Regole tecniche
del servizio di trasmissione di documenti informatici mediante posta elettronica certificata

INDICE

1 MODIFICHE DOCUMENTO

Descrizione Modifica	Edizione	Data
Prima emissione	1	25/10/2005

2 RIFERIMENTI

Codice	Titolo
RFC 1847	Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted
RFC 1891	SMTP Service Extension for Delivery Status Notifications
RFC 1912	Common DNS Operational and Configuration Errors
RFC 2045	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
RFC 2049	Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples
RFC 2252	Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
RFC 2315	PKCS #7: Cryptographic Message Syntax Version 1.5
RFC 2633	S/MIME Version 3 Message Specification
RFC 2821	Simple Mail Transfer Protocol
RFC 2822	Internet Message Format
RFC 2849	The LDAP Data Interchange Format (LDIF) - Technical Specification
RFC 3174	US Secure Hash Algorithm 1 (SHA1)
RFC 3207	SMTP Service Extension for Secure SMTP over Transport Layer Security
RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
ISO/IEC 9594-8:2001	Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks

3 TERMINI E DEFINIZIONI

Termine/Acronimo	Descrizione
CNIPA	Centro nazionale per l'informatica nella Pubblica Amministrazione
PEC	Posta Elettronica Certificata
SMTP	Simple Mail Transfer Protocol
MIME	Multipurpose Internet Mail Extensions
S/MIME	Secure/MIME
TLS	Transport Layer Security
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
CRL DP	Certificate Revocation List Distribution Point
DNS	Domain Name Service
FQDN	Fully Qualified Domain Name
XML	eXtensible Markup Language
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format

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@gestore.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@[dominio_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
originale]
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
escludendo che questo possa avvenire in seguito, si ritiene utile
considerare che l'invio del messaggio potrebbe non andare a buon fine. Il
sistema provvederà comunque ad inviare un ulteriore avviso di mancata
```

```
consegna se nelle prossime dodici ore non vi sarà la conferma della
ricezione da parte del destinatario.
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@[dominio_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
contenuto 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
contenuto 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
contenuto 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 Single value	Indirizzo di posta elettronica a cui inviare le ricevute di presa in carico
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.

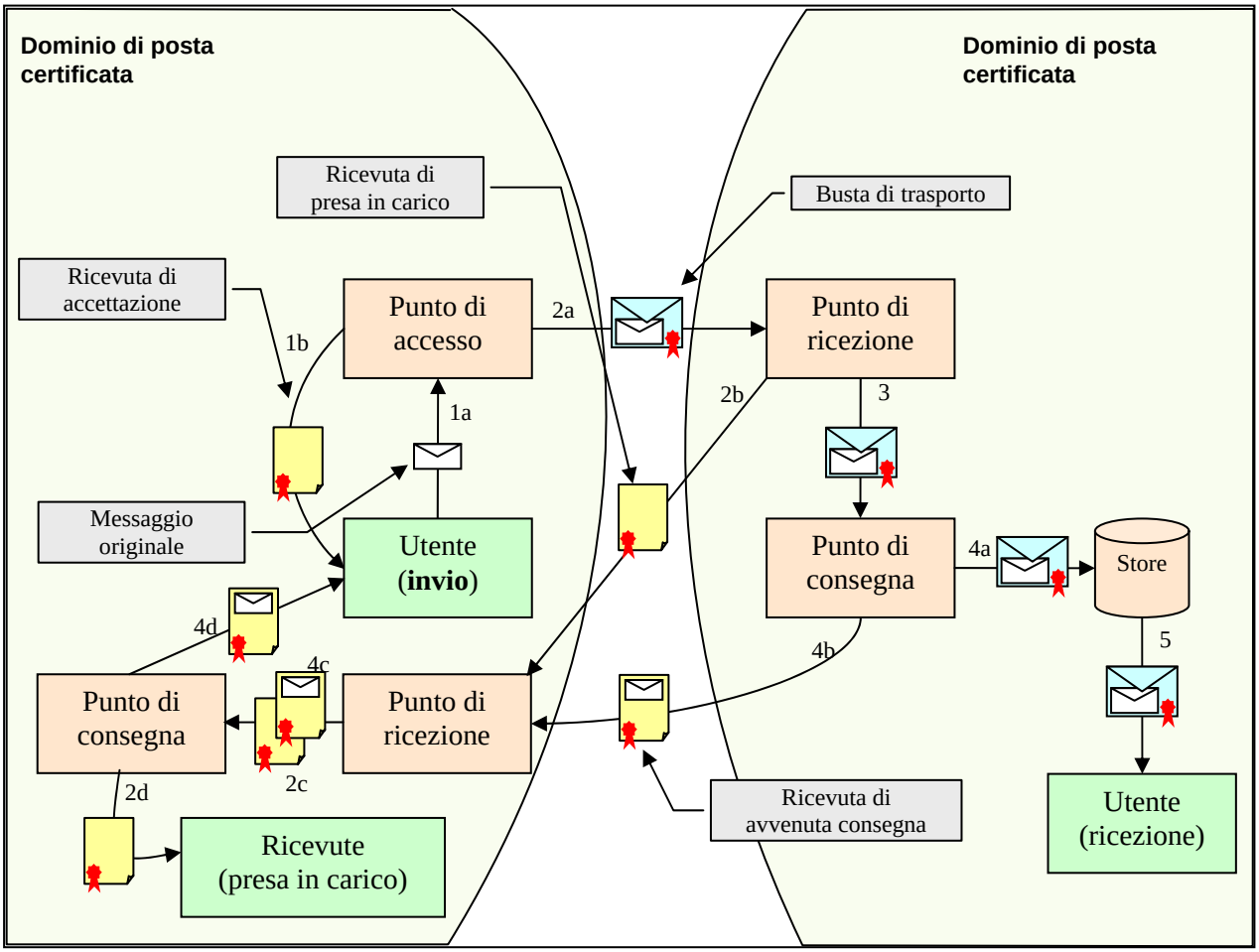
9 APPENDICE A

9.1 Schema logico di funzionamento

Nel seguito viene proposta una rappresentazione grafica che schematizza gli elementi caratteristici di un dominio di posta certificata e le sue interazioni con un altro dominio di posta, sia certificata che non certificata. Il contenuto informativo dei seguenti schemi costituisce parte integrante di questo allegato tecnico.

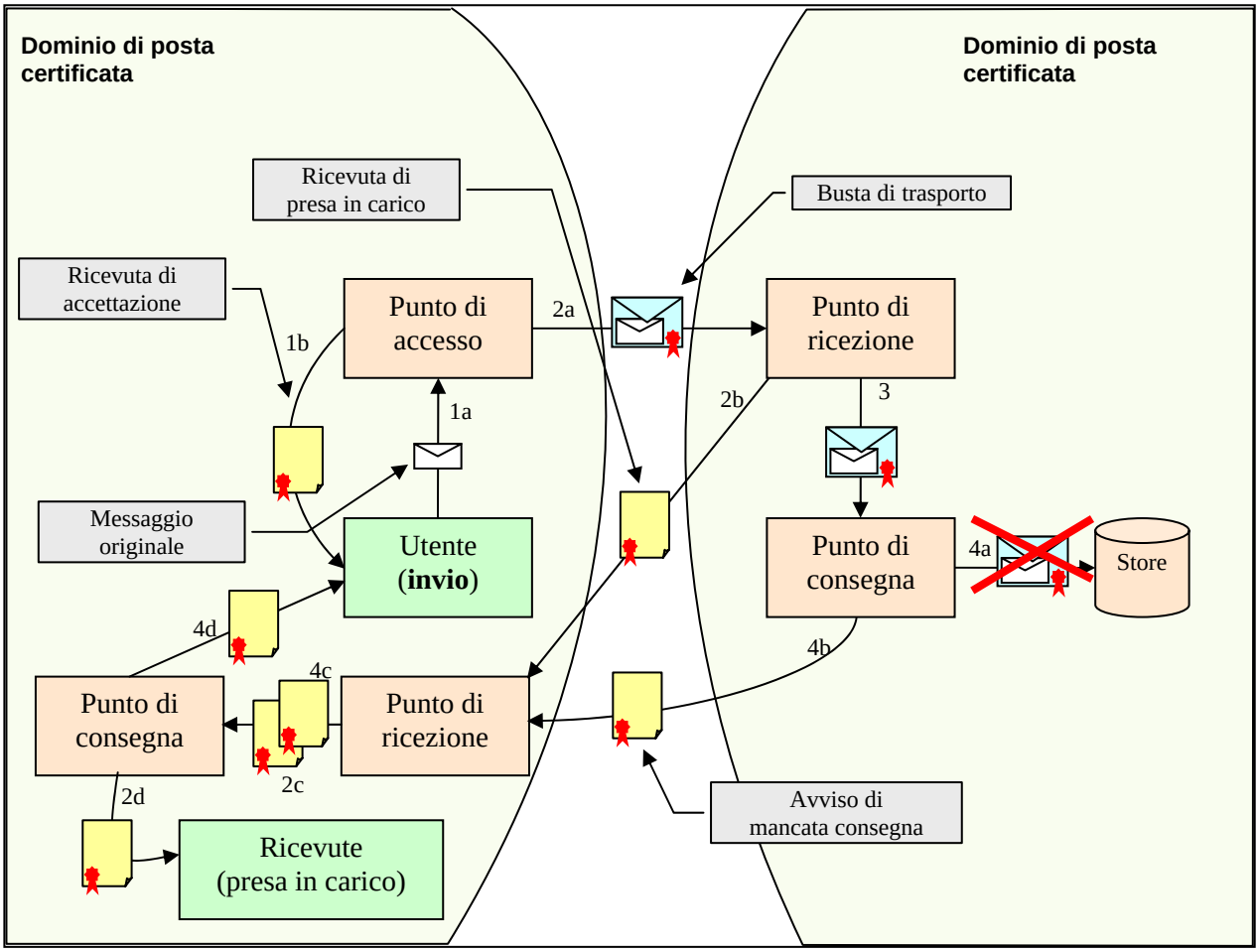
9.1.1 Interazione fra due domini di posta certificata

9.1.1.1 Busta di trasporto corretta e valida con consegna avente esito positivo



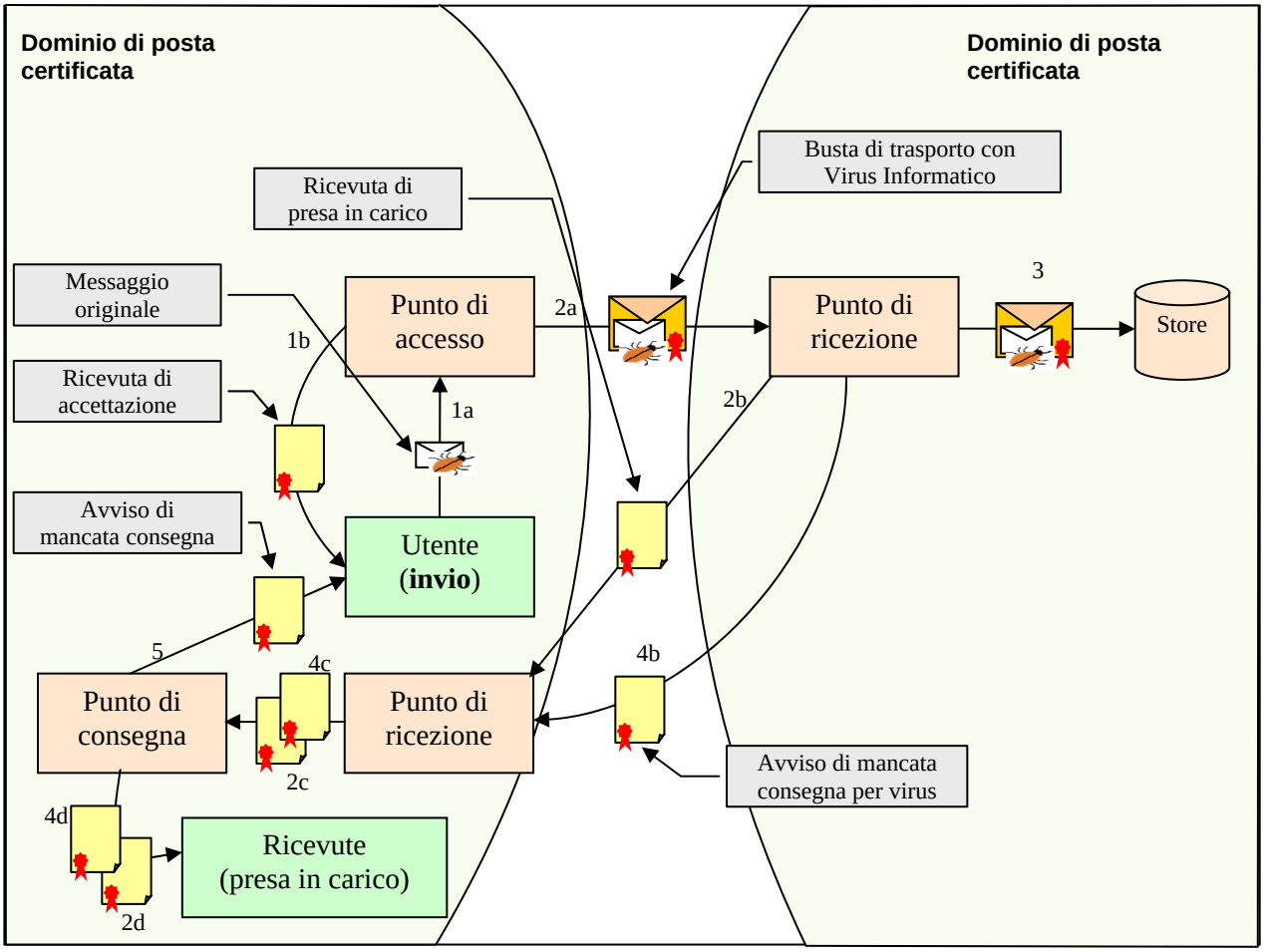
- 1a – l'utente invia una e-mail al Punto di accesso (PdA)
- 1b – il PdA restituisce al mittente una Ricevuta di Accettazione (RdA)
- 2a – il PdA crea una Busta di Trasporto (BdT) e la inoltra al Punto di Ricezione (PdR) del Gestore destinatario
- 2b – il PdR verifica la BdT e crea una Ricevuta di Presa in Carico (RdPiC) che viene inoltrata al PdR del Gestore mittente
- 2c – il PdR verifica la validità della RdPiC e la inoltra al PdC
- 2d – il PdC salva la RdPiC nello store delle ricevute del Gestore
- 3 – il PdR inoltra la BdT al Punto di Consegna (PdC)
- 4a – il PdC verifica il contenuto della BdT e la salva nello store (mailbox del destinatario)
- 4b – il PdC crea una Ricevuta di Avvenuta Consegna (RdAC) e la inoltra al PdR del Gestore mittente
- 4c – il PdR verifica la validità della RdAC e la inoltra al PdC
- 4d – il PdC salva la RdAC nella mailbox del mittente
- 5 – l'utente destinatario ha a disposizione la e-mail inviata

9.1.1.2 Busta di trasporto corretta e valida con consegna avente errore di consegna



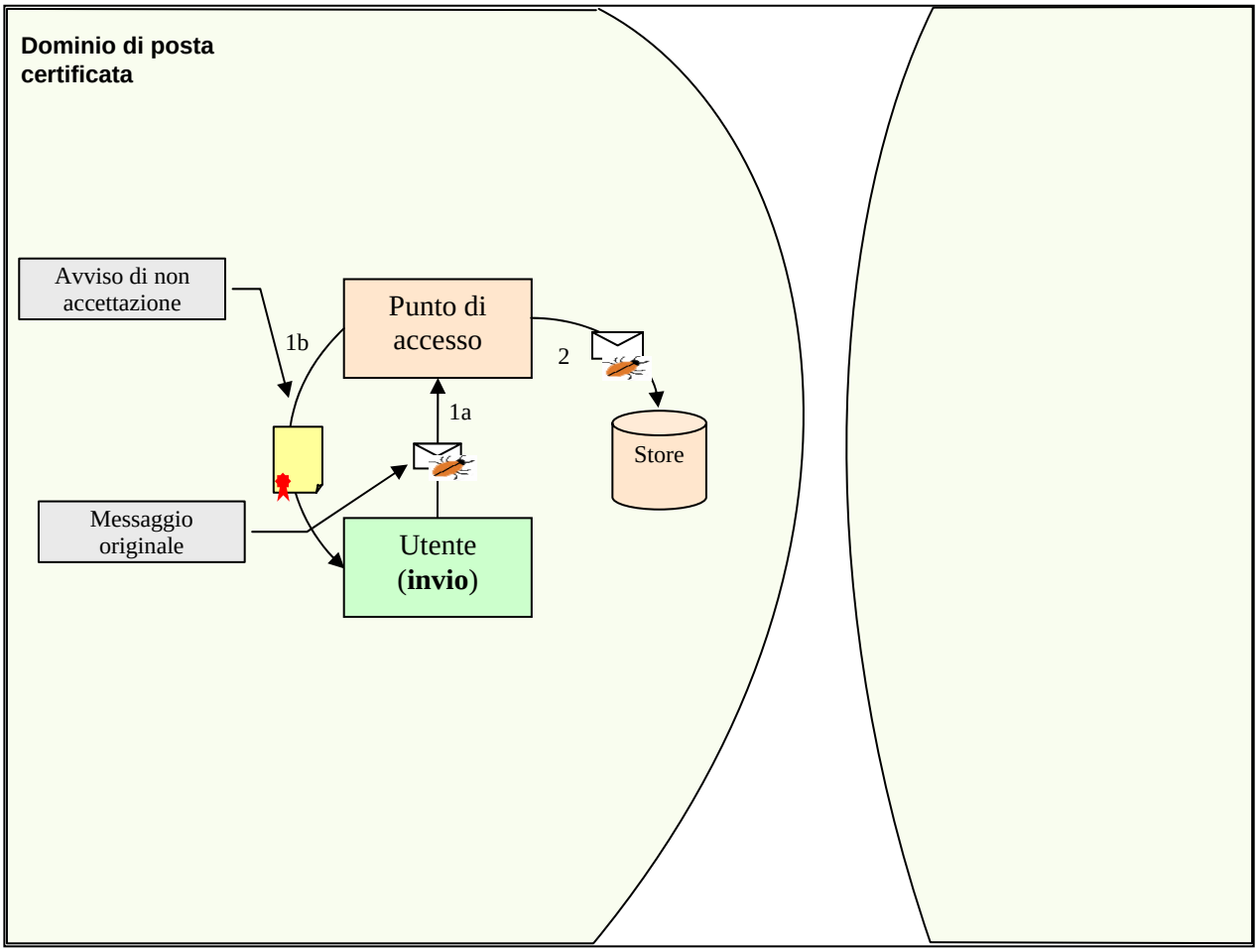
- 1a – l'utente invia una e-mail al Punto di accesso (PdA)
- 1b – il PdA restituisce al mittente una Ricevuta di Accettazione (RdA)
- 2a – il PdA crea una Busta di Trasporto (BdT) e la inoltra al Punto di Ricezione (PdR) del Gestore destinatario
- 2b – il PdR verifica la BdT e crea una Ricevuta di Presa in Carico (RdPiC) che viene inoltrata al PdR del Gestore mittente
- 2c – il PdR verifica la validità della RdPiC e la inoltra al PdC
- 2d – il PdC salva la RdPiC nello store delle ricevute del Gestore
- 3 – il PdR inoltra la BdT al Punto di Consegna (PdC)
- 4a – il PdC verifica il contenuto della BdT ma non riesce a salvarla nello store (es. mailbox del destinatario piena)
- 4b – il PdC crea un Avviso di Mancata Consegna (AMC) e la inoltra al PdR del Gestore mittente
- 4c – il PdR verifica la validità dello AMC e lo inoltra al PdC
- 4d – il PdC salva lo AMC nella mailbox del mittente

9.1.1.3 Busta di trasporto corretta contenente virus informatico non rilevato dal gestore mittente e consegna avente errore di consegna



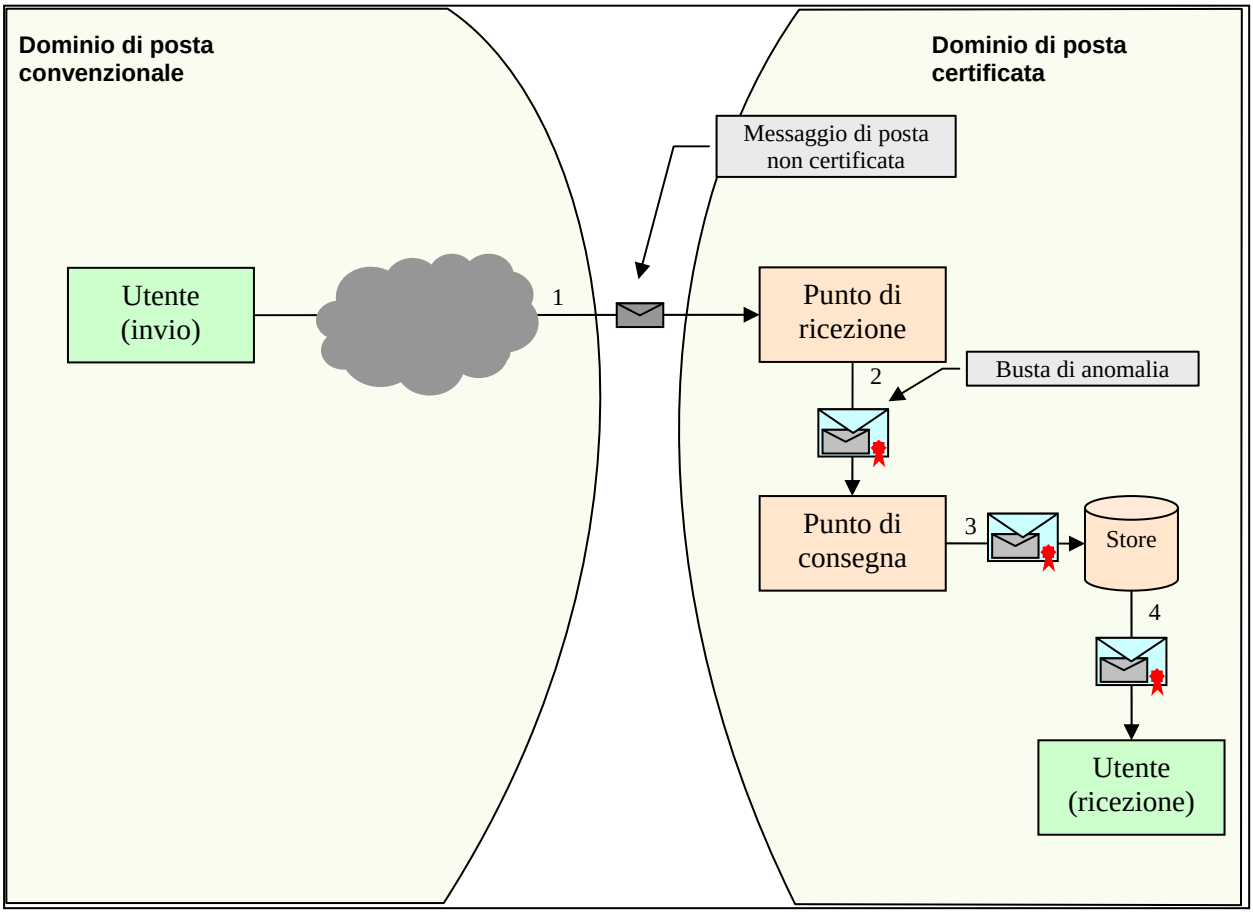
- 1a – l'utente invia una e-mail al Punto di accesso (PdA)
- 1b – il PdA restituisce al mittente una Ricevuta di Accettazione (RdA)
- 2a – il PdA crea una Busta di Trasporto (BdT) e la inoltra al Punto di Ricezione (PdR) del Gestore destinatario
- 2b – il PdR verifica la BdT e crea una Ricevuta di Presa in Carico (RdPiC) che viene inoltrata al PdR del Gestore mittente
- 2c – il PdR verifica la validità della RdPiC e la inoltra al PdC
- 2d – il PdC salva la RdPiC nello store delle ricevute del Gestore
- 3 – il PdR verifica il contenuto della BdT, ne rileva un contenuto potenzialmente pericoloso e non la recapita al destinatario ma la conserva
- 4b – il PdR crea una Avviso di Mancata Consegna per Virus e la inoltra al PdR del Gestore mittente
- 4c – il PdR verifica la validità della RdAC e la inoltra al PdC
- 4d – il PdC salva l'Avviso di Mancata Consegna per Virus nello store delle ricevute del Gestore
- 5 – il PdC crea una Ricevuta di Mancata Consegna (RdE) e la inoltra nella mailbox del mittente

9.1.1.4 Messaggio originale con virus informatico rilevato dal gestore mittente e avviso di non accettazione.



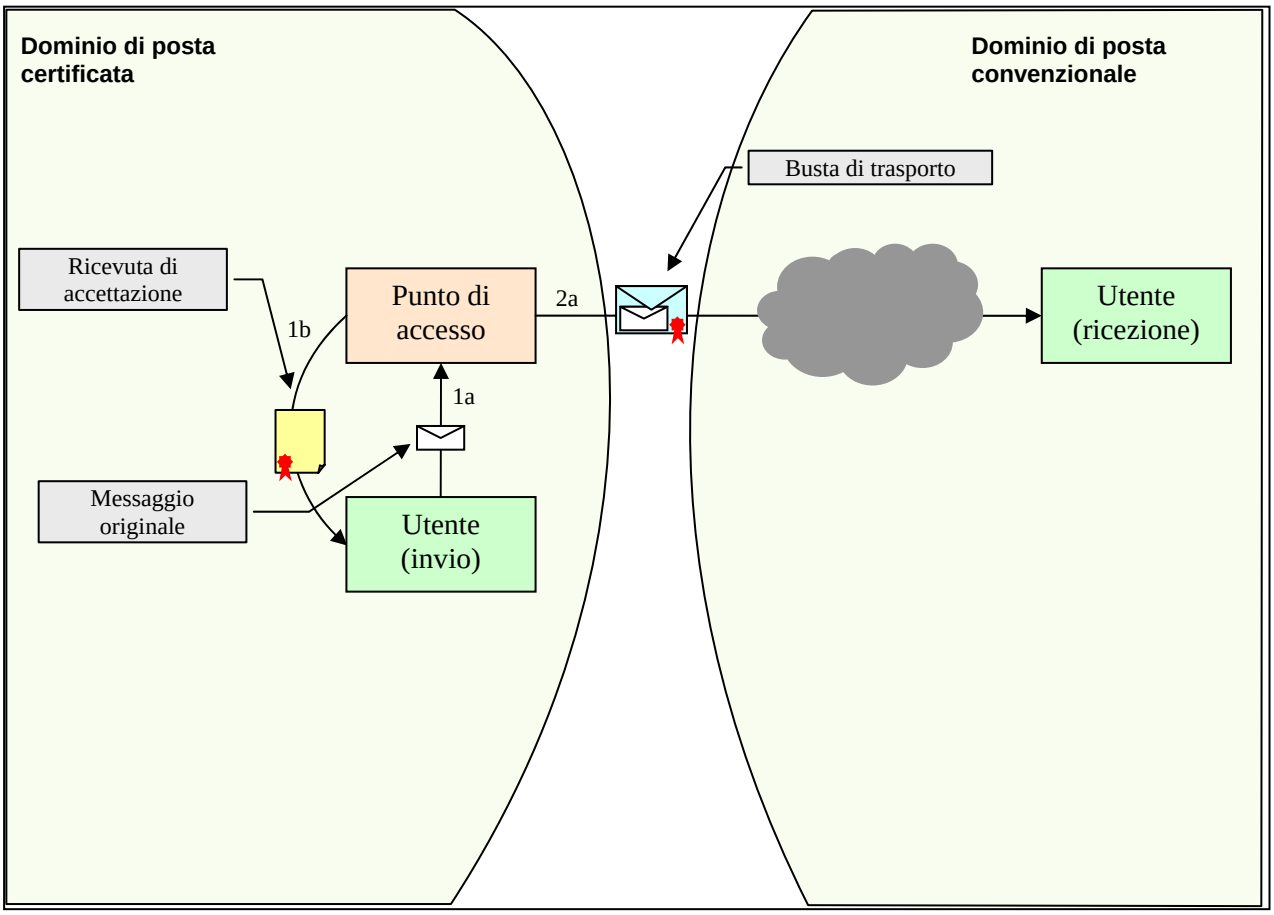
- 1a – l'utente invia una e-mail al Punto di accesso (PdA)
- 1b – il PdA rileva un contenuto potenzialmente pericoloso e restituisce al mittente una Avviso di non accettazione (ANA)
- 2 – il PdA non recapita al destinatario il messaggio ma lo conserva

9.1.2 Interazione fra un dominio di posta convenzionale (mittente) ed un dominio di posta certificata (ricevente)



n.b.: l'immissione di un messaggio di posta ordinaria nel circuito di trattamento della posta certificata è a discrezione del gestore destinatario; i criteri adottati per gestire la posta ordinaria devono essere noti e condivisi dall'utente finale del servizio.

9.1.3 Interazione fra un dominio di posta certificata (mittente) ed un dominio di posta convenzionale (ricevente)



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)].

10.5.3 Esempio

Nel seguito è riportato un esempio di certificato S/MIME conforme ai requisiti minimi descritti nel presente profilo. Sono utilizzati dei valori relativi a gestori immaginari e utilizzati a puro scopo esemplificativo.

a. Certificato d'uso generale in versione annotata

Un asterisco vicino all'etichetta di una estensione sta a significare che tale estensione è stata marcata come CRITICA.

```
VERSION:  3
SERIAL:  11226 (0x2bda)
INNER SIGNATURE:
  ALG. ID:    id-sha1-with-rsa-encryption
  PARAMETER:  0
ISSUER:
  Country Name:              IT
  Organization Name:         Certificatore 1
  Organizational Unit Name:  Certification Service Provider
  Common Name:               Certificatore S.p.A.
VALIDITY:
  Not Before:  Oct  5, 04 09:04:23 GMT
  Not After:   Oct  5, 05 09:04:23 GMT
SUBJECT:
  Country Name:              IT
  Organization Name:         AcmePEC S.p.A.
  Common Name:               Posta Certificata
PUBLIC KEY:  (key size is 1024 bits)
ALGORITHM:
  ALG. ID:    id-rsa-encryption
```

```
  PARAMETER:  0
 MODULUS:   0x00afbeb4 5563198a aa9bac3f 1b29b5be
            7f691945 89d01569 ca0d555b 5c33d7e9
            ...
            d15ff128 6792def5 b3f884e6 54b326db
            cf
 EXPONENT:  0x010001
 EXTENSIONS:
  Subject Alt Name:
  RFC Name:                  posta-certificata@acmepec.it
  Key Usage*:                Digital Signature
  Authority Key Identifier:    0x12345678 aaaaaaaa bbbbbbbb cccccccc dddddddd
  Subject Key Identifier:      0x3afae080 6453527a 3e5709d8 49a941a8 a3a70ae1
SIGNATURE:
 ALG. ID:    id-sha1-with-rsa-encryption
 PARAMETER:  0
 VALUE: 0x874b4d25 70a46180 c9770a85 fe7923ce
        b22d2955 2f3af207 142b2aba 643aaa61
        ...
        d8fd10b4 c9e00ebc c089f7a3 549a1907
        ff885220 ce796328 b0f8ecac 86ffb1cc
```

b. Certificato di uso generale in dump asn.1

```
  0 30  794: SEQUENCE {
  4 30  514:   SEQUENCE {
  8 A0    3:     [0] {
 10 02    1:       INTEGER 2
          :     }
 13 02    2:     INTEGER 11226
 17 30   13:     SEQUENCE {
 19 06    9:       OBJECT IDENTIFIER
          :         sha1withRSAEncryption (1 2 840 113549 1 1 5)
 30 05    0:       NULL
          :     }
 32 30  101:     SEQUENCE {
 34 31   11:       SET {
 36 30    9:         SEQUENCE {
 38 06    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 43 13    2:           PrintableString 'IT'
          :         }
          :       }
 47 31   28:       SET {
 49 30   26:         SEQUENCE {
 51 06    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 56 13   19:           PrintableString 'Certificatore 1'
          :         }
          :       }
 77 31   22:       SET {
 79 30   20:         SEQUENCE {
 81 06    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
 86 13   13:           PrintableString 'Certification Service Provider'
          :         }
          :       }
101 31   32:       SET {
103 30   30:         SEQUENCE {
105 06    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
110 13   23:           PrintableString 'Certificatore S.p.A.'
          :         }
          :       }
          :     }
135 30   30:     SEQUENCE {
137 17   13:       UTCTime '041005090423Z'
152 17   13:       UTCTime '051005090423Z'
          :     }
167 30   66:     SEQUENCE {
169 31   11:       SET {
171 30    9:         SEQUENCE {
173 06    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
178 13    2:           PrintableString 'IT'
          :         }
          :       }
182 31   23:       SET {
184 30   21:         SEQUENCE {
```

```
186 06   3:          OBJECT IDENTIFIER organizationName (2 5 4 10)
191 13   14:         PrintableString 'AcmePEC S.p.A.'
        :         }
        :       }
207 31   26:     SET {
209 30   24:       SEQUENCE {
211 06   3:         OBJECT IDENTIFIER commonName (2 5 4 3)
216 13   17:         PrintableString 'Posta Certificata'
        :         }
        :       }
        :     }
235 30  159:    SEQUENCE {
238 30   13:     SEQUENCE {
240 06   9:       OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
251 05   0:       NULL
        :       }
253 03  141:     BIT STRING 0 unused bits
        :       30 81 89 02 81 81 00 AF BE B4 55 63 19 8A AA 9B
        :       AC 3F 1B 29 B5 BE 7F 69 19 45 89 D0 15 69 CA 0D
        :       55 5B 5C 33 D7 E9 C8 6E FC 14 46 C3 C3 09 47 DD
        :       CD 10 74 1D 76 4E 71 14 E7 69 42 BE 1C 47 61 85
        :       4D 74 76 DD 0B B5 78 4F 1E 84 DD B4 86 7F 96 DF
        :       5E 7B AF 0E CE EA 12 57 0B DF 9B 63 67 4D F9 37
        :       B7 48 35 27 C2 89 F3 C3 54 66 F7 DA 6C BE 4F 5D
        :       85 55 07 A4 97 8C D1 5F F1 28 67 92 DE F5 B3 F8
        :             [ Another 12 bytes skipped ]
        :     }
397 A3  123:    [3] {
399 30  121:      SEQUENCE {
401 30   39:       SEQUENCE {
403 06   3:         OBJECT IDENTIFIER subjectAltName (2 5 29 17)
408 04   32:        OCTET STRING
        :         30 1E 81 1C 70 6F 73 74 61 2D 63 65 72 74 69 66
        :         69 63 61 74 61 40 61 63 6D 65 70 65 63 2E 69 74
        :         }
442 30   14:       SEQUENCE {
444 06   3:         OBJECT IDENTIFIER keyUsage (2 5 29 15)
449 01   1:         BOOLEAN TRUE
452 04   4:         OCTET STRING
        :         03 02 07 80
        :         }
458 30   31:       SEQUENCE {
460 06   3:         OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
465 04   24:        OCTET STRING
        :         30 16 11 11 11 11 AA AA AA AA AA BB BB BB BB CC CC
        :         CC CC DD DD DD DD
        :         }
491 30   29:       SEQUENCE {
493 06   3:         OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
498 04   22:        OCTET STRING
        :         04 14 3A FA E0 80 64 53 52 7A 3E 57 09 D8 49 A9
        :         41 A8 A3 A7 0A E1
        :         }
        :       }
        :     }
        :   }
522 30   13:  SEQUENCE {
524 06   9:    OBJECT IDENTIFIER
        :     sha1withRSAEncryption (1 2 840 113549 1 1 5)
535 05   0:    NULL
        :   }
537 03  257:  BIT STRING 0 unused bits
        :   87 4B 4D 25 70 A4 61 80 C9 77 0A 85 FE 79 23 CE
        :   B2 2D 29 55 2F 3A F2 07 14 2B 2A BA 64 3A AA 61
        :   1F F0 E7 3F C4 E6 13 E2 09 3D F0 E1 83 A0 C0 F2
        :   C6 71 7F 3A 1C 80 7F 15 B3 D6 1E 22 79 B8 AC 91
        :   51 83 F2 3A 84 86 B6 07 2B 22 E8 01 52 2D A4 50
        :   9F C6 42 D4 7C 38 B1 DD 88 CD FC E8 C3 12 C3 62
        :   64 0F 16 BF 70 15 BC 01 16 78 30 2A DA FA F3 70
        :   E2 D3 0F 00 B0 FD 92 11 6C 55 45 48 F5 64 ED 98
        :         [ Another 128 bytes skipped ]
        : }
```