BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS	**BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE**	**CHAMBRES DE RECOURS DE L'OFFICE EUROPÉEN DES BREVETS**

Internal distribution code:

(A) [-] Publication in OJ
(B) [-] To Chairmen and Members
(C) [-] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 17 May 2017

Case Number:	T 2165/11 - 3.5.06
Application Number:	03254769.7
Publication Number:	1387239
IPC:	G06F1/00
Language of the proceedings:	EN

Title of invention:
Secure messaging

Applicant:
SecurEnvoy Plc

Headword:
Secure messaging/SECURENVOY

Relevant legal provisions:
EPC 1973 Art. 56

Keyword:
Inventive step - after amendment

Decisions cited:

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Catchword:

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Case Number: T 2165/11 - 3.5.06

DECISION
of Technical Board of Appeal 3.5.06
of 17 May 2017

Appellant:
(Applicant)

SecurEnvoy Plc
The Square
Basing View
Basingstoke
Hampshire RG21 4EB (GB)

Representative:

Thompson, Andrew John
Withers & Rogers LLP
4 More London Riverside
London SE1 2AU (GB)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted on 21 April 2011 refusing European patent application No. 03254769.7 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman	W. Sekretaruk
Members:	A. Teale
	M. Müller

Summary of Facts and Submissions

I. This is an appeal against the decision, dispatched with reasons on 21 April 2011, to refuse European patent application No. 03 254 769.7 on the basis that the subject-matter of the independent claims according to a main request lacked inventive step in view of the combination of the following documents and common general knowledge:

D1: EP 0 785 661 A2 and
D3: EP 1 041 777 A2.

The subject-matter of the independent claims according to an auxiliary request lacked inventive step in view of the combination of D3 and D1 and common general knowledge, as exemplified by the following document:

D2: US 6 112 078 A.

II. A notice of appeal was received on 1 July 2011 in which the appellant requested that the decision be set aside and made an auxiliary request for oral proceedings. The appeal fee was paid on the same day.

III. With a statement of grounds of appeal, received on 1 September 2011, the appellant submitted amended claims according to a main request. The appellant also reiterated the auxiliary request for oral proceedings. On 13 September 2011 an amended statement of grounds was received, in which errors in point 4.2, which discusses D3, had been corrected.

IV. On 17 April 2014 amended claims according to an auxiliary request were received from the appellant.

V. In an annex to a summons to oral proceedings the board set out its preliminary opinion on the appeal that certain terms in the claims were unclear, Article 84 EPC 1973, and that the claimed subject-matter seemed not to involve an inventive step, Article 56 EPC 1973, starting from D3 and taking into account D1, D2 and the common general knowledge of the skilled person.

VI. With a response received on 10 April 2017 the appellant submitted a "witness statement" by the inventor Mr Kemshall, withdrew the previous auxiliary request, refiled the claims according to the main request and filed amended claims according to new first to fourth auxiliary requests. The appellant also submitted amended description pages according to the main and first to fourth auxiliary requests.

VII. In a communication dated 10 May 2017, sent by the registry on behalf of the board, the board introduced, Article 114 EPC 1973, the following documents in connection with two-factor authentication:

D4: EP 0 745 961 A2 and
D5: US 6 078 908 A.

VIII. Oral proceedings were held on 17 May 2017, attended by the appellant and the inventor. The appellant withdrew the first to fourth auxiliary requests and filed a set of claims and amended description pages according to a new first auxiliary request - A. The appellant's final requests were that the decision be set aside and that a patent be granted on the basis of the main request, dated 10 April 2017, or in the following version:

Description:
pages 1 and 2, filed on 11 March 2011,

pages 3 to 6, filed as First Auxiliary Request - A on 17 May 2017, and
pages 7 to 12, filed on 11 March 2011.

Claims:
1 to 45, filed as First Auxiliary Request - A on 17 May 2017.

Drawings:
sheets 1/12 to 12/12, as originally filed.

At the end of the oral proceedings the board announced its decision.

IX. Claim 1 according to the main request reads as follows:

"A system for secure electronic communication of a secure email message from an originator's computer to a recipient's computer, said system comprising: a message splitter for splitting the secure email message into a first email message and a second message, including removing a security sensitive portion of the secure email message to be contained by the second message; message sending and code requesting means for using a first network connection to send the second message from the originator's computer to an externally accessible store and requesting a reference code from the externally accessible store, said externally accessible store being operative to grant access to stored content of said second message upon presentation of a two factor authentication comprising an authentication code and the reference code; email sending means to send the first email message along with the reference code and notification that content of said second message is in said store, from the originator's computer to the recipient's computer; code sending means, for using a second network connection, to send said authentication code, separately from the reference code, for access by the recipient; accessing means for the recipient's computer to access said externally accessible store using a third network connection; and authentication means for the recipient's computer to provide said externally accessible store, when so accessed, with said two factor authentication for said externally accessible store to grant access to said content of the second message."

X. The independent claims according to first auxiliary request - A read as follows:

"1. A system for secure electronic communication of a secure email message from an originator's computer to a recipient's computer, said system comprising: the originator's computer, an externally accessible store and the recipient's computer; wherein the originator's computer comprises a message splitter, a message sending and code requesting means and an email sending means, the externally accessible store comprises a code sending means and an authentication means, and the recipient's computer comprises an accessing means; and wherein the message splitter is for splitting the secure email message into a first email message and a second message, including removing a security sensitive portion of the secure email message to be contained by the second message; the message sending and code requesting means is for using a first network connection to send the second message from the originator's computer to the externally accessible store and requesting a reference code from the externally accessible store, said externally accessible store being operative to grant access to stored content of said second message upon presentation of a two factor authentication comprising an authentication code and the reference code; the email sending means is for sending the first email message along with the reference code and notification that content of said second message is in said store, from the originator's computer to the recipient's computer; the code sending means is for using a second network connection, to send said authentication code from the externally accessible store, separately from the reference code, for access by the recipient in response to receipt of the second message at the externally accessible store; the accessing means is for the recipient's computer to access said externally accessible store using a third network connection; and the authentication means is for the recipient's computer to provide said externally accessible store, when so accessed, with said two factor authentication for said externally accessible store to grant access to said content of the second message."

"23. A method for secure electronic communication of a secure email message from an originator's computer to a recipient's computer, using a system according to any one of the preceding claims, said method comprising the steps of: splitting, at the originator's computer, the secure email message into a first email message and a second message, including removing a security sensitive portion of the secure email message to be contained by the second message; employing the message sending and code requesting means to send the second message from the originator's computer to the externally accessible store via the first network connection, and to request a reference code from the externally accessible store, said externally accessible store being operative to grant access to stored content of said second message upon presentation of a two factor authentication comprising an authentication code and the reference code; sending the first email message, along with the reference code and notification that content of said second message is in said store, from the originator's computer to the recipient's computer; the externally accessible store connecting by use of the second network connection to send said authentication code, separately from the reference code, for access by the recipient in response to receipt of the second message at the externally accessible store; accessing said externally accessible store from the recipient's computer by use of the third network connection and employing the authentication means to provide said externally accessible store, when so accessed, with the necessary two factor authentication comprising said reference code and said authentication code; and granting access to said content of the second message."

Reasons for the Decision

1. The admissibility of the appeal

In view of the facts set out at points I to III above, the appeal complies with the admissibility criteria under the EPC and is consequently admissible.

2. Summary of the invention

2.1 The application relates to securely communicating an email message from the originator's computer to the recipient's computer, the description acknowledging a prior art approach of storing a message on an Internet-facing web server and delivering the message to the recipient via a secure communication link. This approach has the drawback that, since the web server can be accessed by anyone, means are required to authenticate the recipient, i.e. to establish that the recipient really is who he/she claims to be. While this can be achieved using a password agreed between the originator and the recipient, such bilateral agreements become unworkable as the number of users increases.

2.2 The invention permits a recipient to read a secure message using only standard email software, a web browser and a device, such as a mobile phone, for receiving an authentication code. According to the invention, the message to be sent is split into a "first email message" and a "second message". The second message contains a "security sensitive" portion of the original message and is sent via a first network connection to the store. The first email message, a reference code and a notification that the security sensitive portion is in an external store, are sent via email to the recipient. Second communication means are used to send an authentication code to the recipient, in particular by SMS to the recipient's mobile phone. The recipient then uses a third network connection between his/her computer and the store, to perform two-factor authentication by presenting the authentication code and the reference code to the store to gain access to the security sensitive portion of the original message.

3. The prior art on file

3.1 Document D3

3.1.1 The decision takes D3 as the closest prior art. This is also common ground between the board and the appellant.

3.1.2 D3 relates to an electronic messaging system, for instance using e-mail. All message recipients can read what is termed the "common message" portion of a message, but only selected recipients can access the attached private comments. The comments may be voice messages or video clips; see column 6, lines 8 to 9.

3.1.3 As illustrated in figure 1, the messaging system comprises a message processor 20, for instance an e-mail server (see column 3, lines 16 to 24), that operates to receive and send messages between a number of user stations (22a-c), for instance personal computers connected to the e-mail server by a LAN or a wide area network (WAN) such as the Internet.

3.1.4 According to the flow chart in figure 2, the originator generates a common message (step 50) and selects the recipients of that common message (step 52). The originator then generates one or more comments (step 54) and creates an address list of the recipients authorized to receive those comments (step 56). The common message, its address list, the comments, and their address list are delivered to the message processor for selective delivery to each recipient (step 58). The message processor then delivers the common message portion to all recipients (22b-n, Stations #2-#N) and, according to a first embodiment, also the comments for each individual recipient; see the flow chart in figure 3. As figure 3 shows, creating such customized messages for each recipient may require that multiple copies of the comments, which may be voice messages or video clips (see column 6, lines 8 to 9), be stored at the message processor.

3.1.5 A second embodiment, illustrated in figure 4 and explained in paragraphs [0009] and [0018] to [0020], handles the comments differently. The memory of the message processor may be scarce, making it impossible to create customized messages for each recipient prior to delivery; see paragraph [0018]. The board understands this to mean that, whilst the message processor stores a separate copy of the common message for each recipient, part of its memory storage is used to store only one copy of each comment. In this case each recipient receives the common message, accompanied by a prompt, for instance an icon, indicating that a comment is attached to the message; see column 5, lines 11 to 13. If the user selects the prompt (step 102), then the messaging system asks the recipient for a security code, for instance a password (step 104). If this is correctly entered and the recipient is on the list of recipients to receive the comment (step 106), the messaging system delivers the comment to the recipient (step 108). In the board's view, it is implicit from the use in D3 of a prompt or icon to select a comment that a reference code is used to identify the comment.

3.2 Document D5

3.2.1 D5 relates to "telebanking" (see column 1, line 11), which the board understands to mean online banking, involving a user logging on to a banking system and requesting that for each individual transaction a TAN (Transaction Authorization Number) be generated; see column 2, lines 57 to 62. The TAN is then transmitted by SMS to the user's mobile phone; see column 3, lines 1 to 9. This is two-factor authentication of the user, since the user must provide a password to log on (providing something that the user knows) and also demonstrate possession of the mobile phone (something that the user has).

3.2.2 At the oral proceedings the appellant accepted that two-factor authentication using SMS, such as that disclosed in D5, was generally known at the priority date. According to the appellant however, the skilled person would not have been inclined to use it in a "mission critical" system, since SMS were subject to unpredictable delays or were sometimes never even delivered.

3.3 Document D1

3.3.1 In the early phase of examination in this case, D1 was regarded as the closest prior art, but, in view of amendments, was later replaced by D3.

3.3.2 D1 relates to a multi-media messaging system (MMMS) adapted to allow a registered originator to send a multi-media message to both registered and unregistered recipients, in both cases lacking full multi-media reception capability. According to the abstract and column 7, lines 6 to 34, in the case of registered recipients the MMMS can establish the recipient's native medium and knows their e-mail address. The originator (see figure 1; 100) has, for instance, a LAN-connected PC and a telephone; see column 5, lines 30 to 36. The recipient (see figure 1; 126) may, for instance, be using older equipment capable of receiving only one or only some of the possible media. For example, the recipient may have a LAN-connected PC for generating and receiving e-mail messages and a telephone for generating and receiving audio messages; see column 5, lines 39 to 43. The originator, being registered, already has a mailbox 110. The MMMS creates a mailbox 111 for an unregistered recipient and assigns a mailbox password; see figure 2, steps 202-208. The

MMMS stores the original message in the recipient's mailbox 111 and creates a substitute message containing the native media components of the original message that the recipient is able to receive; see column 7, lines 9 to 12, and figure 2, step 212) together with the password and instructions on how to log into the recipient's mailbox 111 to receive the original message for a limited time; see column 7, lines 31 to 34, and column 8, lines 45 to 51. The substitute message is then sent to the recipient's PC 125; see figure 2, steps 214-218 and column 7, lines 21 to 34.

4. The main request

4.1 The appealed decision

4.1.1 According to the reasons for the decision, the subject-matter of claim 1 differed from the disclosure of D3 in that:

i. the second, security sensitive part of the message was sent to an external store, and

ii. the authentication code was sent using a different network to that used to send the email.

Difference "i" allowed electronic messages to be sent to recipients who were unable to receive messages with particular characteristics. Difference "ii" prevented message interception by sharing a common secret, namely the authentication code and password, with a non-registered user. The two differences were technically unrelated, the first solving the problem of making electronic communication possible where a gateway refused to pass emails which it could not check, for instance because they were partially encrypted. The second difference addressed the problem of sharing a secret whilst avoiding interception by malicious users. Either problem could arise independently of the other.

4.1.2 The first problem was addressed in D1 in which multi-media content which could not be received by a recipient was stored in a "sending messaging system" (see abstract), the recipient being sent instructions on how to access the entire electronic message in the sending messaging system. The skilled person would have recognised that the approach in D1 was more general than the case of non-delivery due to multi-media content and would have applied D1 to solve the first problem in an obvious manner.

4.1.3 Turning to the second problem, the sharing of secrets via a second channel was a matter of common general knowledge in computer security. Hence the skilled person would have solved the second problem without taking an inventive step.

4.1.4 Thus the claimed subject-matter lacked inventive step in view of the combination of D3, D1 and common general knowledge.

4.2 The board's interpretation of the claims

4.2.1 The independent claims of both requests set out a "security sensitive portion" of the secure email message. The board takes the view that what is "security sensitive" in the message is not something which can be decided according to objective criteria, since it is a subjective question depending, for instance, on the wishes of the originator, the recipient or even third parties. Consequently, in the present context, the board understands the message splitter and message splitting steps in the claims to cover merely splitting messages into two arbitrary parts. It is common ground between the board and the appellant that what distinguishes the two parts is how they are subsequently treated.

4.2.2 The independent claims of both requests set out an "externally accessible" store, but give no indication of the distinction between "internal" and "external" in this context. The appellant has argued that the expression "externally accessible" store has to be understood in the light of the description (see page 11, lines 17 to 22) which states that the store can be anywhere on the Internet and can be part of an internal company Intranet system and be assessed from within the Intranet or, externally, through the Internet. Even taking this passage in the description into account, the board does not construe the expression "externally accessible" as limiting the features of the store.

4.2.3 The independent claims of both requests mention first, second and third network connections. In the light of the application (see, for instance, figure 5), the skilled person would construe the three network connections as being distinct. In the case of the first and second network connections this is also explicitly stated in claim 1; the authentication code (sent via the second network connection) is said to be sent separately from the reference code (sent via the first network connection).

4.2.4 Whilst the independent claims according to the main request cover the case in which the message splitter is located in the message processor (20) of D3, the independent claims according to first auxiliary request A have been restricted to the splitter/splitting step being located in the originator's computer. Consequently, while the independent claims of the main request cover the storage of the comments in the email server/message processor 20 in D3, this is excluded in the claims according to first auxiliary request A, which set out the "security sensitive portion" being stored in an additional store to the email server.

4.2.5 The board takes the view that the "code requesting means for using a first network connection" ... for "requesting a reference code from the externally accessible store", set out in claim 1 of both requests, are very broadly defined, since the definition covers any means suitable for eventually causing the requesting of a reference code. In the case in D3 in which prompts/icons are used to indicate the presence of comments, the originator's computer must, in a broad sense, have "code requesting means" because any such comment implies that a reference code may be required in the D3 system (see below).

4.3 The difference features with respect to D3

4.3.1 The board takes the appellant's point that the subject-matter of claim 1 differs from the disclosure of D3 in more features than those set out in the decision.

4.3.2 Although the board initially took the view in the annex to the summons that D3 did not disclose splitting the secure email message in the same sense as that claimed, the board now finds, on further consideration, that the separation of the common message portion from the comments, regarded as the claimed "security sensitive portion", in the message processor 20 in D3 can be considered as the "splitting" set out in the claims.

4.3.3 It is implicit in D3 that the originator's computer comprises message sending means for using a first network connection (the LAN/WAN connection between Station #1,22a and message processor 20) to send the comments to the originator's computer to a store (in the message processor).

4.3.4 The skilled person would understand from the references in D3 to a prompt, for instance an icon, (see column 6, lines 24 to 28) indicating that a comment is attached to the common message portion that the recipient's computer must identify each comment by some form of unique "reference code" when the user selects the prompt/icon. The skilled person would understand that this "reference code" is assigned in the message processor and sent to the recipient's computer with the common message portion and prompt/icon. Hence the transmission in D3 of the common message portion together with a prompt indicating that a comment is attached to the message implies, in the board's view, email sending means to send the first email message along with the reference code and notification that content of said second message is in a store (of the message processor 20), from the originator's computer to the recipient's computer.

4.3.5 D3 also discloses the recipient entering a password before receiving the comment, which the board considers to be an "authentication code" in the sense of the claims. This also implies that a store in the message processor of D3 is operative to grant access to stored comments upon presentation of a two factor authentication comprising an authentication code and a reference code. The board notes that the fact that two-factor authentication is carried out using an authentication code and a reference code does not limit the choice of authentication code and reference code and thus does not further limit the features of the store.

4.3.6 It is implicit in D3, in particular paragraph [0009], lines 33 to 39, that the system comprises accessing means for the recipient's computer (Station #2, 22b) to access the store using a network connection (distinct from the first); see the LAN/WAN connection between Station #2, 22b and message processor 20. It also follows from the same cited passage that the system comprises authentication means for the recipient's computer to provide said store, when so accessed, with said two factor authentication for said store to grant access to the content of a comment. Again, the board points out that the fact that two-factor authentication is carried out using an authentication code and a reference code does not limit the choice of authentication code and reference code and thus does not further limit the features of the authentication means.

4.3.7 The subject-matter of claim 1 consequently differs from the disclosure of D3 in the following features:

a. code requesting means for using the first network connection to request a reference code from the externally accessible store and

b. code sending means for using a second network connection to send said authentication code, separately from the reference code, as a two factor authentication, for access by the recipient.

4.3.8 The board points out that, contrary to its provisional position expressed in the oral proceedings, it follows from the above that claim 1 is not understood as requiring that the comments be stored in a separate store to the common message portion.

4.3.9 The appellant has argued that the claimed subject-matter also differs from the disclosure of D3 in that it allows messages to be sent from an originator to an unprepared recipient without being stopped by content checking gateways in intervening public networks, for instance because the message contains encrypted content which cannot be checked for a virus by the gateway; see page 1, lines 34 to 40. As the claims are not limited to encrypted content, public networks comprising email checking gateways or unprepared recipients, these arguments do not demonstrate further differences between the claimed subject-matter and the disclosure of D3.

4.4 Inventive step, Article 56 EPC 1973

4.4.1 Regarding the objective technical problem starting from D3, the appellant argued in the oral proceedings that the objective technical problem was how to send secure messages to previously undefined recipients. The board does not accept this as the objective technical problem, since it is not always solved by the claimed subject-matter, claim 1 not being limited to previously undefined recipients. Instead, the board takes the view that the difference features address two independent, technically unrelated problems. The first objective technical problem, addressed by difference feature "a", is how to generate the reference code for identifying each comment in D3. The second objective technical problem, addressed by difference feature "b", is to improve the security of recipient authentication. The board regards both problems as obvious starting from D3 at the priority date.

4.4.2 Regarding the first problem, feature "a" specifies that the reference code is generated by the store. The skilled person would implement this feature as a usual matter of design, since the store must be able to identify the comment in order to retrieve it and must further be able to subsequently recognise the correct reference code when it is provided by the recipient's computer to access the comment. The store must provide one or more reference codes when the originator sends the common message portion, comments and their respective recipient lists to the message processor. Hence the email sending means in the originator's computer would necessarily comprise such "code requesting means" (difference feature "a").

4.4.3 Regarding the second problem, D3 states that the recipient has a password. The skilled person would have understood this to mean that the recipient uses the same password to access all comments, posing the risk of a third party gaining access to the password and reading all comments. It would have been an obvious choice for the skilled person to improve the security of recipient authentication by sending the recipient a different password as authentication code for each message.

4.4.4 At the oral proceedings the question was discussed of whether it would have been obvious at the priority date to send the authentication code separately from the reference code via a second network connection, for instance by SMS, for access by the recipient. According to the appellant, at the priority date the SMS system was known to have unpredictable delays and to sometimes fail to deliver the SMS at all. Hence it would not have been used in a "mission critical" system in which users expected a "real-time" response. Instead, tokens, which generated a PIN based on a hash function from a synchronized clock without the need for any network connection, would have been used. The appellant also argued that, whereas in D5 the user requested a TAN and had to wait for the resulting SMS, according to the invention the SMS (and the reference code) were "pushed" to the recipient. Hence the invention did not keep the recipient waiting for the authentication code, and the invention overcame a drawback of the SMS system, namely the perceived unpredictable delay.

4.4.5 Regarding the issue of the invention "pushing" the authentication and reference codes to the recipient, the board understands "pushing" in this context to mean that the codes are "unsolicited" by the recipient. In D3 the "common message" portion and icon/prompt are also "pushed" to the recipient, the recipient already having the password. Hence, according to the invention, as in D3, the recipient does not solicit the authentication and reference codes either. Moreover D5 teaches that the SMS system is sufficiently fast for delivering a TAN to a user in circumstances where the user has solicited the TAN and thus is waiting for it. The skilled person would conclude from D5 that, in a situation where the user had not solicited the authentication code, the speed of the SMS system would be even more acceptable.

4.4.6 Regarding the attractiveness of tokens, as opposed to SMS, for providing an authentication code to the recipient, the board takes the view that the issue to be decided is not whether more attractive alternatives to SMS were available at the priority date for providing authentication codes, for instance the tokens described by the inventor, but whether the skilled person would have regarded the use of a different network channel (distinct from those used to store and retrieve comments, respectively, in/from the store), for instance SMS, to send the authentication code for access by the recipient as an obvious choice. As D5 demonstrates, and the appellant has accepted, SMS was known at the priority date to be at least usable for delivering TANs in a situation in which the user expected a "real time" response, to use the appellant's expression. It is established case law of the boards of appeal of the EPO that a technical solution chosen by the skilled person does not have to be perfect; the skilled person can accept certain disadvantages, for instance unpredicable SMS delays, in order to gain other advantages, for instance improved recipient authentication. In doing so, the skilled person would have selected the delivery of authentication codes to the recipient's mobile phone by SMS, thus providing code sending means for using a second network connection to send said authentication code separately from the reference code for access by the recipient (difference feature "b"), without inventive step.

4.4.7 Hence the subject-matter of claim 1 does not involve an inventive step, Article 56 EPC 1973, in view of the combination of D3 and the common general knowledge of the skilled person, as, for instance, known from D5.

5. First auxiliary request - A

5.1 Independent system claim 1 of the auxiliary request has been restricted with respect to that of the main request by now specifying, amongst other additional features, that the message splitter is comprised in the originator's computer. This specifically excludes the situation in D3 in which message splitting occurs in the message processor 20. A corresponding amendment has been made to independent method claim 23 by now specifying that splitting the secure email message into a first email message and a second message occurs **at the originator's computer** (emphasis by the board).

5.2 This difference feature in both claims has the effect that the second message is no longer sent from the originator's computer via the same route as the first email message, meaning that the second messages are no longer stored together with the first email messages but instead are stored in an additional store.

5.3 The difference feature is not known from either of the documents taken as starting points for assessing inventive step in examination proceedings, namely D1 and D3. In both cases the originator's computer sends the complete message content to the email server/message processor 20 (D3) or the Multi-Media Messaging System MMMS (106) (D1). The realization of a message splitter/message splitting step in the originator's computer implies that some content from the originator's computer bypasses the email server/message processor 20 (D3) or the Multi-Media Messaging System MMMS (106) (D1) altogether in order to reach the recipient's computer. In the board's view, the skilled person would not have made such a technical change as an obvious solution to an obvious technical problem, starting from either D1 or D3.

5.4 Hence the board finds that the subject-matter of the independent claims involves an inventive step, Article 56 EPC 1973.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.
2. The case is remitted to the Examining Division with the order to grant a European patent with the following documents:

description:
pages 1 and 2, filed on 11 March 2011,
pages 3 to 6, filed as First Auxiliary Request - A on 17 May 2017,
pages 7 to 12, filed on 11 March 2011;

claims:
1 to 45, filed as First Auxiliary Request - A on 17 May 2017;

drawings:
sheets 1/12 to 12/12, as originally filed.

The Registrar: The Chairman:

Beschwerdekammern des Europäischen Patentamts
Boards of Appeal of the European Patent Office
Chambres de recours de l'Office européen des brevets

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated