Internal distribution code:

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

Datasheet for the decision of 14 March 2025

Case Number: T 2515/22 - 3.5.01

Application Number: 15708808.9

Publication Number: 3114628

IPC: G06Q20/40

Language of the proceedings: EN

Title of invention:
SYSTEM, DEVICE AND METHOD FOR THE CERTIFICATION OF TRANSACTIONS, ACCESS CONTROL, AND THE LIKE

Applicant:
Tufano, Francesco

Headword:
Certification of transactions/TUFANO

Relevant legal provisions:
EPC Art. 56
RPBA 2020 Art. 13(2)

Keyword:
Inventive step - pairing an electronic code with a biometric code (no - no technical effect)

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 2515/22 - 3.5.01

D E C I S I O N
of Technical Board of Appeal 3.5.01
of 14 March 2025

Appellant: (Applicant)	Tufano, Francesco Via Copernico, 24 20016 Pero (IT)
Representative:	Penza, Giancarlo Bugnion S.p.A. Viale Lancetti, 17 20158 Milano (IT)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 3 August 2022 refusing European patent application No. 15708808.9 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	M. Höhn
Members:	I. Kürten
	L. Basterreix

Summary of Facts and Submissions

I. The appeal is against the examining division's decision to refuse European patent application No. 15708808.9 for lack of inventive step (Article 56 EPC) over D5 (JP 2002 353958 A).

II. With the statement setting out the grounds of appeal, the appellant requested that the decision to refuse the application be set aside and that a patent be granted on the basis of the refused main request.

III. In the communication accompanying the summons to oral proceedings, the Board tended to agree with the examining division that claim 1 lacked an inventive step over D5. The Board also observed that one of the distinguishing features identified by the examining division appeared to lack basis in the application as filed.

IV. In a reply, the appellant filed a new main and auxiliary request along with further arguments in support of inventive step.

V. During the oral proceedings, held via videoconference on 14 March 2025, the appellant confirmed the requests filed with the reply to the communication accompanying the summons.

VI. Claim 1 of the main request reads:

A system (1) for certifying an electronic transaction, comprising:

- a portable physical medium (2) adapted to store an electronic code (5),

- a first reading device (3) for reading a biometric parameter of the user, and

- a code generating device (4) adapted to generate a combined code (7) obtained from a pairing of the electronic code (5) stored on the portable physical medium (2) and of a first biometric code generated from the biometric parameter detected by the first reading device (3), and to store the generated combined code (7) on said portable physical medium (2),

- the portable physical medium (2) being further adapted to store the combined code (7),

- the system (1) further comprising a device (10) comprising a second reading device (11) for reading a biometric parameter of the user at transaction time, the device (10) being adapted to read the combined code (7) stored on the portable physical medium (2), at transaction time, and to generate a new code obtained from a pairing of the electronic code (5) read from the portable physical medium (2) and of a second biometric code generated from the biometric parameter detected by the second reading device (11), the device (10) being further adapted to compare the new code generated at transaction time with the combined code (7) stored on the portable physical medium (2),

- wherein the first and second biometric codes are generated using the electronic code (5) and the respective biometric parameter as input parameters of a transformation function, according to the formula cb = f(ce, pb), where cb is the biometric code, ce is the

electronic code (5), pb is the biometric parameter, and f is the transformation function.

VII. Claim 1 of the auxiliary request adds the following at the end of the first feature:

"wherein the electronic code is stored in a barcode or in a QR code or in a RFID tag or in a microchip or in a SIM."

Reasons for the Decision

1. *Background*

The invention concerns authorising electronic transactions by comparing a first code stored on a portable medium, such as a credit card, with a second code generated during the transaction.

Looking at Figure 1, the first code 7 ("combined code" in claim 1) is generated by a code generation device 4 by pairing (e.g. concatenating) an electronic code 5 stored on the card 2 with a first "biometric code". The biometric code is derived using a "transformation function" applied to the electronic code 5 and a biometric parameter 6 of the user, such as a fingerprint (page 3, line 10 to page 4, line 6).

The second code ("new code" in claim 1) is generated by the same algorithm. It pairs the electronic code 5 read from the card 2 and a second "biometric code" derived from the user's biometric parameter obtained during the transaction. If the two codes match, the transaction is authorised (page 4, line 23 to page 5, line 10).

2. *Admittance*

The Board admits the main and auxiliary requests into the appeal proceedings, as they were filed in response to observations and arguments presented for the first time in the Board's communication accompanying the summons to oral proceedings. In the Board's judgement these are cogent reasons that justify the exceptional circumstances required by Article 13(2) RPBA.

3. *Main request*

3.1 It is common ground that D5 is a good starting point for assessing inventive step.

D5 discloses generating first "collation data" by applying a hash function to a user ID and a user's physical characteristic, such as a fingerprint (e.g. [0047], [0048]), and storing both the user ID and the first collation data on the user's card ([0050]). The user ID in D5 corresponds to the electronic code in claim 1, and the first collation data corresponds to the first biometric code.

During a transaction, the user's biometric characteristic is collected, the user ID is read from the card, and a second "collation data" is generated using the same hash function. This data, which corresponds to the second biometric code in claim 1, is compared to the first collation data (corresponding to the first biometric code) on the card. If they match, the transaction is approved ([e.g. [0053]]).

3.2 Thus, claim 1 differs in that the transaction authorisation codes ("combined" and "new" codes) are

generated by pairing the electronic code with the first or second biometric code, whereas in D5, the authorisation codes are the biometric codes themselves.

3.3 Like the examining division, the Board considers that this difference has no technical effect. The only example of "pairing" in the application (page 3, lines 19 to 21) involves concatenating the electronic code with the biometric code. In this case, both the stored and new combined codes contain the same electronic code. This means that if they differ, the difference would stem from the biometric codes. Consequently, comparing the stored and new combined codes yields the same result as comparing the biometric codes alone, which is already disclosed in D5.

3.4 The appellant argued that the "transformation function" in claim 1 ensured that it was impossible to infer the function's inputs (the electronic code and the biometric parameter) from its output (the biometric code). Since only the biometric code was stored on the portable medium and not the biometric parameter, the biometric parameter could not be retrieved, resulting in greater security.

However, there is no difference between the generation of the biometric codes in claim 1 and in D5. D5 uses a one-way hash function to generate biometric codes (collation data) from the electronic code (user ID) and the user's biometric data (e.g. [0050]). This function corresponds to the "transformation function" in claim 1. Moreover, D5 also does not store the biometric parameter on the user's card, only the first collation data (corresponding to the first biometric code), see e.g. [0048], [0055].

3.5 The appellant further argued that the electronic code in claim 1 differed from the user ID in D5, since the user ID was unique to the user, whereas the electronic code was unique to the physical medium. Moreover, the user ID was assigned in advance and known to the user, whereas the electronic code could be random and unknown to them. According to the appellant, this difference enhanced security and enabled double certification - confirming both the user's identity and the authenticity of the physical medium. This was not possible in D5, since the user ID was not specific to the physical medium.

However, the Board finds no basis for this difference in claim 1, which provides no details about the electronic code. The description only states (page 4, lines 5 to 6) that the biometric code (and, consequently, the combined code) "*varies as a function of the electronic code of the card, thus giving different results*". In the Board's view, this simply means that different electronic codes yield different biometric codes, which is also the case in D5. It does not imply that each card has a unique electronic code.

Furthermore, while the user ID in D5 is unique, this does not mean a user has only one ID. As stated in [0046] of D5, the user ID is assigned by the card issuer, suggesting that a user may have multiple IDs across different issuers and cards. Given its broad definition, the electronic code in claim 1 is therefore indistinguishable from the user ID in D5.

3.6 Finally, the appellant argued that the claimed system provided "two factor protection" by "masking" the user's biometric parameter (e.g. a fingerprint) twice - first by the biometric code and then by the combined

code. This "double masking" supposedly enhanced security compared to D5, where the biometric parameter was masked only once.

The Board, however, does not see a second "masking" in the present case. The combined code is created by "pairing" the biometric code with the electronic code. As mentioned above, the only example of pairing in the application is concatenation. Since the biometric code can be easily extracted from this concatenation, the combined code does not conceal it and does not enhance security.

3.7 Therefore, the Board judges that claim 1 of the main request lacks an inventive step (Article 56 EPC).

4. *Auxiliary request*

4.1 Claim 1 of this request specifies that the electronic code is stored in a barcode, QR code, RFID tag, microchip, or SIM.

4.2 The Board finds that this feature does not establish an inventive step, as it merely lists generally known methods for storing data on a physical medium. Using these known technologies to store the electronic code does not produce any unexpected technical effect.

4.3 The appellant argued that this feature clarified that the electronic code was unique to the physical medium, distinguishing it from the user ID in D5.

The Board is not convinced, as the added feature only defines how the code is stored, not what it contains. A user ID could also be stored in e.g. a barcode or an RFID tag.

4.4 The appellant also argued that the added feature enhanced security by preventing duplication of the electronic code.

The Board disagrees, as storing data in e.g. a barcode or QR code does not protect it from being copied.

4.5 For these reasons, the Board judges that claim 1 of the auxiliary 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 M. Höhn

Decision electronically authenticated