CLAIMS

1. Method of certification of digitally signed electronic mail which is carried out by means of a telecommunications operator, the method comprising:

i. generation by a transmitter (1 ,2,3), which is a user of the telecommunications operator, of at least one electronic mail,

ii. making the electronic mail arrive at a client mail server of the telecommunications operator (4,15),

iii. sending the electronic mail to:

- a mail destination server (7, 24) through the internet (5) to make it arrive at a certified mail destination (8,25), and

- an incoming mail server of the telecommunications operator (9), and sending the electronic mail from the incoming mail server of the telecommunications operator (9) to a certification data processing server which forms a part of the telecommunications operator,

iv. certifying (17), by the certification data processing server, the electronic mail wherein said certification in turn comprises generating a copy (18) of the electronic mail and decomposing the electronic mail into its parts wherein said parts comprise: transmission details, reception details and content of the mail,

the method of certification of the digitally signed electronic mail further comprises:

v. encapsulating (20), by the certification data processing server, the copy (18) of the electronic mail in a container,

vi. generating a certified mail (21), by the certification data processing server, which comprises the encapsulated copy (18) of the electronic mail and making it arrive at a telecommunications operator's outgoing mail server (23,26) from the certification data processing server,

vii. making the certified mail (21) arrive at the mail destination server (7, 24) from the telecommunications operator's outgoing mail server (23,26,38,50),

viii. making the certified mail (21) arrive from the mail destination server (7, 24) to:

- the certified mail destination (8,25), and

- the telecommunications operator's outgoing mail server (23,26,38,50),

ix. the telecommunications operator’s outgoing mail server (23,26,38,50) delivering the encapsulated copy (18) of the electronic mail, for its delivery, waiting for a subsequent time of between 10 minutes and one hour for a subsequent rejection response to avoid the mail destination server accepting everything in the first instance and subsequently rejecting,

x. carrying out a delivery check (27) of the certified mail (21) at the certified mail destination (8,25),

xi. if the certified mail was able to be delivered, generating a certificate (37,49) by means of a certification server (30,41) of the telecommunications operator wherein said certificate comprises:

a. a first part (31 ,42) which in turn comprises: transmission details, reception details and content of the mail, and

b. a second part (34,45) which in turn comprises details of the arrival of the certificate (21) at the telecommunications operator's outgoing mail server (23,26),

wherein a verification (44) subsequent to the generation of the first part (31,42) is carried out said verification (44) comprising checking whether the mail destination server of the certified electronic mail (8,25) is on a list of bouncing/blacklisting servers which by default accept all messages and subsequently reject them when the addressee of the corresponding certified mail (8,25) does not exist; in such a way that the method further comprises:

- adding to the certificate (37,49) details referring to the non-existence of the addressee at the certified mail destination server (8,25), when the verification (44) gives as a result that the certified mail destination server (8,25) is on the list of bouncing/blacklisting servers, or
- composing the second part (34,45) of the certificate (37,49) with all of the transactional details, adding a timestamp (35,48) of a third party and signing the certificate (37,49) with the electronic signature of the telecommunications operator, when the mail destination server (7, 24) is not on the blacklist or bouncing list,

and

xii. making the certificate (37,49) arrive at the transmitter (1,2,3).

2. Method according to claim 1 further comprising checking (10) that the transmitter (1,2,3) has certification privileges by means of comparison with a list of users/privileges, check that is carried out by means of sending the electronic mail to a certification data processing server.

3. Method according to claim 1 further comprising carrying out a dumping of the copy (18) of the electronic mail and its parts, once the copy (18) has been decomposed, in a first database (19,32,43).

4. Method according to claim 1 further comprising carrying out a dumping of the certified mail (21) in a second database (22,33,46) which comprises elements that have been made to arrive at the telecommunications operator's outgoing mail server (23,26,38,50).

5. Method according to any of the preceding claims wherein the delivery check (27) of step x gives as a result a non-delivery of the certified mail (21) at the certified mail destination (8,25), the method further comprising adding to the certificate (37,49) details referring to the non-delivery wherein said details comprise: time of attempted delivery and delivery address.