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

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

Datasheet for the decision of 29 July 2008

Case Number:	T 0511/06 - 3.4.01
Application Number:	00913873.6
Publication Number:	1163623
IPC:	G06K 1/00
Language of the proceedings:	EN

Title of invention:
Methods and apparatus for authentificating the download of information onto a smart card

Patentee:
AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPANY, INC.

Opponent:
GIESECKE & DEVRIENT GmbH

Headword:
-

Relevant legal provisions (EPC 1973):
EPC Art. 56, 104

Keyword:
"Inventive step - (no) non-technical features"
"Apportionment of costs (no)"

Decisions cited:
T 0641/00

Catchword:
-

Case Number: T 0511/06 **-** 3.4.01

DECISION
of the Technical Board of Appeal 3.4.01
of 29 July 2008

Appellant:
(Patent Proprietor)

AMERICAN EXPRESS TRAVEL RELATED SERVICES
COMPANY, INC.
American Express Tower
World Financial Center
New York, NY 10285 (US)

Representative:

Hanna, Peter William Derek
Hanna, Moore & Curley
13 Lower Lad Lane
Dublin 2 (IE)

Respondent:
(Opponent)

GIESECKE & DEVRIENT GmbH
Prinzregentenstr. 159
D-81677 München (DE)

Representative:

Höhfeld, Jochen
Klunker Schmitt-Nilson Hirsch
Patentanwälte
Winzererstrasse 106
D-80797 München (DE)

Decision under appeal:

Decision of the Opposition Division of the European Patent Office posted 3 February 2006 revoking European patent No. 1163623 pursuant to Article 102(1) EPC 1973.

Composition of the Board:

Chairman: H. Wolfrum
Members: F. Neumann
M.-B. Tardo-Dino

Summary of Facts and Submissions

I. The appeal lies from the decision of the opposition division revoking the European patent number 1 163 623 on the ground of lack of inventive step.

II. The appellant (patentee) requested that the decision be set aside and the patent be maintained in amended form with claims as set out in a main request as filed with letter of 10 December 2003, or alternatively with claims as set out in one of four auxiliary requests as filed with letter of 06 October 2005, a fifth auxiliary request (to be considered directly after the first auxiliary request), as filed at the oral proceedings before the opposition division on 10 November 2005, or a further auxiliary request as filed with letter of 19 June 2008. Moreover, the appellant requested a decision regarding an apportionment of costs.

The respondent (opponent) requested that the appeal be dismissed and that the request for apportionment of costs be dismissed. As an auxiliary measure, oral proceedings were requested.

III. During the appeal proceedings, the following citation was taken into account:

E1: US-A-5 809 144.

In addition, reference was made to the following standard text, referred to in the decision as "Rankl-Effing":
Handbuch der Chipkarten; W. Rankl und W. Effing; Carl Hanser Verlag, München, Wien; 1. Auflage 1995.

IV. Independent claim 1 of the appellant's **main request** reads as follows:

"*A system for authenticating download of information, said system comprising:*
an information device (102) having a signature;
at least one external device (112) capable of transferring blocks of information to said information device (102), wherein said blocks of information belong to an information owner (110), and wherein said external device is a third party device remotely located from said information owner (110) and wherein said external device transfers said blocks of information on behalf of said information owner (110);
said information device (102) is configured to perform an acknowledgement process;
said acknowledgement process computes, based upon the contents of said signature, a verifiable acknowledgement of the transferred information and sends said computed acknowledgment to said information owner (110) for verification."

Claim 1 of the **first auxiliary request** differs from claim 1 of the main request in that the final section of claim 1 reads "*said acknowledgement process computes, based upon the contents of said signature, a verifiable acknowledgement of the transferred information, wherein said verifiable acknowledgement is uniquely related to said transferred blocks of information, and sends said computed acknowledgment to said information owner (110) for verification.*"

Claim 1 of the **fifth auxiliary request** differs from claim 1 of the first auxiliary request in that the verifiable acknowledgement is defined as "*wherein said verifiable acknowledgement is uniquely related to said transferred blocks of information, and includes an identification of the third party,*".

Claim 1 of the **second auxiliary request** differs from claim 1 of the first auxiliary request in that it defines "*A system for authenticating download of information to a smart card,*" and the terms "*an information device (102)*" and "*information device (102)*" are replaced by "*a smart card (102)*" and "*smart card (102)*" respectively.

Claim 1 of the **third auxiliary request** differs from claim 1 of the second auxiliary request in that the wording "*a smart card (102) having a signature;*" is replaced by "*a smart card (102) having a signature generated by keys resident on the smart card;*".

Claim 1 of the **fourth auxiliary request** differs from claim 1 of the third auxiliary request in that the first line of claim 1 reads "*A system for authenticating download of an application or applet to a smart card, said system comprising:*" and the term "*a verifiable acknowledgement of the transferred information*" is replaced by "*a verifiable acknowledgement of the transferred application or applet*".

Claim 1 of the "**further auxiliary request**" differs from claim 1 of the main request in that the wording "*an information device (102) having a signature*" is replaced by "*an information device (102) having cryptographic* *keys resident on the device for generating a signature*" and the final section of claim 1 reads "*said information device (102) is configured to perform an acknowledgement process; in which said acknowledgement process computes the signature using the cryptographic keys, based upon the downloaded information, as a verifiable acknowledgement of the successful download of the transferred information and sends said computed acknowledgment to said information owner (110) for verification.*"

Each of the requests includes, in addition, further independent claims and dependent claims, the wording of which is not relevant to the present decision.

V. The arguments of the parties, insofar as they are pertinent to the present decision, are set out below in the reasons for the decision.

Reasons for the Decision

1. The appeal is admissible.

2. In view of the entry into force of the EPC 2000, reference is made to Article 7(1), 2nd sentence of the Revision Act of 29 November 2000 ("Act revising the Convention on the Grant of European Patents (European Patent Convention) of 5 October 1973, last revised on 17 December 1991") and the transitional provisions for the amended and new provisions of the EPC (Decision of the Administrative Council of 28 June 2001), from which it may be derived which Articles of the EPC 1973 are

still applicable in the present case and which Articles of the EPC 2000 shall apply.

3. **Main request - inventive step:**

3.1 In the opinion of the Board, the closest prior art is represented by E1. This document discloses a system for purchasing and delivering digital goods over a network. One of the steps involved in the transaction procedure of E1 is the comparison of first and second cryptographic checksums (col. 6, lines 9-11 and col. 10, lines 9-11). From this comparison, it may be established whether the information which is received by the customer is in fact the "authentic" information, i.e. the information which was sent by the merchant. Thus, E1 discloses a system for authenticating download of information.

The patentee noted that in the system of the contested patent, a third party was involved. It was submitted that in such a system the information owner had to download information to the third party in order for the third party to pass this information on to the customer. Consequently the authentication process of claim 1 provided a guarantee that the information downloaded from the information owner to the third party for further distribution was the same as the information that the customer actually received from the third party. The Board notes however, that claim 1 makes no reference to any transmission of information between the information owner and the third party and therefore cannot be interpreted to mean that the authentication involves checking that the information device (the customer) receives the same information as that which was downloaded from the information owner to the third party. On the basis of what is defined in the claim, the process of authentication is understood to mean that the data which is received by the information device is checked to ensure that it is the same as that which was sent from the party sending the data. As shown above, this is exactly what happens in E1.

3.2 The system of E1 further comprises an information device (the customer computer 10) and an external device (merchant computer 12) capable of transferring blocks of information to the information device 10, wherein said blocks of information belong to an information owner (the merchant) and wherein said external device 12 transfers the blocks of information on behalf of the information owner (column 3, lines 58-60; column 9, lines 29-34).

With regard to the "blocks of information" which are transferred from the external device 12 to the information device 10, the patentee argued that the downloaded data in E1 was encrypted and that the skilled person would realise that the "blocks of information" in claim 1 were raw (i.e. non-encrypted) data. In the Board's view, the wording of claim 1 does not justify the patentee's narrow interpretation as to the format of the data transferred. Nonetheless, the format (i.e. raw or encrypted) of the data makes no difference to the capability of the external device for transferring the information: in both cases, the downloaded data will be comprised of a string of ones and zeros, whether it is encrypted or not. The Board is therefore of the opinion that this argument is of no significance with regard to the subject-matter defined in claim 1.

The patentee further submitted that in E1 there was no reference to the information owner. The merchant in E1 was a middle-man who simply sold the information, but the actual owner of the information, e.g. the copyright owner, had no way of checking that the merchant was downloading the authentic (i.e. not fake or manipulated) article. Again, the Board considers that this argument has no significance with regard to the subject-matter actually defined in claim 1. The merchant in E1 has to be considered to be the information owner. In the absence of any indication to the contrary in E1, there is no reason to doubt that the merchant is the person who owns and is entitled to sell the information.

3.3 In E1, when a customer creates an account server account, the customer receives a key pair which "is used for signatures and authentication within the system" (column 12, lines 29-33).

In the assessment of inventive step, the term "signature" in claim 1 is understood to mean a digital signature. A digital signature is derived from the data which is being sent by applying an algorithm to the data. The algorithm which generates the signature normally involves data compression by means of a hash function and encryption by means of cryptographic keys. The resulting data string is the digital signature. This interpretation is consistent with the conventional understanding of the term "digital signature", as evidenced by section 8.2 of Rankl-Effing, and is the interpretation used in the contested patent itself (paragraph [0016]).

The information device (the customer computer 10) of E1 "has" a signature, in the sense of being able to generate a signature using the above-mentioned key pair.

3.4 In E1, the information device 10 is configured to perform an acknowledgement process. This process computes a verifiable acknowledgement (the digitally signed electronic payment order (EPO)) of the transferred information and sends the computed acknowledgement to the information owner (the merchant) for verification (column 5, line 63 to column 6, line 11). The acknowledgement of E1 (the digitally signed EPO) contains, amongst other items, the "signature" and the second cryptographic checksum (Figure 8; column 5, line 63 to column 6, line 2). Thus the verifiable acknowledgement (i.e. the *complete* digital message which is sent to the merchant) is computed "based upon the contents of said signature". The information contained in the acknowledgment message of E1 is sufficient to enable the owner to verify that the downloaded information was error-free, complete and correct (column 10, lines 9-11) and that the acknowledgement message was sent by the customer.

The patentee argued that the digital signatures in E1 were not used to authenticate the download of information, i.e. were not used to enable the information owner to check that the information received by the customer was in fact the information which the information owner intended the third party to send. However, the Board notes that claim 1 merely defines that the acknowledgment process computes a "verifiable acknowledgement of the transferred information" without further defining what is verified. The patentee's argument therefore finds no reflection in the wording of the claim and is therefore of no significance.

The patentee also argued that the signatures in E1 were used only for verifying the parties involved in the transaction and that no content-related check was made using the signatures, the data authentication having been performed using checksums. Thus, the acknowledgment process, based upon the contents of the signature in E1, did not compute a verifiable acknowledgement of the transferred information, but only of the parties involved. The Board disagrees. As pointed out by the opponent, the signature enables more than just the source to be determined. As discussed in point 3.3 above, a "digital signature" is conventionally derived from the data being sent by encrypting this data using a source-specific set of cryptographic keys. Therefore, the signature is indicative of both the contents and the source.

3.5 Thus, a strict comparison of the individual features of claim 1 with the disclosure of E1 shows that the only difference between the disclosure of E1 and the subject-matter of claim 1 is that the external device is a third party device which is remotely located from the information owner wherein the third party device transfers blocks of information on behalf of said information owner.

However, the fact that this difference exists automatically gives rise to a further difference which is not immediately apparent on a straightforward feature-by-feature comparison of claim 1 with E1. Although the computed acknowledgement in E1 is sent to the information owner (the information owner in E1 being also the party transferring the data), the underlying principle in E1 is that it is the party who sends the data who receives the acknowledgment. Thus, as soon as the information owner no longer sends the data himself, he will no longer receive the acknowledgment. A further implied difference between the subject-matter of claim 1 and the teaching of E1 is therefore that the acknowledgment process of claim 1 sends the computed acknowledgment not (just) to the party who transfers the data, but rather to the remotely located information owner for verification.

3.6 In summary, claim 1 of the main request is distinguished from the disclosure of E1 in that:
(i) the external device is a *third party device* which is remotely located from the information owner, the third party device transferring blocks of information on behalf of the information owner, and
(ii) the information device is configured to perform an acknowledgment process which sends the computed acknowledgment to the *information owner* for verification.

3.7 In order to determine whether the subject-matter of a particular claim involves an inventive step it is usual to apply the problem-solution approach. In accordance with this approach, an invention is to be understood as a technical solution to a technical problem. Where a feature cannot be considered as contributing to the solution of any technical problem by providing a technical effect, it has no significance for the purpose of assessing inventive step (T 641/00, OJ EPO 2003, 352, reasons, point 6). However, technical aspects may be involved with the technical implementation of a non-technical concept. Hence, in order to establish whether claim 1 involves an inventive step, it must first be determined whether the distinguishing features solve a technical problem. In the case that the only recognisable effect of the distinguishing features is of a non-technical nature, it must still nevertheless be assessed whether an inventive step may be considered to lie in the technical implementation of the non-technical concept.

3.8 The objective technical problem has to be formulated taking the closest prior art and the distinguishing features of claim 1 into account. The patentee submitted that the objective technical problem was to be seen as providing means for the information owner to know whether the information, the download of which he had delegated, was really downloaded to the customer.

The Board does not agree with this formulation. In accordance with consistent case law, to arrive at the objective technical problem, it must first be established which technical effect the distinguishing features of the claim achieves. The technical problem is then formulated as the aim and task of modifying or adapting the closest prior art to provide the technical effects that the invention provides over the closest prior art. In the case that a distinguishing feature does not contribute to the solution of a technical problem, it cannot support the presence of an inventive step.

3.9 The effect of the first distinguishing feature (feature (i) in section 3.6 above) is that the information owner can delegate the download of information to a third party. This effect is, however, not technical: it concerns merely the distribution of tasks and consequently relates to a pure business model.

No arguments were presented to explain what the *technical* effect of this specific distinguishing feature could be.

Thus, the first distinguishing feature cannot be considered as contributing to the solution of a *technical* problem by providing a *technical* effect and therefore cannot support an inventive step.

3.10 The effect of the second distinguishing feature (feature (ii) in section 3.6 above) is that the delegating party itself (the information owner) is empowered to verify that the downloaded information has indeed been correctly received by the customer. This effect concerns an administrative aspect arising from the re-distribution of tasks and as such has no technical character.

The patentee insisted that the very nature of the downloading environment means that the verification of downloaded information always has technical character. Neither the opponent nor the Board contested that the system of claim 1 as a whole, or indeed specific components thereof, had technical character. However, in the assessment of inventive step, the distinguishing features have to solve a *technical* problem. In accordance with established case law, this technical problem must be derived from the technical effect of the distinguishing features. Since no technical effect of the second distinguishing feature has been identified, this feature cannot support an inventive step either.

3.11 Considering the particular manner of implementation of the business model, the Board cannot see, nor has it been argued, that the provision of a third-party device remotely located from the information owner in order to transfer blocks of information on behalf of the information owner may provide any specific technical effects or advantages beyond those inherent in the straightforward technical implementation. The provision of the basic components required for enabling the delegation of the downloading tasks to a third party does not require a non-obvious effort by the skilled person. Indeed, this implementation only requires that the third party be provided with a suitable computer which is configured to perform the downloading functions that would normally be performed by the computer of the information owner.

The Board recognises that the adoption of the business model which allows the downloading operations to be delegated to a third party necessarily requires that a decision be made as to whether the party who sends the data should receive the acknowledgement or whether the information owner himself should be sent the acknowledgment. The Board is of the opinion that even when the download task is delegated to a third party, the information owner nevertheless retains responsibility for the transaction and therefore must ensure that the received goods are in fact those which it was intended to sell. Thus, an inevitable result of delegating the download operation carries with it the administrative consequence of routing the acknowledgement message such that the information owner may still ensure that that which was downloaded to the customer was indeed correct and complete.

The technical implementation of this administrative aspect does not involve any further technical effect or advantage and therefore also cannot support an inventive step. Indeed the routing of the acknowledgement message to the information owner requires only the re-configuration of the address to which the acknowledgement message will be sent. The Board cannot see, nor has it been argued, that this particular manner of implementation requires any inventive activity by the skilled person.

3.12 Thus, in the present case, no technical effect can be recognised for either of the distinguishing features of claim 1. These features therefore cannot be considered as contributing to the solution of a technical problem and therefore have no significance for the purpose of assessing inventive step.

Nor can the technical implementation of these features be seen to contribute to an inventive step, since the technical implementation is straightforward and does not give rise to any further technical effects or advantages.

Consequently, the Board is unable to identify any effects other than those inherent in the business model itself. Therefore the subject-matter of claim 1 of the main request lacks an inventive step (Article 52(1) EPC, Article 56 EPC 1973) since the only features which render the subject-matter of claim 1 novel with respect to E1 cannot support an inventive step.

4. **First auxiliary request - inventive step:**

4.1 Claim 1 of the first auxiliary request differs from claim 1 of the main request in that the verifiable acknowledgement is defined as being uniquely related to the transferred blocks of information.

4.2 The Board is of the opinion that this is also the case in the system of E1. The second cryptographic checksum in E1 is computed on the basis of the downloaded information (column 5, lines 60-62). The digitally signed EPO of E1, which contains the second checksum, is therefore related to the transferred blocks of information; the digital signature makes this EPO unique. As pointed out by the opponent, the digitally signed EPO of E1 is in fact "doubly unique" since the computation of the second cryptographic checksum provides a first level of uniqueness, to which the digital signature adds a further level.

4.3 The patentee argued that E1 set out in column 5, lines 60 to 62 that the *second cryptographic checksum* was computed "on the received ... goods", not that the *digital signature* was computed or in any way related to the received goods. Thus, in E1, it was the *cryptographic checksum* - and not the *signature* - which was uniquely related to the transferred information, whereby the signature in E1 was considered by the patentee to be only an identification of the party concerned and not to be derived from an encryption of the data. It was argued that the only "verifiable acknowledgement" in E1 was the signature which permitted the verification of the source of the message to be performed. The patentee therefore considered that the "verifiable acknowledgment" (i.e. the signature) in E1 was neither based on nor uniquely related to the transferred information.

The Board cannot agree with this argument. As explained above, the signature of E1 must be considered to be derived from the data being sent, this data being encrypted using a source-specific set of cryptographic keys. This is the conventional understanding of this term. Thus, the signature of E1 is indeed uniquely related to the transferred blocks of information.

4.4 Therefore, since this feature is known from E1, the only distinguishing features of claim 1 with respect to E1 are those identified in paragraph 3.6 above. For the same reasons as presented with regard to claim 1 of the main request, these features cannot support an inventive step, with the result that claim 1 of the first auxiliary request is not inventive (Article 52(1) EPC, Article 56 EPC 1973).

5. **Fifth auxiliary request - inventive step:**

5.1 Claim 1 of the fifth auxiliary request differs from claim 1 of the first auxiliary request in that the verifiable acknowledgement includes an identification of the third party.

5.2 The patentee submitted that the effect of this feature was that the information owner could verify who had downloaded the information on his behalf. Since in E1 there was no reference to the delegation of the download task to a third party, the need to identify a third party could not be derived from the disclosure of E1. Consequently, this feature could not be seen as obvious in view of E1.

5.3 The Board is of the opinion that this additional feature has no technical effect and therefore does not solve a technical problem. The identification of the parties involved in a business transaction is of an administrative rather than a technical nature. The effect identified by the patentee can only be seen to be administrative. Consequently, this feature cannot be used to support an inventive step. Nor can the technical implementation of this feature be seen to contribute to an inventive step, since the technical implementation is straightforward and does not give rise to any further technical effects or advantages. In particular, the inclusion of the identification of the third party in the verifiable acknowledgment message requires only a straightforward reconfiguration of the list containing the various elements to be transferred.

5.4 Consequently, for the same reasons as given for the main request and the first auxiliary request, the subject-matter of claim 1 of the fifth auxiliary request does not involve an inventive step (Article 52(1) EPC, Article 56 EPC 1973).

5.5 Irrespective of the above findings, it is nevertheless noted that the digitally signed EPO of E1 contains the identification of the customer and the identification of the merchant (column 5, lines 64-67). Thus, the identifications of all participating parties are listed. Consequently, the Board is of the opinion that if a third party were to be involved in the transaction, it would be obvious to include his identification as well.

6. **Second auxiliary request - inventive step:**

6.1 Claim 1 of the second auxiliary request differs from claim 1 of the main request in that the information device is a smart card.

6.2 The patentee submitted that the current claim was intended to define a novel smart card application in which the signature could reside on the card along with the process for computing the acknowledgement based on the downloaded information and then for sending this acknowledgment to a different party (not the party from which the downloaded information was sent) for verification.

The patentee argued that E1 was not a logical starting point for a smart card application of this nature, in particular in view of the fact that an entire specialist text book (Rankl-Effing) existed which discussed specific smart card applications in detail. The only realistic starting point would be a smart card itself. Since in E1, the data was downloaded to a customer *computer*, not to a smart card, there would be no comprehensible reason for a skilled person, starting from a smart card, to take the teaching of E1 into consideration when considering how to download information to a smart card. It was argued that the teaching of E1 was too far removed from the smart card application. It was also argued that Rankl-Effing contained no mention of a smart card configuration which would enable an acknowledgement to be sent back to an information owner once a download from a third party had been received at the smart card. Therefore, using the same starting point as identified in the application, namely a smart card which was capable of receiving a download of digital goods, the skilled person would not be aware of any teaching which would lead him to the subject-matter of claim 1 which defined the configuration of the smart card in terms of the intricacies of the acknowledgment process.

6.3 The Board does not agree that E1 does not represent a suitable starting point for the assessment of inventive step. The closest prior art is that combination of features, disclosed in one single reference, which constitutes the most promising starting point for an obvious development leading to the invention. In selecting the closest prior art, the first consideration is that it should be directed to a similar purpose or effect as the invention or at least belong to the same or a closely related technical field as the claimed invention. In the present case, the system disclosed in E1 is directed to the download of data to a computer and is therefore related to a similar purpose as the invention, the only difference being the end device to which the data is sent. The Board is therefore of the opinion that E1 does indeed represent the closest prior art and is a logical starting point for the assessment of inventive step.

6.4 The disclosure of E1 is directed generally to communication protocols and more particularly to methods of carrying out commercial transactions over a computer network (col. 1, lines 8-10). Starting from E1, the question arises as to which end devices fall under the term "customer computer" and are capable of performing the communication protocol described in E1 to allow the information owner to ensure the completeness and correctness of the downloaded content.

6.5 From the contested patent it may be seen that smart cards which are capable of receiving downloads of digital goods (in particular updated software) are known (column 1, lines 54-58 of the contested patent, corresponding to page 2, lines 7-10 of the published application). The Board considers that a smart card - by virtue of its processor - is also a type of "customer computer" which is capable of receiving downloaded information. Therefore starting from E1 and wishing to apply this download process to a smart card, the skilled person merely has to establish whether the communication protocol of E1 may be implemented on a smart card. As pointed out by the opponent, the textbook Rankl-Effing describes several examples of various challenge-response communication protocols in which acknowledgment messages are generated at the smart card and returned to the terminal. This shows that smart cards are known to be capable of performing a two-way communication protocol. The skilled person would therefore have no difficulty in implementing the download-and-acknowledgement system of E1 on a smart card.

With regard to the argument that the smart card of claim 1 was configured to send the acknowledgement to a different party (and not the third party from whom the information is downloaded), it is noted that the claim does not exclude that the message may be sent to the information owner via the downloading party. Claim 1 merely defines that the information owner is sent the acknowledgment message, the exact pathway which the acknowledgement message follows remaining undefined. The technical implementation of this feature therefore need only involve the configuration of the acknowledgement process such that the verifiable acknowledgment is forwarded from the third party to the information owner. The Board cannot see that this would require any inventive activity by the skilled person.

6.6 It was further argued that the skilled person would not consider applying the teaching of E1 to the download of information to a smart card for two reasons. Firstly, E1 dealt with a range of aspects, e.g. secure payment transactions and building a trust relationship with a customer, which were not relevant when downloading data to a smart card. Secondly, the limited memory and processing capacity of a smart card would make it clearly unsuitable for performing the tasks of the customer computer in E1, the successful integration of the necessary software (e.g. the web browser, money tool and checkbook library) on a smart card being unlikely.

In the view of the Board, although E1 concerns a complex transaction procedure, it may nevertheless be separated down into a number of independent, discrete processes. This is evidenced by the fact that the various phases of the transaction are described under separate headings in E1. E1 describes an entire transaction procedure, from perusing a catalogue through to the secure payment and delivery of the ordered goods. However, the modular nature of the various steps involved in the transaction means that certain phases may be extracted and implemented as independent processes. The Board is of the opinion that E1 effectively provides an overview of the processes involved in all phases of a typical e-commerce transaction, the separate phases of the transaction being independently implementable where appropriate. The skilled person, starting from E1, can therefore select the phases which he requires for his particular type of transaction. In cases in which only certain phases are of interest (e.g. the goods delivery phase and an acknowledgement process), then the complexity of the other phases and the fact that various additional software units are required to perform the other phases would not deter the skilled person from implementing the phases of interest in a less complex system.

6.7 The remaining features which distinguish claim 1 from the disclosure of E1 have been discussed in sections 3.6 to 3.12 above. In particular, the fact that the external device is a third party device and that the acknowledgement message is sent to the information owner cannot be used to support an inventive step because these features are of non-technical nature. Moreover, as shown above, the technical implementation of these features does not involve any further technical effect or advantage and therefore also cannot support an inventive step.

Claim 1 of the second auxiliary request therefore lacks an inventive step (Article 52(1) EPC, Article 56 EPC 1973).

7. **Third auxiliary request - inventive step:**

7.1 Claim 1 of the third auxiliary request differs from claim 1 of the second auxiliary request in that the signature is defined as being generated by keys resident on the smart card.

7.2 As admitted by the patentee, this amendment merely sets out in concrete terms what has been assumed in the analysis of the previous requests. Nevertheless, the patentee held that actually *storing* the keys on the smart card had to be considered as a technical feature and this had to contribute to an inventive step. Moreover, it was argued that E1 taught to store the keys on a repository (column 13, lines 25-33) and that consequently E1 actually led away from this feature with the result that the subject-matter of claim 1 of the third auxiliary request could not be considered to be obvious.

7.3 As a preliminary remark, the Board notes that it is not clear from the term "resident" how long the keys actually reside on the smart card: this term does not necessarily imply permanent storage.

In E1, the signature is generated at the customer computer from an RSA key pair associated with the customer computer (column 12, lines 29-33). Thus, the keys required for generating the signature are resident on the customer computer at least for as long as they are needed to perform the encryption. Therefore claim 1 of the third auxiliary request does not define any additional features which are not already known from E1. Consequently, the argumentation presented with respect to lack of inventive step of claim 1 of the second auxiliary request applies equally to claim 1 of the third auxiliary request. Claim 1 is therefore not inventive (Article 52(1) EPC, Article 56 EPC 1973).

7.4 In addition, it is noted that the storage of private keys specifically on smart cards for use in authentication procedures during data transfer to the smart card is considered by the Board to be commonplace for the skilled person. In this respect, reference is made to section 8.2 of Rankl-Effing which indicates that the role of the smart card in a signature operation is rather straightforward: the RSA keys are stored on the card and are used to provide the signature.

8. **Fourth auxiliary request - inventive step:**

8.1 Claim 1 of the fourth auxiliary request differs from claim 1 of the third auxiliary request in that the "information" which is downloaded is defined as being an "application or applet".

8.2 As indicated by the opponent, the downloading of software is known from E1 (column 1, lines 22-25). Moreover, the prior art portion of the contested patent itself refers to the updating of smart cards to add new applications or to download applets (column 1, lines 54-58 of the patent specification, corresponding to page 2, lines 7-10 of the published application). This additional feature of claim 1 therefore adds nothing new to the subject-matter of the previous requests.

8.3 The patentee explained how the download scheme was intended to function. The applet could, for example, be a sky miles utility which was to be added to an existing American Express smart card. The applet did not have to be encrypted before transmission. The smart card had a public key associated with it which was stored on the card. Once the download of the applet was completed, an acknowledgement message was computed based on the downloaded information and the public key. This acknowledgement message was sent to the information owner who had a private key which enabled him to decode the acknowledgment and to verify the information. It was argued that this scheme - which enabled an information owner to ensure that what he gave a downloading party to download had actually been received by the smart card - had not been disclosed in E1.

8.4 The Board understands that it may have been the intention to define a novel and inventive downloading scheme, but notes that the assessment of inventive step is performed on the basis of the features actually defined in the independent claim, and not on an intended interpretation which does not find reflection in the defined features. As shown above, a feature-by-feature analysis of claim 1 shows that all features of claim 1 are either known from E1, are obvious or do not contribute to an inventive step. Thus, irrespective of what was intended, independent claim 1 of the fourth auxiliary request does not involve an inventive step (Article 52(1) EPC, Article 56 EPC 1973).

9. **Further auxiliary request - inventive step:**

9.1 Claim 1 of the "further auxiliary request" differs from claim 1 of the main request in that it is now defined that cryptographic keys are resident on the information device for generating the signature and that it is the *signature* which is computed as the verifiable acknowledgement.

9.2 The patentee agreed that these features do not add anything to the claimed subject-matter which has not already been discussed in connection with the previous requests. In particular, interpreting the word "signature" in the sense used in Rankl-Effing, i.e. in the sense of the entire encrypted message, the patentee agreed that the computation of the "signature" now defined in claim 1 is not distinguished from the computation of the verifiable acknowledgement defined in claim 1 of the previous requests.

9.3 Therefore, for the same reasons as presented above with regard to the third auxiliary request, claim 1 of the "further auxiliary request" also lacks an inventive step (Article 52(1) EPC, Article 56 EPC 1973).

10. **Apportionment of costs:**

10.1 Article 104(1) EPC 1973, applicable at the time of filing the request, sets out that each party to the opposition proceedings shall bear the costs it has incurred, unless the Opposition Division or Board of Appeal, for reasons of equity, orders a different apportionment of costs incurred during taking of evidence or in oral proceedings.

10.2 No reasons have been submitted by the appellant patentee which would justify a different apportionment of costs. In the present case the patentee simply indicated that he had to face travelling and accommodation expenses for two trips to Munich in order to attend the oral proceedings before the Opposition Division and the Board of Appeal. No arguments were provided for substantiating why equity would justify apportioning costs in favour of the appellant patentee. In the absence of any specific procedural behaviour from the opponent which could amount to an abuse of procedure, the Board notes that the opponent exercised a right recognised by the EPC when filing his opposition and then responding to the appeal, and the expenses borne by the patentee correspond to the expenses made necessary by exercising his defence in normal proceedings. Thus the Board sees no possible basis supporting the request for apportionment of costs.

Order

For these reasons it is decided that:

The appeal is dismissed.

The request for apportionment of costs is rejected.

The Registrar The Chairman

U. Bultmann H. Wolfrum