Internal distribution code:

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

Datasheet for the decision of 14 June 2018

Case Number:	T 1770/13 - 3.4.03
Application Number:	99118731.1
Publication Number:	0989528
IPC:	G07F7/10, G06K19/07
Language of the proceedings:	EN

Title of invention:
Portable electronic apparatus and message processing method for decoding message formats

Patent Proprietor:
Kabushiki Kaisha Toshiba

Opponent:
Giesecke+Devrient Mobile Security GmbH

Headword:

Relevant legal provisions:
EPC 1973 Art. 56
EPC Art. 123(2)

Keyword:

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

Decisions cited:

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Case Number: T 1770/13 - 3.4.03

DECISION
# of Technical Board of Appeal 3.4.03
of 14 June 2018

Appellant: (Patent Proprietor)	Kabushiki Kaisha Toshiba 1-1, Shibaura 1-chome, Minato-ku Tokyo 105-8001 (JP)
Representative:	Horn Kleimann Waitzhofer Patentanwälte PartG mbB Ganghoferstrasse 29a 80339 München (DE)
Respondent: (Opponent)	Giesecke+Devrient Mobile Security GmbH Prinzregentenstraße 159 81677 München (DE)
Representative:	Klunker IP Patentanwälte PartG mbB Destouchesstraße 68 80796 München (DE)
Decision under appeal:	**Decision of the Opposition Division of the European Patent Office posted on 21 June 2013 revoking European patent No. 0989528 pursuant to Article 101(3)(b) EPC.**

Composition of the Board:

Chairman	G. Eliasson
Members:	M. Stenger
	C. Schmidt

Summary of Facts and Submissions

I. The appeal concerns the decision of the opposition division to revoke European patent no. EP0989528 based on European patent application no. 99118731 for lack of inventive step (main request) and non-compliance with Article 123(2) EPC (auxiliary request).

II. At the oral proceedings before the Board, the appellant/proprietor requested the maintenance of the patent according to a main request or according to first to third auxiliary requests, all filed with the grounds for appeal. The claims of the main request correspond to the claims of the main request on which the contested decision was based and the claim of the first auxiliary request corresponds to the claim of the auxiliary request on which the contested decision was based.
The respondent/opponent requested to dismiss the appeal.

III. The following documents will be referred to in this decision
D3: EMV '96, Integrated Circuit Card, Specification for Payment Systems, Version 3.0, June 1996 (1996-06-30)
D4: Handbuch der Chipkarten, 2. Auflage, 1996

IV. Claim 1 of the main request has the following wording (labeling added by the Board on the basis of the labeling used during the opposition procedure):

A portable electronic apparatus comprising:
A) reception means (35) for receiving a message;

B) identification means (31) for identifying a message format of the message received by said reception means; and

C) processing means (31) for
C-5) decoding a command of the message received by said reception means on the basis of the message format identification result obtained by said identification means, and
C-6) performing processing in accordance with the decoded command,

said identification means (31) includes message format identification means for identifying a specific one of
B-i) a first message format containing a command header field and data field,
B-ii) a second message format containing a command header field and encrypted data field,
B-iii) a third message format containing a command header field, data field, and auxiliary data field for guaranteeing validity of the data field,
B-iv) a fourth message format containing a command header field, encrypted data field, and auxiliary data field for guaranteeing the encrypted data field to which the message received by said reception means corresponds; and

said processing means (31) includes
C-3) decryption means (22) for decrypting the encrypted data field,
C-1) verification means for verifying the encrypted data field on the basis of the auxiliary data field,

C-i) first processing means for, when said message format identification means determines that the *received message corresponds to the first message format,*

C-i-5) decoding the command header field contained in the received message, and

C-i-6) performing processing in accordance with a command indicated by the command header field,

C-ii) second processing means for, when said message format identification means determines that the received message corresponds to the second message format,

C-ii-3) causing said decryption means(22) to decrypt the encrypted data field contained in the received message,

C-ii-4) converting the received message into the first message format,

C-ii-5) decoding the command header field contained in the converted message, and

C-ii-6) performing processing in accordance with a command indicated by the command header field,

C-iii) third processing means for, when said message format identification means determines that the received message corresponds to the third message format,

C-iii-1) causing said verification means to verify the data field contained in the received message on the basis of the auxiliary data field contained in the received message,

C-iii-2) deleting the auxiliary data field contained in the received message and

C-iii-4) converting the received message into the first message format provided that the data field is verified,

C-iii-5) decoding the command header field contained in the converted message, and

C-iii-6) performing processing in accordance with a command indicated by the command header field, and

C-iv) fourth processing means for, when said message format identification means determines that the received message corresponds to the fourth message format,
C-iv-1) causing said verification means to verify the encrypted data field contained in the received message on the basis of the auxiliary data field contained in the received message,
C-iv-3 part 1) provided that the encrypted data is verified,
C-iv-2) deleting the auxiliary data field contained in the received message,
C-iv-3 part 2) causing said decryption means to decrypt the encrypted data field, and
C-iv-4) converting the received message into the first message format,
C-iv-5) decoding the command header field contained in the converted message, and
C-iv-6) performing processing in accordance with a command indicated by the command header field.

V. Claim 1 of the first auxiliary request has the following wording (labeling added by the Board in correspondence to the labeling of claim 1 of the main request):

A message processing method comprising:
A) a first step (STEP 1) of receiving a message with an IC card (11);
B) a second step (STEPs 4-14) of identifying a message format of the message received in the first step; and

C-5) a third step (STEP 15) of decoding a command of the message received in the first step on the basis of the message format identification result obtained in the second step, and
C-6) performing processing in accordance with the decoded command,
the second step (STEPs 4-14) includes a fourth step of identifying a specific one of
B-i) a first message format containing a command header field and data field,
B-ii) a second message format containing a command header field and encrypted data field,
B-iii) a third message format containing a command header field, data field, and auxiliary data field for guaranteeing validity of the data field,
B-iv) a fourth message format containing a command header field, encrypted data field, and auxiliary data field for guaranteeing the encrypted data field to which the message received in the first step corresponds,

wherein the fourth step (STEPs 4-10) includes:
B-1) a first message format identification step (STEP 4) of determining whether the format of the received message is the first message format;
B-2) a second message format identification step (STEP 5) of determining whether the format of the received message is the second message format, the second message format identification step (STEP 5) being carried out if it is determined in the first message format identification step (STEP 4) that the format of the received message is not the first message format;
B-4) a fourth message format identification step (STEP 10) of determining whether the format of the received message is the fourth message format; and

the third step (STEP 4-15) includes
C-i) a fifth step (STEP 15) of, when it is determined in the fourth step that the received message corresponds to the first message format,
C-i-5) decoding the command header field contained in the received message (STEP 15), and
C-i-6) performing processing in accordance with a command indicated by the command header field (STEP 15),

C-ii) a sixth step (STEPs 13-15) of, when it is determined in the fourth step that the received message corresponds to the second message format,
C-ii-3) decrypting the encrypted data field contained in the received message (STEP 13),
C-ii-4) converting the received message into the first message format (STEP 14),
C-ii-5) decoding the command header field contained in the converted message (STEP 15), and
C-ii-6) performing processing in accordance with a command indicated by the command header field (STEP 15),

C-iii) a seventh step (STEPs 8-15) of, when it is determined in the fourth step that the received message corresponds to the third message format,
C-iii-1) verifying the data field contained in the received message on the basis of the auxiliary data field contained in the received message (STEP 8),
C-iii-2) deleting the auxiliary data field contained in the received message and
C-iii-4) converting the received message into the first message format provided that the data field is verified (STEP 14),

C-iii-5) decoding the command header field contained in the converted message (STEP 15), and
C-iii-6) performing processing in accordance with a command indicated by the command header field (STEP 15), and

C-iv) an eighth step (STEPs 8-15) of, when it is determined in the fourth step that the received message corresponds to the fourth message format,
C-iv-1) verifying the encrypted data field contained in the received message on the basis of the auxiliary data field contained in the received message (STEP 8),
C-iv-3 part 1) provided that the encrypted data is verified,
C-iv-2) deleting the auxiliary data field contained in the received message (STEP 14),
C-iv-3 part 2) decrypting the encrypted data field (STEP 13) and
C-iv-4) converting the received message into the first message format (STEP 14),
C-iv-5) decoding the command header field contained in the converted message (STEP 15), and
C-iv-6) performing processing in accordance with a command indicated by the command header field (STEP 15);

wherein
D) a verification data checking step (STEP 6) of determining whether verification data for verifying the auxiliary data field is set in the IC card (11), is carried out if it is determined in the second message format identification step (STEP 5) that the format of the received message is not the second message format;
wherein
E) the verifying (STEP 8) on the basis of the auxiliary data field contained in the received message

is carried out, if it is determined in the verification data checking step (STEP 6) that verification data for verifying the auxiliary data field is set in the IC card (11); and wherein
F) the fourth message format identification step (STEP 10) is carried out if it is determined by the verifying (STEP 8) that the data field or encrypted data field is valid.

VI. Claim 1 of the second auxiliary request differs from claim 1 of the first auxiliary request in that features B-1), B-2), B4), D), E) and F) are absent and by the additional features that
G) the second step includes a step (STEP 2) of determining whether the message format of the message received in the first step is permitted or not,
and
H) the third step is comprised in the method provided that the message format is permitted.

VII. Claim 1 of the third auxiliary request differs from claim 1 of the first auxiliary request by the further features G) and H).

VIII. The main arguments of the proprietor with respect to the main request can be summarised as follows:

Document D3 did not disclose the four different message formats B-i), B-ii), B-iii) and B-iv). Likewise, the identification means B) for identifying the four different message formats and the corresponding four different processing means C-i), C-ii), C-iii) and C-iv) with their sub-features were not disclosed in D3. At least, D3 did not disclose features C-iii-2), C-iv-2), C-iv-3 part 1), C-ii-4), C-iii-4) and C-iv-4). Feature C-5) was not disclosed in D3 as well.

These differentiating features provided a standardised internal message format by means of which resources of the IC card could be saved.

IX. The main arguments of the opponent with respect to the main request can be summarised as follows:

The features of the claims were all at least implicitly disclosed in D3. In any case, the patent did not go beyond a straightforward implementation of the standard defined in D3, using the general knowledge of the skilled person as exemplified in D4.

X. The main arguments of the proprietor with respect to the auxiliary requests can be summarised as follows:

The numbering used for designating the steps of the claims should not be construed as implying a temporal order. Thereby, the embodiments of the claims as filed and of figure 5 did not contradict each other. Their individual features could therefore be combined without contravening the requirements of Article 123(2) EPC.

XI. The main arguments of the opponent with respect to the auxiliary requests can be summarised as follows:

The application could not be used as a pool of features that could be combined at will. Further, the order of the steps as defined in the claims could not now be declared to be insignificant, whereby the embodiments of the original claims on the one hand and of figure 5 on the other hand contradicted each other. Mixing features of these different embodiments did not comply with Article 123(2) EPC.

Reasons for the Decision

1. Main request

1.1 Document D3

Document D3 concerns a specification or standard for Integrated Circuit Cards (IC cards or ICC) to be used in payment systems. The standard specifies for example the electromechanical interface of such cards (section I-1.), the commands for financial transactions using these cards (section II-2.) and secure messaging with such cards (section IV-3.). The specification includes different message formats to be used.

This document was considered by both parties to represent the closest state of the art.

Since D3 relates, just like the patent opposed, to messages of different formats received by an IC card, the Board sees no reason to disagree.

1.1.1 Feature A)

Document D3 describes the structure of messages transported between a terminal and a (chip) card (section II-2.1., first sentence). It is thus indispensable that the cards referred to in D3 (which correspond to the portable electronic apparatus of claim 1) comprise reception means for receiving a message. D3 thus discloses feature A). This was not disputed by the proprietor.

1.1.2 Features B-i), B-ii), B-iii) and B-iv)

The Board notes that data exchange between IC cards and terminals is performed using application protocol data units or APDUs. Commands are transmitted to the IC cards by means of command APDUs. The format of these command APDUs in the presence of data is disclosed in D3 in figure II-1, comprises a command header field and a data field and thus corresponds to the first message format B-i) as defined in the claims. This was not disputed by the proprietor.

The proprietor argued that D3 did however not disclose all four message formats defined in the claims (grounds for appeal, page 6, first paragraph to page 7, penultimate paragraph) because secure messaging according to D3 always implied the use of *both* encryption *and* a MAC (grounds for appeal, page 7, all paragraphs except the last one). Thereby, formats 2 and 3 were not disclosed in D3.

However, D3 also discloses messages that are *either* encrypted *or* provided with a MAC.
More specifically, the MAC is presented explicitly as being *optional* for encrypted data fields (Figure IV-6: *MAC (if present)*). Thereby D3 discloses both message formats 2 (if the MAC is not present) and 4 (if the MAC is present) as claimed.
Further, both figures IV-3 and IV-4 show an unencrypted data field that is nonetheless provided with a MAC. This corresponds to message format 3 as claimed.

To summarise, the Board thus concludes that D3 discloses all four message formats corresponding to features B-i), B-ii), B-iii) and B-iv) of the claims in the following passages:
Message format 1, B-i): Figure II-1 and table II-51,
Message format 2, B-ii): Figure IV-6 (in the alternative without MAC),
Message format 3, B-iii): Figures IV-3 and IV-4,
Message format 4, B-iv): Figure IV-6 (in the alternative with MAC).

1.1.3 Feature B)

The proprietor argued (grounds for appeal, page 6, paragraphs 1 and 2, and page 7, last paragraph to page 8, paragraph 5; see also the contested decision page 9, paragraph 5, referring to page 125 of D4) that due to hardware limitations, IC cards often implemented only a limited number of commands and data structures. D3 could thus not be read as disclosing a single IC card capable of handling all four message formats claimed. Consequently, D3 did not disclose the identification means for the four message formats (feature B)).

The Board accepts that the skilled person might consider to implement only a part of the standard set out in D3 if he is obliged to use IC cards with hardware limitations.
However, document D3 concerns a *specification* or *standard*. The very purpose of such a standard is to enable maximum interoperability. Thus, the skilled person would interpret D3 such that the standard set out therein is always to be implemented completely whenever this is possible in view of the hardware of the IC card.
Any IC card implementing this standard completely would then inevitably be capable of handling all message formats defined therein, including the four different message formats defined in claim 1. This implies the presence of some identification means for identifying the format of the messages.
Thus, D3 implicitly discloses feature B) as well.

The Board thereby concurs with the opposition division (contested decision, section 2.2).

1.1.4 Feature C)

Any IC card comprises a microprocessor and thus processing means. D3 therefore discloses feature C). This was not disputed by the proprietor.

1.1.5 Features C-5) and C-6)
The proprietor argued that D3 did at least not explicitly disclose feature C-5).

However, C-5) is formulated in a very broad manner and must be understood as comprising decoding a command of a message that was previously authenticated/decrypted on the basis of the message format identification result.
This does not go beyond what is commonly done in IC cards. This apparent, e.g., from D4, which is a textbook representing a part of the common general knowledge of the skilled person (see the roles of the *Secure Messaging Manager* and the *Kommandointerpreter*, pages 123 and 124).
Thus, feature C-5) is implicitly disclosed in D3.

Likewise, performing processing according to a decoded command as defined in feature C-6) corresponds to the standard operation of an IC card once the command or instruction of a message is decoded by the command interpreter. Therefore, feature C-6) is implicitly disclosed in D3 as well.

1.1.6 Features C-3) and C-1)
The different message formats disclosed in D3 include encrypted data fields and message authentication codes, as argued above. This implies that any IC card complying with the specification of D3 has to include decryption means according to feature C-3) and verification means according to feature C-1).
D3 thus implicitly discloses these two features.

This was not disputed by the proprietor.

1.1.7 Features C-i), C-ii), C-iii), C-iv) and their sub-features

In a similar manner as for feature B), the proprietor argued that D3 did not disclose the four different processing means as defined in the claims (features C-i), C-ii), C-iii), C-iv) and their sub-features), because D3 did not disclose a single IC card capable of handling all four message formats claimed.

However, as argued with respect to feature B), any IC card complying completely with the specification set out in D3 must be capable of handling all the message formats defined in the standard. This implies that such an IC card is provided with processing means for processing the messages of the different message formats defined.
Thus, D3 implicitly discloses the four different processing means defined in features C-i), C-ii), C-iii) and C-iv), as argued by the Opposition Division (page 10, paragraph 1 of the contested decision).

The Board further notes that features C-i-5) and C-i-6) amount to no more than the standard processing of a command APDU as shown in figure II-1 of D3, described, e.g., in D4 (Bild 5.1, the *Kommandointerpreter* decodes the command header field which corresponds to feature C-i-5, while the blocks called *Logical Channel Manager*, *Zustandsautomat*, *Anwendungsbefehl* and *Codeinterpreter* represent the processing step defined in feature C-i-6)).
This argument applies also to features C-ii-5), C-ii-6), C-iii-5), C-iii-6), C-iv-5) and C-iv-6).
Therefore, the Board concurs with the Opposition Division (page 10, paragraph 1 of the contested

decision) that all these features are disclosed in D3 as well.

The data fields in message formats 2 and 4 of D3 (figure IV-6 in both alternatives with and without MAC) are encrypted (to ensure data confidentiality, see section IV-3.). It is thus indispensable to decrypt the corresponding fields before processing can continue. Further, the purpose of a message authentication code MAC is to ensure data integrity and issuer authentication (D3, section IV-3.). In order to fulfill this purpose, a verification of any present MAC would have to be carried out prior to any other handling steps.
It follows therefrom that D3 implicitly discloses features C-ii-3), C-iii-1, C-iv-1 and C-iv-3, parts 1 and 2, as argued by the Opposition Division (page 10, paragraphs 2 to 4 of the contested decision).

1.1.8 The proprietor argued that D3 did not disclose that the auxiliary data, i.e., the MAC, was deleted. Features C-iii-2) and C-iv-2) were thus not disclosed in D3.

The opponent replied that the MAC of D3 would be of no use after the authentication had taken place and that the deletion of the MAC was thus implicitly disclosed in D3.

The Board is not aware of any passage in D3 that indicates what is done with the MAC once the corresponding message has been authenticated. It is, for example, conceivable that the MAC is not deleted from the card after authentication, but stored somewhere in the card for other purposes, such as book-keeping.

The Board thus concludes that features C-iii-2) and C-iv-2) are not directly and unambiguously disclosed in D3.

1.1.9 The proprietor further argued that D3 did not disclose features C-ii-4), C-iii-4) and C-iv-4) concerning the conversion of the second to fourth message format into the first message format.

The opponent replied that the conversion was nothing else than deleting the auxiliary data field after use and decrypting the data field where appropriate. This was implied in D3 by the very existence of the second to fourth formats.

However, as argued before, D3 does not directly and unambiguously disclose *deleting the auxiliary data field contained in the received message*. Thus, even if one follows the argument of the opponent, the converting step would still not be disclosed in D3.

The Board further notes that the patent does not require that the converting steps necessarily correspond only to the deleting and decrypting steps. Instead, the patent can be read such that the conversion or reconstruction into message format 1 is done in addition to the deletion and decryption steps (see [15] to [17] which can be read such that the conversion/reconstruction is performed *after* the decryption/deletion steps). The skilled person would thus not necessarily equate the deletion and decryption step of the claims with the conversion step.

The Board thus concludes that D3 does not disclose features C-ii-4), C-iii-4) and C-iv-4) in a direct and unambiguous manner.

1.1.10 Distinguishing features

The Board thus concludes that the subject-matter of claim 1 differs from what is disclosed in D3 by the feature groups

a) C-iii-2) and C-iv-2)

b) C-ii-4), C-iii-4) and C-iv-4)

1.2 Inventive step

The proprietor argued that the technical effect of the differentiating feature groups a) and b) was a standardisation of the internal message format. This standardisation solved the objective technical problem of saving resources of the IC card by enabling the reuse of program code.

The opponent pointed out that the deletion of the auxiliary data was effectively the only distinguishing feature, since decryption was compulsory whenever encrypted data was present. This was the case in certain formats disclosed in D3.
Deleting unnecessary overhead data was to be considered simply good programming practice, thus being part of the common general knowledge of the skilled person. Further, it was necessary to make sure that the message format could be handled at all. According to D3, one single IC card could handle all four message formats as defined in the patent. Thus, the differentiating feature would be a straightforward consequence of the implementation of the standard disclosed in D3.

As mentioned before, command messages are handled in IC cards in a layered manner (D4, section *Befehlsabarbeitung* on pages 123 to 125, see also Bild 5.1).
The authentication and decryption process is performed by the *Secure Messaging Manager*, which is completely

transparent if no secure messaging takes place (D4, page 123, paragraph 3). That is, a message of a format not subject to secure messaging will simply be passed on by the *Secure Messaging Manager* to the next layer. This is the case for messages of the format shown in figure II-1 of D3, corresponding to message format 1. The next layer, the *Kommandointerpreter*, will then decode the command.

As a consequence of the layered handling, the *Kommandointerpreter* always expects the same command message format, that is, the command APDU format presented in D3 in figure II-1. This is the message format the *Kommandointerpreter* can handle.
To make sure that the *Kommandointerpreter* can handle the messages passed on to it (as pointed out by the opponent), the skilled person would thus design the Secure Message Manager such that any message passed on to the *Kommandointerpreter* is converted into the first message format, if it is not already in the first message format.

In that sense, the *standardisation of the internal message format* evoked by the proprietor has therefore to be seen as a requirement imposed by the layered manner of handling command messages in IC cards.

The skilled person would thus implement features C-ii-4), C-iii-4) and C-iv-4) in a straightforward manner when putting into practice the standard disclosed in D3.

Further, to enable decoding by the *Kommandointerpreter*, any auxiliary data will have to be deleted at least in the sense that is has to be removed from the message that is to be passed on to the *Kommandointerpreter* (prior to or as part of the converting step). Whether the auxiliary data is deleted completely or kept somewhere else for other purposes has no impact on the handling of the command messages. This has therefore to be considered as being a choice the skilled person would make, according to the circumstances, without the exercise of an inventive step.

The skilled person would thus also implement features C-iii-2) and C-iv-2) in a straightforward manner when putting into practice the standard disclosed in D3.

For these reasons, the Board concurs with the opponent that the distinguishing features a) and b) are a straightforward consequence of putting into practice the standard disclosed in D3 in an IC card taking into account the generally known layered structure of command message handling in such cards as exemplified in D4. This finding is in line with section 4 of the contested decision.

The Board therefore comes to the same conclusion as the opposition division (section 6 of the contested decision) that the subject-matter of claim 1 of the main request does not involve an inventive step according to Article 56 EPC 1973 in view of D3 combined with the common general knowledge of the skilled person as exemplified by D4.

2. Auxiliary requests 1 to 3

2.1 Auxiliary request 1

The proprietor indicated that original claims 6 and 10 together with figure 5 and the corresponding original description (paragraph 18 of the published application)

provided a basis in the sense of Article 123(2) EPC for the claim of auxiliary request 1.
The fifth to eighth steps defined in the claim of this request were performed *when*, not *if*, certain conditions were met in the fourth step. Thus, no causal link was established by the claim language.
The step numbering used in the original claims was further not to be construed as implying any temporal order, as could be seen from the formulation *the second step includes a fourth step*. The skilled person would, in view of the application as a whole, be aware that the methods defined in the original claims related to the same issue as the method disclosed in figure 5. These methods did not contradict each other and could thus be combined.

The opponent argued that the first to eighth steps were designated by numbers, not by functions, whereby an order of the steps was defined. The order of the sub-steps to be performed when a certain condition was met was defined in the claim and could not now be declared to be insignificant. The order disclosed in figure 5 was not compatible with the order defined in original claims 6 and 10. The example shown in figure 5 could therefore not be used as a basis for amending these original claims.

The Board concurs with the proprietor that features B-1), B-2), B-4), D), E) and F) are disclosed in the original application in figure 5, while the other features of the claim of auxiliary request 1 are disclosed in original claims 6 and 10.
Thus, each feature of the claim of auxiliary request 1 taken individually has a basis in the original application.

The Board further agrees with the proprietor that the numbers used for designating the steps (first step, second step, ... eighth step) in original claims 6 and 10 can not be seen as implying a certain order. This is apparent not only from the formulation that *the second step includes a fourth step*, but also from the definition that the third step includes the fifth to eighth steps which are mutually exclusive in the sense that, for any given message, only one of these steps will be performed depending on the format of the received message.

However, original claim 10 specifies for each of the fifth to eighth steps what is to be done when it is determined in the fourth step that the received message corresponds to a specific one of the four message formats.
In the case of the seventh and eighth steps of the claims, original claim 10 requires that the verification is performed only when it is determined that the message format is format 3 (seventh step) *or* when it is determined that the message format is format 4 (eighth step).
That is, even if the formulation *when it is determined* in the fifth to eighth steps of original claim 10 is interpreted as defining only a temporal and not a causal link (as argued by the proprietor), the wording of original claim 10 requires that the determination of whether the message has the format 3 or the format 4 is carried out *before* the (encrypted) data field is verified.

In contrast to that, according to figure 5, the verification of the data by means of the auxiliary data field in steps 6 and 8 is performed immediately once it is clear that the message format is neither format 1 nor format 2. That is, according to figure 5, the determination of whether the message has format 3 or 4 in step 10 is carried out *after* the encrypted data field is verified (see also summons of the Opposition Division sent with letter dated 10 July 2012).

Thus, the seventh and the eighth step of original claim 10 define a different order of steps than figure 5. It follows that figure 5 relates to an embodiment that is incompatible with the embodiment of original claims 6 and 10. Thus, the introduction of parts of the method disclosed in figure 5 into original method claims 6 and 10 results in a mixture of two different embodiments for which there is no basis in the original application and which therefore contravenes the requirements of Article 123(2) EPC.

The Board thereby comes to the same conclusion as the Opposition Division (points 7, 8 and 9 of the contested decision).

2.2 Auxiliary requests 2 and 3

The claims of auxiliary requests 2 and 3 also each comprise features based on figure 5 (auxiliary request 2: features G) and H), auxiliary request 3: features B-1), B-2), B-4), D), E), F), G) and H)) in addition to the features of original claims 6 and 10. This was not disputed by the proprietor.

Thus, they also represent a mixture of embodiments which is not disclosed in the original application. Therefore, the claims of both the second and the third auxiliary requests do not comply with the requirements of Article 123(2) EPC.

3. The subject-mater of claim 1 of the main request does not involve an inventive step. The claims of auxiliary requests 1 to 3 do not comply with the requirements of Article 123(2) EPC. Thus, none of the requests on file fulfills the requirements of the EPC and therefore, the appeal must fail.

It is therefore not necessary to discuss the other objections brought forward by the opponent.

Order

For these reasons it is decided that:

The appeal is dismissed.

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 ✦

M. Schalow G. Eliasson

Decision electronically authenticated