REGOLE TECNICO-OPERATIVE PER L'USO DI STRUMENTI INFORMATICI E TELEMATICI NEL PROCESSO CIVILE

INDICE DEI CONTENUTI

Definizioni

Punto di accesso

È il punto che fornisce i servizi di accesso per l'invio di messaggi di posta certificata. Il punto di accesso fornisce i servizi di accesso dell'utente, emissione della *ricevuta di accettazione*, imbustamento del *messaggio originale* nel *messaggio di trasporto*.

Punto di ricezione

È l'entità che riceve il messaggio all'interno di un *dominio di posta certificata*. Corrisponde alla macchina destinata alla ricezione dei messaggi per il dominio. Effettua i controlli sulla provenienza/correttezza del messaggio ed emette la *ricevuta di presa in carico*, imbusta i messaggi errati in un *messaggio di anomalia di trasporto*.

Punto di consegna

Effettua la consegna del messaggio nella casella di posta elettronica dell'*utente di posta certificata* destinatario. Verifica la provenienza/correttezza del messaggio, emette la *ricevuta di avvenuta 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 certificata. La ricevuta di accettazione è firmata con la chiave del *gestore di posta certificata* del mittente.

Ricevuta di presa in carico

È emessa dal *punto di ricezione* verso il *gestore di posta certificata* mittente per attestare l'avvenuta presa in carico del messaggio da parte del *dominio di posta 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.

Ricevuta di avvenuta consegna

Il *punto di consegna* emette al mittente la ricevuta di avvenuta consegna nel momento in cui il messaggio è inserito nella *casella di posta certificata* del destinatario. È rilasciata una ricevuta di avvenuta consegna per ogni destinatario al quale il messaggio è consegnato. La ricevuta di avvenuta consegna porta in allegato i *dati di certificazione* e, per i destinatari primari del messaggio, il *messaggio originale*.

Ricevuta di errore di consegna

Nel caso in cui il *punto di consegna* sia impossibilitato a consegnare il messaggio nella *casella di posta certificata* del destinatario, il sistema emette una ricevuta di errore di consegna per indicare l'anomalia al mittente del *messaggio originale*.

Messaggio originale

È il messaggio originale inviato da un *utente di posta certificata* prima del suo arrivo al *punto di accesso*. Il messaggio originale è consegnato all'*utente di posta certificata* di destinazione per mezzo di un *messaggio di trasporto* che lo contiene.

Messaggio di trasporto

È il messaggio creato dal *punto di accesso*, all'interno del quale è inserito il *messaggio originale* inviato dall'*utente di posta certificata* ed i relativi *dati di certificazione*. Il

messaggio di trasporto è firmato con la chiave del *gestore di posta certificata* mittente. Il messaggio di trasporto è consegnato immodificato nella *casella di posta certificata* di destinazione per permettere la verifica dei *dati di certificazione* da parte del ricevente.

Messaggio di anomalia di trasporto

Quando un messaggio errato/non di posta certificata deve essere consegnato ad un *utente di posta certificata*, il messaggio è inserito in un messaggio di anomalia di trasporto per evidenziare l'anomalia al destinatario. Il messaggio di anomalia di trasporto è firmato con la chiave del *gestore di posta certificata* del destinatario.

Dati di certificazione

Sono un insieme di dati che descrivono il *messaggio originale* e sono certificati dal *gestore di posta certificata* del mittente. I dati di certificazione sono inseriti nelle varie ricevute e sono trasferiti all'*utente di posta certificata* di destinazione insieme al *messaggio originale* per mezzo di un *messaggio di trasporto*. Tra i dati di certificazione sono: data ed ora di invio, mittente, destinatario, oggetto, identificativo messaggio, ecc.

Gestore di posta certificata

È un entità che gestisce uno o più *domini di posta certificata* con i relativi *punti di accesso, ricezione e consegna*. È titolare della chiave usata per la firma delle ricevute e dei messaggi di trasporto. Si interfaccia con altri gestori di posta certificata per l'interoperabilità con altri *utenti di posta certificata*.

Dominio di posta certificata

Corrisponde ad un dominio DNS dedicato alle caselle di posta elettronica degli *utenti di posta certificata*. All'interno di un dominio di posta certificata tutte le caselle di posta elettronica devono appartenere ad *utenti di posta certificata*. L'elaborazione dei messaggi di posta certificata (ricevute utente, messaggi di trasporto, ecc.) deve avvenire anche nel caso mittente e destinatario appartengano allo stesso dominio di posta certificata.

Indice dei gestori di posta certificata

Consiste in un server LDAP posizionato in un'area raggiungibile dai vari *gestori di posta certificata*. Contiene l'elenco dei *domini e dei gestori di posta certificata* con i relativi certificati relativi alle chiavi usate per la firma delle ricevute e dei *messaggi di trasporto*.

Casella di posta 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 certificata. Una casella di posta certificata può essere definita esclusivamente all'interno di un *dominio di posta certificata*.

Utente di posta certificata

È un utente a cui è assegnata una *casella di posta certificata*. Utilizza il *punto di accesso* del proprio *gestore di posta certificata* per inviare messaggi di posta certificata.

Elaborazione dei messaggi

Formato dei messaggi generati dal sistema

Il sistema genera i messaggi (ricevute, messaggi di trasporto e di anomalia di trasporto) 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.
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 i messaggi 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>
```

il relativo messaggio di trasporto generato avrà un campo "From" del tipo:

```
From: "mario.bianchi@dominio.it" <posta-certificata@gestore.it>
```

Per consentire che le risposte al messaggio siano correttamente indirizzate verso il mittente originale, è necessario che l'indirizzo di quest'ultimo sia riportato nel campo "Reply-To". Qualora tale campo non fosse esplicitamente specificato nel messaggio originale, il sistema che genera il messaggio di trasporto provvede a crearlo estraendolo dal campo "From" originale.
Per l'invio delle ricevute, il sistema usa come destinatario il mittente del messaggio originale. Questo è ricavato dal campo "Reply-To" o, in sua assenza, dal campo "From" dell'intestazione originale del messaggio.
Tutti i messaggi generati dal sistema di posta certificata sono identificabili per la presenza di un header specifico. Questo header è utile per impedire loop di messaggi nel caso di scambio tra sistemi che prevedono l'invio di ricevute/messaggi di trasporto. È infatti possibile che un messaggio inviato da una casella di posta certificata e destinato ad un'altra casella anch'essa appartenente al servizio di posta certificata inneschi uno scambio improprio di messaggi. La ricezione di una ricevuta potrebbe infatti far scattare nel sistema la generazione di un'ulteriore ricevuta. Per ovviare a tale problema il sistema deve controllare l'eventuale presenza dell'header identificativo per verificare la natura del messaggio.

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.

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 del messaggio originale (Message-ID)
- la data e l'ora dell'evento
- il mittente del messaggio originale
- l'oggetto del messaggio originale
- il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.)
- il codice identificativo dei messaggi generati (ricevute, errori, ecc.)
- il server mittente

il server destinatario

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

Punto di accesso

Al momento dell'invio di un messaggio di posta certificata il punto di accesso deve accertare l'identità di chi effettua il collegamento. La modalità per l'accertamento dell'identità di un utente abilitato all'utilizzo del servizio deve poter prevedere, ove disponibili, l'utilizzo della carta d'identità elettronica o della carta nazionale dei servizi. Tale verifica è necessaria esclusivamente per garantire che il messaggio sia inviato da un utente del servizio di posta certificata. Il punto di accesso non verifica che il mittente specificato nel messaggio sia congruente con i dati di identificazione dell'utente.
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 un messaggio 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. 0), 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). 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).
Il meccanismo di sicurezza per il colloquio tra i server partecipanti all'infrastruttura di posta certificata è realizzato mediante imbustamento e firma dei messaggi in uscita dal punto di accesso e la loro verifica in ingresso al punto di ricezione. Il messaggio originale (completo di header, testo ed eventuali allegati) è inserito come allegato all'interno di un messaggio di trasporto. Il messaggio di trasporto firmato permette di verificare che il messaggio originale non sia stato modificato durante il suo percorso dal dominio mittente al dominio destinatario. La firma apposta sul messaggio dal sistema mittente è verificata all'arrivo sul server di destinazione.
Il dominio ricevente dovrà effettuare esclusivamente dei controlli formali sul messaggio ricevuto inoltrando il messaggio di trasporto immodificato al destinatario. Rispetto ad una soluzione che prevede la ritrasformazione del messaggio di trasporto nel messaggio originario, si ottiene la visibilità dei dati di certificazione inseriti dal messaggio (testo, XML, ulteriori allegati) permettendone così la verifica da parte del destinatario.
La sicurezza tra mittente e destinatario è completata mediante un meccanismo di protezione per le connessioni esterne all'architettura di posta certificata (tra utente e punto di accesso e 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 realizzate mediante l'uso di protocolli sicuri (es. basati su TLS come imaps, pop3s) o che prevedano l'attivazione di un canale sicuro durante il colloquio (es. SMTP STARTTLS, POP3 STLS).
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 ed il corrispondente messaggio 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.

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.

Qualora il messaggio non fosse formalmente valido, il punto di accesso dovrà non accettare il messaggio all'interno del sistema di posta certificata non emettendo, quindi, la relativa ricevuta di accettazione.

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 messaggio originale]
```

Il primo campo identifica il messaggio come ricevuta di accettazione. Il campo "Subject" indica al destinatario che il messaggio è la ricevuta di una sua comunicazione. È composto dalla stringa "ACCETTAZIONE:" seguita dal subject del messaggio originale a cui la ricevuta fa riferimento.
Il corpo del messaggio di ricevuta è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile secondo un modello riportante i seguenti dati:

```
Ricevuta di accettazione
Il giorno [data] alle ore [ora] ([zona]) il messaggio
"[subject]" proveniente da "[mittente]"
ed indirizzato a:
[destinatario1] (["posta certificata" | "posta ordinaria"])
[destinatario2] (["posta certificata" | "posta ordinaria"])
.
.
.
[destinatarion] (["posta certificata" | "posta ordinaria"])
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. All'interno della ricevuta potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal gestore di posta certificata.

Messaggio di trasporto

Il messaggio di trasporto consiste in un messaggio generato dal punto di accesso e che contiene il messaggio originale ed i dati di certificazione.
Il messaggio 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 0)
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: "[mittente originale]" <posta-certificata@[dominio_di_posta]>
Reply-To: [mittente originale (inserito solo se assente)]
```

Il corpo del messaggio 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]"
indirizzato a:
[destinatario1]
[destinatario2]
.
.
.
[destinatarion]
Il messaggio originale è incluso in allegato.
Identificativo messaggio: [identificativo]
```

All'interno del messaggio 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. Nello stesso messaggio di trasporto è inoltre incluso un allegato XML che specifica in formato elaborabile i dati di certificazione già riportati nel testo. Al messaggio di trasporto possono inoltre essere allegati ulteriori elementi opzionali per specifiche funzionalità fornite dal gestore di posta certificata.

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

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).
Lo scambio di messaggi tra diversi gestori avviene tramite una transazione basata sul protocollo SMTP come definita dalla RFC 2821. 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. Eventuali errori derivanti dal colloquio SMTP (es. destinatari non validi, server non disponibile, ecc.) sono gestiti mediante i meccanismi standard di notifica degli errori propri del protocollo SMTP.
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 un messaggio di trasporto corretto:
  - emette una ricevuta di presa in carico verso il gestore mittente (cfr. 0);
  - inoltra il messaggio di trasporto verso il punto di consegna (cfr. 0);
- se il messaggio in ingresso è un messaggio di trasporto errato/non è un messaggio di trasporto:
  - imbusta il messaggio in arrivo in un messaggio di anomalia di trasporto (cfr. 0);
  - inoltra il messaggio di anomalia di trasporto 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.

Verifiche sui messaggi in ingresso

Al ricevimento di un messaggio presso il punto di ricezione, il sistema effettua una serie di controlli per verificare che il messaggio di trasporto sia corretto/integro:

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.

Controllo della validità della firma

È verificata la correttezza della firma S/MIME del messaggio effettuando il ricalcolo degli algoritmi di firma.

Se tutti i controlli hanno esito positivo, il sistema stabilisce che il messaggio in ingresso è un messaggio di trasporto corretto altrimenti lo considera come errato o di posta ordinaria.

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 un messaggio 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]
```

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. All'interno della ricevuta potranno inoltre essere presenti ulteriori allegati per specifiche funzionalità fornite dal gestore di posta certificata.

Messaggio di anomalia di trasporto

Qualora uno dei test evidenzi un errore nel messaggio in arrivo, il sistema lo inserisce in un messaggio di anomalia di trasporto. 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: "[mittente originale]" <posta-certificata@[dominio_di_posta]>
Reply-To: [mittente originale (inserito solo se assente)]
```

Il corpo del messaggio di anomalia di trasporto 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]"
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.
```

Nel messaggio di anomalia di trasporto 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" del messaggio di anomalia di trasporto è modificato per consentire la verifica della firma da parte del destinatario, i dati di instradamento del messaggio di trasporto (forward path e reverse path) 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.

Punto di consegna

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 esclusivamente a fronte della ricezione di un messaggio di trasporto valido, identificabile dalla presenza dell'header:

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

In tutti gli altri casi (es. messaggi di anomalia di trasporto), 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 in formato elaborabile 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 una ricevuta di errore di consegna (cfr. 0). La ricevuta di errore di consegna è generata, a fronte

di un errore, esclusivamente nei casi previsti per la ricevuta di avvenuta consegna (arrivo di un messaggio di trasporto corretto).

Ricevuta di avvenuta consegna

Le ricevute di avvenuta consegna sono costituite da un messaggio di posta elettronica inviato al mittente e riportante data ed ora di avvenuta consegna, dati del mittente e del destinatario ed 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 messaggio originale]
```

Il primo campo identifica il messaggio come ricevuta di avvenuta consegna. Il campo "Subject" indica al destinatario che il messaggio è la ricevuta di una sua comunicazione. È composto dalla stringa "CONSEGNA:" seguita dal subject del messaggio originale a cui la ricevuta fa riferimento.
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]"
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 per permetterne una elaborazione automatica. 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). Qualora il sistema non potesse determinare con certezza la natura del destinatario (primario od in copia) per problemi di ambiguità del campi "To" e "Cc", la consegna dovrà essere considerata come indirizzata ad un destinatario primario ed includere il messaggio originale completo.

Ricevuta breve di avvenuta consegna

Se all'interno del messaggio di trasporto è presente l'intestazione:

```
X-TipoRicevuta: breve
```

il punto di consegna emette, per i destinatari primari, una ricevuta breve di avvenuta consegna. L'assenza di tale intestazione o un suo diverso valore comportano l'elaborazione della ricevuta di avvenuta consegna secondo le modalità già descritte al punto precedente. Il valore dell'intestazione nel messaggio di trasporto deriva dal messaggio originale (cfr. punto precedente) permettendo così al mittente di determinare 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 precedente.
Alla ricevuta breve di avvenuta consegna è allegato, invece del messaggio originale, un messaggio avente la stessa struttura MIME ma i cui allegati sono sostituiti da altrettanti file di testo contenenti gli hash del file al quale si vanno a sostituire. 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.

Ricevuta di errore di consegna

Nel caso si verifichi un errore nella fase di consegna del messaggio, il sistema genera una ricevuta di errore di consegna da restituire al mittente con l'indicazione dell'errore riscontrato.
Per una ricevuta di errore di consegna gli header contengono i seguenti campi:

```
X-Ricevuta: errore-consegna
Date: [data di emissione ricevuta]
Subject: ERRORE: [subject originale]
From: posta-certificata@[dominio_di_posta]
To: [mittente messaggio originale]
```

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

```
Errore di consegna del messaggio
Il giorno [data] alle ore [ora] ([zona]) nel messaggio
"[subject]" proveniente da "[mittente]"
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 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.

Formati

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, messaggi 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, ricevute, messaggi, ecc. generati dal server. Il riferimento temporale può essere generato con qualsiasi sistema che garantisca uno scarto non superiore ad 1 secondo rispetto al Tempo Universale Coordinato (UTC).

Formato data/ora utente

Le indicazioni temporali fornite dal servizio in formato leggibile dall'utente (testo delle ricevute, messaggi 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.

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).

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).

Messaggio originale

MIME type: `message/rfc822`
Nome allegato: `postacert.eml`

Dati di certificazione

Set di caratteri: `UTF-8`
MIME type: `application/xml`
Nome allegato: `daticert.xml`

Dati di certificazione

Di seguito viene proposto 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-->
<!--"altro" = errore generico-->
<!ELEMENT postacert (intestazione, dati)>
<!ATTLIST postacert
      tipo (accettazione |
            presa-in-carico |
            avvenuta-consegna |
            posta-certificata |
            errore-consegna) #REQUIRED
      errore (nessuno |
              no-dest |
              no-dominio |
              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,
                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 originale-->
<!ELEMENT identificativo (#PCDATA)>

<!--Per le ricevute di consegna e di errore di consegna-->
<!--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)>
```

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. Il contenuto di tale indice è interrogabile sia tramite LDAP che via HTTP su protocollo TLS per garantirne l'autenticità e l'integrità. 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 usando gli attributi "`providerCertificateSubject`" o "`managedDomains`". L'attributo "`LDIFLocationURL`" deve puntare ad un oggetto HTTP/HTTPS, messo a disposizione dal gestore, che contiene un file in formato LDIF secondo RFC 2849. Tale file LDIF è scaricato con cadenza regolare dal sistema

LDAP centralizzato ed applicato sul record relativo al gestore. Il file LDIF che comprende i dati di tutti i gestori di posta certificata è disponibile, come oggetto HTTPS, alla URL puntata dall'attributo "`LDIFLocationURL`" del record "`dn: o=postacert`". Mediante tale LDIF, i singoli gestori dovranno replicare periodicamente il contenuto dell'indice localmente, al fine di migliorare i tempi di risposta del sistema evitando di effettuare richieste LDAP per ogni fase di elaborazione del messaggio.

Di seguito sono riportati gli attributi definiti per lo schema dell'indice dei gestori di posta certificata:

`providerCertificateSubject`	DN	Riporta il "subject DN" contenuto nel certificato usato dal gestore per la firma delle ricevute e dei messaggi di trasporto
`providerCertificate`	Certificate Binary transfer	Certificato/i usato/i dal gestore per la firma delle ricevute e dei messaggi 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 HTTP dove è mantenuta la definizione in formato LDIF del record relativo al gestore (dell'intero indice per il record "`dn: o=postacert`")

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 'providerCertificateSubject'
        DESC 'Subject DN del certificato X.509 del gestore'
        EQUALITY distinguishedNameMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

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 )

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    ( providerCertificateSubject $
                  providerCertificate $
                  providerName $
                  mailReceipt $
                  managedDomains $
                  LDIFLocationURL )
        MAY     ( description ) )
```

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://postacert.ct.rupa.it/postacert.ldif
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.
providerCertificateSubject: C=IT, O=Anonima Posta Certificata S.p.A.,
 Email=posta-certificata@anpocert.it
providerCertificate;binary:: MIIDBjCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQ
 QFADBmMQswCQYDVQQGEwJJVDEpMCcGA1UEChMgQW5vbmltYSBQb3N0YSBDZXJ0aWZp
 Y2F0YSBTLnAuQS4xLDAqBgkqhkiG9w0BCQEWHXBvc3RhLWN1cnRpZmljYXRhQGFucG
 9jZXJ0Lml0MB4XDTAyMTIwOTE3MjQxNVoXDTAzMTIwOTE3MjQxNVowZjELMAkGA1UE
 BhMCSVQxKTAnBgNVBAoTIEFub25pbWEgUG9zdGEgQ2VydGlmaWNhdGEgUy5wLkEuMS
 wwKgYJKoZIhvcNAQkBFh1wb3N0YS1jZXJ0aWZpY2F0YUBhbnBvY2VydC5pdDCBnzAN
 BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAr8J+qKKdxV9LzDMPqwnEy0P8H/KwbI0Szs
 8p6UZajZdpeUK0NcbrvlQyXZNNtSMC2uL09HDyx8agjgZWdhypnehguiSK3bushal5
 RSpMGhiqxmz2b0HhOG73Gfa1Zelqrwqm Elna4MNUaLhbOvTd/sqPUS378w5IaIhWxz
 y34XcCAwEAAaOBwzCBwDAdBgNVHQ4EFgQUN81C0znQWEs0xspZ/aBzsaGvRZMwgZAG
 A1UdIwSBiDCBhYAUN81C0znQWEs0xspZ/aBzsaGvRZOhaqRoMGYxCzAJBgNVBAYTAk
 lUMSkwJwYDVQQKEyBBbm9uaW1hIFBvc3RhIEN1cnRpZmljYXRhIFMucC5BLjEsMCoG
 CSqGSIb3DQEJARYdcG9zdGEtY2VydGlmaWNhdGFAYW5wb2N1cnQuaXSCAQAwDAYDVR
 0TBAUwAwEB/zANBgkqhkiG9w0BAQQFAAOBgQA58BZ+qlqSKpuffzTBpMtbeFkDIxMq
 Ma+ycnxdMNvcWgCmlA9ZiFJsvqYhDDqAXxfHjkrzXuSZkYq6WiQCsLp0aYVy40QCIw
 bOunhrvsxh3vsG5CgN76JzZ95Z/1OCFNhLfqf1VH2NSS8TaYCCi/VO7W1Q1KkcA2V1
 x1QP7McSUw==
mailReceipt: ricevute@anpocert.it
LDIFLocationURL: http://www.anpocert.it/LDIF/anpocert.ldif
```

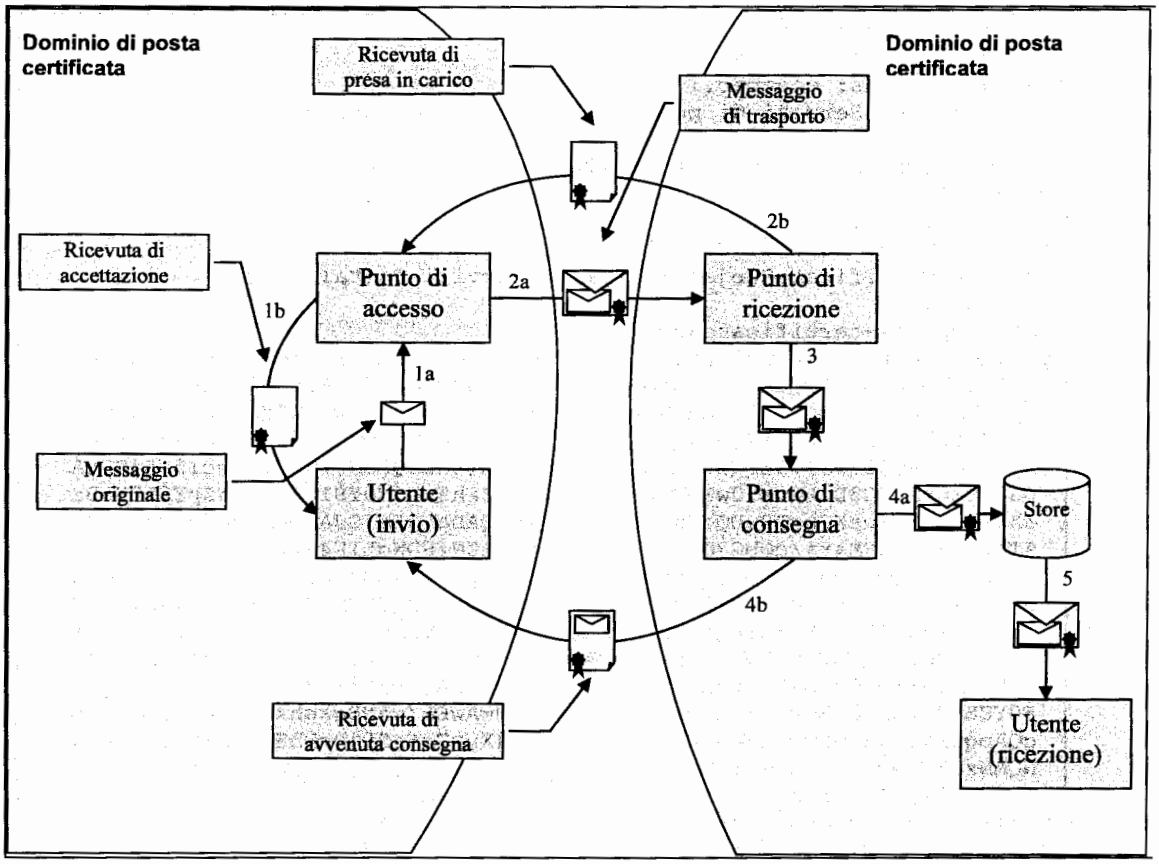
```
managedDomains: posta.anpocert.it
managedDomains: cert.azienda.it
managedDomains: costmec.it
description: Servizi di posta certificata per aziende

dn: providerName=Servizi Postali S.r.l.,o=postacert
objectclass: top
objectclass: provider
providerName: Servizi Postali S.r.l.
providerCertificateSubject: C=IT, O=Servizi Postali S.r.l.,
OU=D.C.C.,
 Email=posta-certificata@serpostal.it
providerCertificate;binary:: MIIDHjCCAoegAwIBAgIBADANBgkqhkiG9w0BAQ
 QFADBuMQswCQYDVQQGEwJJVDEfMB0GA1UEChMWU2Vydml6aSBQb3N0YWxpIFMuci5s
 LjEPMA0GA1UECxMGRC5DLkMuMS0wKwYJKoZIhvcNAQkBFh5wb3N0YS1jZXJ0aWZpY2
 F0YUBzZXJwb3N0YWwuaXQwHhcNMDIxMjA5MTczMjE2WhcNMDMxMjA5MTczMjE2WjBu
 MQswCQYDVQQGEwJJVDEfMB0GA1UEChMWU2Vydml6aSBQb3N0YWxpIFMuci5sLjEPMA
 0GA1UECxMGRC5DLkMuMS0wKwYJKoZIhvcNAQkBFh5wb3N0YS1jZXJ0aWZpY2F0YUBz
 ZXJwb3N0YWwuaXQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKoc7n6zA+sO8N
 ATMcfJ+U2aoDEsrj/cObG3QAN6Sr+lygWxYXLBZNfSDWqLlK4edLr4gCZIDFsq0PIE
 aYZhYRGjhbcuJ9H/ZdtWdXxcwEWN4mwFzlsASogsh5JeqS8db3AlJWkvhO9EUfaCYk
 8YMAkXYdCtLD9s9tCYZeTE2ut9AgMBAAGjgcswgcgwHQYDVR0OBBYEFHPw7VJIoIM3
 VYhuHaeAwpPF51eMMIGYBgNVHSMEgZAwgY2AFHPw7VJIoIM3VYhuHaeAwpPF51eMoX
 KkcDBuMQswCQYDVQQGEwJJVDEfMB0GA1UEChMWU2Vydml6aSBQb3N0YWxpIFMuci5s
 LjEPMA0GA1UECxMGRC5DLkMuMS0wKwYJKoZIhvcNAQkBFh5wb3N0YS1jZXJ0aWZpY2
 F0YUBzZXJwb3N0YWwuaXSCAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQQFAAOB
 gQApqeXvmOyEjwhMrXezPAXELMZwv4qqr5ri4XuxTq6sS9jRsEbZrS+NmbcJ7S7eFw
 NQMNxYFVJqdWoLh8qExsTLXnsKycPSnHbCfuphrKvXjQvR2da75U4zGSkroiyvJ2s9
 TtiCcT3lQtIjmvrFbaSBiyzj+za7foFUCQmxCLtDaA==
mailReceipt: presaincarico@serpostal.it
LDIFLocationURL: http://servizi.serpostal.it/ldif.txt
managedDomains: servizi-postali.it
managedDomains: postaricevuta.it
description: Servizi di posta certificata per il pubblico
```

APPENDICE

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 certificata.



04A010341

GIANFRANCO TATOZZI, *direttore* FRANCESCO NOCITA, *redattore*

(G403130/1) Roma, 2004 - Istituto Poligrafico e Zecca dello Stato S.p.A. - S.