Internal distribution code:

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

Datasheet for the decision of 25 April 2023

Case Number: T 1314/20 - 3.5.01

Application Number: 14833551.6

Publication Number: 3084700

IPC: G06Q20/32, G06Q20/40

Language of the proceedings: EN

Title of invention:
SYSTEM, USER DEVICE AND METHOD FOR AN ELECTRONIC TRANSACTION

Applicant:
Chiptec International Ltd.

Headword:
Biometric transaction authentication using mobile devices/ CHIPTEC

Relevant legal provisions:
EPC Art. 56

Keyword:
Inventive step - use of biometric instead of PIN-based verification to be carried out inside a SIM card (no - obvious alternative)

Decisions cited:
T 0258/03

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 1314/20 - 3.5.01

D E C I S I O N
of Technical Board of Appeal 3.5.01
of 25 April 2023

Appellant: (Applicant)	Chiptec International Ltd. Maduro Plaza Building, Dokweg Willemstad, Curaçao (AN)
Representative:	Jilderda, Anne Ayolt LIOC Patents & Trademarks Zwaanstraat 31 L 5651 CA Eindhoven (NL)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 8 January 2020 refusing European patent application No. 14833551.6 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	M. Höhn
Members:	R. Moser
	L. Basterreix

Summary of Facts and Submissions

I. This case concerns an appeal against the examining division's decision to refuse European patent application No. 14833551.6 for lack of inventive step (Article 56 EPC).

II. The examining division held that claim 1 of the main request was not inventive over D1 (EP 2 234 423 A1). Essentially, they considered that the distinguishing feature, i.e. biometric user verification, was an obvious and commonly known alternative solution to PIN-based verification. D2 (GB 2 368 951 A) was cited as providing exemplary evidence therefor.

The division further considered that the additional features of the first to fifth auxiliary requests were either non-technical in nature, obvious, or known from D1.

III. In the statement setting out the grounds of appeal, the appellant requested that the decision be set aside and the application be granted on the basis of the refused main, or any of the refused first to fifth auxiliary requests, or be remitted to the first instance.

Furthermore, the appellant requested oral proceedings before any decision was taken by the Board to dismiss the appeal.

IV. In a communication under Rule 100(2) EPC, the Board set out its preliminary view of the case. The Board tended to agree with the examining division that claim 1 of the main, first and second auxiliary requests did not involve an inventive step over D1.

The Board further tended not to admit the third to fifth auxiliary requests under Article 12(5) RPBA, as these requests had not been substantiated in appeal.

V. In a reply, the appellant provided further arguments and requested the Board "to reconsider its provisional opinion and allow the appeal".

VI. The Board issued a summons to oral proceedings. In the communication accompanying the summons under Article 15(1) RPBA, the Board maintained the preliminary opinion as set out in its previous communication.

VII. During the oral proceedings before the Board, which took place by videoconference on 25 April 2023, the appellant withdrew the first and third to fifth auxiliary requests.

The appellant's final requests were that a patent be granted on the basis of the refused main or second auxiliary request.

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

VIII. Claim 1 of the main request reads:

System for performing a transaction electronically, comprising:
- a transaction server able and configured to offer and perform a transaction for a user,
- a personal user device of an authorized user,
- capturing means able and configured to capture selected biometric data of the user in electronic form,
- verification means able and configured to compare captured biometric data of the user to stored biometric

data of the authorized user and, in the case of sufficient correspondence therebetween, to generate a verification confirmation, and

- *telecommunication means which enable the user to exchange data comprising a verification confirmation with the transaction server over a telecommunication connection in order to authorize the transaction,*
- *wherein the transaction server is able and configured to receive the verification confirmation and, subject to a successful user verification apparent therefrom, to perform the transaction,*

characterized in that

the user device comprises primary processing means with at least one primary processor unit, primary memory means and a primary control system, which primary processing means are coupled to the capturing means by means of the primary control system,

that the user device comprises an exchangeable module with secondary processing means, comprising at least one secondary processor unit, secondary memory means and a secondary control system,

that the stored biometric data of the authorized user are stored in the secondary memory means of the exchangeable module,

that the secondary processing means of the exchangeable module are able and configured to make a request to the capturing means in order to obtain the captured biometric data,

that the exchangeable module comprises the verification means, wherein the secondary processor unit is able and configured on the basis of program code loaded therein to compare the captured biometric data of the user to biometric data of the authorized user stored in the secondary memory means and, in the

case of sufficient correspondence, to generate the verification confirmation, and

that the program code for the secondary processor unit has been loaded therein without action on the part of the user.

IX. Claim 1 of the second auxiliary request adds at the end of claim 1 of the main request the following feature:

and that the user device comprises input means which are coupled to the processing means and which enable the user to enter a personal access code and provide this in electronic form to the processing means.

X. The appellant's arguments can be summarised as follows:

The invention offered a secure and convenient mechanism for online transaction authentication, without requiring the exchange of sensitive biometric data with a transaction server (see page 2, lines 12 to 15 of the published application).

This was accomplished by storing biometric data and a verification program on a SIM card, which was issued by a trusted body to an authorised user. The verification program generated a "yes/no" message (verification confirmation) and transmitted it to the transaction server. Contrary to D1, this message did not include any sensitive data (see page 3, lines 4 to 15 and page 4, line 26 and following).

The verification confirmation served two purposes: It confirmed that the user was the legitimate owner of the SIM card and that he was authorised to perform the transaction. The latter was due to the fact that the SIM card, which generated the verification

confirmation, was issued only to authorised users (see page 13, lines 4 and following; page 17, lines 8 to 11). This was in contrast to D1 where the mobile device only performed PIN-based authentication, while the server performed the authorisation based on identification data received from the mobile device.

D1 only concerned the secure transmission of identification data to a service provider, without requiring the user to register with the provider (see paragraphs [0003] and [0010]). In D1, the service provider only needed the user's phone number to request the identification data necessary for authorisation. While the data was transmitted upon successful user verification (paragraph [0017]), the verification itself did not provide any information as to whether the user was authorised to use the service (see paragraphs [0044] to [0049]).

There were more distinguishing features (highlighted in *italics*) than those identified by the examining division, namely:

- The user device was that of an *authorised user*. The registration authority in D1 only checked the correctness of the identification data, not the authorisation of a service (paragraph [0036]). Thus, the mobile device in D1 was only used for user authentication (see paragraphs [0048] and [0049]).

- The secondary memory means stored *biometric data of the authorised user*.

- Generating a *verification confirmation*. The PIN verification in D1 did not qualify as verification confirmation as the message transmitted in D1 contained

user sensitive data (paragraph [0048]).

- Telecommunication means for exchanging data comprising the *verification confirmation* and the transaction server receiving *this information*. The server in D1 needed to perform a separate authorisation step.

- *Capturing and verifying biometric data*.

The inventive step reasoning of the examining division was flawed as it did not take into account the above distinguishing features. In particular, it disregarded the technical effect provided by the verification confirmation, which resulted in a more secure and efficient authorisation mechanism. Overall, the technical effect was to provide a more secure, bandwidth-efficient and privacy-preserving means of authorising a transaction.

The skilled person would not have arrived at the claimed invention without the benefit of hindsight. Even if he substituted the PIN with biometric verification, there was no suggestion to delegate the authorisation from the server to the mobile device, as in the invention. It required an inventive step to authorise the user without using identification data.

The additional means for entering a PIN in claim 1 of the second auxiliary request, which combined synergistically with the biometric authentication, provided an even more secure method. The authentication relied on something the user knew and something the user was. Even if the skilled person had adapted D1 to use biometric authentication, it would not have been obvious to add an extra PIN-based authentication in

2013, the priority date of the application.

Reasons for the Decision

Summary of the invention

1. The invention concerns the authentication of electronic transactions with a mobile device. Conventional authentication methods, such as those used in banking, involve bank or credit cards along with PIN or authorisation codes.

   In order to prevent misuse and fraudulent activity, the invention aims to establish a secure user authentication process that also takes into account the user's privacy - see page 1, line 29 to page 2, line 15 of the published application.

2. The key idea of the invention is to store a user's biometric data and relevant verification software on a SIM card ("an exchangeable module ... with secondary processing means" in claim 1). To obtain such a SIM card, the user must present himself at a trusted body, such as a public authority, that has the necessary equipment - see page 13, lines 4 to 24. Once the user receives the SIM card, he is authorised to use it on his mobile device ("a personal user device of an authorized user") to authenticate transactions.

3. To perform a transaction, the user must first authenticate himself through biometric verification, for example by capturing his face. The captured biometric data is then transmitted to the SIM card for comparison with the biometric data stored thereon. If the comparison is successful, a verification

confirmation is transmitted to the transaction server - see page 16, line 20 to page 17, line 11.

Main request, inventive step

4. It is common ground that D1 is a suitable starting point for assessing inventive step.

D1 discloses a method of identifying a user for an online service such as an online tax form filing (paragraph [0029]). This involves two steps: First, the user authenticates himself using his mobile device. Second, once authentication is successful, the mobile device transmits identification data to the service (paragraph [0017]).

Although the term "transaction" is not used in D1, this term is very broad and the Board judges that it encompasses any process of doing business, including the "service" mentioned in D1 (see also page 18, lines 10 to 14 of the application).

To authenticate a user in D1, a SIM card is used which stores a PIN code and a verification program, referred to as "identification application" (see paragraphs [0042] and [0044]). In order to access the service, the user must enter the PIN code, which is then verified by the identification application. If the verification is successful, the identification application generates a message containing identification data, which is transmitted to the server (paragraphs [0046] to [0048]). Based on this identification data, the server authorises the user to access the service (paragraphs [0048] and [0049]).

5. As outlined below, the Board judges that claim 1 pertains only to user authentication and not to authorisation. Therefore, the teaching of D1 concerning authorisation - specifically, the transmission of identification data (which may include biometric data) from the mobile device to the server (see paragraphs [0030], [0048], and [0049]) - is not relevant for the following inventive step analysis.

What is essential, and applies to both the invention and D1, is that the data and software used for user authentication remain on the SIM card and are not transmitted elsewhere.

6. One of the main arguments put forward by the appellant was that in D1, authorisation was delegated to the server, while in the present invention, the mobile device was responsible for both user authentication and authorisation. In the appellant's view, this was reflected in the second feature of claim 1 (" ... of an authorized user") and in the verification means stored on the SIM card. As a result, there was no need to transmit privacy-sensitive identification data, which was used for authorisation, to the server (see page 4, lines 26 to 30).

In the invention, authorisation was granted by the trusted authority that issued the SIM card to the user after verifying his identity. With authorisation established in advance, the user only needed to perform local biometric verification to unlock the SIM card, resulting in both authentication and authorisation.

To illustrate this advantage, the appellant provided the following example: Users were only permitted to purchase tobacco if they were above a certain age. In

D1, any user, including minors, could obtain a SIM card (paragraph [0036]). It was the server's responsibility to verify the user's age, which required transmitting sensitive age information to the server. In contrast, according to the invention SIM cards were only issued to authorised users, i.e., those who were above the legal age (page 13, line 4 and following). Therefore, there was no need to transmit any age information to the server.

7. The Board is not persuaded by these arguments for several reasons.

First and foremost, the claim does not include any details regarding authorising procedures with service providers or the issuance of SIM cards to a particular group of users, namely those who are authorised. It is not clear what criteria would make a user an authorised user. In fact, the claim does not address the concept of authorisation at all, let alone its technical aspects. If a service requires some data additional to the user authentication, such data has to be provided either beforehand or after successful user authentication. According to D1 this is done after authentication. According to claim 1 it is assumed that such data has been provided before authentication. However, claim 1 is a system claim and such measures of providing authorisation related data are outside of the claimed subject-matter and, furthermore, are not suitable to specify the claimed system in a technical way. In view of this, the Board judges that the term "authorized user" also encompasses users in D1 and, thus, is not a distinguishing feature.

8. Even if it were, assuming that the claim included such details, the Board judges that this would relate to a

business, rather than a technical aspect.

For example, a tobacco company and the trusted authority could enter into an agreement specifying that SIM cards are only provided to users who are above the legal age. As a result, the tobacco company would not need to verify the age of the user to authorise a sale, provided that the user is the legitimate owner of the SIM card. In other words, the business agreement determines who is considered an authorised user, while the verification process aims to confirm that the user of the SIM card is the legitimate owner.

9. The specific data required for authorisation may vary depending on business or legal requirements. In the above case for example, authorisation information, such as the user's age, is not necessary at all. As a result, any technical effects derived from limiting or omitting this information - such as a decrease in network traffic or safeguarding user sensitive data - would be mere bonus effects that are not achieved through specific technical means and, therefore, can not contribute to inventive step.

10. Further, if the public authority mistakenly issued a SIM card to a minor, he would be considered an authorised user and be able to authenticate a purchase of tobacco. It is not derivable, neither from the claim nor from the application as a whole, that the verification means would prevent a successful authentication or that the server would deny authorisation in such a case.

Therefore, the Board concludes that, contrary to the appellant's argument, the verification means and the generated verification confirmation according to

claim 1 do not contain any data that would allow for verifying a valid authorisation.

11. The Board further judges that, contrary to the appellant's view, D1 does disclose the generation and transmission of a verification confirmation.

In both the claim and in D1, a message is generated and transmitted to the server after successful user verification. D1 specifies that this message includes identification data, which is data required by the service provider for authorisation purposes (paragraph [0048]). However, the presence of this additional data does not detract from the message's function as a verification confirmation. In other words, when the server in D1 receives the message, this indicates that the user has been verified, regardless of any other data that may be included in the message.

12. Even if the appellant's argument were accepted and the verification confirmation were defined solely in terms of a "yes/no" message without including any user sensitive data, the previous conclusion would still hold true.

The transmission of additional data in D1, such as the user's age or biometric data of an e-passport, is necessary because the service provider requires this information for authorisation purposes. This may compromise user privacy, as argued by the appellant. However, the invention does not address this issue through technical means. Instead, it circumvents the problem through business measures, as explained earlier. Therefore, this aspect can not contribute to the technical character of the claimed subject matter (T 258/03 - *Auction method/HITACHI*, Headnote II, OJ EPO

2004, 575). According to claim 1 the focus is on securing the user specific data on the SIM card used for user authentication. It prevents the confirmation message ever containing any of the user specific biometric data used by the verification software in the SIM card. Also according to D1, the user specific PIN data is kept inside the SIM and any confirmation message generated in reaction to a successful user authentication does not forward the user specific PIN data to the server. Therefore D1 anticipates this security related concept according to claim 1.

13. In view of the above, the Board judges that the distinguishing feature between claim 1 and D1 is:

A. The user authentication is performed using biometric verification. This includes the storage of biometric data and verification software on the SIM card and capturing biometric data using the mobile device.

14. While both the invention and D1 offer ways to authenticate the user, i.e. by verifying that the user of the SIM card is also the legitimate owner, this is, as said before, implemented differently.

The appellant argued that the implementation provided in D1 was more susceptible to fraud, as any person could obtain the SIM card and PIN code and use them for authentication. On the other hand, in the invention, only the authorised user, whose biometric data had been captured and stored on the SIM card by the trusted authority, could authenticate the transaction.

The Board agrees that sharing a PIN code is more straightforward than sharing biometric data, which is

more difficult for fraudsters to access. However, this difference is a widely known and inherent characteristic of biometric verification, and therefore cannot provide the basis for an inventive step.

15. The Board judges that by the application's priority date in 2013, biometric verification had become a widely recognised alternative to PIN-based user verification. The skilled person was knowledgeable about the advantages of biometric verification, such as eliminating the risk of forgetting or stealing a PIN, and would have replaced the PIN-based verification in D1 with biometric verification as a routine task in line with the prevailing technological trends of the time (see also D2, page 1, lines 5 to 13).

To achieve this, starting from D1, the skilled person would have replaced the PIN stored on the SIM with biometric data, replaced the PIN input step with capturing biometric data and replaced the identification application on the SIM card with an application for verifying the captured biometric data. These modifications would have yielded the claimed authentication method and preserved the advantage of keeping the biometric data (used for user authentication) securely on the SIM card, as is the case with the PIN code in D1.

The fact that in D1 (biometric) identification data is transmitted to the server is not, as argued by the appellant, a technical prejudice against modifying the existing authentication method in the above way. As already mentioned, the biometric data in D1 is not used for user authentication. It is merely authorisation data which is required by the service provider and thus, relates to a different aspect not covered by the

claim.

16. In conclusion, the subject-matter of claim 1 of the main request does not involve an inventive step (Article 56 EPC).

Second auxiliary request, inventive step

17. The additional feature of claim 1 of the second auxiliary request relates to:

B. Input means to enter a personal access code (last feature of the claim).

18. Feature B does not combine in a synergistic manner with the above identified distinguishing feature A (see point 13). While an additional PIN input, e.g. to unlock the mobile device, may enhance security, this improvement is not related to the biometric verification. Both features in combination do not produce any apparent technical effect going beyond the sum of their individual technical effects. As a result, they can be assessed separately for inventive step.

19. Feature B is broad, as it encompasses various applications, including unlocking a mobile device using a PIN input. D1 discloses, in addition to the PIN input for authentication, a further PIN input for reading the identification data (paragraph [0035]) which could be interpreted as anticipating feature B.

In any case, the Board judges that a PIN input for unlocking the mobile device was a prevalent, if not the most prevalent, method used at the priority date of the application and, as such, cannot support an inventive

step.

20. Accordingly, the subject-matter of claim 1 of the second auxiliary request does not involve 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