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) [ ] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 20 January 2010

Case Number:	T 0968/06 - 3.5.05
Application Number:	00912743.2
Publication Number:	1159662
IPC:	G06F 1/00
Language of the proceedings:	EN

Title of invention:
Smartcard user interface for trusted computing platform

Patentee:
Hewlett-Packard Company

Opponent:
Giesecke & Devrient GmbH

Headword:
Smartcard user interface/HEWLETT-PACKARD

Relevant legal provisions:
-

Relevant legal provisions (EPC 1973):
EPC Art. 56, 106, 107, 108

Keyword:
"Inventive step - (yes)"

Decisions cited:
J 0010/07

Catchword:
-

Case Number: T 0968/06 **-** 3.5.05

DECISION
of the Technical Board of Appeal 3.5.05 of 20 January 2010

Appellant:
(Opponent)

Giesecke & Devrient GmbH
Prinzregentenstr. 159
D-81677 München (DE)

Representative: -

Respondent:
(Patent Proprietor)

Hewlett-Packard Company
3000 Hanover Street
Palo Alto CA 94304-1112 (US)

Representative:

Roberts, Gwilym Vaughan
Kilburn & Strode LLP
20 Red Lion Street
London WC1R 4PJ (GB)

Decision under appeal: **Interlocutory decision of the Opposition Division of the European Patent Office posted 20 April 2006 concerning maintenance of European patent No. 1159662 in amended form.**

Composition of the Board:

Chairman: D. H. Rees
Members: P. Corcoran
P. Schmitz

Summary of Facts and Submissions

I. This appeal is against the interlocutory decision of the opposition division concerning the maintenance of the European patent No. 1 159 662 in amended form. The opponent, the present appellant, had filed an opposition requesting revocation of the patent in its entirety on the ground that the claims lacked an inventive step. The decision was announced in oral proceedings held on 3 February 2006 and written reasons were dispatched on 20 April 2006.

II. The following documents, with the numbering taken from the opposition proceedings were cited by the opponent in proceedings before the opposition division:

E1: EP 0 552 392 B;

E2: W. Rankl and W. Effing, "Handbuch der Chipkarten", pp.346-349, Carl Hanser Verlag, 1996, ISBN: 3-446-18893-2.

III. A notice of appeal from the appellant was received at the EPO on 20 June 2006 and a written statement setting out the grounds of appeal was received on 18 August 2006. The appeal fee was paid on 20 June 2006.

In the written statement setting out the grounds of appeal, the appellant requested that the decision under appeal be set aside and that the patent be revoked. A further document was cited by the appellant in support of its inventive step objections:

E3: DE 41 31 248 A.

The appellant submitted, in particular, that the independent claims 1, 27 and 29 did not comprise any features which involved an inventive step over E1, or over E1 combined with E2 or E3 (cf. statement of grounds: p.5, item IV).

The appellant also made a precautionary request for oral proceedings.

IV. In a letter dated 22 December 2006 and received at the EPO on the same date, the respondent (proprietor) requested that the appeal be dismissed and the patent be maintained as amended during opposition proceedings. The respondent also made a precautionary request for oral proceedings.

In its submissions, the respondent disputed that the security module mentioned in col.4 l.41 of E1 disclosed the monitoring component required by the claims. The respondent further submitted that, contrary to the finding of the opposition division, the security module of E1 was not a monitoring component configured to perform a plurality of data checks on the computing platform (cf. letter: Section entitled "Novelty", in particular second paragraph, p.3 and paragraph bridging p.3-4). The respondent further submitted that neither E1 nor E3 was prejudicial to the inventive step of the claimed invention (cf. letter: Section entitled "Inventive Step", p.7-8).

V. In a communication accompanying a summons to oral proceedings to be held on 20 January 2010, the board gave its preliminary opinion that the appeal was not allowable.

In particular, the board expressed the opinion that the terms "integrity challenge" and "integrity data" as used in claims 1 and 29 did not appear to have any commonly accepted meaning in the art and that it appeared necessary to interpret them in the light of the description (cf. item 6.1 of the communication).

The board further noted that it was inclined to concur with the respondent's submissions to the effect that the security module of E1 was not a monitoring component in the sense of claim 1 and that it was not inclined to concur with the appellant's submissions to the effect that the authentication procedure disclosed in E1 constituted an integrity challenge in the sense of said claim (cf. items 6.2 and 6.3 of the communication). The board further expressed its preliminary opinion that the cited prior art did not render the subject matter of the independent claims obvious (cf. item 7 of the communication).

VI. In its communication, the board made reference to the following excerpt from the textbook "Smart Card Handbook" by W. Ranke and W. Effing, the authorised English language translation of the German language textbook from which E2 is extracted:

E4: W. Rankl and W. Effing, "Smart Card Handbook", pp.246-250, pp.314-316, p.385-396, ISBN: 0-471-96720-3, John Wiley & Sons Ltd., 1997.

The board noted that, in its opinion, both E1 and E3 disclosed methods of mutual authentication between a smart card and a terminal based on a symmetric challenge-response procedure and that the use of such authentication procedures appeared to be generally known as evidenced by E4 (cf. item 8.3 of the communication). The board therefore expressed the view that it was legitimate in the given circumstances to draw a distinction between a conventional "authentication procedure" such as disclosed in E1 and E3 and an "integrity challenge" as disclosed in the patent in suit (cf. item 8.4 of the communication).

VII. The appellant responded to the board's preliminary opinion with a letter dated 22 December 2009, received at the EPO by telefax on 23 December 2009. In said letter, the appellant submitted, *inter alia*, that the successful execution of an authentication procedure confirmed not only the presence of a secret key but also the correct execution of a particular algorithm and on this basis could be considered to constitute an "integrity challenge" as recited in claim 1.

VIII. In its submissions during oral proceedings before the board the appellant further referred to E4, in particular the first paragraph on p.315 thereof, noting that the correct execution of a particular cryptographic algorithm might be carried out by "terminal software" outside the security module.

IX. At the oral proceedings the appellant confirmed its request that the decision under appeal be set aside and that the patent be revoked. The respondent confirmed its request that the appeal be dismissed.

X. Claim 1 of the patent as maintained during opposition proceedings reads as follows:

"A system of computing apparatus comprising:

> a computing platform (10) having a first data processor (21) and a first data storage means (22); and
> a token device (19, 1101) being physically distinct and separable from said computing platform (10),

characterised by said system further comprising

> a monitoring component (24) having a second data processor (30) and a second data storage means (3, 4) wherein said monitoring component (24) is configured to perform a plurality of data checks on said computing platform (10) and wherein the token device is also physically distinct and separable from said monitoring component; and
>
> wherein in one mode of operation, said token device (19, 1101) operates to make an integrity challenge to said monitoring component (24) and said token device (19, 1101) will not undertake specific actions of which it is capable unless it receives a satisfactory response to said integrity challenge."

Claim 27 of the patent as maintained during opposition proceedings reads as follows:

"A token device comprising a data processor and a memory device, said token device (19, 1101)

> configured to allow performance of at least one data processing or signaling function:
>
> characterised in that said token device (19, 1101) operates to:
>
> receive a request to perform said at least one data processing or signaling function from an element of a computing system;
> generate a request for integrity data from a monitoring component (24) in said computing system to confirm the integrity of the computing system;
>
> receive the integrity data from the monitoring component;
>
> if said integrity data supplied to said token device (19, 1101) is satisfactory, then said token device (19, 1101) allows a said function; and
>
> if said integrity data received by said token device (19, 1101) is unsatisfactory, then said token device (19, 1101) denies said function."

Claim 29 of the patent as amended and maintained during opposition proceedings reads as follows:

> "A method of obtaining verification of a state of a computer entity, said computer entity comprising a computer platform and a monitoring component (24), said method comprising the steps of:
> requesting access to a functionality from a token device (19, 1101);

in response to said request for access to functionality said token device (19, 1101) generating a request signal requesting integrity data from said monitoring component (24) to confirm the integrity of said computer platform;

in response to said request for integrity data, said monitoring component (24) reporting integrity data to said token device (19, 1101), said integrity data describing a result of a monitoring operation;
by receipt of a satisfactory said integrity data, said token device (19, 1101) offers said functionality; and
by receipt of an unsatisfactory said integrity data, said token device (19, 1101) denies said functionality."

XI. At the end of the oral proceedings the chairman announced the board's decision.

Reasons for the Decision

1. *Admissibility*

1.1 The appeal complies with the provisions of Articles 106 to 108 EPC 1973 which are applicable according to J 10/07, point 1 (cf. Facts and Submissions, item III above). Therefore it is admissible.

2. *The appellant's argumentation*

2.1 The appellant has submitted that all of the features of claim 1 are directly or indirectly known from E1 such that the claimed subject-matter does not involve an inventive step over E1 (cf. statement of grounds: p.4, l.18-20). Similar objections are raised in respect of claims 27 and 29 (cf. statement of grounds: p.4, l.22 et seq.). The appellant has further submitted that independent claims 1, 27 and 29 of the amended patent lack inventive step in the light of the disclosure of E1 in combination with E2 or E3 (cf. statement of grounds, p.5, section IV).

Details of the appellant's submissions in support of these objections are summarised below.

2.2 According to the appellant, the authentication procedure disclosed in E1 involves more than merely performing an identity check because the challenge-response procedure disclosed therein will fail in cases where the integrity of the terminal has been tampered with (cf. statement of grounds: paragraph bridging p.3-4 which refers, in particular, to col.5, l.43-48 of E1).

In this regard the appellant further submitted (cf. letter dated 22 December 2009: second paragraph, p.3) that according to E1 a successful authentication requires the presence of a terminal key ("Terminalschlüssel") representing "integrity data" and the correct execution of a cryptographic algorithm, i.e. the terminal function ("Terminalfunktion").

2.3 The appellant thus disputes the distinction drawn by the opposition division between checking identity and checking integrity and submits that in the context of E1 the checking of identity data also involves checking the integrity of the computer platform (cf. statement of grounds: p.4, l.22-29).

2.4 E2 was cited by the appellant in relation to claim 1 as evidence of common general knowledge in relation to the term "security module" ("Sicherheitsmodul") as used in E1 col.4, l.37 ff. (cf. notice of opposition: p.4, l.9-19) and, likewise, in relation to claim 27 as evidence of common general knowledge concerning token devices such as smart cards (cf. notice of opposition: p.5, l.10-14).

2.5 With respect to E3, referring in particular to col.1, l.51 ff. thereof, the appellant has argued that the authentication procedure disclosed therein provides a confirmation that the operation of the terminal has not been manipulated (cf. statement of grounds: p.4, l.4-7; letter dated 22 December 2009: second paragraph on p.3).

2.6 In the letter dated 22 December 2009, the appellant additionally referred to E4, in particular the first paragraph on p.247, in support of the assertion that the successful execution of an authentication procedure confirmed not only the presence of a secret key but also the correct execution of a particular algorithm (cf. letter dated 22 December 2009: final paragraph on p.3).

In its submissions during oral proceedings before the board the appellant further submitted that E4 supported its assertions in this regard in view of the reference to the modification of "terminal software" in the first paragraph on p.315 which indicated that the cryptographic algorithm associated with an authentication procedure might be executed by software residing outside the security module.

3. *The respondent's argumentation*

3.1 The respondent has submitted that E1, whether considered on its own or in combination with E2 or E3, is not prejudicial to the inventive step of the claimed invention (cf. letter of 22 December 2006, p.7, l.4 *et seq.*).

3.2 According to the respondent, E1 fails to disclose a "monitoring component" as recited in claim 1 because the security module disclosed in E1 does not provide equivalent functionality to the claimed "monitoring component" (cf. letter of 22 December 2006, p.3, l.5 *et seq.*).

In this regard, the respondent further submits that the authentication procedure or identity check disclosed in E1 is not a "data check" as recited in claim 1, i.e. a data check performed by a monitoring component on the computing platform (cf. letter of 22 December 2006, paragraph bridging p.3 and p.4).

3.3 The respondent further submits that E1 does not disclose a token device operating to make an integrity challenge or to generate a request for integrity data from a monitoring component, or any other component, of the system of E1 (cf. letter of 22 December 2006, p.3, l.18 *et seq.*).

3.4 As to E2, the respondent submits that the security module disclosed therein is not a monitoring component in the sense of the claimed invention (cf. letter of 22 December 2006, p.5, l.11 *et seq.*).

3.5 As to E3, the respondent argues that its disclosure does not represent common general knowledge and that, moreover, it merely discloses a security module and an authentication procedure substantially similar to that of E1. Thus, according to the respondent, said document fails to disclose a monitoring component and an integrity challenge in the sense of the claimed invention (cf. letter of 22 December 2006, p.5, l.30 *et seq.*)

4. *Claim 1*

4.1 It is common ground between the parties that E1 which relates to a method of mutual authentication between a smart card and a terminal using a challenge-response procedure represents the closest prior art to the subject-matter of claim 1. Furthermore, the respondent has not disputed that E1 discloses the features of the pre-characterising part of independent claim 1 as submitted by the opponent (cf. notice of opposition: Section III, p.3-4). Thus the matter in dispute is essentially the extent to which the features of the characterising part of the claim are rendered obvious by E1 alone or in combination with the other cited prior art.

4.2 The characterising part of claim 1 specifies the following features:

> (i) "a monitoring component (24) having a second data processor (30) and a second data storage means (3, 4) wherein said monitoring component (24) is configured to perform a plurality of data checks on said computing platform (10) and wherein the token device is also physically distinct and separable from said monitoring component."
>
> (ii) "wherein in one mode of operation, said token device (19, 1101) operates to make an integrity challenge to said monitoring component (24) and said token device (19, 1101) will not undertake specific actions of which it is capable unless it receives a satisfactory response to said integrity challenge."

4.3 The appellant's case is, in essence, based on the proposition that the security module disclosed in E1 is functionally identical or otherwise equivalent to a "monitoring component" within the meaning of claim 1 and that the authentication procedure of E1 is functionally identical or otherwise equivalent to an "integrity challenge" within the meaning of claim 1.

4.4 The respondent has disputed that the security module disclosed in E1 provides identical or equivalent functionality to the "monitoring component" of claim 1. The board concurs with the respondent's submissions on this point for the reasons which follow.

4.4.1 According to the appellant, the workstation CPU ("Rechnerstation CPU") of the embodiment of E1 illustrated in Fig.3 corresponds to a computing platform having a first data processor and a first data storage means as recited in claim 1 (cf. notice of opposition: Section III, paragraph bridging p.3-4).

4.4.2 The security module disclosed in E1 is evidently a trusted component which comprises a second data processor and a second data storage means, in particular when E1 is read in combination with the passage of E2 cited by the appellant (cf. 2.4 above). However, this merely establishes that the security module of E1 bears a similarity in structural terms to the "monitoring component" of claim 1 inasmuch as it is a trusted component comprising a second data processor and a second data storage means. This similarity in structural terms does not, however, establish an identity or equivalence in functional terms between the security module of E1 and the "monitoring component" of claim 1

The disclosure of E1 relating to the "security module" is not very detailed and does not appear to go beyond a statement to the effect that it is a component integrated into the terminal T in which the execution of the authentication procedure of Fig.1 takes place (cf. E1: col.2, l.32-36; col.4, l.37-41). In particular, there is no identifiable disclosure in E1 to the effect that the security module is configured to operate as a monitoring component which performs a plurality of data checks on the computing platform (i.e. on the workstation CPU or "Rechnerstation CPU" of Fig.3).

4.4.3 The board further notes in this regard that, in its judgement, the term "data checks" as used in relation to the monitoring component of claim 1 is to be interpreted in the given context in the light of the disclosure as denoting the operations performed by the trusted device in acquiring or collecting an "integrity metric" of the computing platform (cf. patent in suit: in particular [0043], [0071], [0136]). The execution of an authentication procedure involving the generation of authentication parameters in a secure module as disclosed in E1 does not, in the board's judgement, correspond to the performing of data checks on a computing platform by a monitoring component as specified in claim 1.

4.4.4 In view of the foregoing, the board concludes that the security module of E1 is neither identical nor equivalent to a monitoring component which is configured to perform a plurality of data checks on a computing platform as recited in claim 1.

4.5 The respondent has likewise disputed that the authentication challenge disclosed in E1 is identical or equivalent to an "integrity challenge" within the meaning of claim 1. The board also concurs with the respondent's submissions on this point for the reasons which follow.

4.5.1 The authentication challenge disclosed in E1 is a specific example of a generally known technique in the field of smart card systems as evidenced by E4 (see for example, 8.2 Authentication, in particular the introductory section on p.246-247 and 8.2.2 Mutual symmetric authentication, p.249-250). Such authentication procedures are based on the parties possessing shared secret knowledge which is examined via a procedure employing cryptographic algorithms. When a challenged party, e.g. the terminal, provides the correct response to a challenge from its counterpart, e.g. the smart card, this is taken as evidence that the challenged party is in possession of the shared secret knowledge, e.g. a cryptographic key. On this basis the challenged entity is considered to be "authentic" or "genuine" (cf. E4: p.246, first paragraph of Section 8.2 Authentication; Glossary, entry for "Authentication", p.386)

4.5.2 Insofar as can be determined on the basis of the available prior art, the term "integrity challenge" was not an established term of art at the claimed priority date. For this reason the board judges that it is appropriate to interpret the term in the light of the description as denoting a procedure designed to allow a challenging entity, e.g. a smart card, to verify the correct functioning of the computing platform on the basis of an "integrity metric" (cf. patent in suit: in particular [0043], [0074]-[0081] and [0147]).

In this context, the expression "integrity metric" denotes data which is used to verify that the computing platform is functioning correctly, said data having been obtained by monitoring the operation of the computing platform (cf. patent in suit: [0043]). If the data supplied in response to the "integrity challenge" has an expected value, then it may be assumed that the computing platform is operating correctly and further data exchange between the challenging entity, i.e. the smart card, and the computing platform is permitted to proceed, (cf. patent in suit: [0012]; [0054]-[0055]).

An "integrity challenge" in the sense in which this term is used in the patent in suit is not based on verifying possession of shared secret knowledge using cryptographic algorithms as in the case of an authentication challenge but rather it involves verifying that a set of data collected from a computing platform, i.e. the "integrity metric", has an expected value thereby providing confirmation that the computing platform is operating correctly.

4.5.3 In the given circumstances, the board finds that it is appropriate to draw a distinction between an authentication challenge as disclosed in E1 and an "integrity challenge" as disclosed in the patent in suit.

The purpose of an authentication challenge as disclosed in E1 is to provide mutual proof of identity between a trusted token (e.g. a smart card) and a trusted component thereby, in the words of the patent in suit, establishing trust between the trusted token and the trusted device (cf. patent in suit: [0117], col.23, l.57 - col.24, l.2).

The purpose of the "integrity challenge" disclosed in the patent in suit is to permit verification that the computer platform inside the computing entity is operating correctly by virtue of integrity metrics measurement carried out on the computer platform by the trusted component (cf. patent in suit: [0116], col.23, l.43-46) thereby establishing trust in the computer platform (cf. patent in suit: [0117], col.24, l.3-6).

The board further notes in this regard that the authentication challenge issued by the token device in E1 forms part of a bilateral procedure whose purpose is the mutual authentication of two parties, i.e. the token device and the terminal. In contrast the integrity challenge of the patent in suit is essentially a unilateral procedure inasmuch as one party (i.e. the token device) attempts to confirm the integrity of another (i.e. the computing platform) via a trusted device (i.e. the monitoring component). The computing platform does not issue a corresponding integrity challenge to the token device.

4.5.4 In view of the foregoing, the board concludes that the authentication challenge disclosed in E1 is neither identical nor equivalent to an "integrity challenge" within the meaning of claim 1.

4.6 The subject-matter of claim 1 is thus distinguished over E1 in that it specifies a monitoring component which performs a plurality of data checks on the computing platform (cf. 4.4 above) and further specifies that the token device operates to make an integrity challenge to the monitoring component (cf. 4.5 above). These distinguishing features solve the technical problem of permitting the user of the token device to verify the integrity of the computing platform, i.e. to verify that the correct operation of the computing platform has not been subverted.

5. *Observations relating to E2 and E3*

5.1 With respect to E2, it is noted that the passage of this document cited by the appellant in relation to claim 1 (cf. 2.4 above) establishes a structural similarity between the security module of E1 and the "monitoring component" of claim 1. The existence of such a structural similarity does not, however, suffice to establish a functional equivalence between these two entities (cf. observations under 4.4 above). In the board's judgement, E2 neither suggests nor otherwise renders obvious the provision of a monitoring component as recited in claim 1. Neither does it contain any identifiable teaching relating to the provision of an "integrity challenge" within the meaning of claim 1.

5.2 With respect to E3, it is noted that this document discloses a further example of a mutual authentication procedure similar to that of E1 (cf. E3 col.1, l.57 - col.2, l.10; col.2, l.48-68). The observations made under 4.5 above concerning the distinction between an "integrity challenge" as recited in claim 1 and an authentication challenge as disclosed in E1 apply *mutatis mutandis* to E3.

6. *Further observations concerning the appellant's submissions*

6.1 The appellant has submitted, in relation to E1 and likewise in relation to E3, that the authentication procedures disclosed in said documents involve more than just the checking of identity data. The appellant has also referred to E4, in particular the first paragraph on p.247 in support of this assertion. According to the appellant, the successful execution of an "authentication challenge" requires not only the possession of shared secret knowledge but also the correct execution of a cryptographic algorithm.

The appellant has further argued that the reference to the modification of "terminal software" in the first paragraph on p.315 of E4 indicates that the cryptographic algorithm may be executed by software residing outside the security module (cf. 2.6 above).

On this basis, the appellant has submitted that the correct execution of a cryptographic algorithm, in particular by software residing outside the security module, would effectively permit the user of the token device to verify the integrity of the computing platform.

6.2 The appellant's submissions in this regard effectively amount to an assertion that an authentication challenge as disclosed in E1, E3 and E4 is functionally identical or otherwise equivalent to an "integrity challenge" as recited in claim 1. As discussed in 4.5 above, the board finds that it is appropriate in the given circumstances, to draw a distinction between the type of authentication procedure disclosed in the cited prior art documents and an "integrity challenge" as disclosed in the patent in suit.

6.3 It is further noted that although the appellant is in principle correct in stating that the successful execution of an authentication procedure such as disclosed in E1 indicates that the cryptographic algorithm on which the authentication procedure is based has been correctly executed, this does not, in the board's judgement, amount to a verification of the integrity of the computing platform, i.e. providing confirmation that the computing platform is functioning correctly and has not been subverted.

According to E1, the cryptographic algorithm is to be executed inside the security module (cf. E1: col.4, l.37-41). In this case, it is self-evident that its correct execution inside the security module would not allow any inference to be made about the integrity of the computing platform (i.e. the workstation CPU of E1).

Even if the system of E1 were to be modified to have the cryptographic algorithm executed by software residing outside the security module, e.g. on the workstation CPU of E1, its correct execution would merely indicate that this particular algorithm had not been tampered with. In the board's judgement, an indication that a single cryptographic algorithm has executed correctly does not amount to providing a verification of the integrity of the computing platform. The fact that the cryptographic algorithm executes correctly does not exclude the possibility that the integrity of the underlying processing environment has been subverted, e.g. at hardware, BIOS or operating system level (cf. patent in suit [0071], [0078]).

7. In view of the foregoing, the board concludes that the appellant has failed to establish that the distinguishing features of claim 1 over E1 (cf. 4.6 above) are either disclosed by or derivable in an obvious manner from E1 itself or that they are rendered obvious by E1 in combination with E2 or E3. In the board's judgement none of the cited documents teaches or suggests a solution to the stated technical problem which would lead the skilled person to arrive at the subject matter of claim 1.

8. *Claims 27 and 29*

8.1 With reference to claims 27 and 29, the board judges that the term "monitoring component" used in said claims should be interpreted in the light of the disclosure in substantially the same manner as in the case of claim 1 (cf. observations under 4.4 above).

8.2 The board further judges that the term "integrity data" used in said claims is to be interpreted in the light of the disclosure as denoting data relating to an "integrity metric" which is used to verify the correct functioning of the computing platform (cf. observations under 4.5 above, in particular 4.5.2).

8.3 On the basis of the observations made in respect of claim 1 under 4. - 7. above, the board finds that the appellant has also failed to establish that the cited prior art is prejudicial to the inventive step of independent claim 27 or independent claim 29.

9. The board concludes that the appellant has not succeeded in establishing that the subject-matter of the independent claims as amended during opposition proceedings lacks an inventive step. The appeal must therefore be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

R. Schumacher D. H. Rees