

**Internal distribution code:**

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

**Datasheet for the decision  
of 4 July 2014**

**Case Number:** T 2355/09 - 3.5.06

**Application Number:** 03737312.3

**Publication Number:** 1472589

**IPC:** G06F1/00

**Language of the proceedings:** EN

**Title of invention:**  
SUPPORT FOR MULTIPLE LOGIN METHODS

**Applicant:**  
ACTIVCARD IRELAND LIMITED

**Headword:**  
Multiple login methods/ACTIVCARD

**Relevant legal provisions:**  
EPC 1973 R. 86(3), 35(13)  
EPC R. 137(3), 116(1)  
EPC Art. 78(1)(c)  
EPC 1973 Art. 84, 56

**Keyword:**  
Substantial procedural violation - (no)  
Inventive step - (no)

**Decisions cited:**  
G 0007/93, T 0937/09, T 0690/09, T 0996/12, T 0573/12,  
T 0343/08, T 0246/08

**Catchword:**



**Beschwerdekammern  
Boards of Appeal  
Chambres de recours**

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

Case Number: T 2355/09 - 3.5.06

**D E C I S I O N  
of Technical Board of Appeal 3.5.06  
of 4 July 2014**

**Appellant:** ACTIVCARD IRELAND LIMITED  
(Applicant) 30 Herbert Street  
Dublin 2 (IE)

**Representative:** Vienne, Aymeric Charles Emile  
Mathys & Squire LLP  
The Shard  
32 London Bridge Street  
London SE1 9SG (GB)

**Decision under appeal:** **Decision of the Examining Division of the  
European Patent Office posted on 16 July 2009  
refusing European patent application No.  
03737312.3 pursuant to Article 97(2) EPC.**

**Composition of the Board:**

**Chairman** D. Rees  
**Members:** A. Teale  
C. Heath

## Summary of Facts and Submissions

I. The appeal is against the decision of the examining division, the reasons for which were dispatched on 16 July 2009, to refuse European patent application No. 03 737 312.3 on the basis that the main request and the auxiliary request were not admissible, Rule 137(3) EPC, and that consequently there were no claims on file, Article 78(1)(c) EPC.

II. The main request, received on 26 May 2009, the final date for making submissions and/or amendments under Rule 116 EPC, was not admitted by the examining division because amended claim 1 was a combination of previous claim 1 with features of previous dependent claim 6 which had been indicated in the summons to oral proceedings as not being inventive, Article 56 EPC, over the following prior art document:

D1: US 6 052 468 A

and thus did not overcome the objections raised in the summons. Instead the request gave rise to new objections, since amended claim 11 introduced added subject-matter, Article 123(2) EPC.

III. The first auxiliary request, submitted during the oral proceedings held on 23 June 2009, was also not admitted, as amended claim 1 *prima facie* did not overcome the clarity objections, Article 84 EPC, raised in previous communications, did not overcome the inventive step objections, Article 56 EPC, and introduced new objections.

- IV. A notice of appeal was received on 28 September 2009, the appeal fee being paid on the same day. The appellant requested that the decision be set aside and a patent be granted on the basis of the claims, description and drawings on file. The appellant also made an auxiliary request for oral proceedings.
- V. In a statement of grounds of appeal, received on 26 November 2009, the appellant reiterated the requests on file. The appellant further made several allegations of procedural violations by the examining division.
- VI. The board issued a summons to oral proceedings, giving in an annex its preliminary opinion that the allegations of procedural violation were not well-founded. The board was also inclined to admit the requests on file, but expressed doubts whether the application complied with Article 84 and Rule 35(13) EPC 1973 regarding clarity and consistency of terminology, Article 123(2) EPC regarding added subject-matter and Article 54(1) and (2) EPC 1973 regarding novelty, the closest prior art document D1 being closer to the claimed subject-matter than stated in the appealed decision, even prejudicing novelty.
- VII. In a letter dated 4 June 2014 the appellant submitted amended claims according to a main and first, second and third auxiliary requests, amended pages 3a, 4 and 9 of the description according to all requests, amended page 6 of the description and amended drawing sheet 2 according to the first and third auxiliary requests. In a letter dated 5 June 2014 the appellant submitted a marked up copy of amended page 9 of the description.

- VIII. On 16 June 2014 the appellant's representative telephoned the rapporteur to ask whether he had any questions or comments on the amendments received on 4 June 2014 which might avoid the need for oral proceedings. The rapporteur informed him that the board had no questions or comments and that the date for oral proceedings was maintained.
- IX. On 2 July 2014 the appellant's representative telephoned the rapporteur to inform him that the appellant would not be attending the oral proceedings. A written confirmation was received on the same day.
- X. Oral proceedings were held on 4 July 2014 in the absence of the representative, as announced. At the end of the oral proceedings the board announced its decision.
- XI. The appellant requests that the decision be set aside and a patent be granted on the basis of claims 1 to 6 of the main request, claims 1 to 6 of the first auxiliary request, claims 1 to 6 of the second auxiliary request, or claims 1 to 6 of the third auxiliary request, all filed with the letter of 4 June 2014.

The current description and drawings of the application on file are as follows:

Description:

Pages 1, 2, 5, 7 and 8, as originally filed (all requests).

Page 3, as received on 5 May 2008 (all requests).

Page 3a, 4 and 9, as received on 4 June 2014 (all requests).

Page 6, as originally filed (main and second auxiliary requests).

Page 6, as received on 4 June 2014 (first and third auxiliary requests).

Drawings:

Sheets 1 and 3, as originally filed (all requests).

Sheet 2, as originally filed (main and second auxiliary requests).

Sheet 2, as received on 4 June 2014 (first and third auxiliary requests).

XII. Claim 1 of the main request reads as follows:

"A method of encoding stored data on a computer system, the method comprising:  
receiving at least one of several different password data at the computer system;  
transforming an encryption key with each of the at least one of the several different password data in a reversible fashion to produce at least one of several different encoded encryption keys such that the one of the several different password data is required in order to perform a reverse transform and extract the encryption key from the at least one of several different encoded encryption keys;  
storing on the computer device the at least one of the several different encoded encryption keys such that the one of the several different password data and one of a plurality of user authorization processes, in combination, provide access to the encryption key, wherein the user authorization process is a biometric information verification process, wherein the encryption key is encoded with each of the several

different password data to provide different encoded encryption keys such that a combination of one of the plurality of the user authorization processes and a respective password data of the several different password data allows for retrieval and decoding of the encryption key, and wherein the encryption key is for performing at least one of encrypting and decrypting the stored data on the computer system; and encoding stored data on the computer system into encoded data with the encryption key."

The claims according to this request also comprise an independent system claim 4.

XIII. The claims of the first auxiliary request are identical to those of the main request.

XIV. Claim 1 of the second auxiliary request reads as follows:

"A method of encoding stored accessible data on a computer system, said method comprising the steps of: providing at least one of a plurality of different password data for a user to the computer system; transforming an encryption key with each one of said plurality of different password data into various encoded versions of the encryption key, said transforming being done in a reversible fashion allowing reverse transformation and extracting of the encryption key at a later time using said one of several different password data, wherein the one of the several different password data is required in order to perform the reverse transformation and extracting; storing on the computer system the various encoded versions of the encryption key such that a biometric user authentication process in combination with one of



several password data login procedures provide access to the encryption key, wherein said encryption key is stored for said user in the various encoded versions to allow a successful login combination of the biometric user authentication process in combination with the one of the several password login procedures to successfully decode one of said various encoded versions of said encryption key, thereby allowing flexibility for the user for the login combination; and encoding accessible data stored on the computer system into encoded data with the encryption key, wherein the encryption key is further for decoding of the encoded data to obtain said accessible data."

The claims according to this request also comprise an independent system claim 6.

- XV. The claims of the third auxiliary request are identical to those of the second auxiliary request.

### **Reasons for the Decision**

1. *The admissibility of the appeal*

In view of the facts set out as points I, IV and V above, the appeal is admissible, since it complies with the EPC formal admissibility requirements.

2. *Allegations of procedural violations*

2.1 The board finds that the allegations of procedural violations made in the statement of grounds of appeal are unfounded.

2.2 According to G 7/93 (OJ EPO 1994, 775; see point 2.6 of the reasons), if an examining division has exercised its discretion under Rule 86(3) EPC 1973 (corresponding to Rule 137(3) EPC) against an applicant in a particular case and the applicant files an appeal against the way in which such discretion was exercised, it is not the function of a board to review all the facts and circumstances of the case as if it were in the place of the first instance department, in order to decide whether or not it would have exercised such discretion in the same way as the first instance department. If a first instance department is required under the EPC to exercise its discretion in certain circumstances, such a department should have a certain degree of freedom when exercising that discretion, without interference from the boards of appeal. In the circumstances of a case such as that before the referring Board, a board of appeal should only overrule the way in which a first instance department has exercised its discretion if it comes to the conclusion either that the first instance department in its decision has not exercised its discretion in accordance with the right principles or that it has exercised its discretion in an unreasonable way.

2.3 Rule 137(2) EPC gives the applicant the right to amend the application once of its own volition in response to specified communications by the EPO. According to Rule

- 137(3) EPC, no further amendment may be made without the consent of the examining division.
- 2.4 In the present case the appellant had already amended the claims on file once in reply to the communication by the EPO dated 11 September 2006. Thus the admittance of any new request lay within the discretion of the examining division, Rule 137(3) EPC. The division was of the opinion that admitting the main request would give rise to a new objection under Article 123(2) EPC without overcoming the objections set out in the summons. Hence it decided not to admit the main request into the procedure.
- 2.5 The division then gave the appellant the opportunity to draft and file a new request during the oral proceedings. The new request was then also not admitted, as it would *prima facie* not have overcome the clarity objections reiterated in all communications from the examining division, these objections not being addressed by the appellant at any point in the first instance procedure. The new request would also not have overcome the inventive step objection raised during the oral proceedings (see points II.2.2 to II.2.5 in the decision).
- 2.6 Thus, in the view of the the board, the division exercised its discretion under Rule 137(3) EPC in accordance with the right principles for both requests.
- 2.7 The fact that the appellant filed the main request before the final date foreseen by Rule 71a EPC 1973 (corresponding to Rule 116(1) EPC) does not mean that the examining division had no discretion under Rule 137(3) EPC (see T 937/09, point 3.5 of the reasons).

- 2.8 The board further does not accept the appellant's argument that the examining division should have decided upon the last set of admitted claims upon non-admission of the new requests. A non-admittance under Rule 137(3) EPC does not automatically revive the previous set of claims that the examining division had consented to admit, unless the applicant has indicated that it was relying on these as an auxiliary request (See T 690/09, point 8 of the reasons). On the contrary, submitting a new main request automatically leads to the replacement and, in legal terms, to the withdrawal of any previous main requests (see T 996/12, point 4 of the reasons; T 573/12, point 3.6 of the reasons).
- 2.9 Concerning the appellant's argument that the decision and minutes are silent about the appellant's numerous suggestions in the oral proceedings to delete claim 11 in order to address the examining division's objection under Article 123(2) EPC, the board observes that the appellant was given an opportunity to prepare and file an auxiliary request during the oral proceedings (see the minutes, page 3, penultimate paragraph, and points 10 and 13 of the summary of facts and submissions and point 2 of the reasons of the decision). Thus, had the appellant intended to obtain a decision of the examining division on an alternative set of claims without claim 11, it did have the opportunity to file such a request. It apparently decided not to do so.
- 2.10 Furthermore there is no general duty for an examining division to provide feedback to an applicant's reply to a summons to oral proceedings in advance of the oral proceedings (see T 343/08, point 4.2.3 of the reasons).

2.11 Concerning the appellant's criticism with regard to the use of Article 78 EPC as a legal basis for the refusal, the board finds that, as stated in point 5 of the reasons in T 246/08 (cited by the examining division in point 4 of the reasons for the appealed decision), the requirement under Article 78(1)(c) EPC 1973 (that a European patent application have one or more claims) "is a requirement of the application not only for according a filing date, but also for [...] grant".

2.12 Hence the board finds that the examining division did not commit any procedural violations.

3. *The context of the invention*

The application relates to a method of improving the security of data symmetrically encrypted with an encryption key by requiring authorization (paragraphs [0036] and [0037]) through the combination of a biometric user authentication method (figure 2b, 24; figure 3) and a password or token based user authentication method (figure 2b, 23) for its decryption (figure 2b, 26). For this purpose the key used for encryption is encrypted using the user's password and stored only in its encrypted form. The password is hashed and stored only as a hashed password (paragraphs [0030] and [0031]). Thus a hacker tampering with the system can only access biometric templates, encrypted keys and hashed passwords (paragraph [0032]). To decrypt the encrypted data, the user first obtains authorization by a biometric identification method (page 8, lines 7 to 11), typically on a fingerprint scanner (page 8, lines 21 to 22), to access the encrypted key (page 8, lines 26 to 29). To decrypt the key the user enters the password used to encrypt the

key. Only then is the key decrypted and becomes available to decrypt the encrypted data (page 8, line 29, to page 9, line 1). Instead of a password, a security token such as a smart card, a PCMCIA card or a chip can also be used (paragraph [0034]). The biometric identifier provided by the user can be a fingerprint, palmprint, toeprint or retina, voice or behavioural characteristics, such as handwriting or keystroke timing (page 8, lines 21 25, and page 9, lines 8 to 11). To provide flexibility in login options through different combinations of biometric authentication methods and password or token based authentication methods, the key is encrypted in multiple versions for each one of the available password or token based methods (paragraph [0038]).

4. *The admittance of the requests*

The main and first to third auxiliary requests on file were submitted in reply to the board's summons to oral proceedings and hence, according to Article 13(1) RPBA (Rules of Procedure of the Boards of Appeal; see OJ EPO 2007, 536), the board has a discretion whether or not to admit them into the proceedings. Given that the amendments to the claims address the board's objections under Article 84 and Rule 35(13) EPC 1973 raised in the annex to the summons and thus constitute an improved basis for assessing the compliance of the application with the requirements of the EPC, all requests are admitted into the procedure.

5. *Clarity and consistency of terminology, Article 84 and Rule 35(13) EPC 1973*
- 5.1 In the annex to the summons to oral proceedings the board identified different meanings that the terms "key data" and "data key" seem to have in different passages of the application and raised objections under Rule 35(13) EPC 1973, regarding inconsistent terminology throughout the application, and under Article 84 EPC 1973, regarding the clarity of the claims.
- 5.2 The appellant indicated in its letter of 4 June 2014 (page 3, section "**Article 84 Data key**") that the terms "key data" and "data key" were used synonymously in the application, but agreed that these terms referred on some occasions to "password data" and on some occasions to "encryption key". The appellant, however, considered, on each occasion, the applicable meaning to be clear for the person skilled in the art. Nevertheless the claims were amended to address the issues raised by the board.
- 5.3 Although it is doubtful whether the applicable meaning of the terms "key data" and "data key" would be clear to the skilled person "on each occasion" throughout the specification, the board is satisfied that the skilled person would understand the disclosure of the application without undue burden despite the ambiguity in terminology. The board is further satisfied that the claims of all requests are clear enough to constitute a basis for assessing novelty and inventive step. In particular, in amended claims of the requests on file, *inter alia*, the ambiguous terms "key data" and "data key" have been replaced with the terms "encryption key" and "password data".

6. *Document D1*

D1 concerns a method of securing a cryptographic key (column 5, line 35), allowing its portability between systems supporting different user authentication methods (column 6, lines 20 to 24) such as biometric (column 6, line 28; column 7, lines 31 to 33), password-based (column 6, line 30; column 7, lines 34 to 35) and token-based user authentication methods (column 6, line 30; column 7, line 35). The cryptographic key is secured by encrypting it with another cryptographic key (column 6, lines 41 to 43) which may be derived from a password (column 6, lines 48 to 49) which is hashed (column 8, lines 46 to 47). The biometric user authentication method can be a fingerprint, a voiceprint, a face, a palm print and a retinal scan (column 6, lines 27 to 30; column 7, lines 31-33). To enable access to the system with different combinations of user authentication methods in a particular (column 7, lines 55 to 56) or in an arbitrary order (column 7, lines 59 to 60), the cryptographic key is secured either in the given order (column 7, lines 57 to 59) or using all necessary permutations of securing operations (column 7, lines 42 to 52; column 7, lines 59 to 62). Such successive securing and re-securing of the cryptographic key can be done using any number of authentication methods (column 8, lines 29 to 31 and 38 to 43).

7. *The allowability of the main request*

7.1 Claim 1 uses the term "password data" to refer to passwords, i.e. a string of characters known only to the user, as well as to secrets stored on security tokens such as smart cards. This is evident from



dependent claims 2 and 3 which cover respectively a method wherein "receiving one of several different password data comprises receiving a password" and a method wherein "receiving one of several different password data comprises receiving information stored on a smart card" (underlining added by the board), from paragraph [0034] of the description which states that, instead of a password, values originating from a smart card or other possessions such as digital keys, PCMCIA cards and chips can be used, and finally from paragraph [0038] of the description which explicitly uses the term "password data" of claim 1 in line 7 to refer to "a password or a smart card" of the previous sentence providing several examples of combinations of login methods wherein one of the methods in each example is a biometric authentication method (fingerprint, retina, voice, typing interval data) and the others are either a password or a token-based authentication method (password, smart card, password and digital key, password and smart card).

7.2 In view of the above analysis of D1 and the interpretation of the term "password data" used in the claims, the subject-matter of claim 1 differs from the disclosure of D1 in that its method requires the combination of a biometric user authentication method with a non-biometric user authentication method, i.e. either a password or a token, such as a smart card, to access the encryption key. D1 discloses a more flexible system in which any number of authentication methods selected from a plurality of biometric or non-biometric authentication methods, such as password or physical key, could be combined. There is no such requirement that one of the authentication methods be a biometric method and the other one a password- or token-based

method. The board however considers this requirement to be a straightforward design decision that the skilled person would take without an inventive step, Article 56 EPC 1973.

- 7.3 The board does not accept the appellant's view that the method of D1 only teaches using one authentication process, either password-based or biometric, but does not teach combining them. D1 teaches successively combining authentication methods in any number, in particular in column 6, line 66, to column 7, line 64, and column 8, lines 27 to 43. D1 also explicitly discloses combining "password and biometric security" in column 7, lines 14 to 16.
- 7.4 The appellant has argued that D1 teaches away from using biometric methods because biometric methods are costly and limit portability, referring to column 3, lines 18 to 23, column 5, lines 19 to 21 and lines 26 to 28. The board disagrees. The cited passages discuss the background art and make statements on the cost and availability of biometric devices. Elsewhere, for instance column 6, lines 27 to 30, column 7, lines 3 to 6, line 15, lines 31 to 33, and column 8, lines 3 to 6, D1 consistently mentions biometric authentication methods such as fingerprint, voiceprint, facial features, palm print and retinal scan when listing the possible authentication methods that the user can select from.
- 7.5 The appellant has argued that in D1 the encryption keys are stored in key data files, sometimes on a server or database, but not on the computer system storing the data to be encrypted. The board does not accept that the storage of keys in a file can be interpreted as

their not being stored on the computer system. Moreover D1 explicitly states in column 6, lines 40 to 41, that the key data file is stored on the system.

7.6 The board also cannot accept the argument of the appellant that D1 does not disclose encrypting data stored on the computer using the encryption key, as it merely discusses securing of encryption keys and not their use. In the board's view, it is implicit in the overall context of D1 that the encryption keys are at some stage used for their basic purpose, namely to encrypt data.

7.7 The board concludes that the subject-matter of claim 1 of the main request does not involve an inventive step, Article 56 EPC 1973.

8. *The allowability of the first auxiliary request*

8.1 The claims of the first auxiliary request are identical to those of the main request. The first auxiliary request differs from the main request in clarifying amendments to some occurrences of the ambiguous term "key data" on page 6 of the description and in figure 2a. As these amendments to the specification do not change the board's understanding of the claims, the same objections as for claim 1 of the main request apply to claim 1 of the first auxiliary request.

8.2 Thus the subject-matter of claim 1 of the first auxiliary request also lacks an inventive step, Article 56 EPC 1973.

9. *The allowability of the second auxiliary request*

9.1 Although claim 1 of the second auxiliary request is phrased differently from those of the main and first auxiliary requests, the board could not identify any features which could distinguish its subject-matter from that of claim 1 of those requests. Therefore the same objections as for claim 1 of the main request apply to claim 1 of the second auxiliary request.

9.2 Thus the subject-matter of claim 1 of the second auxiliary request also lacks an inventive step, Article 56 EPC 1973.

10. *The allowability of the third auxiliary request*

10.1 The claims of the third auxiliary request are identical to those of the second auxiliary request. The third auxiliary request differs from the second auxiliary request, as the main from the first auxiliary request, in clarifying amendments to some occurrences of the ambiguous term "key data" on page 6 of the description and in figure 2a. Therefore the same objections as for claim 1 of the second auxiliary request apply to claim 1 of the third auxiliary request.

10.2 Thus the subject-matter of claim 1 of the third auxiliary request also lacks an inventive step, Article 56 EPC 1973.

**Order**

**For these reasons it is decided that:**

The appeal is dismissed.

The Registrar:

The Chairman:



B. Atienza Vivancos

D. Rees

Decision electronically authenticated