NON DEVONO*", "*E' RICHIESTO*", "*DOVREBBE*", "*NON DOVREBBE*", "*RACCOMANDATO*", "*NON RACCOMANDATO*" "*PUO'*" e "*OPZIONALE*" nel testo del documento debbono essere interpretate come descritto nel seguito, in conformità alle corrispondenti traduzioni contenute nel documento IETF RFC 2119 [1].

Le parole chiave "*DEVE*" o "*DEVONO*" o "*E' RICHIESTO*" stanno a significare che l'oggetto in questione è un requisito assoluto della definizione.

Le parole chiave "*NON DEVE*" o "*NON DEVONO*" stanno a significare che l'oggetto in questione è un divieto assoluto per la definizione.

Le parole chiave "*DOVREBBE*" o "*RACCOMANDATO*" stanno a significare che, in particolari circostanze, possono esistere valide motivazioni per ignorare la particolare specifica, ma le complete implicazioni di tale scelta debbono essere comprese e pesate con cautela prima di scegliere per un'altra soluzione.

Le parole chiave "*NON DOVREBBE*" o "*NON RACCOMANDATO*" stanno a significare che, in particolari circostanze, possono esistere valide motivazioni perché la specifica sia accettabile o anche utile, ma le complete implicazioni debbono essere comprese e pesate con cautela prima di implementare una soluzione corrispondente.

Le parole chiave "*PUO'*" o "*OPZIONALE*" stanno a significare che una specifica è puramente opzionale. Un soggetto può scegliere di includere l'oggetto perché un particolare mercato lo richieda o perché egli ritenga che il prodotto finale ne risulti migliorato, mentre è possibile che un altro soggetto ometta tale oggetto. Un'implementazione che non include una particolare opzione *DEVE* essere preparata ad interoperare con un'altra implementazione che la include, anche se con ridotte funzionalità. Allo stesso modo, un'implementazione che include una particolare opzione *DEVE* essere preparata ad interoperare con un'altra implementazione che non la include (eccetto per la particolare funzionalità che l'opzione consente).

Così come definito in IETF RFC 3280 [3], si rammenta che per ogni estensione usata all'interno di un certificato deve essere definito se essa verrà marcata critica oppure non critica. Un sistema che utilizzi il certificato *DEVE* rifiutare il certificato stesso se incontra un'estensione marcata critica che non riconosce ed interpreta correttamente, d'altra parte *PUO'* ignorare un'estensione non marcata critica se non la comprende.

10.4 Certificato S/MIME

Nel presente documento è definito il profilo di certificato S/MIME, per l'utilizzo nell'ambito della certificazione di messaggi di posta elettronica certificata effettuato dai gestori del servizio.

Il profilo di certificato S/MIME proposto è basato sugli standard IETF RFC 3850 [4] e RFC 3280 [3] a loro volta basati sullo standard ISO/IEC 9594-8:2001.

10.5 Certificato S/MIME

10.5.1 Informazioni relative al Gestore (subject)

Le informazioni relative al Gestore di PEC titolare del certificato *DEVONO* essere inserite nel campo Subject (Subject DN).

In particolare *DEVE* essere presente nel Subject DN il nome del Gestore del servizio di PEC così come valorizzato nell'attributo providerName pubblicato nell'indice dei gestori PEC (§7.5) . Il providerName del Gestore *DEVE* essere presente nel CommonName oppure nel OrganizationName.

I certificati *DEVONO* contenere un Internet mail address come descritto in RFC 2822 [2]. L'email address *DEVE* essere valorizzato nella estensione subjectAltName e *NON DOVREBBE* essere presente nel Subject Distinguished Name [4(§3)].

subjectDN validi sono:

C=IT, O=AcmePEC S.p.A., CN=Posta Certificata e

C=IT, O=ServiziPEC S.p.A., CN=Posta Certificata

La valorizzazione di altri attributi nel Subject DN, se presente, *DEVE* essere eseguita in conformità allo RFC 3280 [3].

10.5.2 Estensioni del certificato

Le estensioni che *DEVONO* essere presenti nel certificato S/MIME sono:

Key Usage, Authority Key Identifier, Subject Key Identifier, Subject Alternative Name.

L'estensione Basic Constraints (Object ID: 2.5.29.19) *NON DEVE* essere presente [4(§4.4.1)].

La valorizzazione delle estensioni elencate sopra per il profilo descritto è riportata nel seguito.

L'estensione Key Usage (Object ID: 2.5.29.15) *DEVE* avere attivato il bit di digitalSignature (bit 0) e *DEVE* essere marcata critica [4(§4.4.2)].L'estensione *NON DEVE* contenere il bit di nonRepudiation (bit 1) attivato [3(§4.2.1.3)]. L'estensione *PUO'* contenere altri bit attivati corrispondenti ad altri Key Usage, purché ciò non sia in contrasto con quanto indicato in RFC 3280 [3].

L'estensione Authority Key Identifier (Object ID: 2.5.29.35) *DEVE* contenere almeno il campo keyIdentifier e *NON DEVE* essere marcata critica.

L'estensione Subject Key Identifier (Object ID: 2.5.29.14) *DEVE* contenere almeno il campo keyIdentifier e *NON DEVE* essere marcata critica.

L'estensione Subject Alternative Name (Object ID: 2.5.29.17) *DEVE* contenere almeno il campo rfc822Name e *NON DEVE* essere marcata critica.

L'aggiunta di altre estensioni non descritte in questo documento è da considerarsi *OPZIONALE* purché effettuata in conformità allo RFC 3280 [3]; tali estensioni aggiuntive *NON DEVONO* essere marcate critiche [4(§4.4)].

[OMISSIS]

Capitolo 17 Norme attuative del CNIPA

CNIPA/CR/49 - CENTRO NAZIONALE PER L'INFORMATICA NELLA PUBBLICA AMMINISTRAZIONE

CIRCOLARE 24 novembre 2005, n. 49

Modalità per la presentazione delle domande di iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata (PEC), di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.

(G.U. 5 dicembre 2005, n. 283)

La presente circolare indica le modalità con le quali i soggetti, pubblici e privati - che intendono esercitare l'attività di gestori di posta elettronica certificata (PEC), ai sensi dell'art. 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, devono presentare domanda al Centro nazionale per l'informatica nella pubblica amministrazione (di seguito indicato «CNIPA»).

1. Modalità di presentazione delle domande.

La domanda, sottoscritta dal legale rappresentante della pubblica amministrazione o della società richiedente, corredata dei relativi allegati, deve essere inviata, in plico chiuso con l'indicazione del mittente, al CNIPA, via Isonzo 21b - 00198 Roma. La consegna può avvenire tramite servizio pubblico, o privato, oppure a mano nelle ore d'ufficio (9 - 13 e 15 - 17) dei giorni feriali, dal lunedì al venerdì. In caso di consegna a mano, verrà data formale ricevuta di consegna del plico.

In alternativa, la domanda può essere predisposta, per quanto applicabile, in formato elettronico, utilizzando la sottoscrizione con firma digitale, ed essere inviata alla casella di posta elettronica cnipadir@cert.cnipa.it

La domanda deve indicare:

a) la denominazione, o la ragione sociale;

b) la sede legale;

c) il rappresentante legale (nel caso in cui i rappresentanti legali sono più di uno, va indicato il nominativo di ciascuno di loro);

d) l'elenco dei documenti allegati.

E' opportuno che in detta domanda siano indicati anche il nominativo e i recapiti (numeri telefonici, numeri di telefax, indirizzo di posta elettronica) di un referente cui rivolgersi in presenza di problematiche di minore importanza che possono essere risolte anche per le vie brevi.

Al fine di dimostrare il possesso dei requisiti previsti dall'art. 14 del decreto del Presidente della Repubblica n. 68/2005 e di ottemperare a quanto previsto dagli articoli 16, 21, 22 e 23 del decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005, e fatta salva la facoltà di avvalersi delle dichiarazioni sostitutive previste dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante «Testo unico sulla documentazione amministrativa», nel seguito indicato «Testo unico», alla domanda devono essere allegati:

a) una copia autentica dell'atto costitutivo della società;

b) una copia dello statuto sociale aggiornato, rilasciato dalla competente Camera di commercio industria artigianato e agricoltura in data non anteriore a novanta giorni rispetto alla data di presentazione della domanda stessa;

c) il certificato di iscrizione nel registro delle imprese, con dicitura antimafia, rilasciato in data non anteriore a novanta giorni rispetto alla data di presentazione della domanda;

d) una dichiarazione rilasciata dall'organo preposto al controllo o dal soggetto incaricato della revisione contabile ai sensi della normativa vigente, in data non anteriore a trenta giorni rispetto alla data di presentazione della domanda, attestante l'entità del capitale sociale versato, nonché l'ammontare e la composizione del patrimonio netto;

e) un prospetto della situazione patrimoniale, predisposto e approvato dall'organo amministrativo, di data non anteriore a centottanta giorni rispetto a quella di presentazione della domanda (sono tenute a questo adempimento solo le società già operative);

f) una relazione dell'organo preposto al controllo, o del soggetto incaricato della revisione contabile, redatta ai sensi della normativa vigente, sulla situazione patrimoniale di cui alla lettera e);

g) documentazione equivalente a quella prevista ai punti precedenti, legalizzata ai sensi dell'art. 33 del Testo unico (sono tenute a questo adempimento le società costituite all'estero ed aventi sede in Italia);

h) un elenco nominativo che rechi l'indicazione del/dei rappresentante/i legale/i, dei componenti dell'organo di amministrazione e dell'organo di controllo, nonché di eventuali altri soggetti preposti all'amministrazione, con l'individuazione dei relativi poteri. Ognuno dei suddetti soggetti dovrà risultare in possesso, all'atto della domanda, dei requisiti di onorabilità previsti dall'art. 14 del decreto del Presidente della Repubblica n. 68/2005, comprovati:

   1. per i cittadini italiani residenti in Italia:
      aa) dalla dichiarazione sostitutiva di atto di notorietà;
      bb) dal certificato del casellario giudiziale;
      cc) dal certificato relativo ai carichi pendenti;

   2. per le persone che non rientrano nella categoria di cui al precedente alinea:
      aa) dalla dichiarazione, resa davanti a pubblico ufficiale;
      bb) dai certificati attestanti che il soggetto non e' fallito o sottoposto a procedura equivalente.

Le firme apposte sulla documentazione anzidetta devono esser legalizzate con le modalità previste dal citato Testo unico. In alternativa, per i soggetti iscritti nell'albo di cui all'art. 13 del decreto legislativo 1° settembre 1993, n. 385, recante: «Testo unico delle leggi in materia bancaria e creditizia», la dimostrazione del possesso dei requisiti di onorabilità potrà essere assolta mediante apposita dichiarazione sostitutiva di certificazione, resa ai sensi dell'art. 46 del testo unico dal legale rappresentante, comprovante l'iscrizione nel suddetto albo alla data di presentazione della domanda di iscrizione;

i) una copia della polizza assicurativa, o certificato provvisorio impegnativo, stipulata per la copertura dei rischi derivanti dall'attività e dagli eventuali danni causati a terzi, rilasciata da una società di assicurazione abilitata ad esercitare nel campo dei rischi industriali a norma delle vigenti disposizioni;

l) una copia dell'ultimo bilancio, e relativa certificazione, se la società e' stata costituita da più di un anno;

m) una dichiarazione, rilasciata dal presidente della società, attestante la composizione dell'azionariato, con l'indicazione, comunque, dei soggetti partecipanti, in forma diretta o indiretta, al capitale sociale medesimo, in misura superiore al 5%, nonché della data a cui si riferisce detta dichiarazione;

n) una copia del manuale operativo, redatto come indicato al successivo punto 2.1, sottoscritto da un soggetto munito di potere di firma;

o) una copia del piano per la sicurezza, redatto come indicato al successivo punto 2.2, sottoscritto e siglato in ogni foglio da un soggetto munito di potere di firma;

p) una relazione sulla struttura organizzativa, debitamente sottoscritta dal legale rappresentante, che contenga, oltre all'elenco del personale addetto all'erogazione del servizio e dei compiti allo stesso affidati, l'indicazione:

   1. dei nomi dei responsabili delle attività di cui all'art. 21 del decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005;
   2. dei requisiti di competenza ed esperienza del personale di cui al punto precedente;
   3. dello specifico ruolo che il Gestore svolge all'interno della struttura aziendale;
   4. della ripartizione delle varie mansioni svolte nella struttura organizzativa e delle connesse responsabilità;

q) una dichiarazione di piena disponibilità a consentire l'accesso di incaricati del CNIPA presso le strutture dedicate all'erogazione del servizio di posta elettronica certificata, al fine di poter verificare la rispondenza delle stesse ai requisiti tecnici, organizzativi e funzionali di cui alla documentazione allegata alla domanda;

r) una descrizione delle caratteristiche dei dispositivi sicuri utilizzati per la creazione della firma delle ricevute, degli avvisi e delle buste di trasporto. Le caratteristiche di sicurezza di detti dispositivi dovranno essere valutate secondo le specifiche CEN: CWA 14169. Sono altresì ammessi:

   1. i livelli di valutazione E3 e robustezza HIGH dell'ITSEC e EAL 4 della norma ISO/IEC 15408 o superiori;
   2. i livelli di valutazione internazionalmente riconosciuti;
   3. i dispositivi previsti dalla normativa in materia di firma digitale;

s) una dichiarazione d'impegno a comunicare al CNIPA ogni eventuale variazione intervenuta rispetto a quanto dichiarato nella domanda di iscrizione. A seguito di tale comunicazione il CNIPA può procedere ad una nuova, se del caso anche parziale, valutazione dei requisiti o richiedere ulteriore documentazione;

t) una descrizione delle modalità operative del servizio, con riferimento all'implementazione delle regole tecniche (architettura tecnica e funzionale, indicazione dei principali prodotti/componenti software utilizzati).

I certificatori iscritti nell'elenco pubblico di cui all'art. 28, comma 1, del Testo unico sono esentati, in esito a specifica richiesta in tal senso, dalla presentazione della documentazione di cui alle lettere a), b), c), d), e), f), h), l), m), purché in corso di validità, in quanto già prodotta in sede di accreditamento e disponibile presso il CNIPA.

2. Requisiti tecnico-organizzativi.

2.1 Manuale operativo.

Il manuale operativo individua le regole generali e le procedure seguite dal Gestore di posta elettronica certificata (PEC) nello svolgimento della propria attività ed e' pubblicato a garanzia dell'affidabilità dei servizi offerti dal Gestore stesso ai propri utenti e ai loro corrispondenti. Detto manuale e' disponibile per la consultazione ed il download sul sito del Gestore. Oltre ai dati identificativi della versione in uso alla quale si riferisce, il manuale operativo deve contenere, quanto meno:

a) i dati identificativi del Gestore;

b) l'indicazione del responsabile del manuale stesso;

c) i riferimenti normativi necessari per la verifica dei contenuti;

d) l'indirizzo del sito web del Gestore ove e' pubblicato e scaricabile;

e) l'indicazione delle procedure nonché degli standard tecnologici e di sicurezza utilizzati dal Gestore nell'erogazione del servizio;

f) le definizioni, le abbreviazioni e i termini tecnici che in esso figurano;

g) una descrizione sintetica del servizio offerto;

h) la descrizione delle modalità di reperimento e di presentazione delle informazioni presenti nei log dei messaggi;

i) l'indicazione del contenuto e delle modalità dell'offerta da parte del Gestore;

j) l'indicazione delle modalità di accesso al servizio;

k) l'indicazione dei livelli di servizio e dei relativi indicatori di qualità di cui all'art. 12 del decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005;

l) l'indicazione delle condizioni di fornitura del servizio;

m) l'indicazione delle modalità di protezione dei dati dei titolari;

n) l'indicazione degli obblighi e delle responsabilità che ne discendono, delle esclusioni e delle eventuali limitazioni, in sede di indennizzo, relative ai soggetti previsti all'art. 2 del decreto del Presidente della Repubblica n. 68/2005.

Il numero di pagine del manuale operativo deve essere compreso tra cinquanta (50) e cento (100); ogni pagina deve contenere, mediamente, quaranta (40) righe; la dimensione del carattere deve essere pari a dodici punti.

E' data facoltà di limitare le dichiarazioni contenute nel manuale operativo alle sole informazioni non soggette a particolari ragioni di riservatezza.

Il CNIPA si riserva, comunque, a norma dell'art. 14, comma 8, del decreto del Presidente della Repubblica n. 68/2005, di richiedere integrazioni della documentazione presentata e di effettuare le opportune verifiche in merito a quanto dichiarato.

2.2 Piano per la sicurezza.

Il piano per la sicurezza, corredato delle relative procedure attinenti all'organizzazione, in quanto documento riservato, deve essere inserito all'interno del plico contenente la domanda, in busta separata e sigillata da cui risulti la denominazione della pubblica amministrazione o la ragione sociale della società che richiede l'iscrizione e la dicitura «Piano per la sicurezza, versione del ...».

Il piano deve contenere, quanto meno:

a) una descrizione delle procedure utilizzate nell'erogazione del servizio (attivazione dell'utenza e organizzazione del servizio di posta elettronica certificata), con particolare riferimento ai problemi attinenti alla sicurezza, alla gestione dei log-file e alla garanzia della loro integrità;

b) una descrizione dei dispositivi di sicurezza installati;

c) una descrizione dei flussi di dati;

d) l'indicazione della procedura di gestione e conservazione delle copie di sicurezza dei dati;

e) l'indicazione della procedura da seguire al verificarsi di possibili guasti di grande rilevanza che determinino l'arresto del servizio (occorre precisare i tipi di guasti per i quali sono state previste delle soluzioni: calamità naturali, dolo, indisponibilità prolungata del sistema, o altri eventi) e descrizione delle soluzioni proposte per farvi fronte, con informazioni dettagliate circa i tempi e le modalità previste per il ripristino;

f) un'analisi dei rischi (occorre precisare le possibili tipologie di rischio: dolo, infedeltà del personale, inefficienza operativa, inadeguatezza tecnologica, o altro);

g) una descrizione delle procedure per la gestione dei rischi di cui al punto precedente (occorre precisare i tempi di reazione previsti e i nomi dei responsabili tenuti ad intervenire);

h) una dettagliata indicazione dei controlli previsti (occorre indicare, se e' previsto, il ricorso periodico a ispezioni esterne);

i) l'indicazione della struttura generale e della struttura logistica dell'organizzazione e delle relative modalità operative;

j) una sommaria descrizione dell'infrastruttura di sicurezza per ciascun immobile di cui si compone la struttura;

k) una breve descrizione dell'allocazione degli impianti informatici, dei servizi e degli uffici collocati negli immobili che fanno parte della struttura;

l) l'indicazione delle modalità di tenuta dei log dei messaggi;

m) una descrizione della procedura di accesso ai log dei messaggi da parte del personale del Gestore;

n) una descrizione del sistema di riferimento temporale e della marca temporale adottata;

o) una descrizione dei sistemi adottati per garantire la riservatezza e l'integrità delle trasmissioni di messaggi mediante il sistema.

I certificatori qualificati accreditati, iscritti nell'elenco pubblico tenuto dal CNIPA, potranno fare riferimento ai dati ed agli elementi contenuti nel piano della sicurezza già in possesso del CNIPA medesimo.

3. Modalità di esame delle domande.

L'istruttoria delle domande di iscrizione presentate, e la verifica della regolarità della relativa documentazione prodotta, sono effettuate, ai sensi del decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005, dal CNIPA che, una volta conclusa l'istruttoria, adotta il conseguente provvedimento di accoglimento o di reiezione, ovvero, se ritenuta necessaria, si riserva di procedere ad una integrazione di istruttoria.

Il soggetto la cui domanda sia stata oggetto di un provvedimento di reiezione non può presentare una nuova istanza di iscrizione se non sono cessate le cause che hanno determinato, a suo tempo, il mancato accoglimento della domanda di iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata.

CNIPA/CR/51 - CENTRO NAZIONALE PER L'INFORMATICA NELLA PUBBLICA AMMINISTRAZIONE

CIRCOLARE 7 dicembre 2006, n. 51

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, «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. 296 del 12 dicembre 2006.

Premessa.

L'art. 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, «Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'art. 27 della legge 16 gennaio 2003, n. 3», attribuisce, tra l'altro, al Centro nazionale per l'informatica nella pubblica amministrazione (di seguito indicato «CNIPA»):

- la gestione dell'elenco pubblico di cui al medesimo art. 14 (di seguito indicato «elenco»);
- il compito di procedere all'iscrizione nell'elenco dei soggetti in possesso dei requisiti prescritti.

Consequenziale alle richiamate funzioni, e' l'attribuzione al CNIPA, ai sensi dell'art. 14, comma 13, del citato decreto del Presidente della Repubblica n. 68 del 2005, di funzioni di vigilanza e di controllo sull'attività esercitata

dai soggetti iscritti nell'elenco, dalle quali discende altresì il compito di monitorare - anche in collaborazione con le autorità competenti - eventuali casi di esercizio o pubblicizzazione della attività di Gestore di posta elettronica certificata (di seguito indicata «PEC») da parte di soggetti non abilitati.

Successivamente, l'art. 19 del decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005, recante «Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata», ha demandato al CNIPA il compito di definire, con proprie circolari, sia le modalità di inoltro delle domande di iscrizione nell'elenco, sia le modalità dell'esercizio dei richiamati compiti di vigilanza e controllo.

Il CNIPA, con la circolare 24 novembre 2005, n. CNIPA/CR/49, ha provveduto a fornire le indicazioni relative alle modalità con le quali coloro che intendono esercitare attività di gestori di PEC devono presentare domanda. Con la presente circolare si indicano le modalità attraverso le quali il CNIPA svolge la suddetta funzione di vigilanza e di controllo.

1. Test di interoperabilità del sistema di gestione della PEC.

1.1

Ai sensi dell'art. 5 del citato decreto del Presidente della Repubblica n. 68 del 2005 e dell'art. 8 del decreto del Ministro per l'innovazione e tecnologie del 2 novembre 2005 (di seguito indicato «decreto ministeriale»), i sistemi di PEC utilizzati dai gestori devono essere interoperabili. Il CNIPA svolge la funzione di vigilanza e di controllo sulla predetta interoperabilità ai sensi dei successivi punti.

1.2

Ogni Gestore deve superare con esito positivo una serie di test di interoperabilità presso una struttura indicata dal CNIPA. La serie di test e' pubblicata sul sito del CNIPA (www.cnipa.gov.it). Detti test devono essere ripetuti ogni volta che il Gestore apporti modifiche funzionali o tecniche che impattino sull'interoperabilità dei sistemi di PEC. Il Gestore deve, in ogni caso, fornire al CNIPA una casella di PEC per tutto il periodo di esercizio della relativa attività.

1.3

I test di interoperabilità di cui al punto 1.2 sono obbligatori trascorso il termine di trenta giorni solari che decorrono dal giorno successivo a quello della loro pubblicazione sul sito del CNIPA. Quest'ultimo comunica a ciascun Gestore la pianificazione delle rispettive fasi di test.

1.4

Il CNIPA può in qualsiasi momento effettuare verifiche, anche mediante visite presso il Gestore, per accertare la piena interoperabilità del sistema di PEC del Gestore medesimo, anche richiedendo la ripetizione, in tutto o in parte, della serie di test.

2. Vigilanza e controllo sull'esercizio delle attività dei gestori.

2.1

Il CNIPA esercita attività di vigilanza e di controllo al fine di verificare il possesso e il mantenimento dei requisiti previsti per l'iscrizione nell'elenco.

3. Modalità di vendita dei servizi di PEC attraverso canali commerciali.

3.1

Il CNIPA monitora le modalità di vendita dei servizi di PEC attraverso canali commerciali, anche avvalendosi del supporto di terzi, e verifica, in particolare, che le modalità di vendita siano conformi alle prescrizioni di legge e che il rapporto contrattuale sia sempre posto in essere tra il titolare di cui all'art. 1,

lettera t) del decreto ministeriale ed un Gestore; a tal fine, ogni Gestore deve mettere a disposizione del CNIPA, su richiesta di quest'ultimo, le informazioni del caso.

4. Struttura informativa dei gestori.

4.1

Il Gestore organizza una struttura informativa che raccoglie e gestisce le informazioni relative:

a) al numero di caselle in esercizio per ciascun dominio;

b) al numero totale giornaliero di messaggi di PEC in ingresso alle caselle gestite ed in uscita dalle stesse;

c) ai livelli di servizio erogati, con riferimento a quelli previsti dal decreto ministeriale;

d) al numero totale giornaliero di virus rilevati in ingresso ai sistemi gestiti ed in uscita dagli stessi. Le informazioni di cui alle lettere a), b), c), d) devono essere inviate al CNIPA con le modalità e nei tempi definiti al punto 5.

4.2

Il CNIPA può inoltre richiedere ai gestori:

a) informazioni circa il livello di soddisfazione dei propri clienti;

b) le caratteristiche di eventuali servizi aggiuntivi offerti.

4.3

In un'apposita sezione della struttura informativa sono registrate e gestite le informazioni relative a disservizi, segnalazioni e reclami secondo la classificazione riportata nell'allegata tabella «A».

5. Tempi e modalità delle comunicazioni dirette al CNIPA.

5.1

Ogni Gestore e' tenuto a raccogliere le informazioni di cui al punto 4.1 trascorso il termine di sessanta giorni solari decorrenti dalla data di pubblicazione della presente circolare. Dette informazioni devono essere inviate al CNIPA con le cadenze di seguito indicate:

a) con frequenza bimestrale, entro il quindicesimo giorno successivo al termine del bimestre di riferimento, devono essere trasmesse le informazioni relative:

- al numero di caselle in esercizio per ciascun dominio;
- al numero totale giornaliero di messaggi di PEC in ingresso alle caselle gestite ed in uscita dalle stesse;
- al numero totale giornaliero di virus rilevati in ingresso ai sistemi gestiti ed in uscita dagli stessi;

b) con frequenza quadrimestrale, entro il quindicesimo giorno successivo al termine del quadrimestre di riferimento, devono essere trasmesse le informazioni concernenti:

- -i livelli di servizio erogati, con riferimento a quelli previsti dal decreto ministeriale citato in premessa.

5.2

Le informazioni di cui al punto 5.1 devono essere inviate tramite posta elettronica certificata alla casella gestoripec@cert.cnipa.it. Le informazioni di cui alla lettera a) del punto 5.1 devono avere un formato conforme a quanto descritto nel sito del CNIPA. Le informazioni di cui alla lettera b) del punto 5.1 devono essere in formato Adobe PDF.

6. Segnalazioni urgenti al CNIPA di malfunzionamenti gravi.

6.1

I gestori hanno l'obbligo di comunicare al CNIPA, con le modalità e nei tempi indicati al punto 6.2, i disservizi di cui al punto 4, contraddistinti da uno dei seguenti codici: 1A, 1B, 2A, 2B, 3A, 3B, secondo quanto riportato nell'allegata tabella «A».

6.2

In particolare, il Gestore e' tenuto ad informare il CNIPA dell'evento occorso, entro trenta minuti dalla rilevazione dell'evento stesso, utilizzando i recapiti e l'apposito modulo indicati nel sito del CNIPA medesimo. La comunicazione deve fornire anche una prima valutazione dell'incidente e le eventuali misure adottate al riguardo.

7. Sospensione del servizio.

7.1

Nel caso di comportamento anomalo e non circoscritto (codici 1° e 1B della citata tabella «A»), il Gestore e' tenuto a sospendere il servizio, fornendo adeguata e tempestiva informativa ai propri utenti ed agli altri gestori. Ove il Gestore coinvolto non attivi l'autosospensione, il CNIPA dispone la sospensione del servizio.

7.2

Nel caso di comportamento anomalo e circoscritto (codici 2A e 2B della citata tabella «A»), il CNIPA può disporre la sospensione del servizio per il Gestore coinvolto, fino alla rimozione delle cause che hanno determinato detto comportamento anomalo e circoscritto; in tal caso, il Gestore fornisce adeguata e tempestiva informativa ai propri utenti ed agli altri gestori.

7.3

Non appena ripristinata l'operatività, il Gestore comunica al CNIPA l'avvenuta rimozione delle cause che hanno determinato il comportamento anomalo e fornisce parimenti al CNIPA entro una settimana dalla data della comunicazione di cui al presente punto, una circostanziata relazione tecnica sull'accaduto e sui provvedimenti adottati in conseguenza.

7.4

Il Gestore attua l'autosospensione producendo un «avviso di non accettazione per eccezioni formali» relativamente ai messaggi immessi dai propri utenti e non producendo la «ricevuta di presa in carico» per i messaggi destinati ai propri utenti.

7.5

La sospensione del servizio disposta dal CNIPA viene attuata dal Gestore con le medesime modalità previste per l'autosospensione.

7.6

Qualora il Gestore coinvolto non ottemperi a quanto prescritto ai punti 7.1 e 7.2, il CNIPA può disporne la cancellazione dall'elenco.

8. Verifiche periodiche dei gestori.

8.1

I gestori hanno l'obbligo di effettuare verifiche semestrali, i cui esiti sono riportati in relazioni sottoscritte dal responsabile delle verifiche stesse e delle ispezioni, come previsto dal decreto ministeriale, e messe a disposizione, su richiesta, del CNIPA. Dette verifiche devono riguardare, in particolare, le componenti tecniche ed organizzative del sistema di PEC, il sistema di raccolta dei livelli di servizio e le tipologie di contratti di vendita dei servizi di PEC.

9. Verifiche del CNIPA.

9.1

Con riferimento alla dichiarazione di cui alla lettera q) del punto 1 della citata circolare n. CNIPA/CR/49 del 24 novembre 2005, il CNIPA puo' effettuare, con un preavviso di 48 ore, sopralluoghi presso le strutture utilizzate dal Gestore per verificare la conformità del sistema di PEC.

10. Provvedimenti nei confronti dei gestori inadempienti.

10.1

A seguito delle risultanze dell'attività di vigilanza e di controllo, nell'ipotesi di inosservanza di uno o piu' degli obblighi posti a carico del Gestore, il CNIPA può disporre l'inibizione dell'esercizio dell'attività svolta dal Gestore inadempiente, indicando nel contempo il termine entro il quale il Gestore stesso deve conformarsi agli obblighi previsti. Qualora il Gestore non provveda in tal senso nei tempi indicati, il CNIPA può disporre la cancellazione del Gestore medesimo dall'elenco.

10.2

Nel caso in cui il CNIPA disponga la cancellazione di un Gestore dall'elenco rimane in capo al Gestore stesso l'obbligo di conservare e rendere disponibili, su richiesta, i log prodotti nell'ambito dell'attività svolta come previsto dall'art. 11, comma 2, del citato decreto del Presidente della Repubblica n. 68 del 2005. Roma, 7 dicembre 2006

Allegato alla circolare 7 dicembre 2006, n. CNIPA/CR/51 Tabella A Classificazione dei disservizi in relazione agli effetti prodotti e relativi codici identificativi

1. Comportamento anomalo e non circoscritto: comportamento difforme dalle regole tecniche di cui all'art. 17 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, relativo alle funzioni base (trattamento del messaggio originario, ricevute e avvisi) per il quale non e' circoscritto il potenziale impatto (codice 1A, se rilevato dal Gestore; codice 1B, se rilevato da terzi).
2. Comportamento anomalo circoscritto: comportamento difforme dalle regole tecniche di cui all'art. 17 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, relativo alle funzioni base (trattamento del messaggio originario, ricevute e avvisi) per il quale e' circoscritto il potenziale impatto (codice 2A, se rilevato dal Gestore; codice 2B, se rilevato da terzi).
3. Malfunzionamento bloccante: tipologia di malfunzionamento a causa del quale le funzionalità del sistema di PEC, come definite nelle regole tecniche di cui all'art. 17 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, non possono essere utilizzate in tutto o in parte dagli utenti (codice 3A, se rilevato dal Gestore; codice 3B, se rilevato da terzi).
4. Malfunzionamento grave: tipologia di malfunzionamento a causa del quale in alcune circostanze le funzionalità del sistema di PEC, come definite nelle regole tecniche di cui all'art. 17 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, non possono essere utilizzate in tutto o in parte dagli utenti (codice 4A, se rilevato dal Gestore; codice 4B, se rilevato da terzi).

5. Malfunzionamento: situazione a causa della quale le funzionalità del sistema di PEC, come definite nelle regole tecniche di cui all'art. 17 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, in tutto o in parte, risultano degradate ovvero il sistema ha un comportamento anomalo in situazioni circoscritte e per funzionalità secondarie (esclusi: la procedura di identificazione, i messaggi originari, le ricevute, gli avvisi e le buste) (codice 5A, se rilevato dal Gestore; codice 5B, se rilevato da terzi).

Classificazione dei reclami/segnalazioni degli utenti e relativi codici identificativi

RC| Segnalazione di un reclamo relativo al rapporto contrattuale.

AL| Segnalazione di un reclamo relativo alla procedura di accesso al log.

SA| Segnalazione di anomalia/disservizio non imputabili al Gestore (client, collegamento internet, gestione utenze decentrate).

MO Certificati Server

Manuale Operativo per il Servizio "Cnipa Certificati Server" – Certificate Practice Statement –Manuale Operativo – Ver. 1.1 Gennaio 2008

[OMISSIS]

9 CONDIZIONI GENERALI DI EROGAZIONE DEL SERVIZIO

La presente sezione disciplina il rapporto di servizio intercorrente tra CNIPA ed il Richiedente il certificato per server.

Il Richiedente prima di richiedere l'emissione di un certificato è tenuto a leggere ed approvare le condizioni generali di erogazione del servizio riportate all'interno del CPS. Con la sottoscrizione dei moduli di registrazione e di nomina del responsabile server, di cui al paragrafo Registrazione del Richiedente, il firmatario dichiara di aver preso conoscenza ed approvare tali condizioni.

I rapporti per l'erogazione dei servizi di certificazione per server sono sottoposti alla legge italiana. CNIPA, nell'erogazione dei propri servizi, opera conformemente alla normativa sulla protezione dei dati personali (privacy).

9.1 Obblighi del Certificatore

Il CNIPA si impegna a:

- Verificare, secondo quanto descritto all'interno del presente CPS, la correttezza della documentazione fornita con la richiesta di certificazione;
- Rilasciare e rendere pubblico il certificato in accordo ai requisiti descritti nel presente CPS;
- Dare comunicazione, mediante pubblicazione nelle Liste di Revoca (CRL), della revoca dei certificati.

9.2 Obblighi del Richiedente

Il Richiedente è obbligato a:

- Fornire in fase di registrazione informazioni e documentazione veritiere;
- Generare e conservare la propria chiave privata in sicurezza, adottando le necessarie precauzioni per evitare danni, alterazioni o usi non autorizzati della stessa;
- Inviare la richiesta di certificazione con le modalità indicate nel presente CPS;

- Installare il certificato digitale rilasciato da CNIPA in base al presente CPS unicamente sul server corrispondente al nome indicato nel medesimo certificato (relativo al campo CommonName);
- Informare tempestivamente il CNIPA nel caso in cui le informazioni presenti nel certificato rilasciato non siano più valide, richiedendo la revoca del certificato stesso;
- Informare tempestivamente il CNIPA nel caso in cui ritenga che la sicurezza del server su cui è stato installato il certificato possa essere compromessa, richiedendo la revoca del certificato stesso;
- Provvedere immediatamente a rimuovere dal server il certificato per il quale è stata richiesta la revoca.

9.3 Responsabilità del Certificatore

9.3.1 Verso il Richiedente

Il CNIPA non è responsabile nei confronti del Richiedente o di utenti terzi, per eventuali danni, di qualsiasi tipo, derivanti dalla mancata emissione del certificato o da un uso improprio del certificato. La responsabilità di CNIPA, nei confronti del Richiedente o di terzi, è comunque limitata al costo di emissione del certificato, fatti salvi i casi in cui l'art. 1229 del Codice Civile non consente tale limitazione.

9.4 Pubblicazione e directory

9.4.1 Informazioni sulla CA

Il CNIPA, dal 23 dicembre 2005, ha utilizzato il certificato di CA denominato "CNIPA CA2".

Il CNIPA dal 17 dicembre 2007, utilizza un nuovo certificati di CA denominato "CNIPA CA3", operativo per i gestori dal 1° gennaio 2008.

Per l'intero periodo di validità dei certificati server emessi in conformità al presente CPS, CNIPA si impegna a pubblicare sul proprio sito web il presente CPS.

Si riportano di seguito i dati salienti dei certificati di CA dedicati al servizio descritto nel presente CPS:

CNIPA CA2

Dato	Valore
Soggetto (Subject)	C=IT, O= Centro Nazionale per l'Informatica nella PA
Emittente (Issuer)	C=US, O=GTE Corporation, = GTE CyberTrust Solutions, Inc., CN= GTE CyberTrust Global Root
Periodo di validità	Dal 23-12-2005 al 23/12/2012

CNIPA CA3

Dato	Valore
Soggetto (Subject)	C=IT, O= Centro Nazionale per l'Informatica nella PA
Emittente (Issuer)	C=US, O=GTE Corporation, = GTE CyberTrust Solutions, Inc., CN= GTE CyberTrust Global Root
Periodo di validità	Dal 17-12-2007 al 17/12/2014

9.5 Certificati e CRL

I certificati X.509v3 emessi dalle CA sono pubblicati in directory server X.500, accessibili mediante il protocollo LDAP v2 e v3.

Le CRL sono pubblicate nei medesimo Directory LDAP.

Le CRL sono aggiornate nei Directory LDAP una volta al giorno.

Gli indirizzi dei suddetti directory server sono:

- CNIPA CA2 – "ldapca.cnipa.gov.it";
- CNIPA CA3 – "ldapca.spcoop.gov.it".

9.6 Legge applicabile e Foro Competente

Le presenti Condizioni Generali sono soggette alla legge italiana. Per le controversie che dovessero insorgere tra le parti in relazione alle disposizioni del presente CPS, competente a giudicare sarà esclusivamente il Foro di Roma.

10 PROCESSI OPERATIVI

10.1 Registrazione dell'Organizzazione

Questo processo è a cura del richiedente:

L'organizzazione che intende avvalersi dei servizi di certificazione server offerta dal CNIPA invia una lettera nella quale nomina un responsabile dell'organizzazione, comunicandone i riferimenti telefonici ed e-mail, al quale sono assegnati i compiti di interfaccia attiva con il CNIPA nelle fasi di registrazione e regolazione del ciclo di vita del certificato.

10.2 Registrazione del Server

Questo processo è a cura del richiedente. La procedura da seguire, valida per ogni server da certificare, è la seguente:

1. Il Responsabile dell'Organizzazione compila il modulo "Nomina del Responsabile del Server";
2. Il Responsabile del Server compila il modulo "Richiesta di Registrazione";
3. Il Responsabile del Server genera, secondo le modalità previste dal sistema, la coppia di chiavi pubblica/privata da certificare e la relativa richiesta di certificazione (CSR). In particolare, la CSR contiene il nome del server da certificare (CommonName) che, nel caso di Web Server, dovrà corrispondere al dominio internet intestato all'Organizzazione richiedente.
4. La "Richiesta di Registrazione", unitamente alla "Nomina del Responsabile Server" e alla richiesta CSR costituiscono la "Richiesta di emissione certificato".

Il Richiedente deve inviare al CNIPA le richieste di emissione certificato come indicato nella "Procedura per la richiesta di emissione certificato" pubblicata all'indirizzo Internet:

http://www.cnipa.gov.it/firmadigitale/manualeoperativoserver.

10.3 Verifica dei dati

Al ricevimento delle informazioni, il CNIPA provvederà a:

1. controllare il file con la richiesta di certificazione e verificare la coerenza con i dati contenuti nel Modulo di Registrazione;
2. nel caso di certificato Web Server:
   a) Verificare la univocità del nome di tipo X.500 (Distinguished Name, DN) nell'ambito dei propri certificati emessi;
   b) Controllare l'attribuzione del dominio internet relativo al Web Server alla Società/Ente/Amministrazione richiedente la certificazione;
3. verificare l'autenticità della richiesta tramite controllo telefonico o verifica della firma digitale se apposta sui moduli di registrazione e nomina.

Se tutte le verifiche avranno avuto esito positivo, la RA (lato CNIPA) trasmetterà il file con la richiesta di certificazione alla RA (lato Gestore di infrastruttura), che lo trasmetterà alla CA (lato Gestore di infrastruttura), autorizzando la generazione del certificato.

Il CNIPA non darà corso all'emissione del certificato qualora i dati comunicati non risultino corretti o siano incompleti in base ai riscontri delle verifiche poste in essere.

10.4 Generazione del certificato

Una volta ricevuta l'approvazione della RA, la CA verificherà che il formato PKCS#10 della richiesta sia corretto. Se le verifiche previste hanno esito positivo, la CA genera il certificato in accordo al profilo descritto nel paragrafo "Profilo dei certificati". In particolare il DN apparirà come valore del campo Subject del certificato.

Se le verifiche non hanno esito positivo, CNIPA, tramite la propria RA, notifica al richiedente l'evento, richiedendo la generazione di una nuova richiesta di certificazione.

10.5 Pubblicazione del certificato

Il certificato viene pubblicato nel Directory Server X.500 associato alla CA ed inviato all'indirizzo di posta elettronica del Responsabile dell'Organizzazione e al Responsabile del Server autorizzato.

10.6 Accettazione del Certificato

Nel caso il Richiedente riscontri eventuali imprecisioni o difetti del certificato, questi è tenuto ad informare immediatamente il CNIPA tramite comunicazione all'indirizzo di posta elettronica registrazione@cnipa.it. Altrimenti, il certificato verrà ritenuto accettato dal Richiedente.

Se trascorsi 5 (cinque) giorni lavorativi dall'invio al Richiedente non sono pervenute segnalazioni, il certificato verrà considerato accettato.

Accettando il certificato, il Richiedente dichiara di accogliere i termini e le condizioni contenute nel presente CPS.

10.7 Installazione del certificato

Al ricevimento del certificato, il Richiedente potrà installarlo sul server, seguendo le istruzioni dello specifico prodotto utilizzato.

10.8 Variazione dei dati di registrazione

Il Richiedente deve informare tempestivamente il CNIPA nel caso in cui ci siano delle variazioni dei dati contemplati nel paragrafo Registrazione del Richiedente. Se le variazioni riguardano dati presenti sul certificato, il Richiedente deve altresì richiedere per iscritto la revoca del certificato.

Il CNIPA si riserva la facoltà di revocare il certificato del Richiedente nel caso in cui la variazione dei dati di registrazione lo richieda.

10.9 Revoca del certificato

La revoca di un certificato si completa con la sua pubblicazione nella lista di revoca firmata dal Certificatore (CRL). Il certificato revocato non ha più validità ed il Richiedente deve provvedere immediatamente a rimuovere il certificato relativo dal server associato.

10.9.1 Richiesta di revoca da parte del Richiedente

Il Richiedente deve richiedere la revoca del certificato nelle seguenti circostanze:

- nel caso in cui voglia cessare il rapporto con il CNIPA;
- nel caso in cui le informazioni presenti sul certificato rilasciato non siano più valide;
- nel caso in cui ritenga che la sicurezza del server su cui è stato installato il certificato sia stata compromessa.

Quest'ultima circostanza deve essere prontamente rilevata e comunicata; in ogni caso il CNIPA non assume alcuna responsabilità per l'uso improprio della chiave privata associata alla chiave pubblica certificata.

Per richiedere la revoca, il Richiedente deve inviare un fax su carta intestata e appositamente sottoscritto al numero +390685254414, o una mail contenente in allegato detta richiesta sottoscritta digitalmente all'indirizzo registrazione@cnipa.it; in cui venga esplicitamente richiesta la revoca del certificato per server con l'indicazione almeno della Ragione Sociale del Richiedente e del nome del server in oggetto. In seguito alla ricezione del fax, o della email, il CNIPA provvederà ad effettuare un controllo per verificare l'autenticità della richiesta.

La richiesta di revoca sarà verificata dalla RA che, in caso di verifica positiva, inoltrerà la richiesta alla CA.

Il Certificato revocato sarà inserito nella CRL.

Il servizio per richiedere la revoca è attivo dal Lunedì al Venerdì, dalle ore 8:30 alle ore17:00.

10.9.2 Richiesta di revoca da parte della CA

Il CNIPA può autonomamente revocare il certificato di un Richiedente solamente nelle seguenti circostanze:

- evidenza della variazione dei dati contenuti nel certificato;
- evidenza dell'uso improprio del certificato. In ambedue i casi, CNIPA, dopo aver effettuato la revoca, lo comunica al Richiedente.

10.10 Riemissione del certificato

La riemissione del certificato a seguito di variazione dati, revoca o scadenza viene gestita come emissione di un nuovo certificato.

10.11 Gestione degli archivi

Il CNIPA mantiene la documentazione di richiesta di emissione di certificato e di revoca per due anni dopo la scadenza del relativo certificato.

Traccia delle informazioni operative è mantenuta nel database della CA di cui viene effettuato il backup giornaliero.

10.12 Livelli di servizio

La generazione del certificato avviene entro 8 (otto) giorni lavorativi dal ricevimento della Richiesta emissione certificato.

La revoca del certificato avviene entro 2 (due) giorni lavorativi dal ricevimento della richiesta, entro il periodo di disponibilità del servizio (dal Lunedì al Venerdì, dalle 8:30 alle 17:00).

L'accesso ai Directory Server ed alle CRL è disponibile 7 giorni su 7, 24 ore su 24, salvo i fermi per manutenzione programmata.

10.13 Gestione guasti e disaster recovery

Tutti gli elaboratori usati per l'erogazione del servizio di certificazione sono coperti da un contratto di manutenzione che garantisce l'intervento in 8 (otto) ore.

In caso di compromissione dei programmi o dei dati è previsto il loro ripristino a partire dai backup.

11 ASPETTI DI SICUREZZA

11.1 Protezione fisica dei locali

I sistemi tecnologici utilizzati per l'erogazione del servizio sono situati in un'area protetta, il cui accesso è consentito esclusivamente al personale del gestore dell'infrastruttura e del CNIPA espressamente autorizzato, ed è controllato mediante dispositivi di riconoscimento biometrico, autenticazione forte e telecamere a circuito chiuso. Gli edifici dei gestori sono sorvegliati e protetti 24 ore su 24, 7 giorni su 7.

11.2 Sicurezza del sistema di certificazione

La piattaforma di gestione delle attività di certificazione, composta da vari moduli appartenenti alla suite software UniCERT della Baltimore Technologies, offre le seguenti funzioni di sicurezza:

11.2.1 Identificazione e autenticazione

L'accesso ai moduli applicativi della piattaforma avviene mediante identificazione dell'utente. Il meccanismo di autenticazione è previsto anche per l'avvio e/o fermo del servizio legato al modulo applicativo.

11.2.2 Controllo accessi

L'accesso ai moduli applicativi della piattaforma avviene mediante meccanismi di strong authentication. L'accesso ai moduli è consentito solo previa verifica del corretto inserimento della passphrase.

11.2.3 Tracciamento

Tutte le applicazioni in esecuzione all'interno del sistema di certificazione del Certificatore mantengono traccia su appositi database delle operazioni effettuate.

Sono prodotti dei log in formato testo, ove vengono riportate le informazioni relative ad avvio, arresto ed allarmi relativi ai servizi legati ai moduli applicativi, nonché i riferimenti delle eventuali modifiche di configurazione apportate ai servizi.

Ciascuna registrazione all'interno dei log è firmata digitalmente.

11.2.4 Integrità e Non ripudio

- Firma digitale dei messaggi. Tutti i messaggi inviati dai singoli moduli sono firmati in modo digitale.
- Verifica dei messaggi: i moduli verificano tutti i messaggi che ricevono per assicurarsi della loro integrità ed autenticità.
- Archiviazione dei dati: tutti i dati e gli audit log sono registrati nel database relativo a ciascun modulo. Tali registrazioni sono firmate in modo digitale dai moduli proprietari del DB. Ogni registrazione ha un numero d'identificazione univoco.

11.2.5 Comunicazioni

Le comunicazioni tra i moduli avvengono mediante il protocollo PKIX.

11.3 Sicurezza del modulo crittografico

Per la generazione delle firme digitali viene utilizzato l'algoritmo RSA (Rivest-Shamir-Adleman).

Tutti i certificati emessi – a partire dai certificati relativi alle chiavi di certificazione, fino ai certificati relativi alle chiavi pubbliche dei server – vengono firmati utilizzando l'algoritmo RSA. Lo stesso algoritmo RSA deve essere utilizzato dal Richiedente per generare la propria coppia di chiavi. Le chiavi pubbliche dei server hanno lunghezza massima pari a 1024 bit, le chiavi di certificazione sono lunghe 2048 bit.

Per quel che concerne le funzioni di hash, viene utilizzata la funzione definita nello standard ISO/IEC 10118-3:1998 per la generazione dell'impronta digitale: Dedicated Hash-Function 3, corrispondente alla funzione SHA-1.

[OMISSIS]

LL GG Iscrizione IGPEC

Raccomandazioni sul Metodo e sulle Procedure di Iscrizione nell'Elenco Pubblico dei Gestori di Posta Elettronica Certificata – CNIPA – 13/02/2006

[OMISSIS]

Art. 4 Raccomandazioni generali

> Una nota particolare merita la comunicazione con cui i Gestori, una volta accreditati, informano il CNIPA circa la data effettiva di disponibilità del proprio LDIF (Lightweight Directory Interchange Format). Tale comunicazione, necessaria affinché il CNIPA aggiorni in tempo utile l'indice dei Gestori, deve avvenire utilizzando la casella di posta elettronica specificata nella lettera di accreditamento del CNIPA ai Gestori e deve essere inviata al CNIPA con almeno 48 ore di anticipo rispetto alla data di attivazione del servizio.

[OMISSIS]

Art. 4.3. Raccomandazioni tecnico-operative

MANUALE OPERATIVO - Considerazioni generali

Il manuale operativo ha una duplice finalità:

- spiegare alla potenziale utenza, non necessariamente esperta, le finalità, i contenuti e le modalità di accesso ed utilizzazione del servizio;
- dettagliare i contenuti tecnici del servizio in modo da consentire, ad un'utenza professionale, di poterne valutare appieno le caratteristiche.

E' opportuno pertanto che il manuale presentato dal proponente sia uno strumento di facile comprensione per tutti i potenziali clienti del servizio e che quindi presenti, oltre agli approfondimenti di natura tecnica previsti dalla Normativa, una chiarezza espositiva di fondo.

Per quanto riguarda i contenuti, oltre a quanto espressamente richiesto dalla Circolare, si ritiene utile ricordare ai proponenti di presentare un manuale operativo che espliciti con chiarezza i seguenti ambiti/elementi:

- il prospetto di corrispondenza tra i capitoli del manuale e i singoli punti specificati nella circolare;
- l'indirizzo internet dal quale prelevare il manuale operativo nonchè l'indirizzo del sito web del proponente che riporti la descrizione del servizio offerto;
- la descrizione completa ed approfondita delle modalità per l'apposizione e la definizione del riferimento temporale;
- la descrizione puntuale delle modalità di richiesta, reperimento e presentazione all'utente dei log dei messaggi;
- le soluzioni tecniche ed organizzative che realizzano i servizi di emergenza, secondo quanto previsto dall'art. 12 comma 7;
- l'eventuale disponibilità del servizio di customer care, nonché il numero telefonico/numero verde oppure del sito e/o dell'e-mail dello stesso (specificando possibilmente i livelli di servizio previsti);
- la descrizione, da riportare all'interno della sezione "modalità di accesso al servizio", delle procedure di attivazione e di acquisizione del servizio da parte del potenziale cliente.

FAQ Sulla CNIPA/CR/51 - Versione 1.1 del 4 maggio 2007

[OMISSIS]

3. Modalità di vendita dei servizi di PEC attraverso canali commerciali – Punto 3 della circolare 7 dicembre 2006, n. 51.

Quali sono le modalità di commercializzazione dei servizi di PEC?

Oltre alla vendita diretta dei servizi di PEC – ipotesi in cui il Gestore instaura direttamente un rapporto contrattuale con il titolare della casella di posta elettronica e provvede nel contempo ad espletare le procedure di registrazione – è possibile effettuare la vendita dei servizi di PEC attraverso canali commerciali. In questo caso l'intermediario o il distributore - che potrà integrare il servizio di PEC con servizi aggiuntivi prestati direttamente al titolare - dovrà assicurare che il titolare della casella di PEC sottoscriva un apposito modulo avente valore di disciplina contrattuale, dal quale risulti che il servizio di PEC è erogato dal Gestore. L'intermediario/distributore provvederà, inoltre, a indicare al Gestore il titolare della casella e a trasmettere il suddetto modulo, debitamente sottoscritto. In caso di vendita di servizi di PEC attraverso un intermediario/distributore, la procedura di registrazione del titolare avviene secondo le modalità previste dal Gestore di PEC nel proprio manuale operativo.

[OMISSIS]

6. Segnalazioni urgenti al CNIPA di malfunzionamenti gravi – Punto 6 della circolare 7 dicembre 2006, n. 51.

Quali possono essere esempi di eventi riconducibili alla classificazione riportata nella "Tabella A" allegata alla circolare?

Ad integrazione della casistica di cui alla "Tabella A", necessariamente di portata generale, si rappresenta, a titolo meramente esemplificativo (ma non esaustivo) quanto segue:

- comportamento anomalo non circoscritto: invio di PEC a destinatari non indicati dal mittente; la popolazione dei destinatari coinvolti non è individuata univocamente;
- comportamento anomalo circoscritto: mancata emissione, da parte del sistema, delle ricevute di avvenuta consegna per i soli mittenti appartenenti ad un dominio di competenza del Gestore;
- malfunzionamento bloccante: il sistema di autenticazione del Gestore non permette l'accesso al servizio;
- malfunzionamento grave: in presenza di una determinata circostanza non è consentito accedere all'interfaccia web del sistema di PEC;
- malfunzionamento: i tempi di risposta dell'interfaccia web sono significativamente superiori a quelli normalmente percepiti dall'utenza.

Da quando decorre il termine massimo di trenta minuti previsto al punto 6.2 della circolare?

Il termine entro il quale "il Gestore è tenuto ad informare il CNIPA dell'evento occorso" decorre dal momento in cui il Gestore ha concluso la diagnosi del disservizio verificatosi ed ha effettuato "una prima valutazione dell'incidente".

Capitolo 18

Riferimenti tecnici

ETSI TS 102 176-1	Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms
IETF RFC 2119	Key words for use in RFCs to Indicate Requirement Levels
IETF RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
ISO/IEC 9594-8: 2001	Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks – Fourth edition 2001-08-01
ISO/IEC 27001: 2005	Information technology — Security techniques — Information security management systems — Requirements
ISO/IEC 27002: 2007	Information technology — Security techniques — Code of practice for information security management
NIST SP 800-57	NIST Special Publication 800-57; May, 2006; Recommendation for Key Management – Part 1: General

G.R. Blakley, Safeguarding cryptographic keys, AFIPS Conference Proceedings 48 (1979), 313-317.

A. Shamir, How to share a secret, Communications of the ACM 22 (1979), 612-613.