**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 August 2016

**Case Number:** T 1321/11 - 3.5.06

**Application Number:** 07812335.3

**Publication Number:** 2038801

**IPC:** G06F21/00, G06F21/20

**Language of the proceedings:** EN

**Title of invention:**
METHOD AND SYSTEM FOR AUTHENTICATING AN ACCESSORY

**Applicant:**
APPLE INC.

**Headword:**
Authenticating an accessory/APPLE

**Relevant legal provisions:**
EPC 1973 Art. 56

**Keyword:**
Inventive step - after amendment

**Decisions cited:**
T 0641/00, T 0258/03



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

**Catchword:**



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

Europäisches Patentamt
European Patent Office
Office européen des brevets

**Beschwerdekammern**
**Boards of Appeal**
**Chambres de recours**

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

**Case Number: T 1321/11 - 3.5.06**

# D E C I S I O N
# of Technical Board of Appeal 3.5.06
# of 4 August 2016

| | |
|---|---|
| **Appellant:** (Applicant) | APPLE INC.<br>1 Infinite Loop, M/S:3-Pat<br>Cupertino, CA 95014 (US) |
| **Representative:** | Lang, Johannes<br>Bardehle Pagenberg Partnerschaft mbB<br>Patentanwälte, Rechtsanwälte<br>Prinzregentenplatz 7<br>81675 München (DE) |
| **Decision under appeal:** | **Decision of the Examining Division of the European Patent Office posted on 11 January 2011 refusing European patent application No. 07812335.3 pursuant to Article 97(2) EPC.** |

**Composition of the Board:**

| | |
|---|---|
| **Chairman** | W. Sekretaruk |
| **Members:** | A. Teale |
| | M. Müller |

## Summary of Facts and Submissions

I. This is an appeal against the decision, dispatched with reasons on 11 January 2011, by the examining division to refuse European patent application No. 07 812 335.3 on the basis that the subject-matter of claim 1 according to a main and a first auxiliary request lacked inventive step in view of the following document:

D1: US 6 697 944 B1

and that the subject-matter of claim 1 according to a second auxiliary request extended beyond the content of the application as originally filed, contrary to Article 123(2) EPC, and also lacked clarity and support, Article 84 EPC.

II. A notice of appeal was received on 14 February 2011 in which the appellant requested that the decision be set aside and a patent granted. Oral proceedings were requested as an auxiliary measure. The appeal fee was paid on the same day.

III. With a statement of grounds of appeal, received on 23 May 2011, the appellant refiled, as a new main request, the main request forming the basis of the decision and requested that the decision be set aside and a patent granted on the basis of the new main request. The appellant reiterated the auxiliary request for oral proceedings.

IV. In an annex to a summons to oral proceedings the board expressed doubts as to the clarity of claim 1, Article 84 EPC 1973, and as to whether its subject-matter

involved an inventive step, Article 56 EPC 1973, in view of D1.

V. With a response received on 4 July 2016 the appellant submitted amended claims according to auxiliary requests I, II and III. The appellant requested that the decision be set aside and a patent granted on the basis of the main request or one of auxiliary requests I, II and III.

VI. In the oral proceedings, held on 4 August 2016, the appellant filed a new main request, comprising amended claims and an amendment to the description, and requested that the decision under appeal be set aside and that a patent be granted in the following form:

Description pages 1, 1a, 12 and 13, all dated 1 September 2009,
2, dated 4 August 2016, and
3 to 11, as originally filed.

Claims 1 to 12, dated 4 August 2016.

Drawings, sheets 1 to 12, as originally filed.

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

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

"A method of authentication of an accessory (502, 506, 508, 510) by a media player (500"), the method comprising: receiving, by the accessory, an authentication request from the media player (500"), the authentication request initiating an authentication operation

transmitting, by the accessory, an authentication information to the media player (500"), in response to the authentication request, the authentication information being usable by the media player (500") in the authentication operation; allowing the accessory, by the media player, to access an application of the media player during the authentication operation; and transmitting, by the accessory, an authentication signature to the media player (500") for validation, wherein the authentication operation completes upon validation of the authentication signature, wherein if the authentication operation fails, the media player prevents the accessory (502, 506, 508, 510) from any further access to the application of the media player (500")."

The claims according to the main request also comprise an independent claim 11 to a computer program for authentication of an accessory with a media player, wherein the program enables the media player to perform the method steps performed by the media player according to any one of claims 1 to 9, and an independent claim 12 to a system comprising a media player and an accessory, wherein the system is configured to perform the method of authentication as claimed in any of the claims 1 to 9.

## Reasons for the Decision

1. The admissibility of the appeal

In view of the facts set out at points I to III above, the appeal fulfils the admissibility requirements under the EPC and is therefore admissible.

2. Technical summary of the invention

2.1 The application relates to authenticating an accessory, for example a car or home stereo system, connected to a media player such as an "iPod"; see paragraph [0021]. The accessory interacts with an application of the media player using an accessory protocol, for instance the iPod Accessory Protocol (iAP); see page 7, lines 11 to 15. Details of the commands of the accessory protocol, for example those used to transfer information between the media player application and the accessory, are typically freely available to accessory developers.

2.2 In order to prevent the accessory protocol from being used by unauthorized or counterfeit accessories, the media player performs a two-step authentication operation (see below) on the accessory; see page 1, lines 28 to 30, and paragraph [0008]. The description acknowledges a prior art authentication method in which the media player blocks access by the accessory until the entire authentication operation has completed; see paragraphs [0002] to [0005] and [0049]. The invention adopts a different approach: the media player initially allows the accessory to access an application of the media player during the authentication operation and, only if the authentication operation fails, does the media player prevent further access by the accessory. This approach has the advantage that the media player and accessory can interact immediately, avoiding the need to wait until the authentication process has completed successfully. This advantage comes however at a price: accessories which subsequently fail authentication are nevertheless initially allowed to access the application of the media player, albeit only

until the authentication operation fails, and further access is then prevented.

2.3 The authentication operation according to the invention, illustrated in figures 6 and 7, includes, in a first authentication step, the media player sending an authentication request to the accessory, which responds with authentication information; see figure 6; 602 and figure 7, step 704, and paragraph [0057]. The media player receives and validates the authentication information; see figure 7, step 708, and paragraph [0058]. In a second authentication step, the media player sends an authentication signature request to the accessory; see figure 6; 604, figure 7, step 710, and paragraph [0059]. The request may include a random nonce/challenge to be signed by the device. The accessory responds with an authentication signature; see figure 7, step 712. The media player then validates the authentication signature, for instance using a public key; see paragraphs [0052] to [0054] and [0060] and figure 7; step 714.

3. Clarity, Article 84 EPC 1973

In the annex to the summons to oral proceedings the board expressed doubts concerning the clarity of claim 1. In view of the subsequent amendments to the claims, the board is satisfied that the claims are clear.

4. Document D1 (US 6 697 944 B1)

4.1 It is common ground between the appellant and the board that D1 forms the closest prior art on file. D1 relates to a digital content provider or "host" (see column 4, line 1), for instance a PC or server, storing a digital content audio file, for instance in MP3 format, and

comprising an authentication interface and a USB port from which the digital content file may be downloaded by a player device, such as a portable MP3 player device (see column 2, lines 30 to 34), also comprising an authentication interface and a USB port. The portable device communicates with the host via the USB connection and, "pending the establishment of a trusted relationship" (see abstract, lines 10 to 14) - which the board understands in this context to mean "after having established a trusted relationship" - downloads the digital content file from the host. The higher the degree of trust established, the lower the amount of encryption applied by the host to the digital content before it is transferred; see column 4, lines 21 to 43. In the extreme case, in which the host determines that it does not trust the portable device at all, it only transfers non-DRM digital content files to the portable device; see column 15, lines 24 to 27.

4.2 The level of trust relationship is established by an interrogation/response communication protocol; see column 4, lines 44 to 59, and figure 8A, described from column 14, line 26, to column 15, line 15. Figure 9 shows the same communication protocol from the point of view of the portable device. Firstly the host transmits a query to the portable device, requesting device information; see request 122 in figure 8A. The portable device responds with its device description (see figure 8A; 126) and a flag indicating "I can authenticate". The host then generates a challenge (see figure 8A; 138) to the portable device to ascertain its level of trust, and the portable device creates a unique response based on the challenge which includes its ID and is digitally signed (see figure 8A; 140). Based on the unique response and the digital signature information transmitted from the portable device, the

host determines the level of trust of the portable device; see figure 8A; 142. One reason for determining a lower level of trust is that the portable device utilizes removeable media to store the digital content files.

4.3 Hence, regarding the host and portable device in D1 as the claimed "media player" and "accessory", respectively, D1 discloses the following features of claim 1: a method of authentication of an accessory (the portable device) by a media player (the host), the method comprising: receiving, by the accessory, an authentication request (figure 8a; 122) from the media player, the authentication request initiating an authentication operation, transmitting, by the accessory, an authentication information (126) to the media player, in response to the authentication request, the authentication information being usable by the media player in the authentication operation and transmitting, by the accessory, an authentication signature (140) to the media player for validation (see column 4, lines 53 to 59), wherein the authentication operation completes upon validation of the authentication signature.

5. Inventive step, Article 56 EPC 1973

5.1 The appealed decision

5.1.1 According to the reasons for the decision, the subject-matter of the then claim 1 differed from the disclosure of D1 in the steps of:

a. allowing the accessory to access the media player during the authentication operation and

b. if the authentication operation failed, the accessory was locked out from any further access to the media player.

5.1.2 The difference features, which concerned what the accessory was authorized to access, depending on whether it was authenticated or not, were said to be an "authorization scheme" that was, at least in part, based on non-technical aspects. The authorization scheme would have been given to the skilled person as a specification requirement. An authorization scheme was however not the same as a "business scheme" in the sense of decision T 0258/03 (Auction method/HITACHI, OJ 2004, 575); see reasons, 5.7, last sentence. The situation was however analogous to that in T 0258/03 because the alleged improvement in the speed of interaction between the media player and the accessory lay in the modified non-technical authorization scheme rather than in the, admittedly technical, features of blocking/allowing access to a technical system. The objective technical problem was to implement the authorization scheme in the method of D1, and the skilled person would have readily translated the authorization scheme into program code in the media player of D1. Contrary to the statement in paragraph [0027] of the description, the invention did not speed up authentication. Instead the invention used a different type of media player/accessory interaction to allow unsecured access until authentication had completed and thus circumvented the technical problem of speeding up authentication.

5.2 The appeal

5.2.1 The appellant has argued that the objective technical problem upon which the decision was based, namely to

implement the authorization scheme in the method of D1, is flawed because technical implementation details had been included in the formulation of the problem. Hence the "COMVIK approach" (see T 0641/00 "Two identities/ COMVIK", OJ 2003, 352) had not been correctly followed, as a businessman or administrator would not have known what was technically possible, and the authorization scheme involved technical considerations. Moreover the decision was inconsistent in this respect. Point 11.9 of the reasons conceded that, to some extent, the underlying authorization scheme did involve technical considerations, since it concerned the states of a technical system. The modified authorization scheme set out in the decision involved the concepts of parallel processing in the interactions between the media player and the accessory and thus went beyond any business-driven specification requirement which could have been drawn up by a businessman or an administrator. The control of access by the accessory to an application of the media player was also based on technical considerations. Following the "COMVIK approach", the "business requirement" given to the skilled person in the present case would have been to prevent the use of unauthorized or counterfeit accessories with a media player, the prior art solution acknowledged in paragraph [0005] of the description being that the authentication process had to be completed before an accessory could access the media player; see also paragraph [0049].

5.2.2 At the oral proceedings the appellant argued that the invention solved the problem that unauthorized accessories must not be usable with the media player, but that the authorization operation typically took 0.5 seconds, and users of authorized accessories should not have to wait that long to access the media player.

Regarding D1, the appellant accepted that it was implicit in D1 that the media player ran a media player application and was capable of processing different tasks in parallel. The appellant also accepted that, at the priority date, a strategy of initially granting access, for example of passengers to a transport system, and, if a ticket authentication operation subsequently failed, preventing further access (referred to below as the "ticket" prior art), was known from every-day experience, but argued that the situations in which this strategy had been known were entirely different from that of D1. Such a strategy also went against the teaching of D1, which adopted a strategy of preventing any access at all by unauthorized portable devices to the host.

5.3 The board's assessment of inventive step

5.3.1 Regarding the nature of the invention itself, the board notes that, contrary to the statement in the decision (point 11.6), paragraph [0027] of the description does not claim that, as a result of the invention, "the accessory may interact quicker with the media player". According to paragraph [0027] of the description, "... authentication operations are handled in the background such that the media player is operative to process commands after authentication has begun but before the authentication has completed. This allows the media player and the accessory to interact immediately rather than waiting until after the authentication process has completed successfully". The board understands this disclosure to mean that, as a result of the invention, the accessory may interact sooner, rather than more quickly, with the media player.

5.3.2 The method of claim 1 differs from the disclosure of D1 in the following features:

a. allowing the accessory, by the media player, to access an application of the media player during the authentication operation and

b. wherein if the authentication operation fails, the media player prevents the accessory from any further access to the application of the media player.

5.3.3 Both features solve the objective technical problem of, while maintaining access control, allowing authorized accessories to access the media player sooner. This problem would have been obvious for the skilled person starting from D1.

5.3.4 The solution, set out in features "a" and "b", is to initially allow an accessory to access the application of the media player, but to prevent further access if the accessory fails the authentication operation. This solution implies, as the appellant has argued, that authentication of the accessory by the media player, on the one hand, and access by the accessory to an application of the media player, on the other, occur in parallel, whereas these processes occur in series in D1, where authentication is a precondition of access.

5.3.5 The board does not accept the premise in the decision that the access scheme set out in the difference features is an obvious implementation of an aim to be achieved in a non-technical field, namely the "authorization scheme" referred to in the decision. As the appellant has argued, the control of access by the accessory to an application of the media player, set

out in features "a" and "b", concerns the parallel, rather than serial, organisation of the "access" and "authentication" processes, in doing so making use of the parallel processing capabilities of the media player. Thus, the board accepts the appellant's submission that the invention is based on technical considerations. Hence the "authorization scheme" defined in the decision is not an "aim to be achieved in a non-technical field", in the sense of the "COMVIK approach". Consequently features "a" and "b" contribute to the technical character of the claimed subject-matter and thus can also contribute to inventive step. Put another way, the "authorization scheme" would not have been formulated by the notional "businessman" or "administrator".

5.3.6 The access strategy upon which the difference features are based was known *per se* at the priority date from the "ticket" prior art (see above) in passenger transport systems. The appellant has not disputed that it was known to initially grant passengers access to a transport system, and, if authentication of a ticket held by the passenger subsequently failed, to prevent further access to the transport system, for instance by dropping the passenger off at the next station. The board however accepts the appellant's argument that this strategy was known in an entirely different context to that of D1 and consequently would not have been considered by the skilled person starting from D1 and seeking to solve the objective technical problem of, while maintaining access control, allowing authorized accessories to access the media player sooner.

5.3.7 Moreover, if, for the sake of argument, the skilled person starting from D1 had consulted the "ticket"

prior art, he/she would have realized that the strategy upon which it was based, namely initially allowing access to all, went against the strategy taught by D1, which sought to prevent any access, however brief, by unauthorized portable devices to the host. For the same reason, the board also considers that features "a" and "b" are not just the obvious result of starting from D1 and trading-off security and convenience.

5.3.8 Consequently the subject-matter of claim 1 involves an inventive step, Article 56 EPC 1973.

## Order

## For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the examining division with the order to grant a European patent with the following documents:

Description pages 1, 1a, 12 and 13, all dated 1 September 2009,
2, dated 4 August 2016, and
3 to 11, as originally filed.

Claims 1 to 12, dated 4 August 2016.

Drawings, sheets 1 to 12, as originally filed.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated