4 Goals and contents of the document

This document describes the technical rules on how to create and operate certified electronic mail.

5 Definitions

Access point

This is the port supplying access services required to send and read certified mail messages. The access point provides the following services: user identification and access, scanning of the message for viruses, issue of *acceptance receipt*, putting the *original message* into the *transport envelope*.

Reception point

This is the port receiving the message inside a *certified mail domain*. It checks the origin/correctness of the message and issues the *delivery receipt*, puts the wrong message into an *anomaly envelope* and scans ordinary mail messages and *transport envelopes* for viruses and, on the basis of the criteria herein below, it puts the message into a *security envelope*.

Delivery point

It delivers the message to the electronic mail box of the recipient *certified mail user*. It checks the origin/correctness of the message, issues, according to the cases, the *successful delivery receipt* or the *notice of failed delivery*.

Acceptance receipt

This is the receipt, containing the *certification data*, issued to the sender by the *access point* upon sending a certified mail message. The acceptance receipt is signed with the key of the *certified mail provider* of the sender.

Non-acceptance notice

This is the notice issued when the originating provider cannot accept the incoming message. The reason why the message cannot be accepted is written in the receipt text explaining also that the message may not be delivered to the recipient. The non-acceptance notice is signed with the key of the *certified mail provider* of the sender.

Takeover receipt

It is issued by the *reception point* to the originating *certified mail provider* in order to certify successful takeover of the message by the recipient *certified mail domain*. The takeover receipt contains the *certification data* in order to allow to match it to the reference message.

Successful delivery receipt

The *delivery point* issues the successful delivery receipt when the message has entered the *certified mail box* of the recipient. A successful delivery receipt is issued for each intended recipient. The successful delivery receipt has *certification data* attached thereto and, for the primary recipients, the *original message* or an excerpts thereof.

Notice of failed delivery

If the certified mail provider cannot deliver the message to the certified mail box of the recipient, the system issues a notice of failed delivery to report the anomaly to the recipient of the *original message*.

Original message

This is the original message sent by a *certified mail user* before its arrival at the *access point*. The original message is delivered to the recipient *certified mail user* through a *transport envelope* containing it.

Transport envelope
This is the message originated by the *access point*, which contains the *original message* sent by the *certified mail user* and relevant *certification data*. The transport envelope is signed with the key of the originating *certified mail provider*. The transport envelope is delivered unchanged to the intended *certified mail box* in order to allow the recipient to check the *certification data*.

Anomaly envelope
When a wrong/non-certified message must be delivered to a *certified mail user*, the message is put into an anomaly envelope to show the anomaly to the recipient. The anomaly envelope is signed with the key of the recipient *certified mail provider*.

Security envelope
When it is verified that a message received at the *access point* or *reception point* contains a virus, the message is put into a security envelope to inform that on that date, for the provider, a virus was present. The security envelope is signed with the key of the *certified mail provider*.

Certification data
This is a set of data describing the *original message* and certified by the *certified mail provider* of the sender. The certification data is put into the different receipts and sent to the intended *certified mail user* along with the *original message* through a *transport envelope*. The certification data includes sending date and time, sender, recipient, subject, message id etc.

Certified mail provider
This is the individual who administers one or more *certified mail domains* with relevant *access, reception* and *delivery points*. He owns the key used to sign the receipts and envelopes. He relates to the other certified mail providers for interoperability with other *certified mail users*.

Certified mail domain
It is a DNS domain for electronic mail boxes of *certified mail users*. Inside a certified mail domain all electronic mail boxes must belong to *certified mail users*. The processing of certified mail messages (user receipts, transport envelopes etc.) must take place even if sender and recipient belong to the same certified mail domain.

Directory of certified mail providers
This is a LDAP server located in an area that can be reached by the different *certified mail providers*. It contains the list of *certified mail domains and providers* with relevant certificates, i.e. the keys used to sign the receipts and the *transport envelopes*.

Certified mail box
This is an electronic mail box to which a capability is associated which issues *successful delivery receipts* upon reception of certified mail messages. A certified mail box can be exclusively defined within a *certified mail domain*.

Certified mail user
This is a user to whom a *certified mail box* is assigned. He uses the *access point* of its *certified mail provider* to send certified mail messages and to read the certified mail messages received.

6 Message processing

6.1 Format of system-generated messages

PEC system generates messages (receipts, notices and envelopes) in a MIME format. The messages are made up of a descriptive text, for the user, and of a set of attachments (original message, certification data etc.) depending on the type of message.

The message (made up of the set of parts described in the specific sections of this attachment) is then put into a S/MIME v3 structure in a CMS format, signed with the private key of the certified mail provider. The certificate associated to the key used for the signature needs be included in that structure. The S/MIME format used to sign system-generated messages is "`multipart/signed`" (.p7s format) as described in the RFC 2633 §3.4.3.

In order to guarantee the possibility to verify the signatures on certified mail messages, on as many electronic mail clients as possible, X.509v3 certificates used by the certified electronic mail systems shall meet the profile proposed in APPENDIX B.

In order to ensure the possibility to verify the signature by the recipient mail client, the sender of the message shall coincide with the one specified within the certificate used for the S/MIME signature. This mechanism results in the transport envelopes showing in the "From" field an originating mail address other than the one of the original message. In order for the message end-user to gain greater insight in the message, the mail address originating the original message is put in the message as "display name". For example, for an original message having the following "From" field:

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

The relevant transport envelope generated shall have the following "From" field:

From: "On behalf of: mario.bianchi@dominio.it" <posta-certificata@gestore.it>

In order to allow the recipient to send replies to the transport envelope of the right original sender, the latter's address needs to be set out in the "`Reply-To`" field of the transport envelope. If that field is not expressly specified in the original message, the system generating the transport envelope will arrange for its origination by extracting it from the "`From`" field of the original message.

To send receipts, the system uses as recipient only the sender of the original message as specified in the "`reverse path`" of the SMTP protocol. The receipts shall be sent to the certified mail box of the sender without consideration for any "`Reply-To`" field in the message heading.

All certified mail system-generated messages can be identified due to the presence of a specific header. This header is useful to prevent message loops in the event of exchange between systems sending receipts/transport envelopes. It is indeed possible that a message sent from a certified mail box and intended for another mail box belonging to the same certified mail service triggers an inappropriate exchange of messages. Receiving a receipt may trigger the system to generate another receipt. In order to tackle this problem the system shall control any identification header and signature to verify the nature of the message.

In order to determine the certification data, the system considers the elements used to route the message to the recipients. When dialoguing with the SMTP protocol (for example at access and reception points) the "`reverse path`" and "`forward path`" data ("`MAIL FROM`" and "`RCPT TO`") are considered as certification data respectively of sender and recipients. The routing data in the

message body ("To" and "Cc" fields) is exclusively used to distinguish the primary recipients from those to whom the message is copied, if needed; the routing data in the "Ccn" field is not considered valid by the system.

6.2 Log

During the message processing phases at the access, reception and delivery points, the system shall track down all the activities performed. All activities are stored on a log showing the significant data of the activity:

- the univocal identification code assigned to the original message (Message-ID, see 6.3)
- date and time of the event
- sender of the original message
- recipients of the original message
- subject of the original message
- type of event (acceptance, reception, issue of receipts, error etc.)
- the identification code (Message-ID) of the related messages generated (receipts, errors etc.)
- originating provider

The actual data entered in the individual logs depend on the type of tracked activity (message reception, receipt generation etc.)

The possibility to retrieve, upon request, the information contained in the logs shall be guaranteed in compliance with privacy rules.

6.3 Access point

The access point allows a user to access the certified mail services made available by its provider. The fact that a user can access PEC services leads to the requirement that said user shall be authenticated by the system (see 8.3). If the provider is a Public Administration having delivered some certified electronic mail boxes to private parties, in order to comply with the provisions contained in Presidential Decree XXX (Art. 16, subsection 2), it is necessary to assure that the communication takes place only between that private party and the administration that has delivered the mail box; in addition, the provider shall write in the user's manual: "under the provisions contained in Presidential Decree XXX Art. 16, subsection 2, the use by users for purposes other than those for which the mail box was delivered does not constitute valid sending under the above-mentioned decree."

Upon reception of an original message, the access point:

- carries out some formal checks on the incoming message;
- generates an acceptance receipt;
- puts the original message into a transport envelope.

The acceptance receipt tells the sender that his/her message was accepted by the system and certifies date and time of the event. Inside the receipt there is a text that can be read by the user, an XML attachment containing the certification data in an easy format to be processed and any other attachments containing additional features supplied by the provider.

The access point, by using data from the directory of certified mail providers (see 7.5), checks each recipient of the original message to verify whether they belong to the certified mail infrastructure or

they are external users (i.e. Internet mail). This verification is carried out by checking the existence (through a "case insensitive" search) of the recipient domains among the "managedDomains" attributes inside the directory of providers. The acceptance receipt (and relevant certification data) states the type of recipients to inform the sender on the different flow followed by the two groups of messages (certified mail users, external users).

The recipient domain shall exclusively carry out formal checks on the message received by sending the unchanged transport envelope to the recipient.

The univocity of the identification of the original messages accepted shall be guaranteed to the certified mail infrastructure to allow for correct tracking of the messages and relevant receipts. The format of such identification is the following:

[string of characters] @ [provider_mail_domain]

or

[string of characters] @ [mail_server_FQDN]

The original message and corresponding transport envelope shall contain the following header field:

Message-ID: <[message identification]>

If the electronic mail client dialoguing with the access point has already entered a Message ID in the original message to be sent, the ID shall be replaced by the above-mentioned identification. In order to allow the sender to associate the message sent with the corresponding receipts, any Message ID originally present in the message shall be entered in the original message and in the relevant receipts and transport envelope. If the original message ID is present, it shall be made available in the message heading by putting the following header:

X-Reference-Message-ID: [original Message-ID]

that will be included in the receipts and transport envelope and mentioned in the certification data (see 7.4).

6.3.1 Formal checks on incoming messages

At the time of acceptance of the message, the access point shall ensure its formal correctness by verifying that:

- in the message body there is a "Form" filed containing an email address compliant with RFC 2822 specifications §3.4.1;
- in the message body there is a "To" field containing one or more email addresses compliant with RFC 2822 specifications §3.4.1;
- the address of the sender originating the message specified in the routing data (reverse path) is the same as the one specified in the "From" field of the message;
- the addresses of the recipients of the message specified in the routing data (forward path) are the same as the ones specified in the "To" or "Cc" fields of the message;
- the addresses of the recipients of the message contained in the "Ccn" filed are not present.

If the message fails the checks, the access point shall not accept the message inside the certified mail system and issue the relevant non-acceptance notice.

6.3.2 Non-acceptance notice

If the access point does not forward the message, for example due to failed formal checks, the sender receives a non-acceptance notice.

For this non-acceptance notice the headers contain the following fields:

```
X-Receipt: non-acceptance
Date: [date of issue of receipt]
Subject: NON-ACCEPTANCE NOTICE: [original subject]
From: posta-certificata@[mail_domain]
To: [sender]
X-Reference-Message-ID: [Message-ID of the original message]
```

The message body of this receipt is the actual receipt in a readable format containing the following data:

```
Error in message acceptance
On [date] at [time] ([zone]) in the message
“[subject]”coming from “[sender]”
and intended for the user “[recipient]”
a problem was detected that prevents the acceptance of the message
due to [error description].
The message was not accepted.
Message identification: [identification]
```

The same certification data is entered in an XML file, to be attached to the receipt to allow an automatic processing (see 7.4). The receipt may also contain additional attachments for specific features supplied by the certified mail provider; in no case may the original message be entered.

6.3.2.1 Non-acceptance notice due to viruses

The access point shall carry out some checks on the content of the incoming message and shall not accept it if it or any of its attachments are deemed to contain viruses. In this case the *non-acceptance notice due to viruses* shall be issued to give the sender a clear explanation of the reasons that led to message rejection; in that case, the message that has reached the access point shall be put into a Safety Envelope (see 6.3.5) and kept for 30 months according to the provisions contained in the CNIPA Resolution 11/2004, 19th February 2004 (published in the Official Gazette of 9th March 2004, no. 57).

For this non-acceptance notice the headers contain the following fields:

```
X-Receipt: non-acceptance
X-SecurityCheck: error
Date: [date of issue of receipt]
Subject: SECURITY PROBLEM: [original subject]
From: posta-certificata@[mail_domain]
To: [sender]
X-Reference-Message-ID: [Message-ID of the original message]
```

The message body of this receipt is the actual receipt in a readable format containing the following data:

```
Error in message acceptance
On [date] at [time] ([zone]) in the message
“[subject]”coming from “[sender]”
and intended for the user “[recipient]”
a security problem was detected [identification of the type of content detected].
The message was not accepted.
Message identification: [identification]
```

The same certification data is entered in an XML file, to be attached to the receipt to allow an automatic processing (see 7.4). The receipt may also contain additional attachments for specific features supplied by the certified mail provider; in no case may the original message be entered.

6.3.3 Acceptance receipt

The acceptance receipt consists of an electronic mail message sent to the sender and containing date and time of acceptance, sender and recipient data and subject.

The headers of the acceptance receipt shall contain the following fields:

```
X-Receipt: acceptance
Date: [effective date of acceptance]
Subject: ACCEPTANCE: [original subject]
From: posta-certificata@[mail_domain]
To: [sender of the original message]
X-Reference-Message-ID: [Message-ID of the original message]
```

The first field identifies the message as an acceptance receipt. The “`Subject`” field tells the recipient that the message is the receipt of his/her communication. It is made up of the string “`ACCEPTANCE:`” followed by the subject of the original message to which the receipt refers.

The message body of this receipt is the actual receipt in a readable format containing the following data:

```
Acceptance receipt
On [date] at [time] ([zone]) the message
“[subject]”coming from “[sender]”
and intended for:
“[recipient1]” ([“certified mail” “ordinary mail”])
“[recipient2]” ([“certified mail” “ordinary mail”])
-
-
-
“[recipientn]” ([“certified mail” “ordinary mail”])
was accepted by the system and forwarded.
Message identification: [identification]
```

The same certification data is entered in an XML file, to be attached to the receipt to allow an automatic processing. The receipt may also contain additional attachments for specific features supplied by the certified mail provider; in no case may the original message be entered.

6.3.4 Transport envelope

The transport envelope is a message generated by the access point containing the original message and certification data.

The transport envelope takes up the following headers from the original message, that shall thus be left unchanged:

- Received
- To
- Cc
- Return-Path
- Message-ID (as described in 6.3)
- X-Reference-Message-ID (see 6.3)
- X-ReceiptType

On the other hand, the headers herein below shall be changed or entered, if needed:

```
X-Transport: certified-mail
Date: [effective date of acceptance]
Subject: CERTIFIED MAIL: [original subject]
From: “On behalf of: [original sender]” <posta-certificata@[mail_domain]>
Reply-To: [original sender (to be entered only if missing)]
```

The message body of the transport envelope is a text in an immediately readable format available to the recipient of the certified mail message containing the following data:

```
Certified mail message
On [date] at [time] ([zone]) the message
“[subject]”coming from “[sender]”
intended for:
“[recipient1]”
“[recipient2]”
-
-
-
“[recipientn]”
The original message is attached hereto.
Message identification: [identification]
```

Attached to the transport envelope is the whole original message, left unchanged, in a format compliant with RFC 2822 (save for the Message ID) along with header, body and any attachments. The same envelope also contains an XML attachment containing the certification data mentioned in the text in a format that can be processed and additional information on the type of message and type of receipt required (see 7.4). The transport envelope may also have additional elements attached for specific features supplied by the certified mail provider.

Even if the “`From`” field of the transport envelope is changed to allow the recipient to verify the signature, the routing data of the transport envelope (forward path and reverse path of the message) is left unchanged relative to the same data of the original message. This is to guarantee both the forwarding of the message to the original recipients and the return of any error notices on SMTP protocol (as per RFC 2821 and RFC 1891) to the sender of the original message.

6.3.5 Security envelope

The access point and the reception point shall scan the content of the message and relevant attachments for viruses. If the scanning shows the presence of viruses, the message, as is, shall be put into a security envelope, specifying the nature of the potentially dangerous content within, and shall not be forwarded to the recipient but kept for 30 months according to the provisions contained

in CNIPA Resolution 11/2004, 19th February 2004 (publishes in the Official Gazette of 9th March 2004, no. 57). The message, along with header, text and attachments is attached in a format compliant with RFC 2822 to a new message taking up the following headers from the original message, that shall thus be left unchanged:

- Received
- To
- Cc
- Reply-To
- Return-Path
- Message-ID
- X-Reference-Message-ID

On the other hand, the headers herein below shall be changed, or entered if needed:

```
X-SecurityCheck: error
Date: [date of arrival of the message]
Subject: SECURITY PROBLEM: [original subject]
```

The message body of the security envelope is a text in an immediately readable format available to the recipient of the certified mail message containing the following data:

```
Security problem
On [date] at [time] ([zone]) the message
“[subject]”coming from “[sender]”
intended for:
“[recipient1]”
“[recipient2]”
-
-
-
“[recipientn]”
was received.
The message has a potentially dangerous content.
[brief description of the problem detected]
```

6.3.6 Notice of failed delivery due to time run-out

For each message for which an acceptance receipt was generated, the originating provider shall receive, within the terms herein below, a takeover receipt or, as an alternative, a successful delivery receipt. Failing this, the originating provider shall notify its user accordingly by sending two different types of notices of failed delivery with the characteristics herein below.

The first notice of failed delivery, generated by the provider of the sender, notifies the sender that the provider of the recipient, since it has not supplied any evidence in the twelve hours after the sending of the takeover or delivery of the message sent, for technical causes, may not be able to deliver the message. In addition, this notice establishes that if within another twelve hours delivery will not be carried out, an additional notice will be sent on the failed delivery of the message within the 24 hours after sending, as provided for by the rules.

For the notice of failed delivery due to time run-out the headers contain the following fields:

```
X-Receipt: delivery-error-notice
Date: [date of issue of receipt]
```

```
Subject: NOTICE OF FAILED RECEIPT: [original subject]
From: posta-certificata@[mail_domain]
To: [receipts of originating provider]
X-Reference-Message-ID: [Message-ID of the original message]
```

The message body of the first notice of failed delivery is the actual receipt in a readable format containing the following data:

```
Notice of failed delivery
On [date] at [time] ([zone]) the message
“[subject]”coming from “[sender]”
intended for “[recipient]”
was not delivered within the first twelve hours from sending. Not excluding that
this may occur subsequently, it is deemed useful to consider that sending the
message may not be successful. The system will in any case send an additional
notice of failed delivery if in the following twelve hours no confirmation of
reception by recipient is sent.
Message identification: [identification]
```

The same certification data is entered in an XML file, to be attached to the receipt to allow an automatic processing (see 7.4). The receipt may also contain additional attachments for specific features supplied by the certified mail provider; in no case may the original message be entered.

At the end of 24 hours from sending, if the sender has not received a notice of successful or failed delivery, the provider of the sender shall send the second notice to tell the sender that it was not possible to deliver the message sent.

The message body of this notice of failed delivery is the actual receipt in a readable format containing the following data:

```
Notice of failed delivery
On [date] at [time] ([zone]) the message
“[subject]”coming from “[sender]”
intended for the user “[recipient]”
was not delivered within the twenty-four hours after sending. It is believed
that the sending shall be deemed not successful.
Message identification: [identification]
```

The same certification data is entered in an XML file, to be attached to the receipt to allow an automatic processing (see 7.4). The receipt may also contain additional attachments for specific features supplied by the certified mail provider; in no case may the original message be entered.

6.4 Reception point

The reception point allows different certified mail providers to exchange certified mail messages. It is also a port through which ordinary electronic mail messages may be entered in the certified mail circuit (see tables in Appendix A).

As regards ordinary mail, the provider may place before the acceptance point, and therefore outside of the technical/functional architecture of the certified electronic mail, protection systems for any criticalities coming from the Internet. For example, in compliance with the provider’s security policies, it is possible to carry out activities of processing and filtering of ordinary mail messages intended for certified electronic mail users.

The exchange of messages among various providers takes place through a transaction based on the SMTP protocol as defined by RFC 2821. The messages are transferred among providers by using a 7-bit coding both for headers and for the message body and any attachments. Any errors arising out of SMTP dialogue (i.e. invalid recipients, non-available server, exceeding threshold limits etc.) are managed through the standard mechanisms of error notice of SMTP protocol.

The reception point, upon arrival of a message, carries out the following set of tests and activities:

- it checks the correctness/nature of the incoming message;
- if the incoming message is a correct and whole transport envelope:
  - it issues a takeover receipt to the originating provider (see 6.4.1);
  - it forwards the transport envelope to the delivery point (see 6.5);
- if the incoming message is a correct and whole certified mail receipt:
  - it forwards the receipt to the delivery point;
- if the incoming message does not meet the requirements for a transport envelope or a receipt, or is not correct/whole, it is considered an ordinary mail message and thus:
  - it puts the incoming message into an anomaly envelope (see 6.4.2);
  - it forwards the anomaly envelope to the delivery point.

The takeover receipt is issued by the recipient provider of the message to the originating provider. Its aim is to allow the tracking of the message between providers.

Upon reception of a message at the reception point, the system performs a set of checks to verify that the transport envelope/receipt is correct/whole:

- It checks the existence of the signature
  The system verifies that incoming message has a S/MIME signature structure.

- It checks that the signature was issued by a certified mail provider
  The reception point extracts the certificate used for the signature of the incoming message and verifies its presence inside the directory of certified mail providers. To facilitate the checks, it is possible to calculate the SHA1 hash of the certificate extracted and carry out a "case insensitive" search of its hexadecimal representation inside the "`providerCertificateHash`" attributes in the directory. This activity allows to easily identify the originating provider for a subsequent and required check that certificate extracted and the one in the provider's record match.

- It checks signature validity
  The correctness of the message S/MIME signature is verified by re-performing the calculation of the signature algorithms and checking the message CRL. If caches are used for CRL contents, an update interval needs to be adopted so as to guarantee that the data is current in order to minimize any possible delay between the CA issuing the cancellation and the provider adopting the change.
  If the CRL DP managed by CNIPA is not available, the provider shall consider valid the most recent information he/she has.

- It is the Provider's right to carry out other formal checks of the incoming message correctness to ensure that the message is fully compliant with the specifications contained in this technical appendix.

If all checks are successful, the system establishes that the incoming message is a correct transport envelope/receipt, otherwise it considers it an ordinary mail message.

For ordinary mail messages (messages failing one or more checks) coming into the certified mail system, the provider shall scan them for any viruses in order to avoid the access of potentially dangerous electronic mail messages to the certified mail circuit. If an ordinary mail message contains a virus, said virus may be rejected by the reception point before it enters the certified mail circuit, without any particular tackling of the error but in the same way as the messages on a public network. If, on the other hand, the provider decides not to reject the message, the latter will not be delivered to the recipient but put into a Security Envelope and kept for 30 months according to the provisions contained in CNIPA Resolution 11/2004, 19th February 2004 (published in the Official Gazette of 9th March 2004, no. 57).

When, upon reception, the presence of a virus is detected inside a transport envelope, the provider of the recipient issues a notice of failed delivery due to viruses addressed to the delivery point of the originating provider.

The originating provider, upon reception of a notice of failed delivery due to viruses, shall:

1. periodically scan for types of viruses that have not been detected by the antivirus system in order to understand why the virus entered and decide whether it's the case to take action.
2. send a notice of failed delivery due to viruses, intended for the sender of the message.

If a virus is detected, the message that has reached the reception point, on the basis of the above-mentioned rules, along with header, text and attachments, is attached in a format compliant with RFC 2822 to the new message that takes up the following headers from the incoming message, that shall thus be left unchanged:

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

On the other hand, the headers herein below shall be changed or entered, if needed:

```
X-SecurityCheck: error
Date: [date of arrival of the message]
Subject: SECURITY PROBLEM [original subject]
```

The message body of the security envelope is a text in an immediately readable format available to the Provider of the certified mail message containing the following data:

```
Security problem
On [date] at [time] ([zone]) the message
"[subject]"coming from "[sender]"
and intended for:
"[recipient1]"
"[recipient2]"
-
-
-
"[recipientn]"
```

```
was received.
The message content is dangerous.
[brief description of the problem detected]
```

The security envelope contains only the message that has reached the reception point attached thereto.

6.4.1 Takeover receipt

Upon exchanging correct certified mail messages between different certified mail providers and before scanning the transport envelopes for viruses, the recipient provider issues a takeover receipt to the originating provider. The takeover receipts issued relate to the recipients to which the incoming message is sent, as specified in the routing data (forward path and reverse path) of the SMTP transaction. Inside the certification data of the individual takeover receipt the recipients to which it refers are listed. In general, upon the transport envelope, each recipient provider shall issue one or more takeover receipts for the recipients pertaining thereto. The set of those receipts shall cover, failing transport errors, the total message recipients.

The headers of a takeover receipt contain the following fields:

```
X-Receipt: takeover
Date: [date of takeover]
Subject: TAKEOVER: [original subject]
From: posta-certificata@[mail_domain]
To: [receipts of the originating provider]
X-Reference-Message-ID: [Message-ID of the original message]
```

The address for sending receipts to the originating provider is taken from the directory of certified mail providers during the inquiry needed for the verification of the individual who has issued the signature in the verification of the incoming message.

The message body of a takeover receipt contains the following data:

```
Takeover receipt
On [date] at [time] ([zone]) in the message
“[subject]”coming from “[sender]”
and intended for the user “[recipient]”
a problem was detected that prevents the acceptance of the message
due to [error description].
The message was not accepted.
Message identification: [identification]
```

The same certification data is entered in an XML file, to be attached to the receipt to allow an automatic processing (see 7.4). The receipt may also contain additional attachments for specific features supplied by the certified mail provider.

6.4.2 Anomaly envelope

If one of the tests shows an error in the incoming message or is recognized as an ordinary mail message, the system puts it into an anomaly envelope. Before delivery, the message that has reached the reception point along with header, text and attachments is attached in a format compliant with RFC 2822 to a new message that takes up the following headers from the incoming message, that shall thus be left unchanged:

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

On the other hand, the headers herein below shall be changed or entered, if needed:

```
X-transport: error
Date: [date of arrival of the message]
Subject: MEESAGE ANOMALY [original subject]
From: “On behalf of: [original sender]” <posta-certificata@[mail_domain]>
Reply-To: [original sender (entered only if missing)]
```

The message body of the anomaly envelope is a text in an immediately readable format available to the recipient of the message containing the following data:

```
Message anomaly
On [date] at [time] ([zone]) the message
“[subject]”coming from “[sender]”
and intended for:
“[recipient1]”
“[recipient2]”
-
-
-
“[recipientn]”
was received.
Such data was not certified due to the following error:
[brief description of the error detected]
The original message is attached.
```

The anomaly envelope has no attachments thereto, besides the message that has reached the reception point (i.e. certification data), given the uncertainty of the effective origin/correctness of the message.

Even if the “`From`” field of the anomaly envelope is changed to allow the recipient to verify the signature, the routing data of the anomaly envelope (forward path and reverse path of the message) is left unchanged relative to the same data of the original message. This is to guarantee both the forwarding of the message to the original recipients and the return of any error notices on SMTP protocol (as per RFC 2821 and RFC 1891) to the sender of the original message.

6.4.3 Notice of failed delivery due to viruses

If, upon reception, the presence of viruses contained in the Transport Envelope is detected, the system generates a notice of failed delivery to be returned to the originating Provider specifying as address the one used for receipts in the Directory of Certified Mail Providers, indicating the error detected.

For this notice of failed delivery the headers contain the following fields:

```
X-Receipt: delivery-error
X-SecurityVerification: error
X-Sender: [sender of the original message]
Date: [date of issue of receipt]
```

```
Subject: SECURITY PROBLEM: [original message]
From: posta-certificata@[mail-domain]
To: [receipts of originating provider]
X-Reference-Message-ID: [Message-ID of the original message]
```

The message body of this notice of failed delivery is the actual receipt in a readable format containing the following data:

```
Notice of failed delivery due to viruses
On [date] at [time] ([zone]) in the message
“[subject]”coming from “[sender]”
and intended for the user “[recipient]”
a security problem was detected [identification of the type of content detected].
The message was not delivered.
Message identification: [identification]
```

The same certification data is entered in an XML file, to be attached to the receipt to allow an automatic processing (see 7.4). The receipt may also contain additional attachments for specific features supplied by the certified mail provider; in no case may the original message be entered.

Upon arrival of this type of receipt, coming from the recipient provider to the originating provider, the system issues a notice of failed delivery to be returned to the sender specified in the header X-Sender.

For this notice of failed delivery, the headers contain the following fields:

```
X-Receipt: delivery-error
X-SecurityVerification: error
Date: [date of issue of receipt]
Subject: NOTICE OF FAILED DELIVERY: [original subject]
From: posta-certificata@[mail_domain]
To: [original sender]
X-Reference-Message-ID: [Message-ID of original message]
```

The message body of this notice of failed delivery is the actual receipt in a readable format containing the following data:

```
Notice of failed delivery
On [date] at [time] ([zone]) in the message
“[subject]” intended for the user “[recipient]”
a security problem was detected [identification of the type of content detected]
The message was not delivered.
Message identification: [identification]
```

The same certification data is entered in an XML file, to be attached to the receipt to allow an automatic processing (see 7.4). The receipt may also contain additional attachments for specific features supplied by the certified mail provider.

6.5 Delivery point

6.5.1 Tests on incoming messages

Upon arrival of the message at the delivery point, the system verifies its type and establishes whether it should send a receipt to the sender. A successful delivery receipt is issued after the

message has been delivered to the recipient mail box and only upon reception of a valid transport envelope, identifiable by the presence of the header:

```
X-Transport: certified-mail
```

In all other cases (i.e. anomaly envelope, receipts), the successful delivery receipt is not issued. In any case, the message received by the delivery point shall be delivered unchanged to the recipient mail box.

The successful delivery receipt tells the sender that his/her message has been effectively delivered to the specified recipient and certifies date and time of the event through a text that can be read by the user and an XML attachment with certification data in a format that can be processed as well as other attachments for additional features supplied by the provider.

If the message that has reached the delivery point cannot be delivered to the intended mail box, the delivery point issues a notice of failed delivery (see 6.5.3). The notice of failed delivery is generated, upon occurrence of an error, for the delivery of a correct transport envelope.

6.5.2 Successful delivery receipt

Successful delivery receipts are an electronic mail message sent to the sender and containing date and time of successful delivery, sender and recipient data and subject.

The headers of the successful delivery receipts contain the following fields:

```
X-Receipt: successful-delivery
Date: [date of delivery]
Subject: DELIVERY: [original subject]
From: posta-certificata@[mail_domain]
To: [sender of the original message]
X-Reference-Message-ID: [Message-ID of the original message]
```

The first field identifies the message as a successful delivery receipt. The "`Subject`" field tells the recipient that the message is the receipt of his/her communication. It is made up of the string "`DELIVERY`:" followed by the subject of the original message to which the receipt refers.

The message body of this receipt is the actual receipt in a readable format containing the following data:

```
Successful delivery receipt
On [date] at [time] ([zone]) the message
"[subject]"coming from "[sender]"
and intended for "[recipient]"
was delivered to the intended mail box.
Message identification: [identification]
```

The same certification data is entered in an XML file, to be attached to the receipt (see 7.4). The receipt may also contain additional attachments for specific features supplied by the certified mail provider. The successful delivery receipt is issued for each recipient for whom the message is intended.

In issuing the successful delivery receipts, the system distinguishes the primary recipients from those to whom the message is copied. This verification is carried out by analyzing the "`To`"

(primary recipients) and "Cc" (copy to) fields of the message related to the recipient to whom the message is delivered. Only for deliveries to primary recipients, the original message along with header, text and any attachments is put into the successful delivery receipt, besides the attachments described. The system shall adopt a protection logics in assessing the type of recipient (primary or copy to) and in the resulting decision not to put the original message into the successful delivery receipt. If the delivering system cannot determine with certainty the nature of the recipient (primary or copy to) due to ambiguities in the "To" and "Cc" fields, delivery shall be considered as addressed to a primary recipient and include the whole original message.

6.5.2.1 Short successful delivery receipt

In order to streamline the flows, the sender may request a short successful delivery receipt. The short successful delivery receipt contains the original message, replacing the attachments with the relevant cryptographic hashes to reduce the receipt size. In order to allow to check the contents sent it is crucial that the sender keeps unchanged the original attachments of the original message to which the hashes refer.

If the transport envelope contains the heading:

```
X-ReceiptType: short
```

the delivery point issues, for primary recipients, a short successful delivery receipt. The absence of such heading or of a relevant different value to the processing of the successful delivery receipt according to the methods described in 6.5.2. The value of the heading of the transport envelope derives from the original message (see 6.3.4) thus allowing the sender to set the format of the successful delivery receipts related to the primary recipients of the original message. For recipients who receive a copy, the successful delivery receipts behave as described in 6.5.2.

The originating provider has the right, if he/she deems it necessary, to delete the X-ReceiptType header in the original message in order to prevent in whole or in part the request of a Short successful delivery receipt. Such management method shall be documented in the characteristics of the service supplied by the provider.

The fact that the successful delivery receipt is short shall be clearly shown to the sender of the original message, changing the wording "Successful delivery receipt" into "Short successful delivery receipt" in the receipt body.

The short successful delivery receipt has the original message attached where the MIME structure is left unchanged, but whose attachments are replaced by as many text lines containing the hashes of the file to be replaced. The attachments are identified by the presence of the "name" parameter in the "content-type" heading or "filename" in the "content-disposition" heading of the MIME part.

In the case of original messages in S/MIME format one needs not change the integrity of the message structure by changing the MIME parts of the S/MIME construction. The verification of the S/MIME nature of the original message is done by checking the MIME type of the higher level entity (coinciding to the message itself). A S/MIME message may have the following MIME types (as per RFC 2633)

`Multipart/signed`
The MIME type represents an original message signed by the sender according to the structure described by RFC 1874. The message is made up of two MIME parts: the first constituting the message written by the sender before its signature and the second containing the signature data. The second part (generally "application/pkcs7-signature" or "application/x-pkcs7-signature") contains the data added during the phase of signature of the message and shall be left unchanged in order not to affect the total structure of the message.

`Application/pkcs77-mime or application/x-pkcs7-mime`
These MIME types are generally associated to encrypted messages even if some particular implementations may represent signed messages or other cryptographic objects. The message is made up of a single CMS object contained inside the MIME part. Given the impossibility to distinguish any attachments inside the CMS object, the MIME part is left unchanged without being replaced by the relevant hash, determining the issue of a short successful delivery receipt with the same contents as a standard successful delivery receipt.

The identification of the parts not to be replaced with the corresponding hashes shall be based on the MIME type of the message (higher level MIME entity) and on any internal MIME sub-structure. The MIME types of the lower level parts as well as the file names of the parts themselves shall not be used as discriminating elements to avoid any ambiguities with user attachments having the same types and extensions. If the original message contains attachments whose Content-Type is "`message/rfc822`", i.e. it contains a mail message as attachment, the whole attached message is replaced with the relevant hash.

- In general, in the case of original messages in an S/MIME format, the copy of the message contained inside the short successful delivery receipt shall have the following characteristics:

- If the original message is signed, the S/MIME structure and the relevant signature data will be left unchanged. The message will generate an error at any phase of verification of the integrity of the signature, after the replacement of the attachments with relevant hashes.

The algorithm used to calculate the has is the Secure Hash Algorithm 1 (SHA1) as described by RFC 3174 calculated on the whole content of the attachment. In order to distinguish the files containing the hashes from the files to which they refer, the "`.hash`" suffix is added to the term of the original file name. the hash is written inside the file with 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.

6.5.3 Notice of failed delivery

If an error occurs in the phase of message delivery, the system generates a notice of failed delivery to be returned to the sender with an indication of the error detected.

For a notice of failed delivery, the headers contain the following fields:

```
X-Receipt: delivery-error
Date: [date of issue of receipt]
Subject: NOTICE OF FAILED DELIVERY: [original subject]
From: posta-certificata@[mail_domain]
To: [sender of the original message]
X-Reference-Message-ID: [Message-ID of the original message]
```

The message body of a notice of failed delivery is the actual receipt in a readable format containing the following data:

```
Notice of failed delivery
On [date] at [time] ([zone]) in the message
“[subject]” coming from “[sender]”
is intended for the user “[recipient]”
an error was detected [brief error].
The message was rejected by the system.
Message identification: [identification]
```

The same certification data is entered in an XML file, to be attached to the notice to allow an automatic processing (see 7.4). The notice may also contain additional attachments for specific features supplied by the certified mail provider.

Errors detected in the SMTP dialogue phase are managed by standard mechanisms provided for by RFC 2821 and RFC 1891. This system is adopted also for the management of transient errors during SMTP transmission for which the time limit for message storage is run out. In order to guarantee that the sender reports the error in a short time, the systems managing the certified mail traffic shall adopt 8 hours as time limit for message storage.

7 Formats

7.1 Time Reference

For all the operations performed by access/reception/delivery points during the processing of messages, receipts, logs, etc., an accurate time reference is needed. All the events (generation of receipts, transport envelopes, logs, etc.) making up the message processing at the access, reception and delivery points must be based on a single time value detected within the processing itself. In this way, the indication of the message processing instant is univocal in the logs, receipts, messages, etc., generated by the server. The time reference can be generated using any system permanently guaranteeing a deviation not greater than 1 (one) second from the Coordinated Universal Time (UTC)[1].

7.2 User Date/Time Format

The time information is supplied by the service in a format which is readable by the user (text of receipts, transport envelopes, etc.) with reference to the standard time in the moment indicated for the operation being performed. The date format used is “`dd/mm/yyyy`”, whereas the time format is “`hh:mm:ss`”, where *hh* is in the 24-hour format. The time data is followed by the “zone” in brackets, i.e. the difference (in hours and minutes) between the local standard time and the UTC. This value is provided in format “`[+/-] hhmm`”, where the first character indicates a positive or a negative difference.

[1] The specification indicated must be considered as a recommendation and is aimed at improving the coordination between CEM systems interacting among themselves. The similar reference contained in the legislative standard indicates the maximum allowed error for a CEM time reference.

7.3 Attachment Specifications

The characteristic data of the various components of the messages and receipts generated by the certified mail system are reported below. If one of the message parts contains characters with values outside the 0÷127 range (7-bit ASCII), that part shall be properly coded so as to guarantee that the final message is compatible with the 7-bit transport (e.g., quoted-printable, base64).

7.3.1 Body of the Message

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

MIME type `multipart/alternative` can be used to add an HTML format version of the body of the messages generated by the system. In this case, two MIME sub-parts shall be included: one of `text/plain` type and one of `text/html` type. The part in HTML format is to meet the following requirements:

- It must contain the same information reported in the text part;
- It must contain no references to elements (e.g., images, sounds, fonts, style sheets) either inside the message (additional MIME parts) or outside the message (e.g., hosted on the provider server);
- It must have no active contents (e.g., Javascript, VBscript, Plug-in, ActiveX).

7.3.2 Original Message

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

7.3.3 Certification Data

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

7.4 Certification Data Chart

The DTD relating to the XML file that will contain the certification data to be attached to receipts is shown below.

```
<?xml version=”1.0” encoding=”UTF-8”?>

<!—-Use element “postacert” as root-->
<!—-“type” indicates the type of certified mail message-->
<!--Attribute “error” may have the following values-->
<!—-“none” = no errors-->
<!—-“no-addressee” (with type=”delivery-error”) = wrong addressee-->
<!—-“no-domain” (with type=”delivery-error”) = wrong domain-->
<!—-“virus” (with type=”delivery-error”) = computer virus-->
<!—-“virus” (with type=”non-acceptance”) = computer virus-->
<!—-“other” = generic error-->
<!ELEMENT postacert (header, data)>
<!ATTLIST postacert
      Type (acceptance |
```

```
            non-acceptance |
            takeover |
            successful-delivery |
            certified-mail |
            delivery-error |
            delivery-error-notice) #REQUIRED
      error (none |
            no-addressee |
            no-domain |
            virus |
            other) “none”>

<!—-Original message header-->
<!ELEMENT header  (sender,
                  addressees+,
                  replies,
                  subject?)>

<!—-Sender (“From” field) of the original message-->
<!ELEMENT sender (#PCDATA)>

<!--Complete list of addressees (“To” and “Cc” fields)-->
<!--of original message-->
<!—-“type” indicates the type of addressee-->
<!ELEMENT addressees (#PCDATA)>
<!ATTLIST addressees
      Type (external | certificate) “certified”>

<!--Value of field “Reply to” of the original message-->
<!ELEMENT replies (#PCDATA)>

<!--Value of field “Subject” of the original message-->
<!ELEMENT subject (#PCDATA)>

<!--Certified mail message data-->
<!ELEMENT data    (provider-issuer,
                  data,
                  identifier,
                  msgid?,
                  receipt?,
                  delivery?,
                  reception*,
                  extended-error?)>

<!--String describing the provider that certifies data-->
<!ELEMENT provider-issuer (#PCDATA)>

<!--Message processing date/time-->
<!—-“zone” is the difference between the local standard time and UTC in-->
<!--format “[+/-]hhmm”-->
<!ELEMENT date (day, time)>
<!ATTLIST date
      zone CDATA #REQUIRED>

<!--Day in format “dd/mm/yyyy”-->
<!ELEMENT day (#PCDATA)>

<!--Standard time in format “hh:mm:ss”-->
<!ELEMENT time (#PCDATA)>

<!--Message univocal identifier-->
<!ELEMENT identifier (#PCDATA)>
```

```
<!--Original message ID before modification-->
<!ELEMENT msgid (#PCDATA)>

<!--For transport envelopes and delivery receipts-->
<!--Indicates the type of receipt required from sender-->
<!ELEMENT receipt EMPTY>
<!ATTLIST receipt
      type  (normal |
            short) #REQUIRED

<!--For delivery receipts and notices of failed delivery-->
<!--Addressee to whom delivery has been performed/attempted-->
<!ELEMENT delivery (#PCDATA)>

<!--For notices of failed delivery due to computer virus-->
<!—-Addressee of failed delivery-->
<!ELEMENT delivery (#PCDATA)>

<!--For takeover receipts-->
<!--Addressees who the receipt is for-->
<!ELEMENT reception (#PCDATA)>

<!--In case of error-->
<!--Brief error description-->
<!ELEMENT extended-error (#PCDATA)>
```

7.5 Directory of Certified Mail Providers

The directory of certified mail providers is created through a centralized LDAP server containing the data on certified mail providers and domains. The directory base root is "o=postacert" and the DistinguishedNames of the single records are of type "providerName=<name>,o=postacert". The search within the directory is mainly case insensitive using attributes "providerCertificateHash" (upon verification of envelope signature) or "managedDomains" (upon message acceptance). The record of a single provider may contain several "providerCertificate" attributes and the related "providerCertificateHash" attributes in order to enable to manage the renewals of expiring certificates. Sufficiently in advance of the certificate expiry, the provider is to update its own record adding a new certificate whose validity can overlap with the previous certificate. Any previous expired certificates must not be removed from the directory so as to allow to later verify the signature of messages. Attribution "LDIFLocationURL" must point to an HTTPS object, whose certificate will be released by CNIPA and made available by the provider, containing a file in LDIF format according to RFC 2849. In order to guarantee the file authenticity, it shall be signed by the provider using a certificate released by CNIPA for the certified mail service operations. The LDIF file, the signature and the X.509v3 certificate released by CNIPA must be entered in a PKCS#7 structure in binary format ASN.1 DER as file with extension ".p7m". Every day, the centralized LDAP system downloads this file and, after the necessary signature verifications, applies it to the provider record. The LDIF file containing the data on all the certified mail providers will be available - signed using the method described for the single providers - as HTTPS object at the URL pointed to by attribute "LDIFLocationURL" of record "dn: o=postacert". Through this LDIF file, the single providers shall locally replicate the directory contents, on a daily basis, in order to improve the system response times, avoiding to make requests to the central system for each message processing phase.

It is possible for the provider to define several distinct records in order to indicate different secondary operating environments administered. Each record makes reference to the single

secondary operating environment for which it is possible to state specific attributes, possibly distinguished from those relating to the other environments and the main environment. All records must report in attribute "providerName" the name of the provider, whereas attribute "providerUnit" is used to identify the secondary operating environments. The DistinguishedNames of the records relating to the secondary operating environments are of type "providerUnit=<environment>, providerName=<name>, o=postacert". Each provider must have a record associated to its own main operating environment, which can be distinguished by the absence of attribute "providerUnit" in the record and the DistinguishedName. The secondary environment records must not contain attribute "LDIFLocationURL" which is obtained, for all the provider records, from the main environment attributes. If secondary environments are featured, the LDIF file indicated in the main environment record must include the contents of all the provider records.

The attributes defined for the directory of certified mail providers are reported below:

Attribute Name	**Syntax**	**Description**
providerCertificateHash	IA5 string	Hexadecimal hash representation (40 characters) in SHA1 format of the certificate used by the provider for the signature of receipts and envelopes.
providerCertificate	Certificate Binary transfer	Certificate(s) used by the provider for the signature of receipts and transport envelopes.
providerName	Directory string Single Value	Name of the certified mail provider.
mailReceipt	IA5 string Single value	Email address to send the takeover receipts to.
managedDomains	IA5 string	Certified mail domains administered by the provider.
LDIFLocationURL	Directory string Single value	HTTP URL containing the provider record definition in LDIF format (of the entire directory for record "dn: o=postacert")
providerUnit	Directory string Single value	Name of the secondary operating environment (not featured for the main environment)

Here follows the LDAP diagram for the directory of certified mail providers according to the syntax described in RFC 2252:

The following LDIF file is an example of directory of certified mail providers containing a base root and two dummy providers. The certificates entered are two self-signed certificates reported by way of example:

8 Security Features

The indications referring to the certified electronic mail system security features are reported below.

8.1 Signature

The private key and signature operations must be managed using a dedicated hardware device able to guarantee their security in compliance with criteria acknowledged at European and international level.

8.2 Log

Logs must be saved at least every day in order to allow the handling of historical data; every saving operation must require the use of a time stamping, in order to guarantee the availability in time and inalterability of logs. The log data must be subject to a preservation procedure, for a 30-month period, according to the prescriptions of the CNIPA's Resolution 11/2004, of 19th February, 2004 (published in the Official Journal no. 57 of 9th March, 2004).

8.3 Authentication

User access to the CEM services, through an access point, must necessarily contemplate the system authentication by the user. For instance, authentication can require, but is not limited to, the use of a user-id and password or, if available and deemed necessary for the level of the service provided, the electronic identity card or the national service card. The authentication method choice is up to the provider. Authentication is necessary in order to guarantee that the message is sent by a certified mail service user whose identification data is consistent with the sender specified, so as to avoid the sender forgery.

8.4 Safe Dialogue

In order to guarantee the inalterability of the original message sent by the sender, outgoing messages from the access point are put in an envelope and signed, and then verified as they are being received by the reception point. The original message (complete with header, text and possible attachments) is put as attachment inside a transport envelope. The transport envelope signed by the sending provider allows to verify that the original message has not been modified during its transfer from the sending domain to the receiving domain.
The security of the dialogue between the sender and the addressee is ensured by a protection mechanism for all the connections within the certified mail architecture (between user and access point, between providers, between delivery point and user) implemented by using safe channels.

The integrity and confidentiality of the connections between the certified mail provider and the user must be guaranteed by using safe protocols. The protocols acceptable for access include, but are not limited to, the TLS-based ones (e.g., IMAPS, POP3S, HTTPS), those requiring the activation of a safe dialogue during communication (e.g., SMTP STARTTLS, POP3 STLS), and those providing a safe transport channel onto which unsafe protocols can be conveyed (e.g., IPSec.).

The dialogue between providers must be based on the SMTP protocol on TLS transport as described in RFC 3207. The reception point must include and announce the STARTTLS extension support, and accept connections both in clear text (by ordinary mail) and on a protected channel. The sending server must implement communication on a TLS channel and activate it whenever the addressed server announces its protocol support; the certificates used to enable the communication on the TLS channel shall be issued to the Providers by the CNIPA.

In order to guarantee complete traceability in the flow of certified mail messages, messages must not transit on systems outside the certified mail circuit. In the exchange of messages between different providers, all transactions must be made among machines belonging to the certified mail circuit or directly by the provider. Any secondary certified mail domain message reception systems must be directly controlled by the provider. Each certified mail domain shall be associated to the relevant reception point by means of a record of "MX" type defined in the name resolution system according to the RFC 1912 recommendations.

8.5 Viruses

Another important security feature concerning the entire certified electronic mail system is the technical/functional architecture which must prevent any virus from compromising the security of all the possible messages managed; therefore, appropriate antivirus systems must installed and constantly updated in order to avoid any infections, as much as possible, without affecting the certified mail contents as already defined.

8.6 Directory of Certified Electronic Mail Providers

The contents of the directory of certified electronic mail providers can be interrogated via HTTP on SSL protocol exclusively by the accredited Providers having the necessary user certificates, released by CNIPA; this access mode guarantees the authenticity, integrity and confidentiality of data.

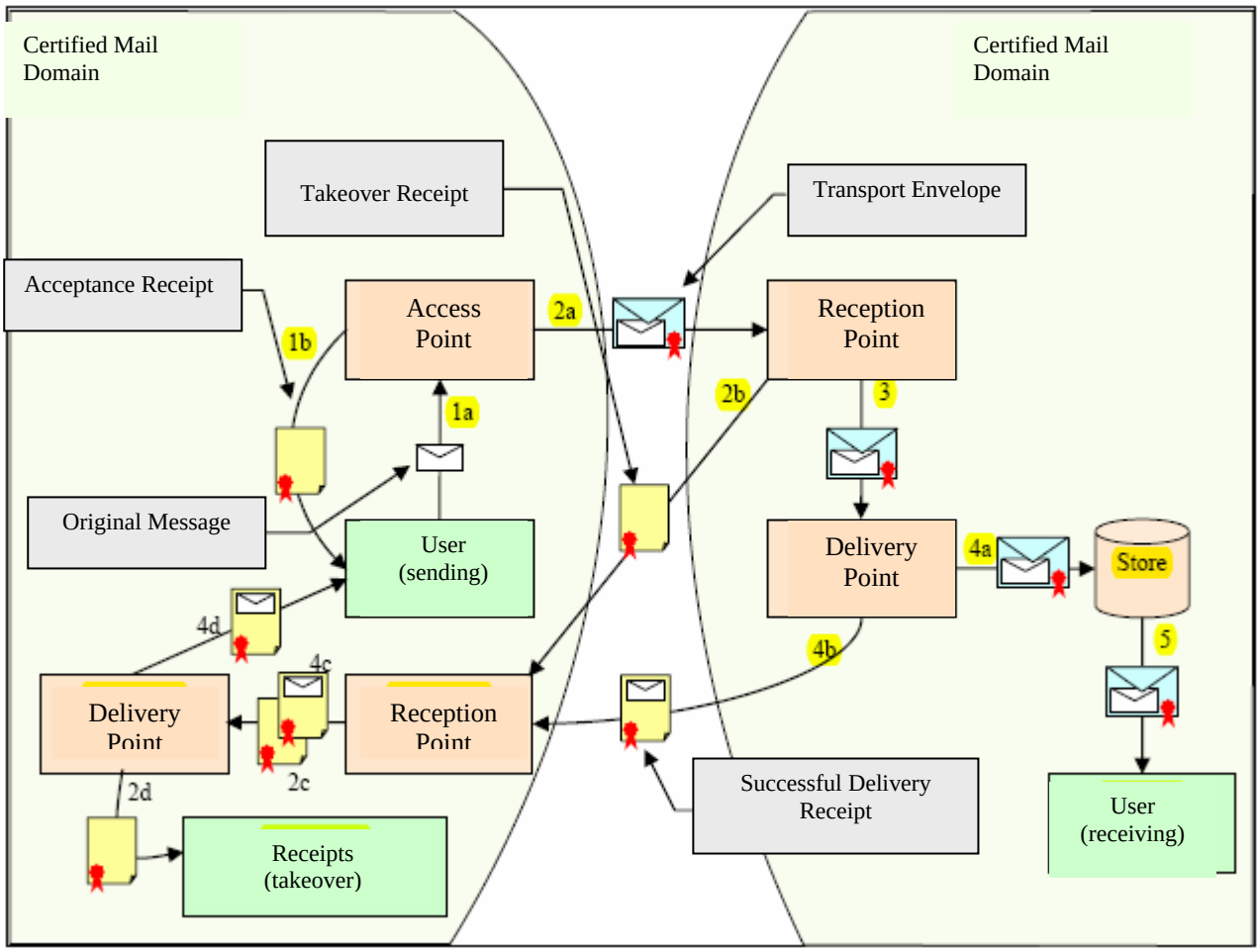
9 APPENDIX A

9.1 Operating Logic Diagram

A diagram showing the characteristic elements of a certified mail domain and its interactions with another mail domain, whether certified or not, is shown below. The information provided by the following diagrams is an integral part of this technical appendix.

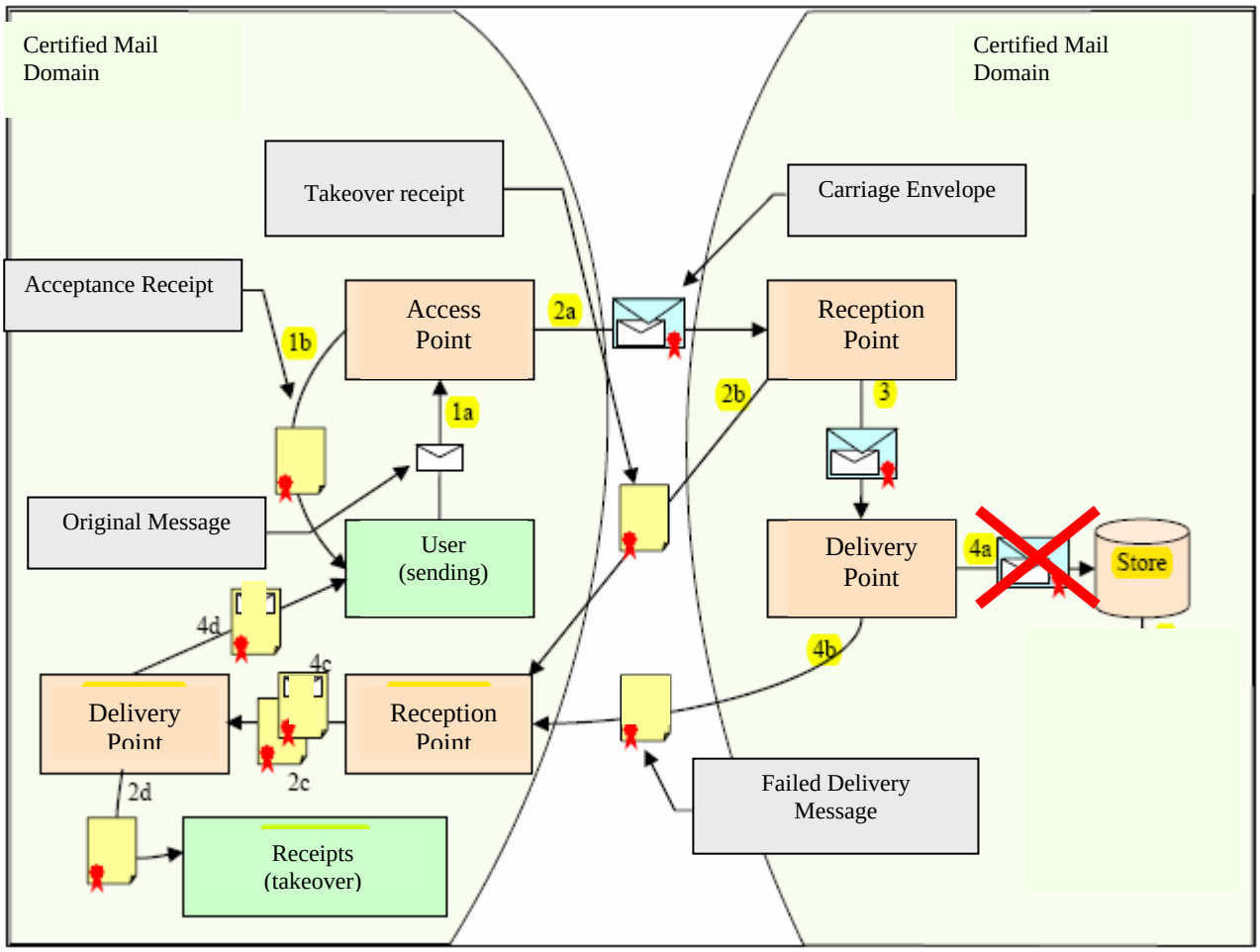
9.1.1 Interaction Between Two Certified Mail Domains

9.1.1.1 Correct and Valid Transport Envelope with Successful Delivery



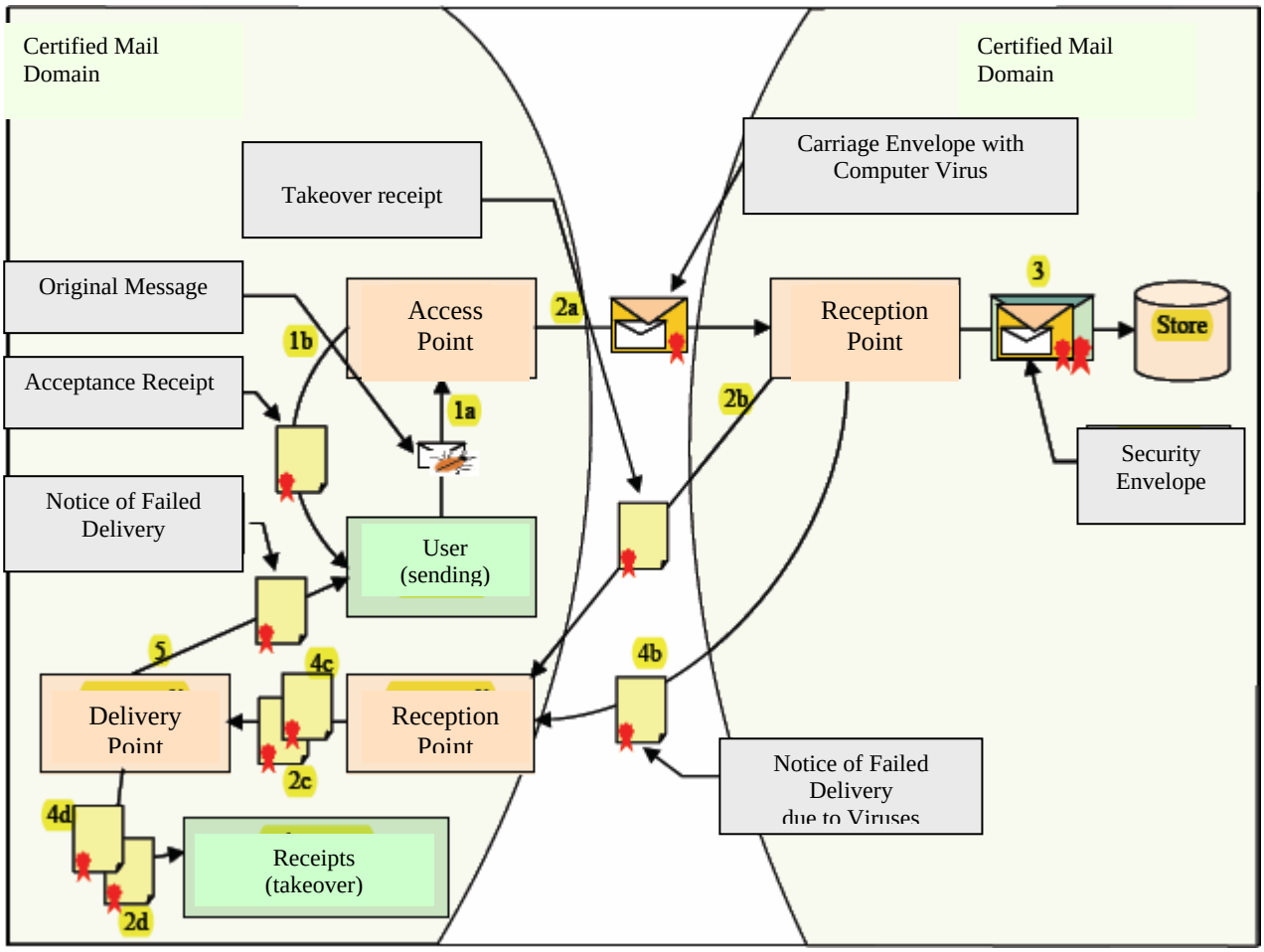
- 1a – The user sends an email to the Access Point (AP);
- 1b – The AP returns an Acceptance Receipt (AR) to the sender;
- 2a – The AP creates a Transport Envelope (TE) and forwards it to the Reception Point (RP) of the addressed Provider;
- 2b – The RP checks the TE and creates a Takeover Receipt (TR) which is forwarded to the RP of the sending Provider;
- 2c – The RP checks the validity of the TR and forwards it to the Delivery Point (DP);
- 2d – The DP saves the TR in the store of Provider receipts;
- 3 – The RP forwards the TE to the DP;
- 4a – The DP checks the contents of the TE and saves it in the store (mailbox of addressee);
    - 5 – The addressed user has the email sent at his/her own disposal;
- 4b – The DP creates a Successful Delivery Receipt (SDR) and forwards it to the RP of the sending Provider;
- 4c – The RP checks the validity of the SDR and forwards it to the DP;
- 4d – The DP saves the SDR in the sender's mailbox.

9.1.1.2 Correct and Valid Transport Envelope with Delivery Featuring a Delivery Error



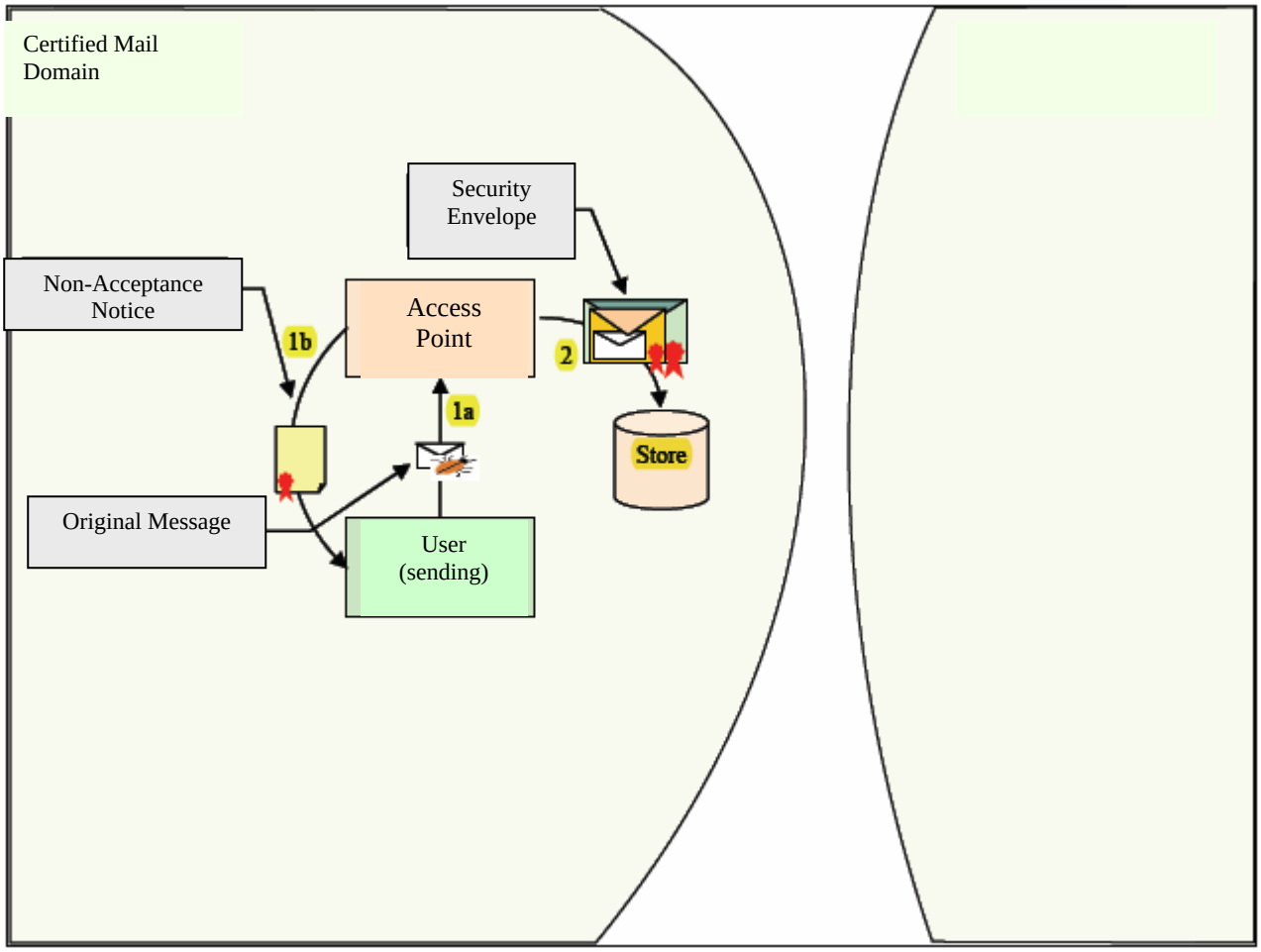
- 1a – The user sends an email to the Access Point (AP);
- 1b – The AP returns an Acceptance Receipt (AR) to the sender;
- 2a – The AP creates a Transport Envelope (TE) and forwards it to the Reception Point (RP) of the addressed Provider;
- 2b – The RP checks the TE and creates a Takeover Receipt (TR) which is forwarded to the RP of the sending Provider;
- 2c – The RP checks the validity of the TR and forwards it to the Delivery Point (DP);
- 2d – The DP saves the TR in the store of Provider receipts;
- 3 – The RP forwards the TE to the DP;
- 4a – The DP checks the contents of the CE and does not manage to save it in the store (e.g., addressee's mailbox full);
- 4b – The DP creates a Notice of Failed Delivery (NFD) and forwards it to the RP of the sending Provider;
- 4c – The RP checks the validity of the NFD and forwards it to the DP;
- 4d – The DP saves the NFD in the sender's mailbox.

9.1.1.3 Correct Transport Envelope Containing a Computer Virus Not Detected by the Sending Provider and Delivery Featuring a Delivery Error



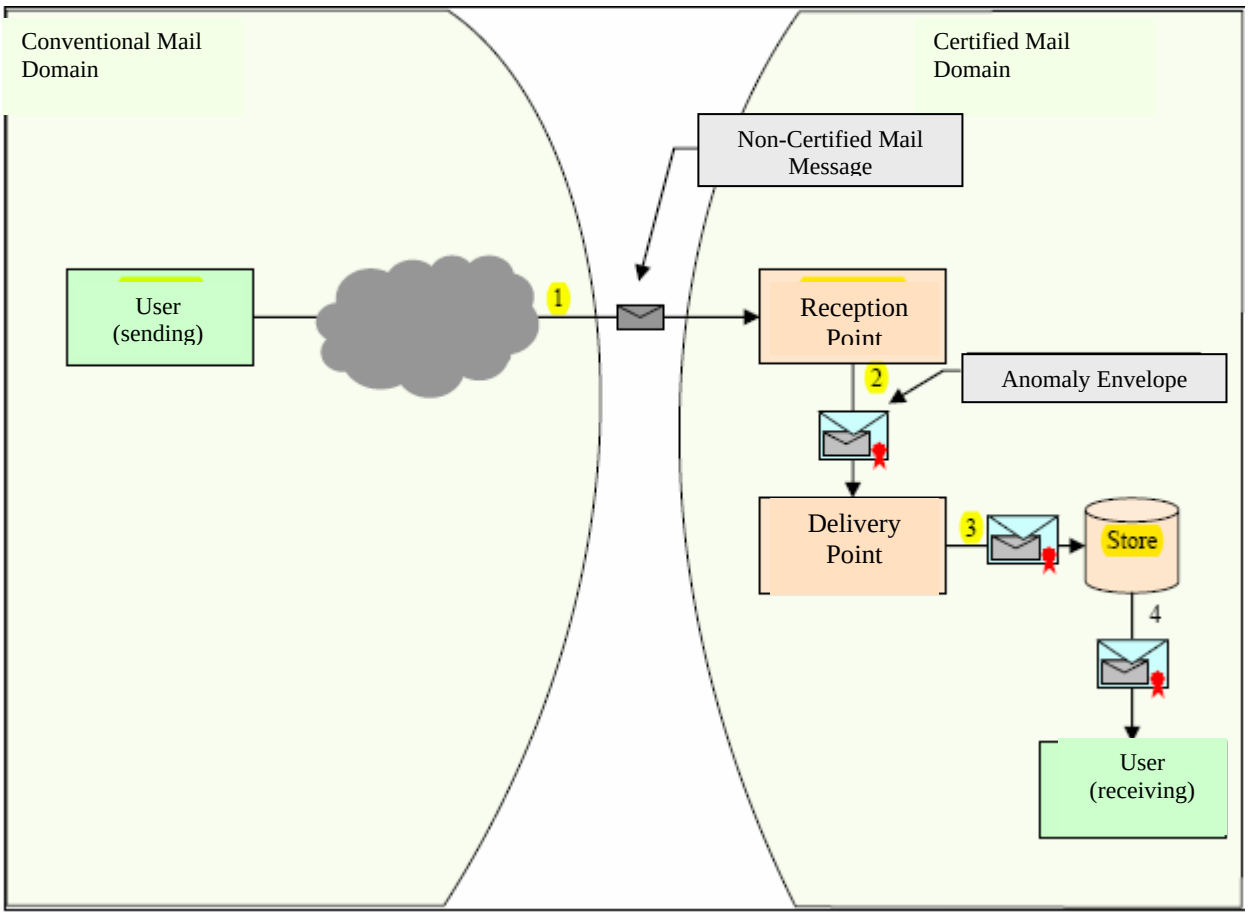
- 1a – The user sends an email to the Access Point (AP);
- 1b – The AP returns an Acceptance Receipt (AR) to the sender;
- 2a – The AP creates a Transport Envelope (TE) and forwards it to the Reception Point (RP) of the addressed Provider;
- 2b – The RP checks the TE and creates a Takeover Receipt (TR) which is forwarded to the RP of the sending Provider;
- 2c – The RP checks the validity of the TR and forwards it to the Delivery Point (DP);
- 2d – The DP saves the TR in the store of Provider receipts;
- 3 – The RP checks the contents of the TE, detects a potentially dangerous contents, then puts the CE in a Security Envelope (SE), keeping it without delivering it to the addressee;
- 4b – The DP creates a Notice of Failed Delivery due to Viruses (NFDV) and forwards it to the RP of the sending Provider;
- 4c – The RP checks the validity of the NFDV and forwards it to the DP;
- 4d – The DP saves the NFDV in the Provider receipt store;
- 5 – The DP creates a Notice of Failed Delivery (NFD) and forwards it to the sender's mailbox.

9.1.1.4 Original Message with Computer Virus Detected by the Sending Provider and Non-Acceptance Notice



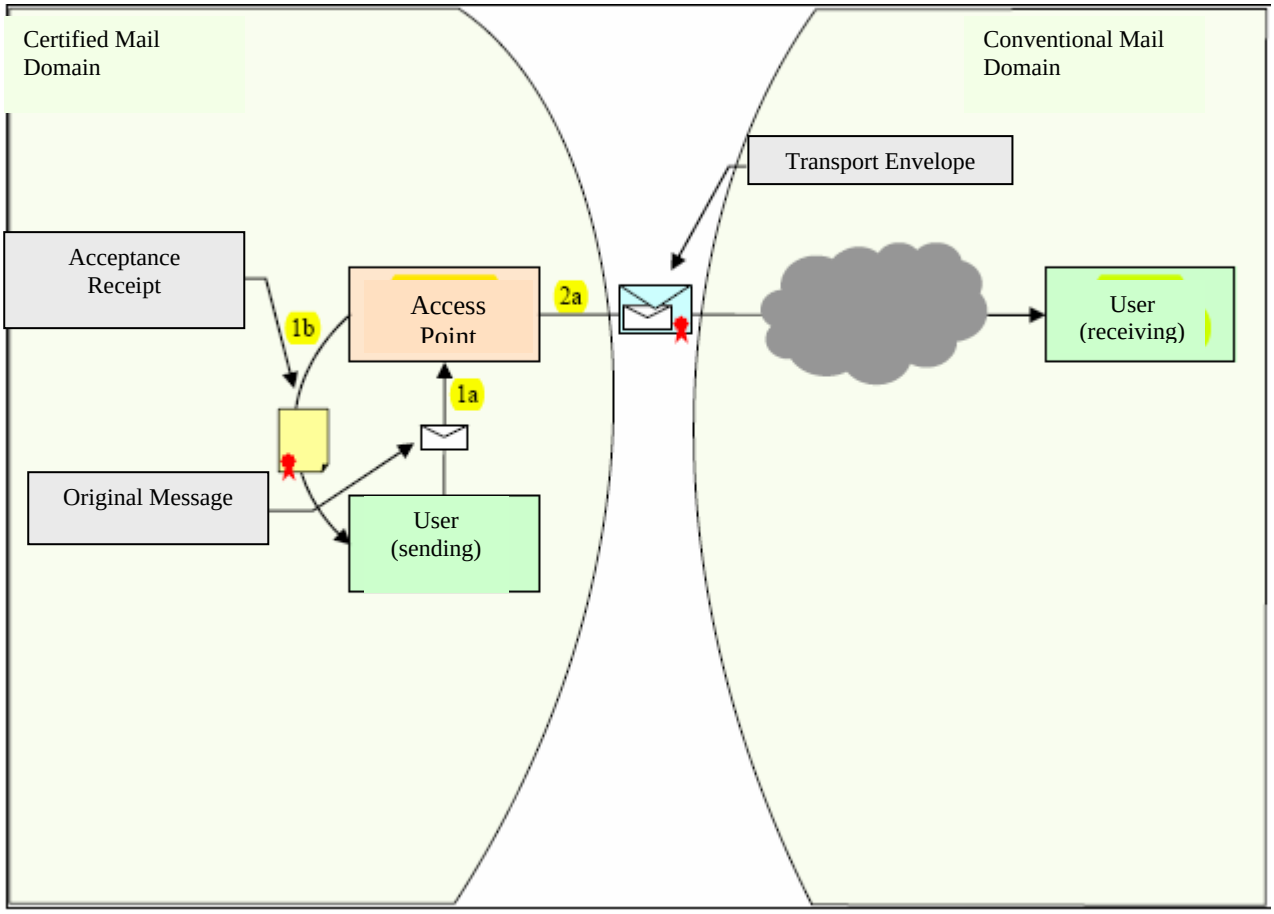
- 1a – The user sends an email to the Access Point (AP);
- 1 b – The AP detects a potentially dangerous content and returns a Non-Acceptance Notice (NAN) to the sender;
- 2 – The AP puts the Original Message in a Security Envelope (SE), keeping it without delivering it to the addressee.

9.1.2 Interaction Between a Conventional Mail Domain (Sender) and a Certified Mail Domain (Receiver)



Note: The addressed provider can decide whether to enter an ordinary mail message into the certified mail processing circuit.

9.1.3 Interaction Between a Certified Mail Domain (Sender) and a Conventional Mail Domain (Receiver)



9.2 Technical/Functional Requirements for a CEM System Client

The requirements to be met by a client in order to provide the user of a generic certified mail system with the minimum set of operating functionalities are listed below:

- Management of the dialogue with access and delivery points using safe channels;
- Management of user authentication upon sending and reception of messages;
- MIME format support according to RFC 2045 – RFC 2049;
- Management of media type "`message/rfc822`";
- Support of character set "`ISO-8859-1 (Latin-1)`".

In addition to the foregoing, in order to guarantee the maximum availability of all the certified mail system functions, the client must include the following functionalities, whether directly or through external programs:

- Check of envelope and receipt signatures -
  support of S/MIME standard version 3 as per RFC 2633;
- Complete access to certification data -
  support for the display and management of attachments in XML format;
- Request for short delivery receipts -
  possibility to enter personalized headers in the message header.

10 APPENDIX B

10.1 Digital Certificate Profile for the Electronic Signature of Certified Electronic Mail Messages

10.2 References

The following documents contain reference definitions and indications mentioned in the text and forming an integral part of the proposal.
References are either specific (identified by the date of publication and/or version number or by the version number) or non specific. For specific references, the subsequent revisions are not applicable, whereas they are applicable for non-specific references.

10.3 Introduction

The key words *"MUST"*, *"MUST NOT"*, *"IS REQUIRED"*, *"SHOULD"*, *"SHOULD NOT"*, *"RECOMMENDED"*, *"NOT RECOMMENDED"*, *"MAY" and "OPTIONAL"* used in the document text must be interpreted as described below, in compliance with the corresponding translations contained in document IETF RFC 2119 [1].

The key words *"MUST"* or *"IS REQUIRED"* refer to an absolute definition requirement.
The key words *"MUST NOT"* refer to an absolute prohibition for the definition.

The key words *"SHOULD"* or *"RECOMMENDED"* mean that, in particular circumstances, there may be valid reasons to ignore the specification referred to, but it is necessary to understand and carefully weigh all the implications thereof before choosing another solution.

The key words *"SHOULD NOT"* or *"NOT RECOMMENDED"* mean that, in particular circumstances, there may be valid reasons to consider the specification referred to as acceptable or even useful, but it is necessary to understand and carefully weigh all implications before implementing a corresponding solution.

The key words *"MAY"* or *"OPTIONAL"* mean that the specification referred to is merely optional. A party may choose to include the object in question when required by a particular market or when he/she believes that the final product is thus improved, whereas another party may omit this object altogether. An implementation not including a particular option *MUST* be able to interact with another implementation including it, although with less functionalities. Likewise, an implementation including a particular option *MUST* be able to interact with another implementation not including it (except for the particular functionality enabled by the option).

As defined in IETF RFC 3280 [3], it should be reminded that for each extension used in a certificate it is necessary to define whether the extension is marked as critical or non critical. A system using the certificate *MUST* reject it if it encounters an extension which is marked as critical and which it does not recognize and interpret correctly; on the other hand, it *MAY* ignore an extension which is not marked as critical if it does not understand it.

10.4 S/MIME Certificate

This document defines the S/MIME certificate profile, for use in the certification of Certified Electronic Mail messages performed by the service providers [6][7].
The S/MIME certificate profile proposed is based on standards IETF RFC 3850 [4] and RFC 3280 [3] which, in turn, are based on standard ISO/IEC 9594-8:2001.

10.5 S/MIME Certificate

10.5.1 Provider Information (Subject)

The information on the CEM provider holding the certificate *MUST* be entered in the Subject field (Subject DN).

In particular, the Subject DN field *MUST* contain the name of the CEM service provider as highlighted in attribute providerName published in the directory of CEM providers (§7.5). The providerName of the provider *MUST* be included in the CommonName or in the OrganizationName.

Certificates *MUST* contain an Internet mail address as described in RFC 2822 [2]. The email address *MUST* be highlighted in extension subjectAltName and *SHOULD NOT* be contained in the Subject Distinguished Name [4(§3)].

Valid subjectDNs are:

C=IT, O=AcmePEC S.p.A., CN=Certified Mail and
C=IT, O=ServiziPEC S.p.A., CN=Certified Mail

The highlighting of other attributes in Subject DN, if any, *MUST* be in compliance with RFC 3280 [3].

10.5.2 Certificate Extensions

The extensions that *MUST* be featured in the S/MIME certificate are:

Key Usage, Authority Key Identifier, Subject Key Identifier, Subject Alternative Name.

Extension Basic Constraints (Object ID: 2.5.29.19) *SHOULD NOT* be featured [4(§4.4.1)].

The highlighting of the extensions listed above for the profile described is reported below.

Extension Key Usage (Object ID: 2.5.29.15) *MUST* have the digitalSignature bit activated (bit 0) and *MUST* be marked as critical [4(§4.4.2)]. The extension *MUST NOT* contain the nonRepudiation bit activated (bit 1) [3(§4.2.1.3)]. The extension *MAY* contain other activated bits corresponding to other Key Usages, provided that this is in line with the indications of RFC 3280 [3].

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

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

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

The addition of other extensions not described in this document is to be considered as *OPTIONAL* provided that it is carried out in compliance with RFC 3280 [3]; such additional extensions *MUST NOT* be marked as critical [4(§4.4)].

10.5.3 Example

An example of S/MIME certificate meeting the minimum requirements described in this profile is reported below. Values concerning imaginary providers are used, by way of example only.

a. General use certificate in the version noted down.

An asterisk near the tag of an extension means that this extension has been marked as CRITICAL.

b. General use certificate in dump asn.1.