Internal distribution code:

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

Datasheet for the decision of 27 June 2024

Case Number: T 0081/22 - 3.4.03

Application Number: 10828363.1

Publication Number: 2500880

IPC: G07G1/12, G06Q10/00, G06Q20/00, G09C1/00, H04L9/32, G06Q20/32, G06Q20/36, G06Q20/38, G06Q20/40, G07F7/10, G07F7/12, G06F21/34

Language of the proceedings: EN

Title of invention:
HANDY TERMINAL AND PAYMENT METHOD USED FOR THE HANDY TERMINAL

Applicant:
NEC Platforms, Ltd.

Relevant legal provisions:
EPC 1973 Art. 56

Keyword:
Inventive step - (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 0081/22 - 3.4.03

D E C I S I O N
of Technical Board of Appeal 3.4.03
of 27 June 2024

Appellant: (Applicant)	NEC Platforms, Ltd. 2-6-1, Kitamikata, Takatsu-ku, Kawasaki-shi Kanagawa 213-8511 (JP)
Representative:	Vossius & Partner Patentanwälte Rechtsanwälte mbB Siebertstrasse 3 81675 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 27 August 2021 refusing European patent application No. 10828363.1 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairwoman	D. Prietzel-Funk
Members:	M. Ley
	J. Thomas

Summary of Facts and Submissions

I. The appeal is against the decision of the examining division refusing European patent application No. 10 828 363 pursuant to Article 97(2) EPC.

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

D1 US 2008/0041933 A1
D3 US 2006/0020821 A1
D4 GB 2 445 231 A
D9 "VeriSign® Code Signing for Microsoft® Authenticode® Technology", 25 October 2005

III. The examining division decided that the subject-matter of claim 1 did not involve an inventive step (Article 56 EPC) in view of D1.

IV. The appellant requested that the impugned decision be set aside and a European patent be granted on the basis of the main request filed as auxiliary request 2 with the letter dated 28 September 2023.

V. Claim 1 of the main request has the following wording (board's labelling):

A handy terminal (1) with payment capability including ***(a)*** *a main board (2) and* ***(b)*** *a keyboard unit (3) connected to each other through a serial interface,*

the main board (2) comprising a ***(a1)*** *main board memory (11) storing an application program (11a) and a payment program (11b),* ***(a2)*** *a main CPU (12) to perform execution processing of the application program (11a)*

and the payment program (11b), and ***(a3)*** *a display unit (13) to display contents of the application program (11a) and the payment program (11b) and contents inputted from outside, the keyboard unit (3) comprising* ***(b1)*** *a common keyboard (22) for inputting data at a time of executing the application program (11a) and inputting a PIN of a credit card at a time of executing the payment program (11b),* ***(b2)*** *a card reader (24) to read information stored in the credit card,* ***(b3)*** *a sub CPU (21) to control various kinds of programs mounted on the keyboard unit (3), and* ***(b4)*** *a keyboard unit memory (23) storing control programs installed in the keyboard unit (3),*
characterized in that:
(c) *the payment program (11b) being a program for use in judging whether it is legitimately released prior to operations of the inputting of the PIN input of the credit card;*
(d) *the main CPU (12) is configured to install (S27) a coupled module consisting of an encrypted first hash value and the payment program (11b) in the main board memory (11) of the main board (2) at a time of installing the payment program (11b), the encrypted first hash value being obtained by encrypting a first hash value by using a secret key for prevention from stealing the first hash value, the first hash value being calculated by using a developed personal computer;*
(e) *the sub CPU (21) is configured to install (S29) a public key in the keyboard unit memory (23) on the keyboard unit (3) at the time of installing the payment program (11b), the public key being prepared in order to decrypt a hash value;*
(f) *the main CPU (12) is configured to separate (S31) the coupled module to the payment program (11b) and the encrypted first hash value in order to perform a*

certification process of the payment program (11b) ***(f*)*** *every time the payment program (11b) is booted;*
(g) *the main CPU (12) is configured to leave (S32) the payment program (11b) in the main board memory (11) of the main board (2) in the certification process of the payment program (11b);*
(h) *the main CPU (12) is configured to transfer (S33) the encrypted first hash value to the keyboard unit (3) in the certification process of the payment program (11b);*
(i) *the main CPU (12) is configured to calculate (S36) a second hash value of the left payment program (11b) in the certification process of the payment program (11b),* ***(j)*** *where each hash value, as used in order to detect alteration of the payment program (11b), is a random number of fixed length produced from given data in the payment program (11b), by using a specified calculation method;*
(k) *the main CPU (12) is configured to encrypt (S38) the calculated second hash value by using an encrypted key to transfer (S39) an encrypted second hash value to the keyboard unit (3) in the certification process of the payment program (11b),*
(l) *wherein the encrypted key is produced (S37) by using a random number on the keyboard unit (3) for prevention from stealing of the second hash value and is sent to the main board (2);*
(m) *the sub CPU (21) is configured to decrypt (S34, S41) the encrypted first hash value and the encrypted second hash value by using the public key and the encrypted key, respectively, in the certification process of the payment program (11b);*
(n) *the sub CPU (21) is configured to compare (S42) the decrypted first hash value and the decrypted second hash value in the certification process of the payment program (11b);*

(o) *if a comparison result shows that the decrypted first hash value is aligned with the decrypted second hash value, the sub CPU (21) is configured to determine that the payment program (11b) is to be certified and to store (S43) a certification result in the keyboard unit memory (23) on the keyboard unit (3) in the certification process of the payment program (11b);*
(p) *a card reader control program (23b) stored in the keyboard unit memory (23) to detect a state of insertion and extraction of the credit card; and*
(q) *a keyboard control program (23a) stored in the keyboard unit memory (23) is to control notification of a key code based on results from the comparison by the sub CPU (21) and on the state of insertion and extraction of the credit card;*
(r) *wherein, when the sub CPU (21) judges that the decrypted first hash value is aligned with the decrypted second hash value and when the insertion of the credit card is detected by the card reader control program (23b), the keyboard control program (23a) notifies the main board (2) of the key code and enables execution of inputting of a PIN code of the credit card,*
(s) *whereas, when the sub CPU (21) judges that the decrypted first hash value is not aligned with the decrypted second hash value, the keyboard control program (23a) denies the notification of the key code to the main board (2) and disables the execution of inputting of the PIN code.*

Claim 2 of the main request has the following wording:

A payment method to be used in a handy terminal (1) including a main board (2) and a keyboard unit (3) connected to each other through a serial interface, the main board (2) comprising a main board memory (11)

storing an application program (11a) and a payment program (11b), a main CPU (12) to perform execution processing of the application program (11a) and the payment program (11b), and a display unit (13) to display contents of the application program (11a) and the payment program (11b) and contents inputted from outside, the keyboard unit (3) comprising a common keyboard (22) for inputting data at a time of executing the application program (11a) and inputting a PIN of a credit card at a time of executing the payment program (11b), a card reader (24) to read information stored in the credit card, a sub CPU (21) to control various kinds of programs mounted on the keyboard unit (3), and a keyboard unit memory (23) storing control programs installed in the keyboard unit (3), the payment program (11b) being a program for use in judging whether it is legitimately released prior to operations of the inputting of the PIN input of the credit card, the payment method characterized by comprising:
an installing step (S27), in the main CPU (12), installs a coupled module consisting of an encrypted first hash value and the payment program (11b) in the main board memory (11) of the main board (2) at a time of installing the payment program (11b),
the encrypted first hash value being obtained by encrypting a first hash value by using a secret key for prevention from stealing of the first hash value, the first hash value being calculated by using a developed personal computer;
an installing step (S29), in the sub CPU (21), installs a public key in the keyboard unit memory (23) on the keyboard unit (3) at the time of installing the payment program (11b), the public key being prepared in order to decrypt a hash value;
a separating step (S31), in the main CPU (12), separates the coupled module to the payment program

(11b) and the encrypted first hash value in order to perform a certification process of the payment program (11b) every time the payment program (11b) is booted;
a leaving step (S32), in the main CPU (12), leaves the payment program (11b) in the main board memory (11) of the main board (2) in the certification process of the payment program (11b);
a transferring step (S33), in the main CPU (12), transfers the encrypted first hash value to the keyboard unit (3) in the certification process of the payment program (11b);
a calculating step (S36), in the main CPU (12), calculates a second hash value of the left payment program (11b) in the certification process of the payment program (11b), where each hash value, as used in order to detect alteration of the payment program (11b), is a random number of fixed length produced from given data in the payment program (11b), by using a specified calculation method;
an encrypting step (S38), in the main CPU (12), encrypts the calculated second hash value by using an encrypted key to transfer (S39) an encrypted second hash value to the keyboard unit (3) in the certification process of the payment program (11b), wherein the encrypted key is produced (S37) by using a random number on the keyboard unit (3) for prevention from stealing of the second hash value and is sent to the main board (2);
a decrypting step (S34, S41), in the sub CPU (21), decrypts the encrypted first hash value and the encrypted second hash value by using the public key and the encrypted key, respectively, in the certification process of the payment program (11b);
a comparing step (S42) in the sub CPU (21) compares the decrypted first hash value and the decrypted second hash value in the certification process of the payment

program (11b);
if a comparison result shows that the decrypted first hash value is aligned with the decrypted second hash value, a determining and storing step (S43), the sub CPU (21) determines that the payment program (11b) is to be certified and stores a certification result in the keyboard unit memory (23) on the keyboard unit (3) in the certification process of the payment program (11b);
a detecting step (S7, S11) in a card reader control program (23b) stored in the keyboard unit memory (23) detects a state of insertion and extraction of the credit card; and
a controlling step in a keyboard control program (23a) stored in the keyboard unit memory (23) controls notification of a key code based on results from the comparison in the comparing step (S42) and on the state of insertion and extraction of the credit card in the detecting step,
wherein, when the sub CPU (21) judges in the comparing step (S42) that the decrypted first hash value is aligned with the decrypted second hash value and when the insertion of the credit card is detected by the card reader control program (23b) in the detecting step (S7), the keyboard control program (23a) in the controlling step notifies the main board (2) of the key code and enables execution of inputting of a PIN code of the credit card, whereas,
when the sub CPU (21) judges in the comparing step (S42) that the decrypted first hash value is not aligned with the decrypted second hash value, the keyboard control program (23a) in the controlling step denies the notification of the key code to the main board (2) and disables the execution of inputting of the PIN code.

VI. The appellant argued that the skilled person would not combine documents D1 with the certification process known from D9, D3 or D4. Such a combination would not lead to the claimed subject-matter, either.

Reasons for the Decision

1. The invention concerns a handy terminal with payment capability and a payment method to be used in the handy terminal. In general, the object of the invention is to provide a settlement function of ensuring security with a simple system even when a keyboard for inputting of an application program and inputting of a PIN code in combination with a display device are commonly used (paragraph [0012] of the application).

2. The appellant argued that, in document D1, the code processor 121 encrypted the PIN information, and notified the encrypted PIN information to the CPU 111 (see D1, paragraphs [0060], [0078], [0096], [0115], Step SA10 in Figure 4, Step SB10 in Figure 7, Step SC10 in Figure 10, and Step SD10 in Figure 13). Moreover, the controller (125, 512, 612, 711) checked each unit of the secured module (120, 510, 610, 710) for any abnormality such as breakage, etc. (see D1, paragraphs [0056], [0074], [0092], [0110], Step SA6 in Figure 4, Step SB6 in Figure 7, Step SC6 in Figure 10, and Step SD6 in Figure 13). These security checks performed in D1 did not concern the settlement of account programs, but were performed at a timing when the CPU 111 started the settlement of the account application program (see D1, paragraph [0055], Step SA4 of Figure 4, Step SB4 of Figure 7, Step SC4 of Figure 10, and Step SD4 of Figure 13).

Thus, D1 taught various security checks for the purpose

of preventing illegal readouts of the PIN information from the secured module 120 (see D1, paragraph [0049]). D1 never performed a certification process of the payment program (the settlement of account application program) in order to prevent the PIN code from being stolen by a malicious program (in contrast to a legitimate payment program; see paragraphs [0024] and [0039] of the description of the present application). In view of said security checks, a certification process similar to those of the prior art was not necessary in D1.

In the present invention, encryption/decryption was carried out in order to "confirm legitimateness" of a payment program by making, in advance, a designated program certification (see paragraph [0015] of the description of the present application). The problems to be solved were completely different between the present invention and Dl.

The "PIN information" or the "card information" described in D1 (see e.g. paragraphs [0008] and [0009] of the description of the present application) were not a "payment program" (see paragraph [0039], Figure 2 of the present application). In other words, D1 failed to disclose features (c) to (s). D1 never judged whether the "settlement of account application program" (the payment program) itself was legitimately released as it was the case of the present invention.

In particular, regarding features (k) and (l), the appellant disagreed with the examining division that they had a "predictable disadvantage" in view of paragraph [0033] of the description of the present application. The fact that the certification process of the payment program as claimed was performed each time

the payment program was booted and the fact that each time an encrypted key was produced by a random number (feature (l)) increased the security of the handy terminal.

The appellant acknowledged that e.g. document D9 (pages 7 and 8) described a well-known technique for code signing and code verification. In D9, the end-user browser merely decrypted the signed hash using the publisher's public key, ran the code through the same hashing algorithm as the publisher, created a new hash, and compared the two hashes. The operations described in D9 were not comparable to those recited by independent claim 1. Although "the signed hash" and "the publisher's public key" of D9 might correspond to "the encrypted first hash value" and "a public key" of the amended claim 1, respectively, "a new hash" of D9 did not correspond to "the decrypted second hash value" as recited by independent claim 1. D9 failed to disclose decryption of the first and second encrypted hash values every time the payment program was booted or executed, and failed to disclose encryption and decryption of a second hash value. D9 never carried out encryption and decryption of a second hash value using an encrypted key produced by using a random number.

D3 disclosed, as the operation subject, a software load system authentication module 68 (see Figure 3 of D3), whereas D4 disclosed as the operation subject a Trusted Platform Module (TPM) chip 309 (see Figures 3 and 4 of D4).

Hence, a combination of D1 with either D3, D4 or D9 would not lead the skilled person to the subject-matter of claim 1.

3. For the board, document D1 discloses a handy terminal (Figures 1 and 3, [0034], [0035], [0038], "*transaction terminal device 100*") with payment capability including a main board (110, Figure 3, [0038]) and a keyboard unit (120, Figure 3, [0043]) connected to each other through an interface ([0045], Figure 3),
the main board (110) comprising a main board memory (112, Figure 3, [0038], [0039]) storing an application program and a payment program ([0039]), a main CPU (111, [0038]) to perform execution processing of the application program ([0052], Figure 4, SA1) and the payment program ([0055], Figure 4, SA4), and a display unit (114, Figure 3, [0038], [0040], [0062]) to display contents of the application program and the payment program and contents input from outside, the keyboard unit (120) comprising a common keyboard (122, Figure 3, [0043]) for inputting data at a time of executing the application program ([0052], Figure 4, SA2) and inputting a PIN of a credit card at a time of executing the payment program ([0055], Figure 4, SA4, [0059], SA9), a card reader (123, Figure 3, [0043]) to read information stored in the credit card ([0047]), a sub CPU (121, Figure 3, [0041], [0043]) to control various kinds of programs mounted on the keyboard unit (120, [0058] to [0060]), and a keyboard unit memory (implicit) storing control programs installed in the keyboard unit (120).

Hence, document D1 discloses features (a), (b), (a1) to (a3) and (b1) to (b4), while the interface between the main CPU 121 and the sub CPU 111 is not characterized as "serial" interface.

In document D1, the main CPU 111 is configured to encrypt communications to the keyboard unit 120 ([0038], [0045]) and the sub CPU 121 is configured to

decrypt communications from the main board 110 ([0045]).

The handy terminal of D1 further includes a card reader control program stored in the keyboard unit memory to detect a state of insertion and extraction of the credit card ([0047], [0059], [0060], Figure 4, SA9, SA10; it is implicit that the insertion of the card is detected, as it precedes a step of allowing the customer to enter PIN information and reading card information from the card).

In document D1, a keyboard control program stored in the keyboard unit memory is to control notification of a key code based on the state of insertion and extraction of the credit card ([0059], [0060], Figure 4, SA9, SA10; the PIN is not entered using the keyboard 122, encrypted by the code processor 121 and notified by the code processor 121 to the CPU 111 until once the card has been inserted in the card reader). When the credit card is detected by the card reader control program, the keyboard control program notifies the main board of the key code and enables execution of inputting of a PIN code of the credit card (implicit).

4. Hence, the board agrees with the examining division and the appellant that D1 does not disclose the following distinguishing features:

- the main board and keyboard unit are connected to each other through a serial interface
- the main CPU is configured to perform steps according to features (d), (f), (f*), (g), (h), (i), (j), (k) and (l)
- the sub CPU is configured to perform steps according to features (e), (m), (n), (o)

- the keyboard control program stored in the keyboard unit memory it to control notification of a key code based on results from the comparison by the CPU (features (q), (r) and (s)).

5. Regarding the nature of the interface between the main board/unsecured module 110 and the keyboard unit/ secured module 120, the board shares the examining division's conclusions, which were not contested by the appellant. The associated objective technical problem is to implement the interface between main and sub CPUs 111 and 121 of D1. Implementing the interface between the main board and keyboard unit as a serial interface cannot be considered as anything more than an obvious design choice (i.e., the choice between a parallel and a serial interface) that the skilled person would make depending on the circumstances.

6. Regarding the remaining distinguishing features (i.e. the steps of the certification process to validate the integrity of the payment program before it is allowed that such a program obtains an input PIN), the board concurs with the examining division's formulation of the objective technical problem, namely to improve the security of the terminal of D1 vis-a-vis malicious programs running on the terminal. This seems not to be contested by the appellant.

7. It also appears undisputed that a well-known technique for code signing and code verification comprises the following steps:

1. the code publisher:
    1. computes a hash value of the code,

2. encrypts the hash value with the publisher's private key to create a digital signature of the code, and
3. provides a package containing the code, the digital signature and the publisher's certificate (or just the publisher's public key) to a user of the code;

2. after the user of the code optionally verifies the code publisher's certificate, the user of the code verifies the authenticity and integrity of the code by
1. decrypting the digital signature with the code publisher's public key to obtain the hash value calculated by the publisher,
2. calculating a new hash value of the code, and
3. comparing the hash value calculated by the code publisher to the new hash value; if they are equal, the code is verified as originating from the code publisher and being uncorrupted.

Such process is also known from D3 (paragraphs [0034], [0035], Figure 3), D4 (page 9, line 28 to page 10, line 9, Figure 4, steps 440 to 460) and D9 (pages 7 and 8).

8. The board thus agrees with the examining division that the skilled person wishing to solve the objective technical problem associated with said remaining distinguishing features might use this type of process to verify the authenticity of the payment program of D1.

9. The appellant argued that D1 disclosed that the LED controller 125 performs security checks of each unit of the secured module 120 for any abnormality such a breakage, etc.(see D1, paragraphs [0056], [0074], [0092], [0110]). In said second module, a wiring that

connected all units was hardened by resin, which mitigated the possibility of signal tapping. If a detector identified an illegal and forceful tapping of the signal, the contents of the ROM 12 and the RAM 13 were destroyed, see paragraphs [0013] and [0044] of D1. The appellant argued that, consequently, there was no reason to perform the certification process as claimed in D1.

The board is not convinced by this argument, because the security checks performed in D1 concern the physical integrity of the device and, in particular, of the secured module 120. Despite the security measures disclosed in D1, the skilled person would understand that there is still a need for further increasing the security, and in particular, to make sure that the programs running on the processor 111 of the unsecured module 110 are legitimately released and installed. Hence, the skilled person, wishing to solve the objective technical problem, would not be demotivated by the security checks already performed in D1.

10. However, the skilled person implementing the known process in the handy terminal of D1 would not arrive at the claimed subject-matter.

10.1 The examining division argued that the skilled person would have to take three decisions:

1. where to store the digital signature of the code (in claim terms: the first hash value encrypted with a secret key) and the publisher's public key (in claim terms: the public key): on the unsecured module processor (in claim terms: main board) or the secured module processor (in claim terms: keyboard unit);

2. when to verify the digital signature of the code: only when the code is installed, every time the application is started, periodically, etc.;

3. where to perform the different steps involved in the verification of the digital signature (see above): on the secured module processor or on the unsecured module processor.

10.2 Regarding the first and third decisions, the board agrees with the examining division that the coupled module including an encrypted first has value and the payment program would be installed on the unsecured module 110 (main board). In D1, the payment program (to be certified) is installed and runs on the main CPU 111 of the unsecured module 110 (see D1, paragraph [0052]).

Contrary to the appellant's view, neither claim 1 nor the description related to the embodiment of figures 1 to 4 provides any indication that splitting up the certification process between two processors would certify or authenticate the operation of the claimed keyboard unit or the data transfer between the main CPU and the sub CPU. Hence, implementing the certification process known from the prior art gives the skilled person the choice between two straightforward alternatives: provide the public key on the unsecured module 110 and perform the entire certification process within this module or provide the public key on the secured module 120 and perform the certification process partly within this module.

Hence, it is obvious to arrange the handy terminal of D1 such that the secured module 120 (keyboard unit) receives the public key for decryption after having received the encrypted first hash value from the

unsecured module 110.

In a next step, the "new" or second hash value must be calculated in the processor 111 of the unsecured module 110, i.e. where the payment program is stored, and then transmitted (in an encrypted way, see paragraph [0045] of D1) to the code processor 111 of the secured module 120. The decryption of the encrypted first hash value and its comparison with a "new" hash value is performed within the secured module 120, i.e. by code processor 121.

In summary, it is obvious to configure the main CPU and the sub CPU of D1 such that the main CPU performs steps in accordance with features (d), (f), (g), (h), (i), (j) and the sub CPU performs steps (e), the decryption of the first hash value according to feature (m) and the comparison according to features (n) and (o). However, in document D1, such certification process is performed at least once after the installation of the payment program, contrary to what is required by feature (f*).

Obviously, in case the payment program is found not authenticated, the execution of inputting a PIN code is disabled.

10.3 Regarding the second decision that the skilled person has to take (see section 10.1 above), it is not obvious to perform the certification steps each time the payment program is booted.

The claimed frequency of performing the certification process is not generally known. In the context of the second decision to be taken, the examining division referred to document D4, page 9, lines 5 to 7. However,

D4 discloses performing a certification process when once a program is selected for being used, but does not motivate the skilled person to start a certification process in D1 every time the payment program is booted or executed.

The board follows the appellant's argument that performing a certification process of the payment program every time the payment program is booted contributes to the objective technical problem and is not obvious from the common general knowledge or suggested by the prior art at hand.

10.4 Moreover, as also pointed out by the appellant, the process of D9, as described e.g. in section 7. above, does not include steps of encrypting and decrypting the second hash value using an encrypted key produced by a random number, but only generates a "new hash value".

When implementing this known certification process in D1 (see section 10.2 above), data (namely the hash values) is necessarily transferred between both processors 111 and 121. Paragraph [0045] of D1 does not provide any specific details about the encryption/ decryption of data transferred between both modules in D1. It is undisputed that generating an encryption key using a random number is known to the skilled person. It seems that this would be an obvious implementation of the encryption/decryption performed in the processors 111 and 121 of D1. Generating the random number and the associated key by the sub CPU 121 of D1 appears to be an obvious choice between two possibilities, as it could either generated by the main CPU 111 or the sub CPU 121.

According to the impugned decision, the claimed manner of encrypting/decrypting the second hash value by means of a key produced in the keyboard unit and sent to the main board was not seen to be particularly advantageous, as the "encrypted key" could be readily intercepted by an eavesdropper. As there was no unexpected technical advantage, said features would not contribute to an inventive step. However, even an undesired, but possible stealing of the "encrypted key" and the "encrypted second hash value" is not detrimental to the certification process of the payment program as such, as argued by the appellant.

Thus, the board accepts the appellant's argument that the specific encryption according to features (k) and (l) in conjunction with performing the certification process every time the payment program is booted, i.e. feature (f*), contributes to the solution of the objective technical problem. As the certification process is performed each time the payment program is booted, each time a "random number" is generated and an "encrypted key" is produced (features (k) and (l)), which improves the security of the terminal of D1 vis-a-vis malicious programs running on the terminal.

11. Hence, when configuring the main CPU and the sub CPU of D1 as described in section 10.2 in order to solve the objective technical problem, the skilled person would not arrive at the claimed handy terminal defined in claim 1 in an obvious way.

12. Thus, the subject-matter of claim 1 and the subject-matter of claim 2, *mutatis mutandis*, involve an inventive step (Article 56 EPC).

The board is satisfied that the wording of claims 1

and 2 overcomes the objection under Article 123(2) EPC raised in the board's communication pursuant to Article 15(1) RPBA and that the description filed during oral proceedings is adapted to the claims.

A European patent is therefore to be granted. Thus, the appeal is allowable.

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 with order to grant a patent in the following version:

Description: Pages 1 to 18 received by email during oral proceedings before the board.

Claims: No. 1 and 2 according to the main request filed as auxiliary request 2 with letter dated 28 September 2023.

Drawings: Sheets 1/4 to 4/4 filed with entry into the regional phase before the EPO.

The Registrar: The Chairwoman:

B. Atienza Vivancos D. Prietzel-Funk

Decision electronically authenticated