Internal distribution code:

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

Datasheet for the decision of 30 October 2020

Case Number: T 2192/15 - 3.4.03

Application Number: 08853918.4

Publication Number: 2232418

IPC: G06Q10/00, A47B67/00, G06F19/00

Language of the proceedings: EN

Title of invention:
ACTIVE TAG-BASED DISPENSING

Applicant:
CareFusion 303, Inc.

Headword:

Relevant legal provisions:
EPC Art. 52(1), 56

Keyword:
Inventive step - after amendment - (yes)

Decisions cited:

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

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

Case Number: T 2192/15 - 3.4.03

D E C I S I O N
of Technical Board of Appeal 3.4.03
of 30 October 2020

Appellant: (Applicant)	CareFusion 303, Inc. 3750 Torrey View Court San Diego, CA 92130 (US)
Representative:	Epping - Hermann - Fischer Patentanwaltsgesellschaft mbH Postfach 20 07 34 80007 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 10 July 2015 refusing European patent application No. 08853918.4 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	T. Häusser
Members:	A. Böhm-Pélissier
	G. Decker

Summary of Facts and Submissions

I. The appeal is against the decision of the Examining Division to refuse European patent application No. 08 853 918. The refusal was based on the ground of lack of novelty and inventive step (Articles 54 and 56 EPC) and added subject-matter (Article 123(2) EPC).

II. **Reference** is made to the following document:

D5 = US 2007/0268138 A1

III. The Appellant (Applicant) **requests** that the decision under appeal be set aside and that a patent be granted on the basis of the Main Request or the 1st to 6th Auxiliary Requests as indicated in the letter dated 19 October 2020.

The application documents of the Main Request are as follows:
Claims: 1-14 as filed with letter dated 19 October 2020;
Description: pages 1-11, filed with letter dated 19 October 2020;
Drawings: sheets 1/9-9/9 as published.

IV. The independent claims of the Main Request read as follows (Board's labelling "(A)" to "(G)" and "(A')" to "(G')"):

Claim 1:
(A) A method of sensing dispensation of a product from a storage device having an antenna, the method comprising the steps of:

providing a first product with a first wireless tag within a service area of the antenna;
establishing wireless communication between the first wireless tag and the antenna, wherein the step of establishing wireless communication includes:
(B) establishing a mesh network (340) of wireless links amongst a plurality of wireless tags; and
establishing a first wireless link between the first wireless tag of the first product and a first one of the plurality of wireless tags; and
establishing a second wireless link between a second one of the plurality of wireless tags and the antenna;
(C) monitoring the wireless communication and a network topology of the mesh network,
(D) wherein monitoring the wireless communication comprises monitoring the first wireless link; and
(E) determining whether the first wireless tag of the first product was removed and returned to the storage device when the location of the first wireless tag in the topology has changed,
(F) while maintaining topology information in a way that temporarily removing the first wireless tag of the first product causes the links of the first wireless tag to be removed from the mesh network and replaced elsewhere in the topology
(G) such that spoofing the system by removing the first product, but not the first wireless tag, from the system can be detected.

Claim 8:
(A') A dispensation-sensing system, comprising:
a securable storage area:
an antenna operable to receive and transmit signals within the securable storage area; and
a processor configured to:

establish wireless communication between the antenna and a first wireless tag of a first product disposed within the securable storage area, and
monitor the wireless communication;
(B') wherein the processor is configured to establish wireless communication by establishing a mesh network (340) of wireless links amongst a plurality of wireless tags, establishing a first wireless link between the first wireless tag of the first product and a first one of the plurality of wireless tags, and establishing a second wireless link between a second one of the plurality of wireless tags and the antenna;
(D') wherein the processor is configured to monitor the wireless communication by monitoring the first wireless link and
(C') a network topology of the mesh network; and
(E') wherein the processor is further configured to determine whether the first wireless tag of the first product was removed and returned to the storage device when the location of the first wireless tag in the topology has changed,
(F') while maintaining topology information in a way that temporarily removing the first wireless tag of the first product causes the links of the first wireless tag to be removed from the mesh network and replaced elsewhere in the topology
(G') such that spoofing the system by removing the first product, but not the first wireless tag, from the system can be detected.

Reasons for the Decision

1. The invention as claimed

1.1 The invention generally relates to dispensation of products and to active tag-based dispensing. Centralized inventory systems are frequently used in the medical community to track and dispense medical products such as medications, medical devices, etc. Keeping close track of these items is desirable. For a caregiver, it is important to be able to quickly and accurately locate a needed item and protect it from theft to the extent possible.

1.2 In such a centralized inventory system, medical products are stored in a storage area, such as a wall cabinet or other secure location. The dispensation of the products from the storage area may be tracked by requiring authorized users to indicate in a tracking log which products and what quantity thereof they have removed from the storage area. These systems, however, rely upon the compliance of the users to track the dispensation of products therefrom, and are thus prone to error and abuse (see page 1 of the description of the application).

1.3 The invention proposes tracking the dispensation of products from storage areas with wireless tags. "Cheating" the system can be detected by continuously monitoring the links between the tags, i. e. by monitoring the topology of the mesh network of the tags. When a product is removed from the storage area, but the packaging of the product with the tag is returned to the storage area, the mesh topology changes. This means that the relative links between the

tags are changed by temporarily removing the link from the mesh network and replacing it elsewhere in the topology. Thereby spoofing the system by removing a product, but not the tag from the system, can be detected.

2. Article 123(2) EPC

2.1 Feature (D) of original claim 4 and Feature (B) of original claim 5 as well as Features (C) and (E)-(G) from the description of the application have been added to original claim 1 resulting in independent method claim 1 of the Main Request. Basis in the description can be found in the paragraph bridging pages 1 and 2, page 8, lines 13-27, and page 5, lines 15-24. Corresponding amendments have been effected in relation to independent system claim 8 of the Main Request.

2.2 New dependent claims 13 and 14 have been added based on the paragraph bridging pages 6 and 7 of the description of the application.

2.3 Therefore the amendments comply with the provisions of Article 123(2) EPC.

3. Inventive Step

3.1 Closest prior art

Document D5 concerns the monitoring of a plurality of RFID tags which form a mesh network and, coming functionally closest to the claimed invention as detailed below, is considered the closest prior art.

3.2 D5

3.2.1 D5 discloses in paragraphs [0094], [0095], [0121], [0145] - [0147] an RFID tag network. In Figures 8A / 8B and in paragraphs [0238] ff. a mesh network is described disclosing Features (A), (B) and (D).

3.2.2 As to Feature (C) D5 discloses (paragraphs [0088] and [0147]) that removal of devices is foreseen and that a detailed history and location can be looked up at any time. This is considered a disclosure of the monitoring of the topology of the system.

3.3 Difference

However, detecting whether a tag has been removed and returned to the storage device without the corresponding product is not disclosed in document D5.

D5 therefore fails to disclose Features (E)-(G) of claim 1 of the Main Request and the corresponding Features (E')-(G') of claim 8 of the Main Request, in particular monitoring the topology in a way that temporarily removing the first wireless tag of the first product causes the links of the first wireless tag to be removed from the mesh network and replaced elsewhere in the topology, such that spoofing can be detected.

3.4 **Effect and problem**

The effect of these distinguishing features is that "cheating" the system can be detected, i. e. that a product is removed and the empty package is returned to the initial position.

The problem can therefore be formulated as preventing unauthorised removal of objects from the dispensation system and therefore reliably preventing "spoofing". "Spoofing" in the context at issue means removing the product, but not the tag, from the system.

3.5 Non-Obviousness

3.5.1 The Board agrees with the Appellant in that D5 merely discloses monitoring the real physical location of a tag. Contrary to the teaching of D5, a location in the claimed topology is not a physical location but rather a virtual position with respect to a specific organisation of network links in a network which is – at least to a certain degree – independent of the tag's actual physical location.

3.5.2 In D5 the physical location of the RFID tag is tracked rather than an organisation of links between devices in a mesh network. D5 is directed to providing a system and method for monitoring an object to replace conventional RFID tag locating systems and methods employing triangulation techniques that are complex and expensive (see D5, paragraphs [0012]-[0015]). D5 requires the relative locations of relay devices to be known, thereby allowing for determining the location of each RFID tag from the locations and/or times at which its transmitted identifying information is received by a relay device or calculating the locations corresponding to a particular transmission.

3.5.3 The inventive concept of the claimed subject-matter is based on the fact that if the removed wireless tag is returned to the storage device, said virtual position within the network topology is very likely different

from before the removal. Therefore this allows to detect "spoofing".

3.5.4 The Board further notes that in D5 ship, train or truck containers are investigated in the sense of detecting whether a container is opened and products / tags are removed or unallowed products together with their tags are inserted. The context of D5 is therefore different from the present invention, where it should be detected whether one and the same tag was removed and reinserted into the system rather than whether a container was opened, a tag was removed or a tag was inserted into the container.

3.5.5 Figures 8A and 8B disclose a mesh network of tags inside and outside shipping containers. The tags may communicate by transfer of messages between each other. The problem of cheating ("tampering") the system is addressed e. g. in paragraphs [0252]-[0253] and [0290]. However, the skilled person, in view of the context of custom controls and the like in D5, would not have the incentive to modify the system of D5 for detecting whether the content of a package is removed and the package with the tag is reinserted into the container.

3.5.6 The system described in D5 provides the possibility of triggering an alarm, if an unauthorized action is performed. This may be the case if a container is opened and/or a product is removed and/or an unauthorized product is inserted. D5 furthermore discloses a procedure of detecting a new device after a possible alarm was provided in view of relay messages received sequentially from the tags (cf. flow diagram in Figure 8B).

3.5.7 This however teaches away from the solution proposed by the invention. According to the invention removal of a tag as well as new links are monitored and after evaluation of the new links an alarm may be triggered. Furthermore, "tampering" alarm is triggered if a new tag link corresponds to a removed link, but in a different topological environment. In the method of D5, in contrast, first an alarm is triggered in response to relay messages from the tags indicating tampering and then new links are investigated. This teaches away from first investigating new links and then deciding whether tampering has taken place as proposed by the invention.

3.5.8 The skilled person has no incentive to modify the system of D5, first because the investigation of shipping containers in D5 has a different purpose than the monitoring in the present invention and the problem of "spoofing" does not occur. Furthermore, in D5 there is already a possibility implemented to detect unallowed removal of products or "tampering". Hence, even if the skilled person were to consider finding a solution to the problem of "spoofing", i. e. detecting whether a tag was removed and the same tag was reinserted into the container, they would trigger the alarm if a specific dislocation condition (cf. paragraphs [0185]/[0290]) within a predetermined time threshold (cf. paragraphs [0185]/[0290]) is met and the product is returned to the same physical location. However, they would not be led to considering that the relative links of the tags are investigated after removal and reinsertion of a tag and that the new link constellation is used for triggering the alarm.

3.5.9 The solution of the problem starting from D5 would lead to a straightforward solution, which would not imply maintaining topology information in a way that

temporarily removing the tag causes the links of the tag to be removed from the mesh network and replaced elsewhere in the topology. The solution starting from D5 would also not reliably detect the removal of the content of a package, if the package with the tag is returned within a short time interval to the storage device.

3.5.10 **To summarise**, the present invention provides a different and more reliable solution than what the skilled person would implement when solving the problem starting from D5. Since the skilled person would, when starting from D5 and attempting to solve the posed problem, arrive at a solution as indicated above, they would not seek for another solution. D5 teaches to monitor absolute positions, i. e. physical locations of the tags. Nothing in D5 or any other cited document teaches to monitor the relative positions of the tags by monitoring the links between the tags in the mesh network for detecting spoofing, if one and the same tag is removed and reinserted within a different topology. In particular, nothing in the cited prior art suggests monitoring a changing network topology by monitoring a change in the virtual organisation of links and monitoring that the links of a tag are removed from the mesh network and replaced elsewhere in the topology, such that spoofing the system by removing products, but not tags, from the system can be detected.

3.5.11 Consequently, none of the cited prior art discloses or suggests Features (E)-(G) of claim 1 of the Main Request or the corresponding Features (E')-(G') of claim 8 of the Main Request. Therefore, the subject-matter of claims 1 and 8 of the Main Request involves an inventive step (Article 52(1) EPC) within the meaning of Article 56 EPC.

4. Conclusion

For the above reasons the board is of the opinion that the application and the invention to which it relates, in the version according to the appellant's Main Request, meet the requirements of the EPC. Hence, a patent is to be granted on the basis of that request (Articles 97(1) and 111(1) EPC). Consideration of the appellant's Auxiliary Requests is therefore not necessary.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the department of first instance with the order to grant a patent in the following version:
Claims: 1-14 as filed with letter dated 19 October 2020;
Description: pages 1-11, filed with letter dated 19 October 2020;
Drawings: sheets 1/9-9/9 as published.

The Registrar: The Chairman:

S. Sánchez Chiquero T. Häusser

Decision electronically authenticated