**Internal distribution code:**

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

**Datasheet for the decision of 13 February 2023**

**Case Number:** T 2321/19 - 3.5.07

**Application Number:** 09153764.7

**Publication Number:** 2224348

**IPC:** G06F17/24, G07F7/08

**Language of the proceedings:** EN

**Title of invention:**
System and method for capturing user inputs in electronic forms

**Applicant:**
BlackBerry Limited

**Headword:**
Capturing user inputs in electronic forms/BLACKBERRY

**Relevant legal provisions:**
EPC Art. 56
RPBA 2020 Art. 11

**Keyword:**
Inventive step - main request, first and second auxiliary requests (no)
Remittal to the department of first instance - third auxiliary request (yes)

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 2321/19 - 3.5.07**

# D E C I S I O N
# of Technical Board of Appeal 3.5.07
# of 13 February 2023

| | |
|---|---|
| **Appellant:** (Applicant) | BlackBerry Limited<br>2200 University Avenue East<br>Waterloo, ON N2K 0A7 (CA) |
| **Representative:** | MERH-IP Matias Erny Reichl Hoffmann<br>Patentanwälte PartG mbB<br>Paul-Heyse-Strasse 29<br>80336 München (DE) |
| **Decision under appeal:** | **Decision of the Examining Division of the European Patent Office posted on 4 April 2019 refusing European patent application No. 09153764.7 pursuant to Article 97(2) EPC** |

**Composition of the Board:**

| | |
|---|---|
| **Chair** | J. Geschwind |
| **Members:** | C. Barel-Faucheux |
| | P. San-Bento Furtado |

## Summary of Facts and Submissions

I. The appellant (applicant) appealed against the decision of the examining division refusing European patent application No. 09153764.7 filed on 26 February 2009.

II. The decision cited *inter alia* the following documents:

D1: US 2004/0243520 A1 published on 2 December 2004
D1': US 7 343 351 B1 published on 11 March 2008
D2: US 6 873 974 B1 published on 29 March 2005
D5: US 6 697 839 B2 published on 24 February 2004

The examining division decided that the subject-matter of claims 1, 7 and 13 of the main request and of the first and second auxiliary requests, the subject-matter of clams 1, 6 and 11 of the third and fourth auxiliary requests, and the subject-matter of claims 1, 4 and 7 of the fifth auxiliary request did not involve an inventive step within the meaning of Article 56 EPC, when taking prior-art document D1 as starting point or alternatively, for the first auxiliary request, document D5.

III. In the statement of grounds of appeal, the appellant requested that the decision under appeal be set aside and a patent be granted on the basis of the claims of one of the main and first to fifth auxiliary requests, all six requests as considered in the contested decision, and the sixth and seventh auxiliary requests, both submitted with the statement of grounds of appeal.

IV. In the communication accompanying the summons to oral proceedings, the board expressed the preliminary view that the subject-matter of claim 1 of the main request

and first to seventh auxiliary requests lacked an inventive step over document D1.

V. In a letter filed in preparation for the oral proceedings, the appellant maintained its pending requests while providing further arguments.

VI. Oral proceedings took place on 13 February 2023. At the end of the oral proceedings, the Chair announced the board's decision.

VII. The appellant's final requests were that the decision under appeal be set aside and that a patent be granted on the basis of the main request or one of the first to fifth auxiliary requests, all six requests as considered in the decision under appeal, or the sixth or seventh auxiliary request submitted with the grounds of appeal. As a further auxiliary request, the appellant requested that the case be remitted to the department of first instance for further prosecution on the basis of the third auxiliary request.

VIII. Claim 1 of the main request reads as follows (itemisation as proposed by the board):

[A] "A method of capturing inputs in a fillable electronic form (600, 600A) into an electronic wallet (148),

[B] wherein the fillable electronic form (600, 600A) is provided by an online website vendor’s module that is executed on a server (350), comprising:

[C] accessing the fillable electronic form (600, 600A) from a wireless handheld device (100);

[D] receiving valid verification data input at the wireless handheld device (100) to populate the fields in the fillable electronic form with the secured information from the electronic wallet;

[E] upon determining whether one or more changes have been made in any field in the fillable electronic form (600, 600A),

[E1] requesting further valid verification data input at the wireless handheld device (100) to receive information from the fields in the fillable electronic form (600, 600A) to update secured information in the electronic wallet (148); and

[E2] upon receiving the further valid verification data input at the wireless handheld device (100), receiving the information from the fields in the fillable electronic form (600, 600A) and writing the information into corresponding record fields as secured information in the electronic wallet (148)."

IX. Claim 1 of the first auxiliary request differs from claim 1 of the main request in that

- the text "the electronic wallet (148) is provided at a wireless handheld device (100) and" has been added before "the fillable electronic form (600, 600A) is provided by an online website vendor's module" in feature B,
- the text "the wireless handheld device (100)" replaced the text "a wireless handheld device (100)" in feature C, and
- the reference sign "(148)" has been added at the end of feature D,

and in that

- the text "at the wireless handheld device (100)" has been added at the end of the claim.

X. Claim 1 of the second auxiliary request reads as follows:

"A method of capturing inputs in a fillable electronic form (600, 600A) into an electronic wallet (148), wherein the electronic wallet (148) is provided at a wireless handheld device (100) and the fillable electronic form (600, 600A) is provided by an online website vendor's module that is executed on a server (350), the wireless handheld device (100) including a processor (102) for enabling execution of plural software applications (134) on the wireless handheld device (100), the software applications (134) including the electronic wallet (148), wherein the electronic wallet (148) has an update module (151) and a wallet security module (149) configured to allow controlled access to the electronic wallet (148),
the method comprising:
accessing the fillable electronic form (600, 600A) from the wireless handheld device (100);
receiving, upon the wallet security module (149) of the electronic wallet (148) requiring a user of the wireless handheld device (100) to provide verification data, valid verification data input at the wireless handheld device (100) to populate the fields in the fillable electronic form with secured information from the electronic wallet (148);
requesting, upon determining whether one or more changes have been made in any field in the fillable electronic form (600, 600A), further valid verification data input at the wireless handheld device (100) to receive information from the fields in the fillable electronic form (600, 600A) to update the secured information in the electronic wallet (148) by the update module (151) of the electronic wallet (148); and
receiving, upon receiving the further valid verification data input at the wireless handheld device (100), the information from the fields in the fillable electronic form (600, 600A) and updating the secured

information stored in the electronic wallet (148) by the update module (151) of the electronic wallet (148), including writing the information into corresponding record fields as secured information in the electronic wallet (148) at the wireless handheld device (100)."

XI. Claim 1 of the third auxiliary request differs from claim 1 of the second auxiliary request in that the text "by at least one of a fingerprint press, a swipe input, a voice password and a voice command" has been added before "to populate the fields in the fillable electronic form with secured information from the electronic wallet (148)" and after "receiving, upon receiving the further valid verification data input at the wireless handheld device (100)".

XII. For the present decision it is not necessary to reproduce the text of claim 1 of the other auxiliary requests here.

XIII. The appellant's arguments, where relevant to this decision, are discussed in detail below.

## Reasons for the Decision

*The application*

1. The application relates to electronic forms and to a system and method for capturing user inputs made in those forms as well as a system and method for making electronic payments, in particular with a wireless hand-held device in a wireless operating environment (paragraphs [0001], [0026] and [0027] of the published application).

2. The wireless hand-held device 100 may include an electronic wallet 148 having, among other things, a security module 149 and an update module 151 (paragraph [0035]; Figure 1). The wireless hand-held device 100 may have access to online vendors having web servers 350, 360 from which a user of the wireless hand-held device may electronically purchase goods or services (paragraph [0038]; Figure 3).

3. Amended information entered into a fillable electronic form on a web server may be captured and copied back to the electronic wallet 148 in a secure manner. User authorisation is required to update the information. The user is required to enter amended information in a fillable electronic form once and to copy any amended information back to the electronic wallet either to overwrite the original information or to save the amended information as alternative information (paragraphs [0063] and [0065]).

*Main request*

4. For the wording of claim 1 of the main request and its itemisation by the board, reference is made to point VIII. above.

*Main request - Inventive step*

*5. Discussion on the disclosure of features A and B*

5.1 Document D1 discloses a transaction system 100 used in electronic commerce to conduct purchase transactions, the transaction system 100 including at least one customer computer 110, a merchant computer 120, a security server 130 and a digital wallet server 140 (paragraph [0033], Figure 1A). To conduct a

transaction, customer 110 establishes a connection through network 102 with a merchant 120. When a purchase is to be made, customer 110 accesses wallet server 140. Wallet server 140 may include functionality for completing purchase forms affiliated with merchant computer 120 (paragraph [0037]).

5.2 A user may apply for a digital wallet by contacting a Web server such as a wallet server 140 on network 102. The user completes a registration form to apply for the wallet. Wallet server 140 receives demographic, account and other information (e.g. address, shipping address, name, credit card number, and the like) from an authentication server 306 (or from another server on a private network). This information may be used to configure a wallet client 214 that is unique to the particular user. This information is also used to pre-fill the wallet client (paragraph [0085]).

5.3 If the wallet application is approved, a card reader and a special code (such as a cryptographic key, a password, etc.) are provided to the user. The user then registers for the online wallet service by electronically contacting wallet server 140 and authenticating to the server with the card and/or with the special code. After providing the special code, the user receives a specially configured copy of the wallet software which may be installed on customer computer 110. Configuration information for a particular user is thus associated with a code that is provided to the user, who may later present the special code to authenticate him/herself with wallet server 140 to obtain a copy of the wallet that has already been pre-configured with data specific to the particular user (paragraph [0086]). The special code can be

considered a "(valid) verification data input" within the meaning of claim 1.

5.4 In document D1, when a user indicates a desired purchase at an on-line merchant's site, a checkout user interface 802 of a digital wallet is displayed. Much of the user-specific information that a user would normally have to enter at the merchant checkout (for example, name, address, e-mail address, credit card information, etc.) is already known by the digital wallet and is pre-filled in the digital wallet checkout window 802. The user can edit the pre-filled information (paragraphs [0063] to [0065]; Figure 8).

5.5 Therefore, features A and B are disclosed in document D1.

*6. Discussion on the disclosure of features C and D:*

7. Concerning feature C, the invention of document D1 may use Wireless Application Protocol (WAP) phones (paragraph [0097]; see also paragraphs [0032] and [0058]) corresponding to a "wireless handheld device" of claim 1.

7.1 The appellant argued that the entire thrust of document D1 was an implementation using a PC as the client computer, to which a smart card reader 204 for reading a smart card 202 was attached (the appellant referred to Figure 2). No enabling details were provided in D1 as to how a wireless hand-held device could be adapted to access a fillable electronic form. D1 did not even discuss a possible connection of a card reader via USB to a wireless electronic device. D1 lacked an enabling disclosure for the implementation on

a wireless hand-held device (statement of grounds, page 3, last paragraph).

7.2 The board is of the opinion that the use of a wireless hand-held device is disclosed in D1 (see point 7. above). In document D1, the user can register for the online wallet service by electronically contacting wallet server 140 and authenticating to the server by using a special code as an alternative to a card reader (paragraph [0086]). The board further notes that claim 1 does not include any novel features specifically adapted to implementation on a wireless hand-held device.

7.3 The appellant argued that the use of a smartcard together with a wireless handheld device was not apparent in 2004 when D1 was drafted. The skilled person would have understood that a possible implementation of the customer device would require a personal computer having the possibility of being connected with a smartcard. The board notes however that the last sentence of paragraph [0049] of D1 explicitly states that while the embodiments described in D1 use a smartcard, "other intelligent tokens, for example a global system for mobile communication (GSM) mobile phone, can be substituted for the smartcard".

7.4 The appellant argued that the "special code" mentioned in paragraph [0086] of D1 was for the configuration of the wallet client and not for login into the system for performing a transaction (letter of reply to the board's communication, page 2). The board notes however that document D1 discloses in paragraphs [0010] and [0037] that the user provides valid verification data ("digital credentials"), as in feature D of claim 1, when the user wants to conduct a transaction.

7.5 The appellant also argued that the usage of a smartcard was mandatory in D1 (otherwise processing of the cryptographic challenges would not be possible and no security token would be available), and user authentication was performed during user login, before generation of the security token by the cryptographic process, and well before any purchase transaction and pre-filling of a checkout window (window 802 as shown in Figure 8) (letter of reply to the board's communication, paragraph bridging page 2 to page 3).

7.5.1 The board notes that, while paragraph [0087] of D1 starts with "customer 110 suitably initiates a transaction by logging in to wallet server 140 using smartcard 202", it goes on to state that "a form entry and submission button for user/password login and a hypertext link for smartcard login are provided as part of the login page". The user might select one particular form of logging in (in the example given, a "smartcard login"). Password login, or login with a code, is an alternative option to login with a smartcard. Thus, while embodiments with a smartcard are disclosed in detail in document D1, the board does not consider that according to D1 usage of a smartcard is absolutely necessary to achieve the security measures envisaged in document D1. This is also confirmed by paragraph [0010], describing existing digital wallet technology: in order to gain access to the wallet data, the customer authenticates himself/herself by supplying either an ID/password or a smartcard.

7.5.2 In addition, even when a smartcard is used, it includes identifying information (such as a digital certificate) that uniquely identifies the card (paragraph [0037]). This "identifying information" also constitutes a

"valid verification data input" within the meaning of claim 1 of the main request.

7.5.3 The board further notes that paragraph [0058] of document D1 teaches that the system can be implemented on, for example, a wireless electronic device or "any other similar device" and on an operating system like "Palm OS".

7.6 The appellant argued that feature D was not disclosed in document D1. It stated that in claim 1, "at least implicitly", the input of data was by the user of the wireless hand-held device (denoted "first argument" in the following) and "receiving valid verification data..." (in feature D) was performed after feature C (denoted "second argument"). As regards population of HTML forms (as well as the digital wallet checkout window), this occurred in D1 many steps after the entry of the PIN for use with the smartcard (statement of grounds, page 4, first paragraph and last sentence of third paragraph). Thus, in D1, any input of "valid verification data" (see step D of claim 1) by the user occurred prior to step C. A technical effect of these differences was that the user could see the type/nature of form before entering valid verification data, and that the fields were displayed in populated form only if such valid verification data was entered, thus enhancing security, as the populated data could be sensitive (statement of grounds, paragraph bridging page 4 to page 5).

7.6.1 The board is however of the opinion that feature D is disclosed in document D1 in paragraph [0037] and in paragraphs [0063] to [0066], with reference to Figure 8. According to these passages of D1, when a customer makes a purchase, the customer uses the

digital credentials to authenticate to the wallet server. The wallet server completes the transaction, including completing "the purchase forms affiliated with the merchant computer" using the digital wallet. Paragraph [0063] clearly explains that much of the information that a user would normally have to enter is pre-filled. Therefore, the first and second arguments are not convincing.

7.7 The appellant further argued that D1 did not explain when and how window 804 shown in Figure 8 was accessed/ displayed. No field of this electronic form 804 was filled or populated with secured information from the electronic wallet. Thus, even if it were possible to access window 804 before the user login/authentication mentioned above, window 804 would not be the (same) fillable electronic form accessed in step C of claim 1 and then populated with the secured electronic information from the electronic wallet upon receiving valid verification data input in step D (which we will denote "third argument") (letter of reply to the board's communication, first full paragraph of page 3).

7.8 Concerning the second and third arguments, a fillable electronic form as a checkout user interface 802 is shown on the right side of Figure 8 of document D1 and some information about the user is pre-filled, such as "Blue from American Express" under the "Credit Card" field or "HOME" under the "Shipping Address" field. This pre-filled information is "secured information", since it is provided in a secure manner by the digital wallet, and can be edited (paragraph [0063] together with Figure 8). Accessing this pre-filled electronic form and editing it takes place after valid verification data has been received (see paragraph

[0037] and point 7.6.1 above). In this case, step C occurs prior to step D.

7.9 The board notes that, in document D1, when a user goes to the previously visited page, the digital wallet, in addition to populating the form with fields that are retrieved from the wallet system, will also populate the form with values that had previously been remembered. When pre-filling the form, the wallet will securely retrieve field values from the server (paragraph [0066]). Thus the pre-filled form is populated with secured information contained in the electronic wallet together with information provided by the remembering function.

7.10 Therefore, the board considers that features C and D are disclosed by document D1.

*8. Discussion on the disclosure of feature E:*

8.1 The board notes that, in document D1, the process by which the user interacts with a Web site can either be fully automated or can be user-mediated: in this case the digital wallet can pre-fill form fields for the user, but the user can correct, change, or complete any fields that require further data entry (paragraph [0077]). Moreover, paragraph [0063] discloses that the user can edit the pre-filled information. Thus the method disclosed by document D1 implicitly determines whether one or more changes have been made in any field in the fillable electronic form.

Therefore, the board considers that feature E is disclosed in document D1.

9. Consequently, the distinguishing features of claim 1 of the main request having regard to document D1 are features E1 and E2.

10. The appellant argued that a technical effect of the "further valid verification data" was that updates/ changes to data securely stored in the wallet could only be made by persons in possession of the further valid verification data, thereby "enhancing security and integrity of (potentially sensitive) data stored on the electronic wallet of the wireless hand-held device" (statement of grounds, page 6, first full paragraph). The board agrees with this technical effect.

11. The appellant stated that the distinguishing features provided the benefits over D1 that a fillable form could be accessed from a mobile wireless hand-held device in a more efficient, secure and reliable manner in a system in which the electronic wallet was locally provided, in contrast to a separate wallet server, and in that operability and security were improved; even if the user made changes in already populated fields, the wallet information could conveniently be automatically updated in the electronic wallet, secured by another verification, in order to also update previously stored information rather than remembering manually input fields other than those that were automatically populated by the wallet (statement of grounds of appeal, paragraph bridging pages 6 and 7).

12. The appellant formulated the technical problem as "how to enhance the security and reliability of capture of data from online forms, for use with an auto-fill function" (statement of grounds of appeal, page 7, first full paragraph, and page 9, third paragraph).

The board finds that the appellant formulated the problem too broadly and agrees with the examining division that the distinguishing features solve the objective technical problem of "prevent[ing] corruption of the data in the electronic wallet by an unauthorised person" (decision, page 6, second full paragraph).

13. The examining division argued that document D1, paragraph [0002], under "Field of the invention", related to systems for authenticating and conducting business over the Internet. Thus the person skilled in the art would always be seeking to maximise security. Paragraphs [0086] and [0087] explicitly stated that additional verification checks could be added to improve security. Adding such further verification when the user made updates which should be stored to the wallet would thus be an obvious solution to the objective technical problem for a person skilled in the art starting from the teaching of document D1.

13.1 The appellant argued that "[t]o the extent that D1 indicates that (compared with the main embodiments thereof) security in relation to the wallet may be further enhanced, the person skilled in the art is directed to do so through further security measures implemented server-side [...] rather than implementing further security measures (requiring additional input of verification data) on the client PC" (statement of grounds of appeal, paragraph bridging page 7 to page 8; the appellant referred to paragraphs [0051] and [0097] of document D1). The auto-remember function of D1 did not benefit from further verifications since the wallet information was not updated to update changes but only remembered fields not previously populated (statement

of grounds of appeal, page 8, third full paragraph). The other cited documents did not fill the gaps left by document D1 (statement of grounds of appeal, last two lines of page 8). In the absence of any additional/ appropriate hints or prompts in document D1 towards the specific combination of features of the independent claims, the subject-matter of the independent claims was not rendered obvious by document D1. It was maintained that concluding that the invention would be obvious in light of document D1 was only possible based on an *ex-post facto* analysis of the claimed subject-matter (statement of grounds, first full paragraph of page 9).

14. The appellant argued that document D1 already suggested an extensive login/user authentication process via smartcard and a cryptographic process that resulted in a security token provided to the user device (to establish identity and securely interact with the wallet server), which was to be used in a subsequent transaction (reference was made to paragraph [92] of document D1). There was no reason why the skilled person would add further user verification data input to the system of document D1. Given the extensive user validation at user login in document D1 and the usage of security tokens before a purchase transaction comprising access to a fillable electronic form was performed, there was no reason for the skilled person to consider another user verification data input after a fillable form was accessed.

When considering the disclosure of D1, the skilled person would not be motivated to add a data update function for any field in an electronic form that was populated by an electronic wallet and that was later changed by the user. In addition, requesting twofold

user validation data input after accessing the electronic form and before saving data changes was not necessary in D1 and would be more inconvenient for the user. Thus, it would not be obvious for the skilled person to add all these measures to the system of D1, and consequently the claimed method of the main request was based on an inventive step.

15. However, the board is of the opinion that it is standard practice to require valid verification data to avoid unauthorised access to data, and document D1 already discloses using verification data when using the electronic wallet to pre-fill forms. It would thus be obvious for the skilled person seeking to prevent data corruption by an unauthorised person to request further valid verification data input at the wireless hand-held device upon determining that one or more changes have been made in any field of the fillable electronic form and before updating secured information in the electronic wallet.

16. Thus, claim 1 of the main request is not inventive (Article 56 EPC).

*First auxiliary request - Inventive step*

17. Claim 1 of the first auxiliary request differs from claim 1 of the main request essentially in that it is specified that "the electronic wallet (148) is provided at a wireless handheld device (100)".

18. The appellant argued that D1 suggested a server-based approach comprising a wallet server 140 and a wallet client 214 to access the data on the wallet server (reference was made to paragraphs [0037], [0039] and [0057] of document D1) after having established a

secured communication link between client and server (reference was made to paragraphs [0088] to [0090]). The secured information was stored on the wallet server and it was the wallet server that filled the fields of an electronic form with data from the wallet for a purchase transaction (reference was made to paragraphs [0010], [0037] and [0096]).

19. The appellant further argued that since D1 was completely focused on a server-based wallet system, the skilled person would not be motivated to consider a change to a wireless handheld device-based wallet implementation. In fact, this would require a number of significant changes to the disclosure of D1 (including wallet and auto-remember functions) that a skilled person would not consider without exercising inventive skill.

20. This feature is however hinted at in document D1: after providing a special code, a user can receive a specially configured copy of the wallet software which may be installed on the customer computer or wireless hand-held device (see paragraph [0086]) (see also decision, point 21). Moreover, paragraph [0097] discloses that servers coupled to network 102 may provide various functionalities to the multiple clients 110 through server languages by providing scripts (or code) from the server to the client. The scripts are interpreted and executed by a browser program in for example Wireless Application Protocol (WAP) phones that support Wireless Markup Language(WML) scripts.

21. At the date of filing of the present application, the different options of client/server architectures were well known and it would be an obvious option for the

skilled person to implement the digital wallet at the client.

22. Thus, claim 1 of the first auxiliary request is not inventive (Article 56 EPC).

*Second auxiliary request - Inventive step*

*23.* Claim 1 of the second auxiliary request differs from claim 1 of the first auxiliary request essentially in that it is specified that

- the wireless handheld device (100) includes "a processor (102) for enabling execution of plural software applications (134) on the wireless handheld device (100), the software applications (134) including the electronic wallet (148), wherein the electronic wallet (148) has an update module (151) and a wallet security module (149) configured to allow controlled access to the electronic wallet (148)";
- the receiving step D is performed "upon the wallet security module (149) requiring a user of the wireless handheld device (100) to provide verification data";
- the secured information is updated by the update module (151) of the electronic wallet (148); and
- in the step at the end of the claim, upon receiving further validation data the step is performed of "updating the secured information stored in the electronic wallet (148) by the update module (151) of the electronic wallet (148), including" writing the information into corresponding record fields as secured information.

24. The examining division argued that the additional features of the second auxiliary request were "obvious

implementation details of the provision of the electronic wallet at the wireless hand-held device" (decision, point 23).

25. The appellant argued that a technical effect of the distinguishing features was that extensive wireless communication with wallet servers, security servers and/or authorisation servers was avoided, reducing or minimising wireless traffic, and entry of verification data to enable auto-fill and data change was facilitated through simple interaction (e.g. fingerprint scan). Bandwidth and processor/battery usage could be reduced.

The subject matter of claim 1 of the second auxiliary request addressed the problem of how to enhance the security and reliability of capture of data from online forms, for use with an auto-fill function on a wireless hand-held device, while minimising resource usage. Document D1 taught away from the claimed subject-matter.

26. The board notes that the electronic wallet of document D1 implicitly comprises an update module, since the user may change data in the pre-filled forms, and a security module, since the user is required to enter credentials, such as a code, in order to use the digital wallet (paragraphs [0037] and [0063]). Indeed, the only functionality specified in the claim for the security module is that it allows controlled access to the electronic wallet and requires a user to provide verification data. Document D1 discloses a security server 130 as shown in figure 3. The "security engine 304" resides outside a firewall to administer data transfers between the security server 130 and the customer 110 or wallet server 140. An authorisation

server 306 retaining valuable confidential information such as a database 310 may be suitably maintained on an internal network for enhanced security. But D1 also states that the functionality of security engine 304 and authorisation server 306 may be combined or separated (paragraphs [0050] and [0051]; Figure 3).

26.1 The appellant argued that both servers 304, 306 were components of the security server 130, which was clearly a distinct entity that was separated from the customer computer 110 by the data network 102 (reference was made to Figures 1A to 1C). There was no indication in document D1 that the security server and its components could be made part of the customer computer. Actually, paragraph [0034] suggested increased security if the security server 130 was connected, separately from data network 102, via networks 150, 152 with merchant server 120 and wallet server 140. Thus, the skilled person would even be discouraged from abandoning the server architecture, which according to paragraph [0037] was essential to achieve the desired security enhancements.

27. The appellant argued that D1 was suggesting storing the sensitive wallet data on the wallet server and making the security checks on the server-side, and there was no apparent reason why the skilled person would do away with the system architecture of document D1.

28. As explained for the higher ranking requests, the board is of the opinion that document D1 discloses providing the electronic wallet at a wireless handheld device and that the skilled person would consider modifying the system of D1 to move functionality from the server to the client. When implementing such a client-based solution, it would be an obvious implementation option

for the skilled person to include the update and security modules in the client.

The additional features are thus mere obvious implementation options once the skilled person decides, without exercising inventive skill, to change the wallet to the user device. These implementation options are within the ordinary skills of a programmer.

29. Therefore, claim 1 of the second auxiliary request is not inventive (Article 56 EPC).

*Third auxiliary request*

30. Claim 1 of the third auxiliary request differs from claim 1 of the second auxiliary request in that the "verification data" and the "further verification data" are input at the wireless hand-held device by at least one of a fingerprint press, a swipe input, a voice password and a voice comment.

*Request for remittal to the examining division for further prosecution on the basis of the third auxiliary request, Article 11 RPBA 2020*

31. None of the (non-post-published) cited documents discloses this additional feature.

32. In the decision, the examining division argued that claim 1 of the third auxiliary request merely listed four well known forms of verification data input any of which could be employed at the wireless electronic device. It would be a mere matter of choice for the person skilled in the art to use any of the suggested forms of verification data input according to the

specific hardware being used and the known security gains of each of the data input forms.

33. During the oral proceedings before the board, the appellant argued that it was very difficult, thirteen years after the date of filing of the present application, to assess what was the common general knowledge of the person skilled in wireless hand-held devices at the date of filing of the application, especially since the technology of mobile phones had evolved very quickly at that time. The appellant suggested that, since there was no documentary evidence of the common general knowledge, the board should consider remitting the case to the department of first instance for further prosecution.

34. The board considers that this aspect of the common general knowledge of the skilled person is highly relevant to decide on inventive step.
In the present situation, the appellant should be given the opportunity to argue and discuss in two instances about the relevant evidence, if any, relating to the relevant common general knowledge. These are special reasons under Article 11 RPBA 2020 for remitting the case to the examining division for further prosecution on the basis of the third auxiliary request.

**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 for further prosecution on the basis of the third auxiliary request.

The Registrar: The Chair:

S. Lichtenvort J. Geschwind

Decision electronically authenticated