Internet Draft F. Gennai
Intended status: Informational A. Shahin
Expires: February 08, 2011 ISTI-CNR
C. Petrucci
DigitPA
A. Vinciarelli
July 29, 2010

Certified Electronic Mail
draft-gennai-smime-cnipa-pec-08.txt

Status of this Memo

Copyright Notice

Abstract

Since 1997, the Italian Laws have recognized electronic delivery systems as legally usable. In 2005 after two years of technical

tests, the characteristics of an official electronic delivery service, named certified electronic mail (in Italian "Posta Elettronica Certificata") were defined, giving the system legal standing.

Design of the entire system was carried out by the National Center for Informatics in the Public Administration of Italy (DigitPA), followed by efforts for the implementation and testing of the service. The DigitPA has given the Italian National Research Council (CNR), and in particular The Institute of Information Science and Technologies at the CNR (ISTI), the task of running tests on providers of the service to guarantee the correct implementation and interoperability. This document describes the certified email system adopted in Italy. It represents the system as it is at the moment of writing, following the technical regulations that were written based upon the Italian Law DPR. November 2, 2005.

Table of Contents

1. Introduction

Since 1997, the Italian Laws have recognized electronic delivery systems as legally usable. In 2005 after two years of technical tests, the characteristics of an official electronic delivery service, named certified electronic mail (in Italian Posta Elettronica Certificata, from now on "PEC") were defined, giving the system legal standing.
This document represents the English version of the Italian specfications, (http://www.cnipa.gov.it/site/_files/Pec-def.pdf) which will be the ultimate PEC reference.

1.1. Scope

To ensure secure transactions over the Internet, cryptography can be associated with electronic messages in order to provide some guarantee on sender identity, message integrity, confidentiality, and non-repudiation of origin. Many end-to-end techniques exist to accomplish such goals, and some offer a high level of security. The downside of end-to-end cryptography is the need for an extensive penetration of technology in society, because it is essential for every user to have asymmetric keys and certificates signed by a Certification Authority. Along with that, users would need to have an adequate amount of knowledge regarding the use of such technology.

PEC on the other hand uses applications running on servers to digitally sign messages, thus avoiding the complexity end-to-end systems bring about. By doing so, the user needs only have an ordinary mail client with which to interact. The downside is that the level of security drops, since the protection does not cover the entire transaction. Nonetheless, application is simpler and does not require specific user skills, making it easily more widespread among users.

This document describes PEC's technical aspects and features. It presents the details of the protocol and the messages that are sent between service providers, introducing the system adopted by the Italian government for the exchange of certified emails.

1.2. Notational Conventions

1.2.1. Requirement Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [REQ].

1.2.2. Acronyms

CMS:	Cryptographic Message Syntax
CNIPA:	Italian National Agency for Digital Administration (Centro Nazionale per l'Informatica nella Pubblica Amministrazione)
CNR:	Italian National Research Council (Consiglio Nazionale delle Ricerche)
CRL:	Certificate Revocation List
CRL DP:	Certificate Revocation List Distribution Point
DNS:	Domain Name Service
DTD:	Document Type Definition
FQDN:	Fully Qualified Domain Name
ISTI:	The Institute of Information Science and Technologies at the CNR (Istituto di Scienza e Tecnologie dell'Informazione "A.Faedo")
LDAP:	Lightweight Directory Access Protocol
LDIF:	LDAP Data Interchange Format
MIME:	Multipurpose Internet Mail Extensions
PEC:	Certified Electronic Mail (Posta Elettronica Certificata)
S/MIME:	Secure/MIME
SMTP:	Simple Mail Transfer Protocol
TLS:	Transport Layer Security
XML:	eXtensible Markup Language

1.2.3. Terminology and Definitions

Certification data: A set of data certified by the sender's PEC provider that describes the original message. It includes: date and time of dispatch, sender email address, recipient(s) email address(es), subject, and message ID.

Certified electronic mail: A service based on electronic mail, as defined by the [SMTP] standard and its extensions, which permits the transmission of documents produced with informatics tools.

DigitPA: Ex-CNIPA.

Holder: The person or organization to whom a PEC mailbox is assigned.

Message sent: A PEC message is considered sent when the sender's PEC provider, after several checks, accepts the email and returns an acceptance PEC notification to the sender.

Message received: A PEC message is considered received when it is stored in the receiver's mailbox, after which the receiver PEC provider returns a delivery PEC notification to the sender.

Msgid: Is the message ID generated by the email client, as defined in [EMAIL], before the message is submitted to the PEC system.

Ordinary mail: Non-PEC email messages.

Original message: Is the user-generated message before its arrival to the sender access point. The original message is delivered to the recipient inside a PEC transport envelope.

PEC domain: Corresponds to a DNS domain dedicated to the holders' mailboxes.

PEC mailbox: An electronic mailbox for which delivery PEC notifications are issued upon reception of PEC messages. Such a mailbox can be defined exclusively within a PEC domain.

PEC msgid: Is a unique identifier generated by the PEC system, which will substitute the msgid.

PEC provider: The entity that handles one or more PEC domains with their relative points of access, reception, and delivery. It is the holder of the key that is used for signing PEC notifications and envelope, and it interacts with other PEC providers for interoperability with other holders.

PEC provider's key: Is a key released by DigitPA to every PEC provider. It is used to sign PEC notifications and envelopes, and to authorize access to the PEC providers directory.

PEC providers directory: Is an LDAP server positioned in an area reachable by all PEC service providers. It constitutes the technical structure related to the public list of PEC service providers and contains the list of PEC domains and service providers with relevant certificates.

Service mailbox: A mailbox for the sole use of the provider, dedicated for the reception of take in charge and virus detection PEC notifications.

Time stamp: A digital evidence with which a temporal reference, that can't be repudiated, is attributed to one or more documents.

2. PEC model

2.1. System-generated messages

The PEC system generates messages in MIME format composed of a descriptive textual part and other [MIME1] parts, the number and content of which varies according to the type of message generated.

A system-generated message falls into one of the following categories:

o Notifications;

o Envelopes.

The message is inserted in an S/MIME v3 structure in CMS format and signed with the PEC provider's private key. The X.509v3 certificate associated with the key MUST be included in the aforementioned structure. The S/MIME format used to sign system-generated messages is the "multipart/signed" format (.p7s), as described in section 3.4.3 of [SMIMEV3].

To guarantee the verifiability of signatures on as many mail clients as possible, X.509v3 certificates used by certified email systems MUST abide by the profile found in section 6.5.

In order for the receiving mail client to verify the signature, the sender address MUST coincide with the one indicated within the X.509v3 certificate. For this mechanism, PEC transport envelopes MUST indicate in the "From:" field a single author's address which is different from the one contained in the original message. To allow for better message usability by the receiving user, the author's mail address in the original message is inserted as a "display name". For example, a "From:" field such as:

```
From: "John Smith" <john.smith@domain.example.com>
```

would result in the following "From:" value in the respective PEC transport envelope:

```
From: "On behalf of: john.smith@domain.example.com"
                         <certified-mail@provider.example.com>
```

Both "From:" and "Sender:" fields MUST contain the same value. In order for replies to be correctly sent back to the proper destination, the "Reply-To:" field in the PEC transport envelope MUST contain the same unaltered value of the original message's "Reply-To:" field. When it is not explicitly specified in the original message, the system that generates the PEC transport envelope creates it by extracting the information from the "From:" field in the original message.

When PEC notifications are sent, the system MUST use the original message sender's address as the destination address, as is specified in the reverse path data of the SMTP protocol. PEC notifications MUST be sent to the sender's PEC mailbox without taking into account the "Reply-To:" field, which might be present in the original message's header.

All system-generated PEC messages are identifiable for having a specific header defined in PEC according to the type of message generated.

To determine the certification data, the elements used for the actual routing of the message are employed. In SMTP dialog phases, the reverse path and forward path data ("MAIL FROM" and "RCPT TO" commands) are thus considered certification data of both the sender and the recipients respectively. Addressing data present in the message body ("To:" and "Cc:" fields) are used solely in order to discriminate between primary and carbon copy recipients when necessary; addressing data present in the "Bcc:" field MUST be considered invalid by the system.

2.1.1. Message types

All system-generated messages inherit their header fields and values from the original message, with extra fields added according to the type of message generated.

2.1.1.1. PEC notifications

They have the purpose of informing the sending user and interacting providers of the progress the message is making within the PEC network.

2.1.1.1.1. Success PEC notifications

Indicates an acknowledgment on the provider's side for the reception or handling of a PEC message. More specifically, it can indicate one of 3 situations: acceptance, take in charge, or delivery.

Added header fields are:

- X-Ricevuta

- X-Riferimento-Message-ID

The field "X-Ricevuta" (Notification) indicates the type of PEC notification contained in the message, whereas "X-Riferimento-Message-ID" (Reference Message-ID) contains the message ID generated by the mail client.

Body contents differ according to notification type. This is described more thoroughly in chapter 3.

- An acceptance PEC notification informs the user that his provider has accepted the message and will be taking care of passing it on to the provider(s) of the addressee(s).

- A take in charge PEC notification is an inter-provider communication only, it MUST NOT be sent to the users. With this notification, the receiving provider simply informs the sending one that it has received a PEC message, and will take the responsibility of forwarding it to the addressee(s). From then on, the sender provider is no longer held responsible as to the whereabouts of the message, but is limited to notifying its user of the success or failure of delivery.
- Delivery PEC notifications take place as the final communication of a transaction, indicating overall success in handing the message over to the addressee(s).

2.1.1.1.2. Delay PEC notifications

Delay PEC notifications are sent out 12 hours after a message has been dispatched from the sending provider, and no take in charge or delivery PEC notification was received. These have the sole purpose of notifying the user of the delay.

If another 12 hours go by without any sign of a take in charge or delivery PEC notification (amounting to a 24-hour delay), another delay PEC notification is dispatched to the user informing him of the possible delivery failure. The provider will not keep track of the delay any further.

2.1.1.1.3. Failure PEC notifications

They are sent when there is some error in transmission or reception. More specifically, a failure PEC notification can indicate either a formal-exception error, or a virus detection.

Added header fields are:

- X-Ricevuta;

- X-Riferimento-Message-ID;

- X-VerificaSicurezza [optional]

"X-Ricevuta" (Notification) and "X-Riferimento-Message-ID" (Reference Message-ID) have the same roles as indicated in section 2.1.1.1.1 (Success Notifications). "X-VerificaSicurezza" (Security Verification) is an optional header field, used for virus-related PEC notifications.

Body contents differ according to notification type. This is described more thoroughly in chapter 3.

2.1.1.2. PEC envelopes

Messages entering the PEC network are inserted within specific PEC messages, called envelopes, before they are allowed to circulate further within the network. These envelopes MUST inherit the following header fields, along with their unmodified values, from the message itself:

o Received

o To

o Cc

o Return-Path

o Reply-to (if present)

Depending on the type of message requesting admission into the PEC network, it will be inserted either in a "Transport Envelope", or in a "Anomaly Envelope". Distinction will be possible through the addition of the "X-Transport" header field.

2.2. Basic structure

```
             +-------------+               +------------+
             |    +--+     |               |            |
             |    |AP|     |      PEC      |            |
   +----+    |    +--+     |   messages &  | +---+ +--+ |    +----+
   |user|<-->|             |<------------->| |InP| |DP| |<-->|user|
   +----+    | +--+  +---+ | notifications | +---+ +--+ |    +----+
             | |DP|  |InP| |               |            |
             | +--+  +---+ |               |            |
             +-------------+               +------------+
                  PEC                            PEC
                 sender                        receiver
                provider                       provider
```

where:

AP = Access Point
DP = Delivery Point
InP = Incoming Point

2.2.1. Access point

This is what the user client at the sender side interacts with, giving the user access to PEC services set up by the provider.

Such access MUST be preceded by user authentication on the system (see section 5.2). The access point receives the original messages its user wishes to send, runs some formal checks, and acts according to the outcome:

- o if the message passes all checks, the access point generates an acceptance PEC notification and inserts the original message inside a PEC transport envelope;

- o if a formal exception is detected, the access point refuses the message and emits the relevant non-acceptance PEC notification (see section 3.1.1);

- o if a virus is detected, the access point generates a non-acceptance PEC notification and inserts the original message as is in the provider's special store.

Generation of the acceptance notification indicates to the user that the message was accepted by the system, certifying also the date and time of the event. The notification MUST contain user-readable text, and an XML part containing the certification data.
The notification MAY also contain other attachments for extra features offered by the provider.

Using the data available in the PEC providers directory (see section 4.5), the access point runs checks on every recipient in the "To:" and "Cc:" fields present in the original message to verify whether they belong to the PEC infrastructure or to non-PEC domains. Such checks are done by verifying the existence, through a case insensitive search, of the recipients' domains in the "managedDomains" attribute found within the PEC providers directory. Therefore, the acceptance PEC notification (and relevant certification data) relates, for each address, the typology of its domain; PEC or non-PEC.

The identifier (from now on PEC msgid) of accepted original messages within the PEC infrastructure MUST be unambiguous in order to consent correct tracking of messages and relative PEC notifications. The format of such an identifier is:

```
[alphanumeric string]@[provider mail domain]
```

or:

```
[alphanumeric string]@[FQDN mail server]
```

Therefore, both the original message and the corresponding PEC transport envelope MUST contain the following header field:

```
        Message-ID: <[unique identifier]>
```

When an email client that is interacting with the access point has already inserted a Message ID (from now on msgid) in the original message, that msgid SHALL be substituted by a PEC msgid. In order to allow the sender to link the message sent with the relative PEC notifications, the msgid MUST be inserted in the original message as well as the relative PEC notifications and transport envelope. If present, the msgid is REQUIRED in the original message's header by adding the following header field:

```
X-Riferimento-Message-ID: <[original Message ID]>
```

which will also be inserted in the PEC transport envelope and notifications, and related in the certification data (see section 4.4).

2.2.2. Incoming point

This point permits the exchange of PEC messages and notifications between PEC providers. It is also the point through which ordinary mail messages can be inserted within the system of certified mail.

The exchange of messages between providers takes place through SMTP-based transactions, as defined in [SMTP]. If SMTP communication errors occur, they MAY be handled using the standard error notification mechanisms, as provided by SMTP in [SMTP] and [SMTP-DSN]. The same mechanism is also adopted for handling transitory errors, that result in long idling periods, during an SMTP transmission phase. In order to guarantee that an error is returned to the user as defined in section 3.3.3, the systems that handles PEC traffic MUST adopt a time limit for message idleness equal to 24 hours.

Once a message arrives, the incoming point runs the following list of checks and operations:

o verifies correctness and type of the incoming message;

o if the incoming message is a correct and undamaged PEC transport envelope:

  - emits a take in charge PEC notification towards the sender provider (section 3.2.1);

  - forwards the PEC transport envelope to the delivery point (section 3.3).

o if the incoming message is a correct and undamaged PEC notification, forwards the notification to the delivery point.

- o if the incoming message does not conform to the prerequisites of a correct and undamaged PEC transport envelope or notification, but comes from a PEC provider, i.e. passes the verifications regarding existence, origin, and validity of the signature, then the message MUST be propagated towards the recipient.
  Therefore, the incoming point:

  - inserts the incoming message in an anomaly envelope (section 3.2.2);

  - forwards the anomaly envelope to the delivery point.

- o if the incoming message does not originate from a PEC system, i.e. fails verifications regarding existence, origin, and validity of the signature, then the message will be treated as ordinary email, and, if propagated to the recipient:

  - is inserted in an anomaly envelope (section 3.2.2);

  - the anomaly envelope is forwarded to the delivery point.

The take in charge PEC notification is generated by the receiving provider and sent to the sending provider. Its purpose is to keep track of the message in its transition from one provider to another, and is therefore strictly intra-provider communication; the end user knows nothing about it.

To check the correctness and integrity of a PEC transport envelope or notification, the incoming point runs the following tests:

- o Signature existence - the system verifies the presence of an S/MIME signature structure within the incoming message;

- o Signature origin - the system verifies whether or not the signature belongs to a PEC provider by extracting the certificate used for signing and verifying its presence in the PEC providers directory. To ease the check, it is possible to calculate the certificate's [SHA1] hash value and perform a case-insensitive search of its hexadecimal representation within the "providerCertificateHash" attribute found in the PEC providers directory. This operation allows to easily identify the sender provider for subsequent and necessary matching checks between the extracted certificate and the one present in the provider's record;

- o Signature validity - S/MIME signature correctness is verified by recalculating the signature value, checking the entire certification path, and verifying the [CRL] and temporal validity of the certificate. In case some caching mechanism is used for CRL

contents, an update interval MUST be adopted so that the most up-to-date data is guaranteed, thus minimizing the possible delay between a publication revocation by the Certification Authority and the variation acknowledgment by the provider;

- Formal correctness - the provider performs sufficient and necessary checks to guarantee that the incoming message is compliant with the formats specified in this document (PEC transport envelope and notifications).

If a virus-infected PEC transport envelope passes the checks just mentioned it is still considered correct and undamaged. The presence of the virus will be detected in a second phase, during which the contents of the PEC transport envelope are verified. Thus, the incoming point will refrain from forwarding the message to the recipient, instead sending the appropriate PEC notification of non-delivery and storing the virus-infected message in the provider's special storage.

In case ordinary mail messages are received, the PEC provider SHALL perform virus checks in order to prevent the infiltration of potentially dangerous mail messages within the PEC system. If a virus is detected in an ordinary mail message, the latter can be discarded at the incoming point before it enters the PEC system. In other words, no special treatment is reserved for the error, but a handling that is conformant to the procedures usually followed for messages going through the Internet.

When the receiving provider detects a virus inside a PEC transport envelope during the reception phase, it emits a virus detection PEC notification to the sending provider, which then realizes its checks failed to detect that virus. When this happens, the sending provider MUST:

- check what virus typologies were not detected by its own antivirus to verify the possibility of interventions

- send a virus-induced non-delivery PEC notification to the sender's mailbox.

2.2.3. Delivery point

Is the point that receives messages from the incoming point and forwards them to the final recipient.

It MUST run a series of tests on received messages before forwarding them to the user (see section 3.3.1). It first verifies the typology of the message, and decides whether or not a PEC notification should be issued to the sender. The delivery PEC notification (section

3.3.2) is emitted after the message was delivered to the recipient's PEC mailbox and only at reception of a valid PEC transport envelope (sections 2.2.2 and 3.1.5).

In all other cases, such as anomaly envelopes and PEC notifications, the delivery PEC notification is not emitted. Regardless, the message received from the delivery point MUST be delivered unmodified to the recipient's mailbox.

The delivery PEC notification indicates to the sender that the message sent was in fact conveyed to the specified recipient's mailbox, and certifies the date and time of delivery through use of user-readable text and an XML part containing certification data, along with other possible attachments added for extra features offered by the provider.

If a PEC transport envelope received at the delivery point can't be delivered to the destination mailbox, the delivery point emits a non-delivery PEC notification (section 3.3.3). If, on the other hand, the delivery error concerns a message that arrives from Internet (i.e. a non-PEC message), no such notification is emitted.

2.2.4. Storage

Each provider MUST dedicate a special storage for the deposition of any virus-infected messages encountered. Whether the virus be detected by the sender's access point or the receiver's incoming point, the provider that detects it MUST store the mail message in its own storage, and keep it for 30 months.

2.2.5. Provider service mailbox

For exclusive use of the provider, dedicated to the reception of PEC notifications in 2 cases only:

o take in charge notifications; and

o virus detection notification.

2.2.6. Provider service email address

Each provider MUST register a special purpose email address for use when sending PEC transport envelopes and notifications, as delineated in section 3. This address MAY conincide with that of the service mailbox described in section 2.2.5.

2.3. Log

The server administrator MUST keep track of any and all operations

carried out in a specific message log file. The information kept in the log for each operation is the following:

- o message ID (the value present in the Message-ID header field in the original message)

- o date and time of event

- o sender of original message

- o recipient(s) of original message

- o subject of original message

- o event type (reception, delivery, PEC notification emission, etc)

- o Message-IDs of related generated messages

- o sending provider

The service provider MUST store this data and preserve it unmodified. Italian laws have specified that the service provider retain the data for 30 months.

3. Message processing

3.1. Access point

The access point acts as a submission service as defined in [SUBMISSION].

3.1.1. Formal checks on messages

When the access point receives a message the user wishes to send, it MUST guarantee said message's formal conformity as defined in [EMAIL], and verify that the:

- o [EMAIL] header section contains a "From:" header field holding a [EMAIL] compliant email address;

- o [EMAIL] header section contains a "To:" header field holding one or more [EMAIL] compliant email addresses;

- o sender's address, specified in the SMTP reverse path, coincides with the one in the message's "From:" header field;

- o recipients' addresses specified in the SMTP forward path coincide with the ones present in the "To:" or "Cc:" header fields of the message;

- "Bcc:" header field does not contain any value;

- total message size falls within the limits accepted by the provider. Such limits apply depending on the number of recipients as well; by multiplying it to the message size, the outcome MUST fall within the limits accepted by the provider. Italian Laws have specified this limit as being 30MB.

If the message does not pass the tests, the access point MUST NOT accept the message within the PEC system, thus emitting the relative PEC notification of non-acceptance.

3.1.2. Non-acceptance PEC notification due to formal exceptions

When the access point cannot forward the message received due to failure in passing formal checks, the sender is notified of such an outcome. If the error is caused by the message failing size checks, a non-acceptance PEC notification is sent as long as the size remains bound by a certain limit. If the size exceeds said limit, error handling is left to SMTP.

The notification header will contain the following fields:

```
X-Ricevuta: non-accettazione
Date: [date of notification emission]
Subject: AVVISO DI NON ACCETTAZIONE: [original subject]
From: certified-mail@[mail domain]
To: [original sender]
X-Riferimento-Message-ID: [Message-ID of original message]
```

The notification body will contain a text part that constitutes the actual notification in readable format according to a model that relates the following information:

```
Error in message acceptance
On [date] at [time] ([time zone]), in the message "[subject]"
originating from "[original sender]" and addressed to:
[recipient_1]
[recipient_2]
.
.
[recipient_n]
a problem was detected which prevents its acceptance due to
[error description].
The message was not accepted.
Message identification: [Message-ID]
```

The same certification information is inserted in an XML file to be added to the notification body, thus allowing automatic checks on

the message (section 4.4). Parsing MUST be done on the XML part only. Additional parts MAY be included by the provider for provider-specific services. Regardless, the original message MUST NOT be included. The message MUST follow the format described in section 4.3.

3.1.3. Non-acceptance PEC notification due to virus detection

The access point MUST run some tests on the content of messages it receives from its users and reject them if a virus is detected. In which case, a virus-detection-induced non-acceptance PEC notification MUST be emitted to clearly inform the user of the reason the message was refused.

The notification header contains the following fields:

```
     X-Ricevuta: non-accettazione
     X-VerificaSicurezza: errore
     Date: [notification emission date]
     Subject: AVVISO DI NON ACCETTAZIONE PER VIRUS: [original
              subject]
     From: certified-mail@[mail_domain]
     To: [original sender]
     X-Riferimento-Message-ID: [Message-ID of original message]
```

The body contains a readable text part according to the following model:

```
     Error in message acceptance due to virus presence
     On [date] at [time] ([time zone]), in the message "[subject]"
     originating from "[original sender]" and addressed to:
     [recipient_1]
     [recipient_2]
     .
     .
     .
     [recipient_n]
     a security problem was detected [ID of detected content type].
     The message was not accepted.
     Message identification: [Message-ID]
```

The same certification data is inserted in an XML file added to the notification to allow for automatic checks (section 4.4). Parsing MUST be done on the XML part only. Additional parts MAY be included by the provider for provider-specific services. Regardless, the original message MUST NOT be included. The message MUST follow the format described in section 4.3.

3.1.4. Acceptance PEC notification

The acceptance PEC notification is a message sent to the sender, containing date and time of acceptance, sender and recipient data, and subject.

The header contains the following fields:

```
X-Ricevuta: accettazione
Date: [actual date of acceptance]
Subject: ACCETTAZIONE: [original subject]
From: certified-mail@[mail_domain]
To: [original sender]
X-Riferimento-Message-ID: [Message-ID of original message]
```

The message body contains a text part that constitutes the notification in readable format, according to a model that relates the following information:

```
Acceptance PEC notification
On [date] at [time] ([time zone]), the message "[subject]"
 originating from "[original sender]" and addressed to:
[recipient_1] (["certified mail" | "ordinary mail"])
[recipient_2] (["certified mail" | "ordinary mail"])
.
.
.
[recipient_n] (["certified mail" | "ordinary mail"])
was accepted by the system and forwarded to the recipient(s).
Message identification: [Message-ID]
```

The same certification data is inserted in an XML file added to the notification message, allowing automatic checks on it (section 4.4). Parsing MUST be done on the XML part only. Additonal parts MAY be included by the provider for provider-specific services. The message MUST follow the format described in section 4.3.

3.1.5. PEC Transport envelope

A PEC transport envelope is a message generated by the access point which contains the original message as well as certification data.

As mentioned in section 2.1.1.2, the PEC transport envelope inherits from the original message the values of the following header fields, which MUST be related unmodified:

- Received

- To

- Cc

o Return-Path

o Reply-To (if present)

On the other hand, the following fields MUST be modified, or inserted if necessary:

```
X-Trasporto: posta-certificata
Date: [actual date of acceptance]
Subject: POSTA CERTIFICATA: [original subject]
From: "On behalf of: [original sender]"
                     <certified-mail@[mail_domain]>
Reply-To: [original sender] (inserted only if not present)
Message-ID: [PEC message ID generated as explained in 2.2.1]
X-Riferimento-Message-ID: [message ID of original message]
X-TipoRicevuta: [completa/breve/sintetica]
```

The "X-TipoRicevuta" field indicates the type of delivery PEC notification the sender wishes to receive - complete, brief, or concise.

The body of the PEC transport envelope contains a text part that constitutes the readable format of the message according to a model that relates the following certification data:

```
Certified mail message
On [date] at [time] ([time zone]), the message "[subject]" was
sent by "[original sender]" and addressed to:
[recipient_1]
[recipient_2]
.
.
.
[recipient_n]
The original message is included in attachment.
Message identification: [Message-ID]
```

Within the PEC transport envelope, the entire, non-modified original message is inserted in a [EMAIL]-compliant format (except for what has been said regarding the Message ID), as well as an XML part which contains the certification data that was already related in text format, and information on the type of message and PEC notification requested (section 4.4). Parsing MUST be done on the XML part only. Additional parts MAY be included by the provider for provider-specific services. The message MUST follow the format described in section 4.3.

Note that the routing data of the PEC transport envelope (forward and reverse paths) remain unaltered.

3.1.6. Timeout delivery error PEC notification

If the sending provider doesn't receive a take in charge or delivery PEC notification from the receiving provider within 12 hours after message dispatch, it informs the user that the recipient's provider might not be able to deliver the message. In case the sending provider doesn't receive a delivery PEC notification within 24 hours after message dispatch, it emits another non-delivery PEC notification to the user by the 24-hour timeout, but not before 22 hours have passed.

Such a communication takes place through a PEC notification of non-delivery due to timeout, the header of which contains the following fields:

```
X-Ricevuta: preavviso-errore-consegna
Date: [date of notification emission]
Subject: AVVISO DI MANCATA CONSEGNA PER SUP. TEMPO MASSIMO:
         [original subject]
From: certified-mail@[mail_domain]
To: [original recipient]
X-Riferimento-Message-ID: [Message-ID of original message]
```

The body of the first non-delivery PEC notification (12-hour timeout) contains a text part that represents the readable format of the notification which will relate the following data:

```
Non-delivery PEC notification
On [date] at [time] ([time zone]), the message
"[subject]" originating from "[original sender]"
and addressed to "[recipient]"
has not been delivered within the first 12 hours following
its dispatch. Not excluding that the message might eventually
be delivered, it is deemed useful to consider that dispatch
might not have a positive outcome. The system will see to
sending another non-delivery PEC notification if in the
following twelve hours no confirmation is received from the
recipient.
Message identification: [Message-ID]
```

On the other hand, 24-hour-timeout induced PEC notifications, which have the same header as described above, will have the following text in their body:

```
Non-delivery PEC notification
On [date] at [time] ([time zone]), the message
"[subject]" originating from "[original sender]"
and addressed to "[recipient]"
```

has not been delivered within 24 hours of its dispatch.

The transaction is deemed to be considered terminated with a negative outcome.
Massage identification: [Message-ID]

The same certification data is inserted in an XML file added to both PEC notification types to allow automatic checks (section 4.4).

Parsing MUST be done on the XML part only. Additional parts MAY be added for services supplied by the PEC provider. Regardless, the original message MUST NOT be included. The message MUST follow the format described in section 4.3.

A timeout PEC notification is generated if one of the following scenarios occurs:

- the sending provider receives a take in charge PEC notification during the first 12 hours following message dispatch, but does not receive a delivery PEC notification at all. In this case it would be a 24-hour timeout PEC notification.
- the sending provider does not receive a take in charge PEC notification, but receives a delivery PEC notification after 12 hours and before the 24-hour timeout. In this case it would be a 12-hour timeout PEC notification.
- the sending provider doesn't receive either a take in charge nor a delivery PEC notification. In this case 2 timeout PEC notifications are generated; a 12-hour and a 24-hour timeout PEC notification.

3.2. Incoming point

3.2.1. Take in charge PEC notification

When correct PEC transport envelopes (as defined in section 2.2.2.) are exchanged between PEC providers, the receiver MUST send a take in charge PEC notification to the sender. The single dispatched notification concerns all recipients who belong to the same provider, and to whom the incoming message was addressed, as stated in the routing data (forward and reverse paths) of the SMTP transaction. Within the certification data of a single take in charge PEC notification, all recipients of the message to which it refers are listed. In general, when receiving a PEC transport envelope, each provider MUST emit one or more take in charge PEC notifications to cover, in absence of SMTP transport errors, all the recipients in its jurisdiction.

The header of a take in charge PEC notification contains the following fields:

```
X-Ricevuta: presa-in-carico
Date: [date of take in charge]
Subject: PRESA IN CARICO: [original subject]
From: certified-mail@[mail_domain]
To: [sender provider service mailbox]
X-Riferimento-Message-ID: [Message-ID of original message]
```

The provider's service email address is obtained from the PEC providers directory during the necessary queries made in the signature verification stage.

The body contains a text part that follows the underlying model:

```
take in charge PEC notification
On [date] at [time] ([time zone]), the message "[subject]"
originating from "[original sender]" and addressed to:
[recipient_1] (["certified mail" | "ordinary mail"])
[recipient_2] (["certified mail" | "ordinary mail"])
.
.
.
[recipient_n] (["certified mail" | "ordinary mail"])
was accepted by the system.
Message identification: [Message-ID]
```

The same certification data is inserted in an XML file which is added to the notification message to allow for automatic checks (section 4.4). Parsing MUST be done on the XML part only. Additional parts MAY be added by the provider for provider-specific services. The message MUST follow the format described in section 4.3.

3.2.2. Anomaly envelope

If the tests on an incoming message detect an error, or the message is identified as being ordinary mail and the provider is set to forward it to the recipient, the system MUST insert such a message in an anomaly envelope. Before delivery, the entire message received at the incoming point is inserted in an [EMAIL]-compliant format as a [MIME1] part inside a new message that MUST inherit the unmodified values for the following header fields from the received message:

- Received

- To

- Cc

- Return-Path

- Message-ID

Whereas, the following header fields MUST be modified or inserted:

```
     X-Trasporto: errore
     Date: [message arrival date]
     Subject: ANOMALIA MESSAGGIO: [original subject]
     From: "On behalf of: [original sender]"
                          <certified-mail@[mail_domain]>
     Reply-To: [original sender (inserted only if not already
               present)]
```

The body contains a user-readable text part according to a model that relates the following data:

```
     Message anomaly
     On [date] at [time] ([time zone]), the message "[subject]"
     originating from "[original sender]" and addressed to:
     [recipient_1]
     [recipient_2]
     .
     .
     .
     [recipient_n]
     was received.
     The data has not been certified due to the following error:
     [concise description of error]
     The original message is attached.
```

Due to uncertainty regarding origin and/or conformity of the message received, the anomaly envelope MUST NOT contain [MIME1] parts other than the entire message that arrived at the incoming point.

Note that the routing data of such an envelope (forward and reverse paths) remain unaltered. Doing so guarantees both message forwarding to the recipients, and reception of SMTP error notifications, if any occur, by the sender (as specified in [SMTP] & [SMTP-DSN]).

3.2.3. Virus detection PEC notification

If the incoming point receives virus-infected PEC messages, it MUST NOT forward them. Rather it MUST inform the sending provider, which will in turn inform the sending user, of the failed transmission. A separate PEC notification of virus detection MUST be sent on behalf of every recipient within the provider's domain.

In case a virus is detected during the reception phase of a message whose origin was asserted through sender signature verification, the system generates a virus-detected PEC notification indicating the error found, and sends it to the sending provider's service mailbox.

The header of this PEC notification contains the following fields:

```
X-Ricevuta: rilevazione-virus
X-Sender: [original sender]
Date: [date of notification emission]
Subject: PROBLEMA DI SICUREZZA: [original subject]
From: certified-mail@[mail_domain]
To: [sender provider notifications]
X-Riferimento-Message-ID: [Message-ID of original message]
```

The body contains a readable text part according to a model that relates the following data:

```
Virus detection PEC notification
On [date] at [time] ([time zone]), in the message "[subject]"
originating from "[original sender]" and addressed to
"[recipient]"
a security problem was detected [ID of content type detected].
Message identification: [Message-ID]
```

The same certification data is inserted in an XML file and added to the notification to allow for automatic checks (section 4.4). Parsing MUST be done on the XML part only. Additional parts MAY be included by the provider for provider-specific services. Regardless, the original message MUST NOT be included. The message MUST follow the format described in section 4.3.

The message body MUST contain the reason for which the transmission could not be completed.

3.2.4. Virus-induced delivery error PEC notification

At the reception of a virus detected PEC notification from the receiving provider, the sender provider emits a non-delivery PEC notification to the sending user.

The header for this notification contains the following fields:

```
X-Ricevuta: errore-consegna
X-VerificaSicurezza: errore
Date: [date of notification emission]
Subject: AVVISO DI MANCATA CONSEGNA PER VIRUS: [original
         subject]
From: certified-mail@[mail_domain]
To: [original sender]
X-Riferimento-Message-ID: [Message-ID of original message]
```

The body is contains a readable text part according to a model that relates the following data:

```
Delivery error PEC notification due to virus
On [date] at [time] ([time zone]), in the message "[subject]"
addressed to "[recipient]"
a security problem was detected [ID of content type detected
by the anti-virus].
The message was not delivered.
Message identification: [Message-ID]
```

All the information necessary for the construction of such a PEC notification can be obtained from the correlated virus-detected PEC notification.

The same certification data is inserted in an XML file and added to the notification message to allow for automatic checks (section 4.4). Parsing MUST be done on the XML part only. Additional parts MAY be included by the provider for provider-specific services. The reason the transaction was not completed MUST be specified in the message, which MUST follow the format described in section 4.3.

3.3. Delivery point

3.3.1. Checks on incoming messages

When a message arrives at the delivery point, the system verifies:

O message type

O whether or not a PEC notification has to be returned.

3.3.2. Delivery PEC notification

A delivery PEC notification is issued only after a correct PEC transport envelope (sections 2.2.2. and 3.1.5) has been delivered to the recipient's mailbox.

In all other cases (e.g. anomaly envelopes, PEC notifications), the delivery PEC notification is not issued. Regardless, the message received at the delivery point MUST be delivered to the recipient's mailbox unchanged.

This notification tells the user that his/her message has been successfully delivered to the specified recipient. It includes readable text that certifies the date and time of delivery, sender and receiver data, and the subject. It also contains an XML certification data file and other optional parts for functionalities offered by the provider.

The following fields are inserted in the header:

```
X-Ricevuta: avvenuta-consegna
Date: [delivery date]
Subject: CONSEGNA: [original subject]
From: certified-mail@[mail_domain]
To: [original sender]
X-Riferimento-Message-ID: [Message-ID of original message]
```

The value of the "X-TipoRicevuta" header field in the PEC transport envelope is derived from the original message, thus allowing the sender to determine the type of delivery PEC notification requested from the primary recipients of the original message.
The notification MUST follow the format described in section 4.3.

3.3.2.1. Delivery PEC notification: complete

This is the default value for delivery PEC notifications. When no value for the "X-TipoRicevuta" is specified, or when it contains the value "complete", the system will require a complete delivery PEC notification from addressees in the "To:" field, while a concise PEC notification (section 3.3.2.3) will be required from those in the "Cc:" field. The distinction between primary recipients and those in carbon copy is done through an analysis of the "To:" and "Cc:" fields. For PEC notifications sent on behalf of primary recipients, a complete copy of the original message along with any attachments is inserted in the notification. In case the system in charge of delivery is not able to determine the recipient type due to ambiguity problems in the "To:" and "Cc:" fields, delivery MUST be considered as if addressed to a primary recipient and include the complete copy of the original message.

The notification body contains a readable text part that relates certifcation data according to the following model:

```
Delivery PEC notification
On [date] at [time] ([time zone]), the message "[subject]"
originating from "[original sender]" and addressed to
"[recipient]"
was placed in the destination's mailbox.
Message identification: [Message-ID]
```

The same certification data is inserted in an XML file and added to the notification (section 4.4), along with any other parts that MAY inserted by the provider for provider-specific services. Parsing MUST be done on the XML part only. The delivery PEC notification MUST be issued on behalf of every recipient of the message, and MUST follow the format described in section 4.3.

3.3.2.2. Delivery PEC notification: brief

In order to decrease the amount of data flowing, it is possible for the sender to ask for a delivery PEC notification in "brief" format. The brief delivery PEC notification contains the original message and a ciphered hash value for each of its parts. The hash value SHOULD be calculated on base64 encoded parts. As specified in section 5.3, PEC messages MUST transit only on machines that belong to the PEC network, and which MUST NOT alter the encoding of the message during its transition/processing.

NOTE: Even though PEC uses these relaxed specifications, PEC interoperability tests between over 20 service providers have never revealed any problems. This is probably due to mail servers leaning more towards leaving the messages they receive intact without applying any changes. But issues might arise if a server decides to modify encoded parts; for example, change the base64 line length, whose hash value calculated at the receiver's end would then differ from that at the sender's side.

To be able to verify the transmitted contents it is necessary for the sender to keep the unaltered original copy of the part(s) to which the hash values refer.

If the PEC transport envelope contains the header

```
X-TipoRicevuta: breve
```

the delivery point emits a brief delivery PEC notification on behalf of the primary recipients, and a concise one (section 3.3.2.3) on behalf of carbon copy recipients. The value of the header field in the PEC transport envelope is derived from the original message.

The notification body contains a readable text part according to a model that relates the following certification data:

```
Brief delivery PEC notification
On [date] at [time] ([time zone]), the message "[subject]"
originating from "[original sender]" and addressed to
"[recipient]"
was placed in the destination's mailbox.
Message identification:  [Message-ID]
```

The same certification data is inserted in an XML file and added to the notification (section 4.4), along with other parts which MAY be included for specific provider-supplied services. Parsing MUST be done on the XML part only.The delivery PEC notification is issued on behalf of every recipient of the message, and MUST follow the format described in section 4.3.

The MIME structure of the original message is unaltered as it is added to the notification, but each MIME part with a "name" parameter in the header field "Content-Type," or a "filename" parameter in the header field "Content-Disposition" MUST be substituted by a text file containing that MIME part's hash value.

When the original message has an S/MIME format, it is necessary not to alter the integrity of the message structure. Verification of the S/MIME part in the original message takes place when the MIME type of the top-level entity (which coincides with the message itself) is checked. An S/MIME message MAY have the following MIME types (as per [SMIMEV3]):

- multipart/signed

  Represents an original message signed by the sender using the structure described in [MIME-SECURE]. The message is made up of 2 MIME parts: the first is the message itself before the application of the sender's signature, whereas the second contains signature data. The second part (generally of type "application/pkcs7-signature" or "application/x-pkcs-signature") contains data added during the signing phase and MUST be left unchanged to avoid compromising the overall message structure;

- "application/pkcs7-mime" or "application/x-pkcs7-mime"

  The message is composed of a sole CMS object within the MIME part. Given that attachments cannot be separated from the CMS object, the MIME part is left intact (i.e., it is not replaced by the hash value); therefore, the brief PEC notification is the same as the complete PEC notification.

If the original message contains parts whose Content-Type is "message/rfc822", i.e. contains an email message as attachment, the entire attached message is substituted with its corresponding hash value.

Therefore, when emitting a brief delivery PEC notification, the provider MUST:

1. Identify and extract all the parts from the first MIME part of the multipart/signed S/MIME message;

2. calculate the hash values of all the files attached by the sender to the original message;

3. substitute originals with their hash values.

In general, in the case of original messages in S/MIME format, the

copy of the message inserted within the brief delivery PEC notification will have the following characteristics:

- if the original message is signed, the S/MIME structure and signature-relative data will remain unchanged. The message will generate an error in a future signature integrity verification phase following the substitution of attachments with the corresponding hash values.

- if the original message contains the "application/pkcs7-mime" or "application/x-pkcs7-mime" MIME type, attachments present in the message will not be substituted by their hash values, due to impossibility of identification within a CMS structure.
  The content of the brief delivery PEC notification will coincide with that of a normal delivery PEC notification.

The algorithm used for hash calculation is the [SHA1], calculated on the entire content of the part. To allow distinction between hash files and the files to which they refer, the suffix ".hash" is added to the original filename. The hash value is written in the file using a hexadecimal representation as a single sequence of 40 characters. The MIME type of these attachments is set to "text/plain" to highlight their textual nature.

3.3.2.3. Delivery PEC notification: concise

If the PEC transport envelope contains the header

```
     X-TipoRicevuta: sintetica
```

the delivery point emits, both to primary and carbon copy recipients, a concise delivery PEC notification that does not contain the original message.

The message body of the notification contains a readable text part according to a model that relates the following certification data:

```
     Concise delivery PEC notification
     On [date] at [time] ([time zone]), the message "[subject]"
     originating from "[original sender]" and addressed to
     "[recipient]"
     was placed in the destination's mailbox.
     Message identification:  [Message-ID]
```

The same certification data is inserted within an XML file and added to the notification (section 4.4), along with additional parts that MAY be included for provider-specific services. Parsing MUST be done on the XML part only. The notification is sent to each one of the recipients to whom the message is delivered, and MUST

follow the format described in section 4.3.

The concise delivery PEC notification follows the same emission rules as the delivery PEC notification; added to it is only the XML file containing the certification data, not the original message.

3.3.3. Non-delivery PEC notification

If an error occurs during the delivery of a correct PEC transport message, the system returns to the sender a non-delivery PEC notification that indicates the error condition.

The header will contain the following fields:

```
X-Ricevuta: errore-consegna
Date: [date of notification emission]
Subject: AVVISO DI MANCATA CONSEGNA: [original subject]
From: certified-mail@[mail_domain]
To: [original sender]
X-Riferimento-Message-ID: [Message-ID of original message]
```

The notification body contains a readable text part according to a model that relates the following data:

```
Non-delivery PEC notification
On [date] at [time] ([time zone]), in the message "[subject]"
originating from "[original sender]" and addressed to
"[recipient]"
an error was detected.
The message was refused by the system.
Message identification:  [Message-ID]
```

The same certification data is inserted within an XML file and added to the notification in order to allow for automatic checks (section 4.4). Parsing MUST be done on the XML part only. Additional parts MAY be included by the PEC provider for provider-specific services. The notification MUST follow the format described in section 4.3.

3.4. Sender and receiver belonging to the same domain

PEC messages MUST be processed even if both sender and receiver(s) belong to the same PEC domain.

3.5. Example: Complete transaction between 2 PEC domains

A correct transaction between two PEC domains goes through the following steps:

- The sending user sends an email to his provider's Access Point;

- The Access Point runs all checks and emits an acceptance PEC notification to the user;

- The Access Point creates a PEC transport envelope and forwards it to the Incoming Point of the receiving provider;

- The receiver's Incoming Point verifies the PEC transport envelope and creates a take in charge PEC notification to be sent to the sending provider;

- The sender's Incoming Point verifies the validity of the take in charge PEC notification and forwards it to the Delivery Point;

- The sender's Delivery Point saves the take in charge PEC notification in the provider's service mailbox;

- The receiver's Incoming Point forwards the PEC transport envelope to the receiver's Delivery Point;

- The receiver's Delivery Point verifies the contents of the PEC transport envelope and saves it in the recipient's mailbox;

- The receiver's Delivery Point creates a delivery PEC notification and sends it to the sender's Incoming Point;

- The sender's Incoming Point verifies the validity of the delivery PEC notification and forwards it to the sender's Delivery Point;

- The sender's Delivery Point saves the delivery PEC notification in the sending user's mailbox;

- The receiving user has the message at his disposition.

NOTE: Some of these steps might occur in parallel, thus the interaction might complete in a different order.

4. Formats

4.1. Temporal reference

For all operations carried out during message, notification, and log elaboration processes by the access, incoming and delivery points, it is necessary to have an accurate temporal reference available. All events (generation of PEC notifications, transport envelopes, logs, etc) that constitute the transaction of message elaboration at the access, incoming, and delivery points MUST employ a sole temporal value obtained from within the transaction itself.

Doing this renders the instant of message elaboration unambiguous within PEC logs, notifications, messages, etc, generated by the server.

4.2. User date/time

Temporal indications supplied by the service in readable format (text in PEC notifications, transport envelopes, etc) are provided with reference to the legal time at the moment of the operation. Following is the specification using the syntax description notation definted in [ABNF].

```
date-fullyear   = 4DIGIT
date-month      = 2DIGIT  ; 01-12
date-mday       = 2DIGIT  ; 01-28, 01-29, 01-30, 01-31 based on
                          ; month/year
time-hour       = 2DIGIT  ; 00-23
time-minute     = 2DIGIT  ; 00-59
time-second     = 2DIGIT  ; 00-58, 00-59, 00-60 based on leap second
                          ; rules
time-offset     = "(" ("+" / "-") time-hour ":" time-minute ")"

partial-time    = time-hour ":" time-minute ":" time-second

full-date       = date-mday "/" date-month "/" date-fullyear
full-time       = partial-time time-offset
```

NOTE: For number of days in a month, leap year, and leap second restrictions see section 5.7 of [TIMESTAMP].

4.3. Format of a PEC message body

This section describes the characteristics of the various components of PEC messages and notifications generated by a PEC system. If one of the message parts contains characters with values outside of the range 0-127 (7-bit ASCII), that part will have to be adequately encoded so that 7-bit transportation compatibility is guaranteed (e.g. quoted-printable, base64 as per [MIME1]).

Before applying the signature, the message body has Content-Type: multipart/mixed. Each part is described in the sections below. The first part is the user readable text generated by the PEC system, while the second and third parts are interchangeable in order and contain the original message and the XML file for the certification data.

4.3.1. User readable text

Character set: ISO-8859-1 (Latin-1)
MIME type: text/plain or multipart/alternative

The multipart/alternative MIME type MAY be used to add an HTML version of the body of system-generated messages. In this case, two sub-parts MUST be present: one of type text/plain, the other text/html. For the HTML part:

- it MUST contain the same information as related in the text part;

- it MUST NOT contain references to elements (e.g. images, sounds, font, style sheets) neither internal to the message (added MIME parts) nor external (e.g. hosted on the provider's server);

- MUST NOT have active content (e.g. JavaScript, VBscript, Plug-in, ActiveX).

4.3.2. Original message

MIME type: message/rfc822
Attachment name: postacert.eml

4.3.3. Certification data

Character set: UTF-8
MIME type: application/xml
Attachment name: certdata.xml

4.4. Certification data scheme

Following is the DTD relative to the XML file that contains certification data attached to PEC notifications.

```
    <!--Use the element "postacert" as root-->
    <!--"tipo" indicates the typology of the PEC message-->
    <!--The attribute "errore" can have the following values-->
    <!--"nessuno" = no error-->
    <!--"no-dest" (with type="errore-consegna") = -->
    <!--                                        wrong recipient-->
    <!--"no-dominio" (with type="errore-consegna") = -->
    <!--                                           wrong domain-->
    <!--"virus" (with type="errore-consegna") = virus-->
    <!--"virus" (with type="non-accettazione") = virus-->
    <!--"altro" = generic error-->
    <!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">

      <!--Header of the original message-->
      <!ELEMENT intestazione (mittente,
                              destinatari+,
                              risposte,
                              oggetto?)>

      <!--Sender ("From" field) of the original message-->
      <!ELEMENT mittente (#PCDATA)>

      <!--Complete list of recipients ("To" and "Cc" fields)-->
      <!--of the original message-->
      <!--"tipo" indicates the typology of the recipient-->
      <!ELEMENT destinatari (#PCDATA)>
      <!ATTLIST destinatari
            tipo (certificato | esterno) "certificato">

      <!--Value of the "Reply-To" field of the original message-->
      <!ELEMENT risposte (#PCDATA)>
      <!--Value of the "Subject" field of the original message-->
      <!ELEMENT oggetto (#PCDATA)>

      <!--PEC message data-->
      <!ELEMENT dati (gestore-emittente,
                      data,
                      identificativo,
                      msgid?,
                      ricevuta?,
                      consegna?,
                      ricezione*,
                      errore-esteso?)>

      <!--Descriptive string of the provider that certifies -->
      <!--the data-->
      <!ELEMENT gestore-emittente (#PCDATA)>
```

```
          <!--Date/time of message elaboration-->
```

```
       <!--"zona" is the difference between local time and UTC in -->
       <!--"[+|-]hhmm" format-->
       <!ELEMENT data (giorno, ora)>
       <!ATTLIST data
             zona CDATA #REQUIRED>

       <!--Day in "dd/mm/yyyy" format-->
       <!ELEMENT giorno (#PCDATA)>
       <!--Local hour in "hh:mm:ss" format-->
       <!ELEMENT ora (#PCDATA)>

       <!--PEC msgid-->
       <!ELEMENT identificativo (#PCDATA)>

       <!--msgid of the original message before modifications-->
       <!ELEMENT msgid (#PCDATA)>

       <!--For PEC transport envelopes and delivery notifications-->
       <!--indicate the type of PEC notification requested by the-->
       <!--sender-->
       <!ELEMENT ricevuta EMPTY>
       <!ATTLIST ricevuta
             tipo (completa |
                   breve    |
                   sintetica ) #REQUIRED>

       <!--For delivery, non-delivery, virus-induced non-delivery, -->
       <!-- virus detection, and timeout PEC notifications-->
       <!--Recipient address to which delivery has been carried -->
       <!--out/tried-->
       <!ELEMENT consegna (#PCDATA)>
       <!--For take in charge PEC notifications-->
       <!--recipients for whom it is the relative PEC notification-->
       <!ELEMENT ricezione (#PCDATA)>

       <!--In case of error-->
       <!--brief description of the error-->
       <!ELEMENT errore-esteso (#PCDATA)>
```

4.5. PEC providers directory scheme

The PEC providers directory is created through a centralized LDAP server that contains the providers' data and their corresponding PEC mail domains.

Following are the directory scheme's attributes:

- providerCertificateHash: hash of provider's certificate

- providerCertificate: provider certificate

- providerName: provider name

- mailReceipt: provider reception email address

- managedDomains: managed domains

- LDIFLocationURL: provider LDIF record URL

- providerUnit: secondary operating environment name

The directory's base root is "o=postacert" and the "DistinguishedName" of single records is of the type "providerName=<name>, o=postacert". Search within the directory is carried out mainly in case-sensitive mode using the "providerCertificateHash" attribute (during envelope signature verification phase) or the "managedDomains" attribute (during message acceptance phase). It is possible for the record of a single provider to contain multiple "providerCertificate" with the related "providerCertificateHash" attributes in order to allow the handling of the renewal of expiring certificates. The provider MUST make sure to update its record with sufficient advance before the certificate expiration date, by adding a new certificate whose validity overlaps that of the previous one.

The data of all PEC providers is encompassed in a [LDIF] file which is available as an [HTTPS] object, and can be found at the URL to which the 'LDIFLocationURL' attribute in the "dn: o=postacert" record points (see section 4.5.6). To guarantee authenticity, that file MUST be signed by the provider for the operations regarding its PEC services using the method described for single providers. The file, the signature, and the X.509v3 certificate MUST be inserted in a PKCS#7 structure in binary ASN.1 DER format as a file with ".p7m" extension. The centralized [LDAP] system downloads that file on a daily basis and, after suitable verifications of the signature, applies it to the provider's record.

Through the [LDIF] file, single providers MUST keep a copy of the directory locally, updated on a daily basis, in order to improve system performance by avoiding continuous request dispatches to the central system for every message elaboration phase.

If secondary environments are present, the [LDIF] file indicated in the main environment's record MUST relate the contents of all the provider-relevant records.

4.5.1. providerCertificateHash attribute

The 'providerCertificateHash' attribute is a hexadecimal representation of the hash in SHA1 format of the X.509v3 certificate used by the provider for PEC notifications and envelope signatures.

```
    ( 1.3.6.1.4.1.16572.2.2.1  NAME 'providerCertificateHash'
      DESC 'Hash SHA1 of X.509 certificate in hexadecimal format'
      EQUALITY caseIgnoreIA5Match
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{40} )
```

The IA5String (1.3.6.1.4.1.1466.115.121.1.26) syntax is defined in [LDAP-SYNTAXES].

4.5.2. providerCertificate attribute

The 'providerCertificate' attribute lists the certificate(s) used by the provider to sign PEC notifications and transport envelopes.

```
    ( 1.3.6.1.4.1.16572.2.2.2  NAME 'providerCertificate'
      DESC 'X.509 certificate in ASN.1 DER binary format'
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.8 )
```

The Certificate Binary transfer (1.3.6.1.4.1.1466.115.121.1.8) syntax is defined in RFC 2252.

NOTE: By the time this draft is written, and after PEC had several implementations up and running, RFC 2252 was rendered obsolete by [LDAP-SYNTAXES], which removed the definition of the Binary syntax (see [LDAP-SYNTAXES] Appendix B. point 12.).

4.5.3. providerName attribute

The 'providerName' attribute contains the name of the PEC provider. All records MUST contain their provider's name in this attribute.

```
    ( 1.3.6.1.4.1.16572.2.2.3  NAME 'providerName'
      DESC 'PEC provider'
      EQUALITY caseIgnoreMatch
      SUBSTR caseIgnoreSubstringsMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768}
      SINGLE-VALUE )
```

The Directory String (1.3.6.1.4.1.1466.115.121.1.15) syntax is defined in [LDAP-SYNTAXES].

4.5.4. mailReceipt attribute

The 'mailReceipt' attribute contains the provider's email address to which take in charge and virus detection PEC notifications are sent.

```
    ( 1.3.6.1.4.1.16572.2.2.4 NAME 'mailReceipt'
      DESC 'E-mail address of the service mailbox'
      EQUALITY caseIgnoreIA5Match
      SUBSTR caseIgnoreIA5SubstringsMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{256}
      SINGLE-VALUE )
```

The IA5String (1.3.6.1.4.1.1466.115.121.1.26) syntax is defined in [LDAP-SYNTAXES].

4.5.5. managedDomains attribute

The 'managedDomains' attribute lists the PEC domains that are handled by the provider.

```
    ( 1.3.6.1.4.1.16572.2.2.5 NAME 'managedDomains'
      DESC 'Domains handled by the PEC provider'
      EQUALITY caseIgnoreIA5Match
      SUBSTR caseIgnoreIA5SubstringsMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

The IA5String (1.3.6.1.4.1.1466.115.121.26) syntax is defined in [LDAP-SYNTAXES].

4.5.6. LDIFLocationURL attribute

The 'LDIFLocationURL' attribute contains an [HTTPS] URL that points to the location of the [LDIF] file defining the provider's record. When the attribute is present in the record "dn: o=postacert", then it contains the definition of the entire directory in [LDIF] format.

Secondary environment records MUST NOT contain the 'LDIFLocationURL' attribute which is obtained from the main environment's attributes for all records connected to the provider.

```
    ( 1.3.6.1.4.1.16572.2.2.6 NAME 'LDIFLocationURL'
      DESC 'URL of the LDIF file that defines the entry'
      EQUALITY caseExactMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
      SINGLE-VALUE )
```

The Directory String (1.3.6.1.4.1.1466.115.121.1.15) syntax is defined in [LDAP-SYNTAXES].

4.5.7. providerUnit attribute

The 'providerUnit' attribute contains the name of secondary operating environments - and attribute not present for the main environment. It is possible for the provider to define several

distinct records, each indicating a single, different secondary operating environment, for which it is possible to declare specific attributes that are, if need be, distinct from those relative to the main and other environments.

The "DistinguishedName" of the records relative to the secondary operating environments are of the type "providerUnit=<environment>,providerName=<name>,o=postacert". Every provider MUST have a record associated to its own main environment, distinguishable for the absence of the "providerUnit" attribute within the record and the DistinguishedName.

```
( 1.3.6.1.4.1.16572.2.2.7 NAME 'providerUnit'
  DESC 'Name of the secondary operative environment'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768}
  SINGLE-VALUE )
```

The Directory String (1.3.6.1.4.1.1466.115.121.1.15) syntax is definted in [LDAP-SYNTAXES].

4.5.8. LDIFLocationURLObject object class

The schema definition of the 'LDIFLocationURLObject' Object Class:

```
Name:           LDIFLocationURLObject
Description:    Class for the insertion of a LDIFLocationURL
                attribute
OID:            ( 1.3.6.1.4.1.16572.2.1.1 )
Kind:           auxiliary
SubclassOf:     top
MAY Contain:    ( LDIFLocationURL )
```

4.5.9. provider object class

The schema definition of the 'provider' Object Class:

```
Name:           provider
Description:    PEC provider
OID:            ( 1.3.6.1.4.1.16572.2.1.2 )
SubclassOf:     top
MUST Contain:   ( providerCertificateHash $
                  providerCertificate $
                  providerName $
                  mailReceipt $
                  managedDomains )
MAY Contain:    ( description $
                   LDIFLocationURL $
```

```
                         providerUnit )
```

4.5.10 LDIF file example

The following LDIF file represents an example of a providers' directory, containing a base root and 2 fictitious providers. The inserted certificates are two self-signed certificates used for example purposes only:

```
       dn: o=postacert
       objectclass: top
       objectclass: organization
       objectClass: LDIFLocationURLObject
       o: postacert
       LDIFLocationURL: https://igpec.rupa.example.com/igpec.ldif.p7m
       description: Base root for the PEC providers directory
       dn: providerName=Anonymous Certified Mail S.p.A.,o=postacert
       objectclass: top
       objectclass: provider
       providerName: Anonymous Certified Mail S.p.A.
       providerCertificateHash:
        7E7AEF1059AE0F454F2643A95F69EC3556009239
       providerCertificate;binary::
        MIIDBjCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQQFADBmMQswCQYDVQQGEw
        JJVDEpMCcGA1UEChMgQW5vbmltYSBQb3N0YSBDZXJ0aWZpY2F0YSBTLnAu
        QS4xLDAqBgkqhkiG9w0BCQEWHXBvc3RhLWNlcnRpZmljYXRhQGFucG9jZX
        J0Lml0MB4XDTAyMTIwOTE3MjQxNVoXDTAzMTIwOTE3MjQxNVowZjELMAkG
        A1UEBhMCSVQxKTAnBgNVBAoTIEFub25pbWEgUG9zdGEgQ2VydGlmaWNhdG
        EgUy5wLkEuMSwwKgYJKoZIhvcNAQkBFh1wb3N0YS1jZXJ0aWZpY2F0YUBh
        bnBvY2VydC5pdDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAr8J+qK
        KdxV9LzDMPqwnEy0P8H/KwbI0Szs8p6UZajZdpeUK0Ncbrv1QyXZNNtSMC
        2uL09HDyx8agjgZWdhypnehguiSK3busha15RSpMGhiqxmz2b0HhOG73Gf
        alZelqrwqmElna4MNUaLhbOvTd/sqPUS378w5IaIhWxzy34XcCAwEAAaOB
        wzCBwDAdBgNVHQ4EFgQUN8lC0znQWEs0xspZ/aBzsaGvRZMwgZAGA1UdIw
        SBiDCBhYAUN8lC0znQWEs0xspZ/aBzsaGvRZOhaqRoMGYxCzAJBgNVBAYT
        AklUMSkwJwYDVQQKEyBBbm9uaW1hIFBvc3RhIENlcnRpZmljYXRhIFMucC
        5BLjEsMCoGCSqGSIb3DQEJARYdcG9zdGEtY2VydGlmaWNhdGFAYW5wb2Nl
        cnQuaXSCAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQQFAAOBgQA58B
        Z+q1qSKpuffzTBpMtbeFkDIxMqMa+ycnxdMNvcWgCm1A9ZiFJsvqYhDDqA
        XxfHjkrzXuSZkYq6WiQCsLp0aYVy40QCIwbOunhrvsxh3vsG5CgN76JzZ9
        5Z/1OCFNhLfqf1VH2NSS8TaYCCi/VO7W1Q1KkcA2VlxlQP7McSUw==
       mailReceipt: ricevute@anpocert.example.com
       LDIFLocationURL: https://anpocert.example.com/anpocert.ldif.p7m
       managedDomains: mail.anpocert.example.com
       managedDomains: cert.company.example.com
       managedDomains: costmec.example.com
       description: Certified mail services for companies
```

```
        dn: providerName=Postal Services S.p.A,o=postacert
```

```
    objectclass: top
    objectclass: provider
    providerName: Postal Services S.p.A
    providerCertificateHash:
     e00fdd9d88be0e2cc766b893315caf93d5701a6a
    providerCertificate;binary::
     MIIDHjCCAoegAwIBAgIBADANBgkqhkiG9w0BAQQFADBuMQswCQYDVQQGEw
     JJVDEfMB0GA1UEChMWU2Vydml6aSBQb3N0YWxpIFMuci5sLjEPMA0GA1UE
     CxMGRC5DLkMuMS0wKwYJKoZIhvcNAQkBFh5wb3N0YS1jZXJ0aWZpY2F0YU
     BzZXJwb3N0YWwuaXQwHhcNMDIxMjA5MTczMjE2WhcNMDMxMjA5MTczMjE2
     WjBuMQswCQYDVQQGEwJJVDEfMB0GA1UEChMWU2Vydml6aSBQb3N0YWxpIF
     Muci5sLjEPMA0GA1UECxMGRC5DLkMuMS0wKwYJKoZIhvcNAQkBFh5wb3N0
     YS1jZXJ0aWZpY2F0YUBzZXJwb3N0YWwuaXQwgZ8wDQYJKoZIhvcNAQEBBQ
     ADgY0AMIGJAoGBAKoc7n6zA+sO8NATMcfJ+U2aoDEsrj/cObG3QAN6Sr+l
     ygWxYXLBZNfSDWqL1K4edLr4gCZIDFsq0PIEaYZhYRGjhbcuJ9H/ZdtWdX
     xcwEWN4mwFzlsASogsh5JeqS8db3A1JWkvhO9EUfaCYk8YMAkXYdCtLD9s
     9tCYZeTE2ut9AgMBAAGjgcswgcgwHQYDVR0OBBYEFHPw7VJIoIM3VYhuHa
     eAwpPF5leMMIGYBgNVHSMEgZAwgY2AFHPw7VJIoIM3VYhuHaeAwpPF5leM
     oXKkcDBuMQswCQYDVQQGEwJJVDEfMB0GA1UEChMWU2Vydml6aSBQb3N0YW
     xpIFMuci5sLjEPMA0GA1UECxMGRC5DLkMuMS0wKwYJKoZIhvcNAQkBFh5w
     b3N0YS1jZXJ0aWZpY2F0YUBzZXJwb3N0YWwuaXSCAQAwDAYDVR0TBAUwAw
     EB/zANBgkqhkiG9w0BAQQFAAOBgQApqeXvmOyEjwhMrXezPAXELMZwv4qq
     r5ri4XuxTq6sS9jRsEbZrS+NmbcJ7S7eFwNQMNxYFVJqdWoLh8qExsTLXn
     sKycSnHbCfuphrKvXjQvR2da75U4zGSkroiyvJ2s9TtiCcT3lQtIjmvrFb
     aSBiyzj+za7foFUCQmxCLtDaA==
    mailReceipt: takecharge@postalser.example.com
    LDIFLocationURL: https://postalser.example.com/ldif.txt.p7m
    managedDomains: postal-services.example.com
    managedDomains: receivedmail.example.com
    description: Certified mail services for the public
```

The following LDIF file represents an example of a PEC providers' directory, containing a base root and 2 fictitious providers, the first of which handles a secondary environment as well. The certificates inserted are 2 self-signed certificates used for example purposes only:

```
    dn: o=postacert
    objectclass: top
    objectclass: organization
    objectClass: LDIFLocationURLObject
    o: postacert
    LDIFLocationURL: https://igpec.rupa.example.com/igpec.ldif.p7m
    description: Base root for the PEC providers directory

    dn: providerName=Anonymous Certified Mail S.p.A.,o=postacert
    objectclass: top
    objectclass: provider
```

```
      providerName: Anonymous Certified Mail S.p.A.
```

```
providerCertificateHash:
 7E7AEF1059AE0F454F2643A95F69EC3556009239
providerCertificate;binary::
 MIIDBjCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQQFADBmMQswCQYDVQQGEw
 JJVDEpMCcGA1UEChMgQW5vbmltYSBQb3N0YSBDZXJ0aWZpY2F0YSBTLnAu
 QS4xLDAqBgkqhkiG9w0BCQEWHXBvc3RhLWNlcnRpZmljYXRhQGFucG9jZX
 J0Lml0MB4XDTAyMTIwOTE3MjQxNVoXDTAzMTIwOTE3MjQxNVowZjELMAkG
 A1UEBhMCSVQxKTAnBgNVBAoTIEFub25pbWEgUG9zdGEgQ2VydGlmaWNhdG
 EgUy5wLkEuMSwwKgYJKoZIhvcNAQkBFh1wb3N0YS1jZXJ0aWZpY2F0YUBh
 bnBvY2VydC5pdDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAr8J+qK
 KdxV9LzDMPqwnEy0P8H/KwbI0Szs8p6UZajZdpeUK0Ncbrv1QyXZNNtSMC
 2uL09HDyx8agjgZWdhypnehguiSK3busha15RSpMGhiqxmz2b0HhOG73Gf
 alZelqrwqmElna4MNUaLhbOvTd/sqPUS378w5IaIhWxzy34XcCAwEAAaOB
 wzCBwDAdBgNVHQ4EFgQUN8lC0znQWEs0xspZ/aBzsaGvRZMwgZAGA1UdIw
 SBiDCBhYAUN8lC0znQWEs0xspZ/aBzsaGvRZOhaqRoMGYxCzAJBgNVBAYT
 AklUMSkwJwYDVQQKEyBBbm9uaW1hIFBvc3RhIENlcnRpZmljYXRhIFMucC
 5BLjEsMCoGCSqGSIb3DQEJARYdcG9zdGEtY2VydGlmaWNhdGFAYW5wb2Nl
 cnQuaXSCAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQQFAAOBgQA58B
 Z+q1qSKpuffzTBpMtbeFkDIxMqMa+ycnxdMNvcWgCm1A9ZiFJsvqYhDDqA
 XxfHjkrzXuSZkYq6WiQCsLp0aYVy40QCIwbOunhrvsxh3vsG5CgN76JzZ9
 5Z/1OCFNhLfqf1VH2NSS8TaYCCi/VO7W1Q1KkcA2VlxlQP7McSUw==
mailReceipt: notifications@anpocert.it.example
LDIFLocationURL: http://anpocert.example.com/anpocert.ldif.p7m
managedDomains: mail.anpocert.example.com
managedDomains: cert.company.example.com
managedDomains: costmec.example.com
description: Certified mail services for companies
dn: providerUnit=Secondary Environment, providerName=Anonymous
 Certified Mail S.p.A.,o=postacert
objectclass: top
objectclass: provider
providerName: Certified Mail S.p.A.
providerUnit: Secondary Environment
providerCertificateHash:
 7E7AEF1059AE0F454F2643A95F69EC3556009239
providerCertificate;binary::
 MIIDBjCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQQFADBmMQswCQYDVQQGEw
 JJVDEpMCcGA1UEChMgQW5vbmltYSBQb3N0YSBDZXJ0aWZpY2F0YSBTLnAu
 QS4xLDAqBgkqhkiG9w0BCQEWHXBvc3RhLWNlcnRpZmljYXRhQGFucG9jZX
 J0Lml0MB4XDTAyMTIwOTE3MjQxNVoXDTAzMTIwOTE3MjQxNVowZjELMAkG
 A1UEBhMCSVQxKTAnBgNVBAoTIEFub25pbWEgUG9zdGEgQ2VydGlmaWNhdG
 EgUy5wLkEuMSwwKgYJKoZIhvcNAQkBFh1wb3N0YS1jZXJ0aWZpY2F0YUBh
 bnBvY2VydC5pdDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAr8J+qK
 KdxV9LzDMPqwnEy0P8H/KwbI0Szs8p6UZajZdpeUK0Ncbrv1QyXZNNtSMC
 2uL09HDyx8agjgZWdhypnehguiSK3busha15RSpMGhiqxmz2b0HhOG73Gf
 alZelqrwqmElna4MNUaLhbOvTd/sqPUS378w5IaIhWxzy34XcCAwEAAaOB
 wzCBwDAdBgNVHQ4EFgQUN8lC0znQWEs0xspZ/aBzsaGvRZMwgZAGA1UdIw
 SBiDCBhYAUN8lC0znQWEs0xspZ/aBzsaGvRZOhaqRoMGYxCzAJBgNVBAYT
```

AklUMSkwJwYDVQQKEyBBbm9uaW1hIFBvc3RhIENlcnRpZmljYXRhIFMucC

```
         5BLjEsMCoGCSqGSIb3DQEJARYdcG9zdGEtY2VydGlmaWNhdGFAYW5wb2Nl
         cnQuaXSCAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQQFAAOBgQA58B
         Z+q1qSKpuffzTBpMtbeFkDIxMqMa+ycnxdMNvcWgCm1A9ZiFJsvqYhDDqA
         XxfHjkrzXuSZkYq6WiQCsLp0aYVy40QCIwbOunhrvsxh3vsG5CgN76JzZ9
         5Z/1OCFNhLfqf1VH2NSS8TaYCCi/VO7W1Q1KkcA2VlxlQP7McSUw==
        mailReceipt: notifications@secondary.anpocert.example.com
        managedDomains: management.anpocert.example.com
        managedDomains: personnel.anpocert.example.com
        description: Corporate internal services
        dn: providerName=Postal Services S.r.l.,o=postacert
        objectclass: top
        objectclass: provider
        providerName: Postal Services S.r.l.
        providerCertificateHash:
         e00fdd9d88be0e2cc766b893315caf93d5701a6a
        providerCertificate;binary::
         MIIDHjCCAoegAwIBAgIBADANBgkqhkiG9w0BAQQFADBuMQswCQYDVQQGEw
         JJVDEfMB0GA1UEChMWU2Vydml6aSBQb3N0YWxpIFMuci5sLjEPMA0GA1UE
         CxMGRC5DLkMuMS0wKwYJKoZIhvcNAQkBFh5wb3N0YS1jZXJ0aWZpY2F0YU
         BzZXJwb3N0YWwuaXQwHhcNMDIxMjA5MTczMjE2WhcNMDMxMjA5MTczMjE2
         WjBuMQswCQYDVQQGEwJJVDEfMB0GA1UEChMWU2Vydml6aSBQb3N0YWxpIF
         Muci5sLjEPMA0GA1UECxMGRC5DLkMuMS0wKwYJKoZIhvcNAQkBFh5wb3N0
         YS1jZXJ0aWZpY2F0YUBzZXJwb3N0YWwuaXQwgZ8wDQYJKoZIhvcNAQEBBQ
         ADgY0AMIGJAoGBAKoc7n6zA+sO8NATMcfJ+U2aoDEsrj/cObG3QAN6Sr+l
         ygWxYXLBZNfSDWqL1K4edLr4gCZIDFsq0PIEaYZhYRGjhbcuJ9H/ZdtWdX
         xcwEWN4mwFzlsASogsh5JeqS8db3A1JWkvhO9EUfaCYk8YMAkXYdCtLD9s
         9tCYZeTE2ut9AgMBAAGjgcswgcgwHQYDVR0OBBYEFHPw7VJIoIM3VYhuHa
         eAwpPF5leMMIGYBgNVHSMEgZAwgY2AFHPw7VJIoIM3VYhuHaeAwpPF5leM
         oXKkcDBuMQswCQYDVQQGEwJJVDEfMB0GA1UEChMWU2Vydml6aSBQb3N0YW
         xpIFMuci5sLjEPMA0GA1UECxMGRC5DLkMuMS0wKwYJKoZIhvcNAQkBFh5w
         b3N0YS1jZXJ0aWZpY2F0YUBzZXJwb3N0YWwuaXSCAQAwDAYDVR0TBAUwAw
         EB/zANBgkqhkiG9w0BAQQFAAOBgQApqeXvmOyEjwhMrXezPAXELMZwv4qq
         r5ri4XuxTq6sS9jRsEbZrS+NmbcJ7S7eFwNQMNxYFVJqdWoLh8qExsTLXn
         sKycPSnHbCfuphrKvXjQvR2da75U4zGSkroiyvJ2s9TtiCcT3lQtIjmvrF
         baSBiyzj+za7foFUCQmxCLtDaA==
        mailReceipt: takecharge@postalser.example.com
        LDIFLocationURL: http://postalser.example.com/ldif.txt.p7m
        managedDomains: postal-services.example.com
        managedDomains: receivedmail.example.com
        description: Certified mail services for the public
```

5. Security-related aspects

5.1. Digital signature

It is recommended that a dedicated hardware module be used to handle private key and signature operations, the specifications of which are outside the scope of this document. It's up to the PEC providers to conform to security requisites expected for the service.

5.2. Authentication

User access to PEC services through the access point MUST be allowed only upon successful user authentication on the system.

For example, authentication might use user-ID and password, or, if available and considered necessary for the type of service provided, an electronic ID card or the national services card. Choice of authentication method is left to the better judgment of the service provider. Authentication is necessary to guarantee as much as possible that the message is sent by a PEC user whose identification data is congruent with the specified sender, so as to avoid falsification of the latter.

5.3. Secure interaction

To guarantee that the original message remains unaltered during transaction, envelopment and signature are applied on outgoing messages at the access point, and subsequent verification of incoming messages is done at the incoming point.

All communications within the PEC network MUST use secure channels. Integrity and confidentiality of connections between PEC provider and user MUST be guaranteed through the use of secure protocols, such as those based on [TLS] and those that create a secure transport channel on which non-secure protocols can transmit (e.g. IPSec).

The interaction between providers MUST take place using SMTP on [TLS], as per [SMTP-TLS]. The incoming point MUST provide and announce its support for the STARTTLS extension, as well as accept both unencrypted connections (for ordinary mail) and protected ones. To guarantee complete traceability in the flow of PEC messages, these MUST NOT transit on systems external to the PEC network. When exchanging messages between different providers, all transactions MUST take place between machines that belong to the PEC network or are directly managed by the provider. An "MX" type record MAY be associated to each PEC domain defined within the system for name resolution, in which case secondary reception systems specified in that record MUST be under direct control of the provider. All in conformance with [SMTP].

5.4. Virus

Another important security aspect that concerns the PEC system, is related to the technical and functional architecture which MUST block the presence of viruses from endangering the security of all handled messages. It is therefore REQUIRED to have installations and continuous updates of anti-virus systems that hinder infections as

much as possible without intervening on the content of the certified mail, in compliance with what has been discussed thus far.

5.5. S/MIME certificate

In this document the S/MIME certificate profile is defined for use in the certification of PEC messages done by the providers. The proposed profile of the S/MIME certificate is based on the IETF standards [SMIMECERT] and [CRL], which in turn are based on the standard ISO/IEC 9594-8:2001.

5.5.1. Provider-related information (subject)

The information related to the PEC provider holder of the certificate MUST be inserted in the "Subject:" field (Subject DN). More precisely, the Subject DN MUST contain the PEC provider's name as it is in the "providerName" attribute published in the PEC providers directory (section 4.5), but the Subject DN does not have to match the Provider entry DN in the LDIF. The providerName MUST be present in the CommonName or OrganizationName attributes of the Subject field in the certificate.

Certificates MUST contain an Internet mail address, which MUST have a value in the subjectAltName extension, and SHOULD NOT be present in the Subject Distinguished Name.

Valid subjectDN are:

```
C=IT, O=AcmePEC S.p.A, CN=Posta Certificata

C=IT, O=ServiziPEC S.p.A, CN=Posta Certificata
```

Valorization of other attributes in the Subject DN, if present, MUST be done in compliance with [CRL].

5.5.2. Certificate extensions

Extensions that MUST be present in the S/MIME certificate are:

o Key Usage

o Authority Key Identifier

o Subject Key Identifier

o Subject Alternative Name

The Basic Constraints extension (Object ID:2.5.29.19) MUST NOT be present.

The valorization of the above listed extensions for the described profile follows.

The Key Usage extension (Object ID: 2.5.29.15) MUST have the digitalSignature bit (bit 0) activated and MUST be marked as critical. The extension MAY contain other active bits corresponding to different Key Usage, as long as that doesn't contrast with the indications in [CRL].

The Authority Key Identifier (Object ID:2.5.29.35) MUST contain at least the keyIdentifier field, and MUST NOT be marked as critical.

The Subject Key Identifier extension (Object ID: 2.5.29.14) MUST contain at least the keyIdentifier field, and MUST NOT be marked as critical.

The Subject Alternative Name (Object ID: 2.5.29.17) MUST contain at least the rfc822Name field, and MUST NOT be marked as critical.

Adding other extensions that have not been described in this document is to be considered OPTIONAL, as long as it remains compliant with [CRL]; such added extension MUST NOT be marked as critical.

5.5.3. Example

Following is an example of an S/MIME certificate compliant with the minimal requisites described in this profile. Values used are of fictitious providers generated for example purposes only.

5.5.3.1. General-use certificate in annotated version

An asterisk near the label of an extension means that such an extension has been marked as critical.

```
VERSION: 3
SERIAL: 11226 (0x2bda)
INNER SIGNATURE:
  ALG. ID: id-sha1-with-rsa-encryption
  PARAMETER: 0
ISSUER:
  Country Name: IT
  Organization Name: Certifier 1
  Organizational Unit Name: Certification Service Provider
  Common Name: Certifier 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: Certified Mail
       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
```

5.5.3.2. General-use certificate 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 ]
             : }
```

5.6. PEC providers directory

The contents of the PEC providers directory MUST be queried via [HTTP] on SSL, as described in [TLS], exclusively by licensed providers that have the necessary user certificates; this access modality guarantees authenticity, integrity and confidentiality of data.
Each provider downloads the LDIF file through an [HTTPS] session, which is authenticated by checking the X.509 certificate issued by a certification authority.

6. PEC system client technical and functional prerequisites

This section lists the prerequisites that must be respected by a client in order to guarantee the minimal operative functionalities to the user of a general PEC system:

o handling of access and delivery points through secure channels;

o handling of user authentication in message dispatch and reception which make use of standard protocols, such as [IMAP], [POP3] and [HTTP];

o support for MIME format according to [MIME1] and [MIME5];

o support for "ISO-8859-1 (Latin-1)" character set;

o support for S/MIME v3 standard, as in [SMIMEV3], for verification of signatures applied to PEC envelopes and notifications.

7. Security Considerations

All security considerations from [CMS] and [SMIMEV3] apply to applications that use procedures described in this document.

The centralized LDAP server is a critical point for the security of the whole PEC system. An attack could compromise the whole PEC system. PEC providers that periodically download the LDIF file

SHOULD use the best security technology to protect it from local attacks. A PEC provider could be compromised if an attacker changed a certificate or modified the list of domains associated to it in the LDIF file that was copied to the PEC provider system.

When verifying the validity of the signature of a message, the recipient system SHOULD verify that the certificate included in the [CMS] message is present in the LDIF file (section 4.5), and that the domain extracted by the [EMAIL] "From:" header is listed in the managedDomains attribute associated to said certificate.

8. IANA Considerations

8.1. Registration of PEC message header fields

This document defines new header fields used in the messages that transit in the PEC network. As specified and required by [HEADERS-IANA], this document registers new header fields as Provisional Message Header Fields as follows.

8.1.1. Header field: X-Riferimento-Message-ID

Applicable protocol: mail [EMAIL]

Status: provisional

Author/Change controller:

Claudio Petrucci
DigitPA
Viale Carlo Marx 31/49
00137 Roma
Italy
EMail: PETRUCCI@digitpa.gov.it

Specification document: this I-D, section 2.2.1, Appendix A.

8.1.2. Header field: X-Ricevuta

Applicable protocol: mail [EMAIL]

Status: provisional

Author/Change controller:

Claudio Petrucci
DigitPA
Viale Carlo Marx 31/49
00137 Roma

Italy
EMail: PETRUCCI@digitpa.gov.it

Specification document: this I-D, sections 2.1.1.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.6, 3.2.1, 3.2.3, 3.2.4, 3.3.2, 3.3.3, Appendix A.

8.1.3. Header field: X-VerificaSicurezza

Applicable protocol: mail [EMAIL]

Status: provisional

Author/Change controller:

Claudio Petrucci
DigitPA
Viale Carlo Marx 31/49
00137 Roma
Italy
EMail: PETRUCCI@digitpa.gov.it

Specification document: this I-D, sections 2.1.1.1.3, 3.1.3, 3.2.4, Appendix A.

8.1.4. Header field: X-Trasporto

Applicable protocol: mail [EMAIL]

Status: provisional

Author/Change controller:

Claudio Petrucci
DigitPA
Viale Carlo Marx 31/49
00137 Roma
Italy
EMail: PETRUCCI@digitpa.gov.it

Specification document: this I-D, sections 3.1.5, 3.2.2, Appendix A.

8.1.5. Header field: X-TipoRicevuta

Applicable protocol: mail [EMAIL]

Status: provisional

Author/Change controller:

Claudio Petrucci
DigitPA
Viale Carlo Marx 31/49
00137 Roma
Italy
EMail: PETRUCCI@digitpa.gov.it

Specification document: this I-D, sections 3.1.5, 3.3.2, 3.3.2.1,
3.3.2.2, 3.3.2.3, Appendix A.

8.2. Registration of LDAP object identifier descriptors

This document defines new LDAP attributes and object classes for object identifier descriptors. As specified and required by [LDAP-IANA], this document registers new descriptors as follows per the Expert Review.

8.2.1. Registration of Object Classes

Subject: Request for LDAP OID Registration

Descriptor (short name): See comments

Object Identifier: See comments

Person & email address to contact for further information:
See "Author/Change Controller"

Usage: object class

Specification: (I-D)

Author/Change Controller:

Claudio Petrucci
DigitPA
Viale Carlo Marx 31/49
00137 Roma
Italy
EMail: PETRUCCI@digitpa.gov.it

Comments:

The following object identifiers and associated object classes are requested to be registered.

OID	Object Class
1.3.6.1.4.1.16572.2.1.1	LDIFLocationURLObject
1.3.6.1.4.1.16572.2.1.2	provider

Please also see the associated registration request for the providerCertificateHash, providerCertificate, providerName, mailReceipt, managedDomains, LDIFLocationURL, and providerUnit attribute types.

8.2.2. Registration of Attribute Types

Subject: Request for LDAP OID Registration

Descriptor (short name): See comments

Object Identifier: See comments

Person & email address to contact for further information:
See "Author/Change Controller"

Usage: attribute type

Specification: (I-D)

Author/Change Controller:

Claudio Petrucci
DigitPA
Viale Carlo Marx 31/49
00137 Roma
Italy
EMail: PETRUCCI@digitpa.gov.it

Comments:

The following object identifiers and associated attribute types are requested to be registered.

OID	Object Class
1.3.6.1.4.1.16572.2.2.1	providerCertificateHash
1.3.6.1.4.1.16572.2.2.2	providerCertificate
1.3.6.1.4.1.16572.2.2.3	providerName
1.3.6.1.4.1.16572.2.2.4	mailReceipt
1.3.6.1.4.1.16572.2.2.5	managedDomains
1.3.6.1.4.1.16572.2.2.6	LDIFLocationURL
1.3.6.1.4.1.16572.2.2.7	providerUnit

Please also see the associated registration request for the LDIFLocationURLObject and provider object classes.

9. References

9.1. Normative References

[ABNF] Crocker, D., Editor, and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 5234, January 2008.

[CMS] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 5652, Vigil Security, September 2009.

[CRL] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housely, R. and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[EMAIL] P. Resnick, Editor, "Internet Message Format", RFC 5322, QUALCOM Incorporated, April 2001.

[HEADERS-IANA] Klyne, G., Nottingham, M., and J. Mogul, "Registration Procedures for Message Header Fields", RFC 3864, September 2004.

[HTTP] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P. and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[HTTPS] Rescorla, E., "HTTP Over TLS", RFC 2818, RTFM, Inc., May 2000.

[IMAP] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4 rev1", RFC 3501, University of Washington, March 2003.

[LDAP] K. Zeilenga, Editor, "Lightweight Directory Access Protocol (LDAP): Technical Specification Raod Map", RFC 4510, OpenLDAP Foundation, June 2006.

[LDAP-IANA] Zeilenga, K., "Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Direcotry Access Protocol (LDAP)", RFC 4520, OpenLDAP Foundation, June 2006.

[LDAP-SYNTAXES] Legg, S., Editor, "Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules", RFC 4517, eB2Bcom, June 2006.

[LDIF] Good, G., "The LDAP Data Interchange Format (LDIF) - Technical Specification", RFC 2849, iPlanet e-commerce Solutions, June 2000.

[MIME1] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

[MIME5] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples", RFC 2049, November 1996.

[SUBMISSION] Gellens, R. and J. Klensin, "Message Submission for Mail", RFC 4409, April 2006.

[POP3] Myers, J. and M. Rose, "Post Office Protocol - Version 3", RFC 1939, May 1996.

[REQ] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, Harvard University, March 1997.

[SHA1] Eastlake, D. and P. Jones, "US Secure Hash Algorithm 1 (SHA1)", RFC 3174, September 2001.

[MIME-SECURE] Galvin, J., Murphy, S., Crocker, S. and N. Freed, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", RFC 1847, October 1995.

[SMIMEV3] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, January 2010.

[SMIMECERT] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling", RFC 5750, January 2010.

[SMTP] Klensin, J. Editor, "Simple Mail Transfer Protocol", RFC 5321, AT&T Laboratories, April 2001.

[SMTP-DSN] Moore, K., "Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications

(DSNs)", RFC 3461, University of Tennessee, January 2003.

[SMTP-TLS] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC 3207, Internet

Mail Consortium, February 2002.

[TIMESTAMP] Klyne, G. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, July 2002.

[TLS] Dierks, T. and E.Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

10. Acknowledgments

The Italian document on which this document is based, is a product of the collaboration of many with the supervision of the National Center for Informatics in the Public Administration of Italy (DigitPA).

Appendix A: Italian fields and values in English

NOTE: The right column represents a translation of the Italian fields for readability's sake only. Header fields that MUST be used are the ones in the left column.

X-Riferimento-Message-ID	Reference Message ID
X-Ricevuta	Notification
non-accettazione	non acceptance
accettazione	acceptance
preavviso-errore-consegna	delivery error advance notice
presa-in-carico	take charge
rilevazione-virus	virus detection
errore-consegna	delivery error
avvenuta-consegna	message delivered
X-VerificaSicurezza	Security Verification
errore	error
X-Trasporto	Transport
posta-certificata	certified mail
errore	error
X-TipoRicevuta	Notification Type
completa	complete
breve	brief
sintetica	concise
certificatore	certificator

Subject values:

Accettazione	ACCEPTANCE
Posta certificata	CERTIFIED MAIL
Presa in carico	TAKE IN CHARGE
Consegna	DELIVERY
Anomalia messaggio	MESSAGE ANOMALY
Problema di sicurezza	SECURITY PROBLEM
Avviso di non accettazione	NON ACCEPTANCE PEC NOTIFICATION
Avviso di non accettazione per virus	VIRUS DETECTION INDUCED NON ACCEPTANCE PEC NOTIFICATION
Avviso di mancata consegna	NON DELIVERY PEC NOTIFICATION
Avviso di mancata consegna per virus	NON DELIVERY DUE TO VIRUS PEC NOTIFICATION
Avviso di mancata consegna per sup. tempo massimo	NON DELIVERY DUE TO TIMEOUT PEC NOTIFICATION

Italian terms in the DTD relative to the certification XML file:

accettazione	acceptance
altro	other

avvenuta-consegna	delivered
certificato	certificate
consegna	delivery
data	date
dati	data
destinatari	recipients
esterno	external
errore	error
errore-consegna	delivery error
errore-esteso	extensive error
gestore-emittente	transmitting provider
giorno	day
identificativo	identifier
intestazione	header
mittente	sender
no-dest(inatario)	no recipient
no-dominio	no domain
non-accettazione	non acceptance
nessuno	none
oggetto	subject
ora	hour
posta-certificata	certified mail
preavviso-errore-consegna	delivery error advance notice
presa-in-carico	take in charge
ricevuta	receipt
ricezione	receipt (the act of receiving)
rilevazione-virus	virus detection
risposte	replies
tipo	type

Appendix B: Change History

[[This entire section is to be removed upon publication.]]

B.1 Changes between draft-gennai-smime-cnipa-pec-03 and draft-gennai-smime-cnipa-pec-04

Removed legal mentions in section 1.1.

Changed terminology in 2.1. System-generated messages
sender <-> author

Preceded all "transport envelope" and "notification" mentions by "PEC" to avoid confusion with the SMTP transport envelope and DSN notifications.

Changed section 5.1

Edited Appendix A

Updated authors' addresses

B.2 Changes between draft-gennai-smime-cnipa-pec-04 and draft-gennai-smime-cnipa-pec-05

Added translation of Italian terms in the DTD relative to the XML certification file.

Fixed syntax errors in the DTD.

B.3 Changes between draft-gennai-smime-cnipa-pec-05 and draft-gennai-smime-cnipa-pec-06

Corrected use of terminology ("header field", "message body") throughout draft.

Replaced all mentions of CNIPA with DigitaPA, except in 1.2.2 and 1.2.3.

Section 1. Introduction; added reference and link to Italian specifications document.

Section 1.2.3 Terms and defs; edited "time stamp" definition; added "ordinary mail" and " DigitPA" definitions; removed redundant definitions.

Section 2.1. System-generated messages; added [MIME1] reference.

Section 2.2.1 Access Point: reference correction (6.2 -> 5.2).

Section 2.2.2. Incoming point; added [SHA1] & [CRL] references; removed "understand the motivations" in point: "o check what virus typologies were not detected by its own antivirus to understand the motivations and verify the possibility of interventions."

2.2.3 Delivery point; re-wrote non-delivery notification part.

Added section 2.2.6. Provider service email address.

Sections 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.2.1, 3.2.3, 3.2.4, 3.3.2.1, 3.3.2.2, 3.3.2.3, 3.3.3 edits:
parsing the XML part only requirement, cross reference to 4.3 and re-write (corrected use of terms "header", "attachment" and "message body").

Section 3.3.2.2: added SHOULD requirement on hash value calculations on base64.

Section 3.5. Example; note about possible parallelism of some steps.

Section 4.2. User date/time; added format specification in ABNF notation.

Section 4.3.1; removed MIME type: multipart/alternative.

Section 4.5 PEC providers directory scheme; entirely re-written; added HTTPS reference; edited urls to use "example.it" domains.

Sections 4.3. & 4.3.1; title edit.

Section 5.3 Secure interaction; added reference to [SMTP]. Removed redundant text. Re-wrote MX record part.

Section 5.6. PEC providers directory; more details on how it currently works.

Section 6.; references to IMAP, POP3, HTTP

Section 8. IANA Considerations: added registration request templates for new message header fields and LDAP attributes & object classes.

Section 9. References; added ABNF, CRL, HEADERS-IANA, HTTP, HTTPS, IMAP, LDAP-IANA, LDAP-SYNTAXES, POP3, and TIMESTAMP references; updated all obsolete references.

Updated authors' email addresses

B.4 Changes between draft-gennai-smime-cnipa-pec-06 and draft-gennai-smime-cnipa-pec-07

Section 2.2.2; edited part concerning virus detection.

Section 2.2.3; re-wrote last paragraph.

Section 3.1.1; corrected use of terms; re-wrote some points to be clearer.

Section 3.3.2.2; edited the part concerning hash substitution.

Section 4.2; fixed the note.

Section 4.3; removed restriction on charset encoding; added more detail to describe message structure.

Section 5.2; edited the "MUST" requirement.

Section 5.3; edited the "MUST" requirement concerning MX records.

Section 5.5.1; edited clarficiation regarding Subject DN.

Appendix A; removed dashes from English column. Added note.

Replaced all occurrences of "certmail" with "postacert".

Updated authors' addresses.

Authors' Addresses

Francesco Gennai
ISTI-CNR
Via Moruzzi, 1
56126 Pisa
Italy

Email: francesco.gennai@isti.cnr.it

Alba Shahin
ISTI-CNR
Via Moruzzi, 1
56126 Pisa
Italy

Email: alba.shahin@isti.cnr.it

Claudio Petrucci
DigitPA
Viale Marx 31/49
00137 Roma
Italy

Email: petrucci@digitpa.gov.it

Alessandro Vinciarelli
Via delle Vigne di Morena 113
00118 Roma
Italy

Email: alessandro.vinciarelli@gmail.com

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.