Internal distribution code:

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

Datasheet for the decision of 15 April 2025

Case Number: T 0520/22 - 3.5.01

Application Number: 16815522.4

Publication Number: 3394805

IPC: G06Q10/08, G06Q50/22, G06Q10/06, G06F21/32

Language of the proceedings: EN

Title of invention:
SYSTEM, METHOD AND DEVICE FOR PROCESSING A TRANSACTION

Applicant:
GB-E Holding Company (Global Business Enterprises) Limited

Headword:
Logging the transfer of a product/GB-E

Relevant legal provisions:
EPC Art. 56

Keyword:
Inventive step - using a dual device for biometric authentication (no - obvious design choice)

Decisions cited:
T 0641/00, T 1082/13

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

Case Number: T 0520/22 - 3.5.01

D E C I S I O N
of Technical Board of Appeal 3.5.01
of 15 April 2025

Appellant: (Applicant)	GB-E Holding Company (Global Business Enterprises) Limited Level 3, Suite No. 2436 Tower Business Park Tower Street Swatar BKR 4013 (MT)
Representative:	Barker Brettell LLP 100 Hagley Road Edgbaston Birmingham B16 8QQ (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 20 October 2021 refusing European patent application No. 16815522.4 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Chandler
Members:	R. Moser
	E. Mille

Summary of Facts and Submissions

I. This case concerns the applicant's appeal against the decision of the examining division to refuse European patent application No. 16815522.4.

II. The examining division held that claim 1 of the sole request defined an administrative logistics scheme implemented in a straightforward manner on well-known hardware, i.e. a computer with a display, two smart card readers, two fingerprint or finger vein scanners and a barcode scanner or RFID reader (see points 2.17 to 2.20 of the decision).

III. In the statement setting out the grounds of appeal the appellant requested that the decision be set aside and by implication a patent be granted on the basis of the refused request, filed during oral proceedings on 14 September 2021.

The appellant essentially argued that the examining division, by disregarding key technical features, such as a single supply change management device with a pair of card readers and scanners and a predefined transaction interval of 10 seconds, failed to correctly apply the "Comvik" approach (see T 0641/00 - *Two identities/COMVIK*). Taking the correct approach it would not have led to the conclusion that the claimed implementation was obvious.

IV. In the communication accompanying the summons to oral proceedings, the Board tended to agree with the appellant that claim 1 was not a straightforward mapping of the non-technical requirements underlying the claimed method (see point 8 of the communication),

as found by the examining division.

However, it was of the preliminary view that claim 1 lacked an inventive step over D1 (WO 2013/106584 A1), see *ibid.* point 10.

V. Oral proceedings took place by videoconference on 15 April 2025. The appellant confirmed their written requests.

At the end of the oral proceedings the Chairman announced the Board's decision.

VI. Claim 1 of the sole request reads:

A method for processing a transaction via a supply chain management device (7012), the supply chain management device (7012) including a pair of biometric fingerprint or finger vein scanners (7013, 7015), a pair of card readers (7017, 7019), and a product identifying component including one or both of a barcode scanner (7021) and a RFID tag reader, the method including the steps of:

obtaining an identifier of an operator handling a product and an identifier of a recipient of the product via the pair of card readers (7017, 7019) from a credential storage device of the operator and of the recipient;

authenticating at least the operator and the recipient by comparing biometric information from the operator and recipient obtained via the pair of biometric fingerprint or fingerprint vein scanners (7013, 7015) to biometric information obtained via the pair of card readers (7017, 7019) from the credential storage device of the operator and of the recipient;

activating the product identifying component (7021)

if the operator is authenticated;

obtaining an identifier of the product using the product identifying component (7021) only if the operator is authenticated;

and updating a remotely maintained record to associate the identifiers of the operator and recipient with the identifier of the product;

wherein the operator is authenticated prior to obtaining the identifier of the product and the identifiers of the operator and recipient and the identifier of the product are obtained within a predefined transaction time interval of 10 seconds or less, outside of which the transaction is operably cancelled,

and wherein the remotely maintained record is updated to associate identifiers of an operator and recipient with the identifier of the product for any or each stage of a supply chain through which the product moves.

VII. The appellant's arguments are discussed in the reasons for the decision.

Reasons for the Decision

1. *Background of the invention*

1.1 The invention relates to a method for monitoring and tracking transactions in a supply chain, specifically the distribution of goods from a supplier to a recipient. An example is the delivery of a pharmaceutical product from a pharmacist to a customer (page 13, lines 15 to 17 of the application as filed).

The primary objective is to improve "transparency, traceability, allocation and accountability of

resources along the supply chain" (page 12, lines 31 and 32) - a goal that proves challenging with existing systems (page 1, lines 19 to 23).

1.2 This is achieved by requiring that the transaction satisfy specific conditions: both the supplier and recipient must be present and successfully identify and authenticate themselves. Only after authentication may the supplier scan the product identifier. A data record on a remote server is subsequently updated, linking the identifiers of the supplier, recipient, and product.

1.3 Authentication is performed via biometric verification, using separate smart card readers and fingerprint sensors for each participant, all integrated into a single supply chain management device 7012 - see Figure 6. Each participant's biometric data is stored on their individual smart card and matched against a live sample captured by the fingerprint sensor.

1.4 An additional feature of the process is a time constraint: all three identifiers must be captured within a predefined interval - such as 10 seconds - in a so-called "virtual handshake" (see page 21, lines 16 to 21). If this condition is not met, the transaction is cancelled.

2. *Claim 1, inventive step*

2.1 The Board judges that claim 1 is not inventive over D1.

D1 discloses monitoring/tracking of care events which includes biometric authentication of a provider and receiver of a medicine, scanning the medicine and the storage of all this information on a remote server (see page 27, lines 5 to 9 and page 39, lines 5 to 23). Such

care events thus fall under the transaction in claim 1. D1 further discloses that, to be valid, a care event, in particular the authentication of both participants, must be completed within a predefined time period (page 20, line 19 to page 21, line 2).

It is common ground that claim 1 differs from D1 by the following underlined features (see point 11 of the Board's communication):

F1. The device includes a pair of biometric scanners, not a single one.

F2. In addition, the device includes a pair of card readers to read biometric information stored on a smart card ("credential storage device").

F3. The product scanner is activated after authentication.

F4. The transaction time interval is 10 seconds or less and refers to the collection of the parties' and product's identifiers.

2.2 The Board notes that the concept of identification/ authentication of the participants involved in a product transfer and its registration or tracking on a abstract level does not involve technical considerations.

This includes the transaction rules, i.e. the conditions that must be met for a transaction to be considered valid, secure or compliant. In the present case, these are that both participants need to authenticate, that the product identifier can only be obtained after the provider is authenticated (F3) and

that participants have to meet in person and the overall transaction time is less than 10 seconds (F4).

None of these aspects are based on technical considerations, but are either formulated by a business person or reflect legal requirements, such as "The Drug Supply Chain Security Act" (see page 21, lines 23 to 25 of the application as filed). For instance, the time interval is arbitrary and is set "such that at least two or more of the identifiers are obtained near simultaneously, forming a 'virtual handshake'" (see page 10, lines 22 to 27).

In terms of hardware, the above distinguishing features boil down to using smart cards for biometric authentication and a dual device, i.e. a device having a pair of (smart card) readers and (fingerprint) scanners.

2.3 The appellant argued that the distinguishing features F1, F2 and F4 - and to a lesser extent also F3 - provided a synergistic technical effect, namely ensuring a reliable and secure transfer of products in a supply chain.

This was achieved by using a smart card for biometric authentication and a pair of readers/scanners in a single device. The use of a dual device in conjunction with the specific time interval ensured that both the provider and recipient were present at the same time when performing the transaction ("virtual handshake"). The time parameter in claim 1 was different from that referred to by the Board in decision T 1082/13, point 2.4, where a timeout criterion was used in a non-technical context.

2.4 In the appellant's view the synergistic effect was based on the following facts:

Using a smart card for locally retrieving a user's biometric data (F2), instead of remotely querying a database as in D1, enabled a speedier authentication. This effect was enhanced by using a single device with a pair of readers/scanners (F1 and F2) as this enabled the two participants to authenticate in parallel and (almost) simultaneously (F4).

The appellant further argued that D1 taught away, as it would not be practical to enforce that the care event take place within 10 seconds. There was no incentive to modify D1 to arrive at a dual device comprising a pair of readers/scanners. The use of a smart card for biometric authentication as such might be obvious, however, not in combination with the remaining features.

2.5 Firstly, in the Board's view, not all of the alleged effects are actually achieved as they depend on conditions that are unspecified.

For example, given the lack any database information, if the remote database is small, querying it may be faster than a process that involves finding and inserting a smart card into the reader. Similarly, while the use of a dual device may accelerate the authentication step as such, it does not necessarily reduce the overall transaction time, which also depends on the time required to scan the product. The feature of specifying the transaction time of 10 or less seconds does not change this as it is merely an overall constraint on the system which is not connected to its specific technical features (cf. point 2.2 above).

Similarly, feature F3 is also unrelated to reducing authentication or transaction time. It may even increase the transaction time, as the provider must complete authentication before scanning the product identifier.

The distinguishing features also do not enhance the reliability or security of product transfers compared with D1. Any differences, such as permitting the product to be scanned only after authentication, merely reflect the underlying non-technical transaction rules (cf. 2.2).

2.6 Secondly, the Board judges that the distinguishing features are a mere aggregation which have to be assessed separately for inventive step.

Specifically, the effects relating to speeding up the authentication process, namely by using a smart card and a pair of readers/scanners, do not provide a synergistic effect. While both may contribute to faster authentication, they operate independently. For instance, using a smart card instead of a remote database is functionally unrelated to whether authentication occurs via a single or dual device. As such, the combination does not yield a technical effect beyond the sum of their individual contributions.

2.7 The Board further judges that the solution to each partial problem is obvious.

Firstly, using smart cards as an option for biometric authentication was well-known before the priority date of the application (see point 12 of the Board's communication), a fact that was not contested by the appellant.

Secondly, the use of a dual device instead of a single device, as disclosed in D1, offers at most subjective advantages for certain users - for example, in terms of practicality. However, it does not, in itself, solve the problem of enabling a transaction within a 10 second time interval. While it may help ensure, though not guarantee, that both participants are physically present during the transaction, this is also achieved in D1 (see, for instance, page 38, lines 8 to 17). Moreover, as the examining division observed, it is obvious that certain steps can be accelerated by duplicating hardware components, thereby allowing multiple users to input data in parallel when appropriate (see point 2.21 of the decision). A skilled person would choose between a single or dual device based on specific circumstances - such as perceived convenience, cost considerations, or portability. These are standard design trade-offs that, in the present case, do not support the presence of an inventive step.

The appellant's arguments that imposing a 10 second time interval would not be practical in D1 amounts to saying that there is a non-technical prejudice against modifying D1 in this direction. However, there is no indication of any technical prejudice that would prevent the skilled person from setting such a time interval, if required. In the Board's view, and consistent with T 1082/13, point 2.4, the timeout criterion reflects non-technical considerations - specifically, a rule for defining a valid transaction time. Implementing this using, for example, time stamps of scanning events would be a routine task for the skilled person (see also D1, page 4, lines 6 to 15).

2.8 The Board further observes that the choice between a single or dual device has no apparent impact on the security or reliability of the transaction, contrary to the appellant's assertion.

2.9 For these reasons, the Board judges that claim 1 of the sole request lacks an inventive step (Article 56 EPC).

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

T. Buschek W. Chandler

Decision electronically authenticated