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

Datasheet for the decision
of 2 February 2016

Case Number: T 1584/13 - 3.5.06

Application Number: 03254057.7

Publication Number: 1443379

IPC: G06F1/00

Language of the proceedings: EN

Title of invention:
Mobile communication system and mobile terminal having function of desactivating mobile communication viruses and method thereof

Applicant:
Curitel Communications, Inc.

Headword:
Virus monitoring/CURITEL

Relevant legal provisions:
EPC 1973 Art. 56

Keyword:
Inventive step (no)

Decisions cited:

Catchword:

Case Number: T 1584/13 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 2 February 2016

Appellant: (Applicant)	Curitel Communications, Inc. San 136-1, Ami-ri, Bubal-eub Ichon-shi, Kyoungki-do 467-860 (KR)
Representative:	Weickmann & Weickmann Postfach 860 820 81635 München (DE)
Decision under appeal:	Decision of the Examining Division of the European Patent Office posted on 3 January 2013 refusing European patent application No. 03254057.7 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman	W. Sekretaruk
Members:	M. Müller
	A. Teale

Summary of Facts and Submissions

I.   The appeal lies against the decision of the examining
        division, with reasons dispatched on 3 January 2013, to
        refuse European patent application No. 03 254 057.7 for
        lack of an inventive step in view of the following
        documents:

        D1: US 6 240 530 B1
        D4: "Security on the Gateways", White paper, MicroWorld
             Software Services, 2000, XP002245105
        D5: US 5 889 943 A.

II.   Notice of appeal was filed on 27 February 2013, the
        appeal fee being paid on the same day. A statement of
        grounds of appeal was received on 3 May 2013. The
        appellant requested that the decision under appeal be
        set aside and that a patent be granted on the basis of
        the claims pursued in the oral proceedings of 6 Decem-
        ber 2012 before the examining division and re-filed with
        the grounds of appeal, that is based on claims 1-11
        according to the main request and claims 1-10 according
        to the auxiliary request. The appellant also made an
        auxiliary request for oral proceedings.

III.   In an annex to a summons to oral proceedings, the board
        informed the appellant of its preliminary opinion that
        the independent claims of both requests, namely 1 and 8
        of the main request and 1 and 7 of the auxiliary re-
        quest, lack inventive step over D1, D4 and D5, Article
        56 EPC 1973.

IV.   In response to the summons, the appellant did not file
        either amendments or arguments. Instead, with a letter
        dated 23 December 2015, it withdrew its request for oral

proceedings, informed the board that no one would be attending the oral proceedings in the name of the applicant, and stated that it expected to receive "a decision on basis of the state of the file".

V.   The board then cancelled the oral proceedings.

VI.   Claim 1 according to the main request reads as follows:

"A method for inactivating viruses in a mobile communication system having a plurality of mobile terminals (111, 112, 113, 114), comprising the following steps:

a)   at a virus monitoring unit associated with the mobile communication system:
      detecting virus infection of data received from at least one first mobile terminal (111; 112; 113; 114), wherein the first mobile terminal has a virus vaccine program stored therein;

b)   at the virus monitoring unit:
      analyzing virus information of the detected virus infection when data are virus infected

c)   at the virus monitoring unit:
      choosing suitable one of virus vaccine programs that are stored in a database according to the virus information, and
      curing the data received from the first mobile terminal (111; 112; 113; 114) to inactivate the virus,
      wherein the cured data is transmitted to a destination mobile terminal;

d)   at the virus monitoring unit:
      notifying said first mobile terminal about virus infection;

e)   at the first mobile terminal (111; 112; 113; 114):

receiving the virus infection notification from the
virus monitoring unit and, in response to receiving
said virus infection notification, detecting a
virus infection of the first mobile terminal to
inactivate viruses by using said virus vaccine
program stored therein; and

f)   transmitting a vaccine request message to the virus
monitoring unit to receive a virus vaccine program
suitable for the detected virus to thereby
inactivate the virus by using the received virus
vaccine program when the virus vaccine program
previously stored in the mobile terminal can not
inactivate the virus."

Claim 1 according to the auxiliary request is identical
to claim 1 of the main request except for the following
text added at the end:

"..., wherein the vaccine request message includes
vaccine program information, virus information and
capability information of the first mobile terminal."

Reasons for the Decision

1.   The following reasons are based on the board's analysis
presented in the annex to the summons to oral procee-
dings, on which the appellant chose not to comment.

The invention

2.   The application relates to virus protection for mobile
terminals, and more specifically to the protection of
data in transit and the provision of up-to-date
"vaccine" programs to mobile terminals.

2.1   The application relates to a number of mobile phones
        which communicate via base stations and a mobile swit-
        ching center (see fig. 1). So called "vaccine" programs
        are installed on the mobile devices. The base stations
        and the mobile switching center, but not the mobile
        devices, have access to a database of vaccine programs
        and a virus monitoring unit (VMU).

2.2   When data is transmitted from one mobile device to
        another, it is determined (by the VMU) whether the data
        is infected. The suitable vaccine is retrieved from the
        DB and applied, and the "cured" data is forwarded. In
        passing, it is noted that the term "vaccine" appears to
        be an inappropriate metaphor for a program which is used
        as a cure and after an infection has been diagnosed
        rather than before and for prophylaxis. The receiving
        mobile device is also informed about the infection. The
        mobile device then checks whether a suitable vaccine is
        locally available and, if not, requests it from the VMU
        via the base station.

Claim construction

3.   Claim 1 of both requests contains a few linguistically
        imprecise and ambiguous formulations which might be
        considered to render the claim unclear. The board con-
        siders however that claim 1 is clear enough to allow an
        assessment of inventive step. To this end, claim 1 is
        construed as follows.

3.1   Step e) of claim 1 specifies that "in response to [a]
        virus infection notification", "a virus infection" is
        detected and later, in step f), reference is made to the
        "detected virus". The board takes it that the virus
        detected at the mobile device is meant to be the same as

the one detected in the transmitted data and notified to the mobile device.

3.2   Step e) of claim 1 specifies that the first mobile terminal "detect[s] a virus infection [...] to inactivate viruses [...]". The board takes the view that the skilled person would read the phrase "to inactivate viruses [...]" as "in order to inactivate viruses [...]" and, hence, the corresponding phrase as a statement of purpose.

3.3   According to step f) of claim 1, a "suitable" vaccine program is requested "when the virus vaccine program previously stored [...] can not inactivate the virus". This language leaves open whether the suitable program is requested when the stored vaccine program is known or assumed to be unsuitable to inactivate the virus or only after an attempt to inactivate it has failed.

3.4   In step f) of claim 1, the phrase "program suitable for the detected virus to thereby inactivate the virus by using the received virus vaccine program" is grammatically unclear. The board takes the view that the skilled reader of claim 1 would construe that phrase to mean "program suitable for inactivating the detected virus".

Inventive step

4.   The subject-matter of claim 1 of both requests consists of two parts which appear to be only loosely connected with each other.

4.1   Steps a)-c) specify a central "virus monitoring unit" for detecting a virus infection in data in transit between two mobile devices, for example in email messa-

ges, to eliminate the detected virus and to forward the
resulting "cured" data.

4.2   Steps e) and f), with the exception of the "in response"
        phrase of step e), specify that the mobile unit
        determines whether a local vaccine program "can" inacti-
        vate a virus and, if not, requests from the virus mo-
        nitoring unit a vaccine program which can.

4.3   Step d) specifies that the virus monitoring unit noti-
        fies the mobile terminal about the detected virus in-
        fection and step e) specifies that the mobile terminal
        acts "in response" to this notification.

5.   Both parts are connected with each other in that the
        first "triggers" the second and in that the "suitable"
        vaccine program is requested from the same unit having
        detected the virus infection in the transmitted data.

5.1   The board considers that what happens at the mobile
        device is essentially independent of what happened
        previously at the virus monitoring unit.

5.2   The appellant claims the following synergistic effect of
        the two parts (see e.g. grounds of appeal, page 15,
        point 9): because the mobile terminal requests a sui-
        table vaccine program from the virus monitoring unit,
        which has just "cured" the transmitted data from that
        virus, the requested vaccine program must already be
        available at the virus monitoring unit (see grounds of
        appeal, points 8-10, resp. last sentences).

5.3   The board is not convinced by this argument, considering
        that, on the assumption that the data base available to
        the VMU is up-to-date and complete, the availability of

the required vaccine program does not depend on whether
the VMU has just deleted a virus from data in transit.

The prior art

6.   In the decision under appeal, the assessment of inven-
        tive step started from D1. The board agrees that this is
        a suitable choice but prefers an assessment starting
        from D4 or D5.

7.   D4 and D5 disclose virus checking of emails in transi-
        tion at a gateway server (D4, see *e.g.* abstract, 3rd
        para.) or "gateway node" (D5, col. 5, lines 18-24). Both
        disclose that the sender of an email in which a virus
        was found is informed accordingly (D4, p. 5, penult.
        para.; D5, col. 20, lines 41-63).

Main request

8.   In the board's view, each of D4 and D5 discloses the
        preamble of claim 1 and steps a) - d).

8.1   Thus the differences are steps e) and f), i.e. the steps
        taken by the sender of the infected data. The board
        finds these differences to solve the problem of
        determining and deleting the cause of the virus infec-
        tion of the transmitted data.

8.2   The board considers that this problem is one the skilled
        person, given either of D4 and D5, can reasonably be ex-
        pected to address. It would be an obvious reaction for a
        sender, to the notification that a virus infection was
        found in a sent email, to determine whether this
        infection originated in the sending computer and, if so,
        to try to delete the virus.

8.3   It has been a matter of convention for years, dating
       back well before the priority date in the present case,
       that client computers are equipped with some sort of
       antivirus software. Hence doing this for the sender com-
       puters of D4 and D5 does not require an inventive step.
       The board notes that this also applies to mobile devi-
       ces, in particular in view of the fact that many conven-
       tional computers are "mobile".

8.4   Furthermore, if antivirus software is available on the
       mobile device, the board considers it obvious that the
       "mobile terminal" will either run this program or, at
       least, consider whether it should be run. Typical anti-
       virus software must be regularly updated to remain
       effective against new viruses. It would thus be obvious
       for the mobile terminal to determine whether the locally
       available vaccine program is up-to-date and, if not,
       consider it "unsuitable" and download an up-to-date ver-
       sion.

8.5   Whether this up-to-date version is requested from the
       VMU or some other server is, in the board's judgment, a
       marginal and obvious choice.

8.6   Starting from D4 or D5, therefore, the board finds the
       subject-matter of claim 1 of the main request to be ob-
       vious in view of common general knowledge of antivirus
       software, Article 56 EPC 1973.

Auxiliary request

9.   Claim 1 of the auxiliary request specifies that the
       request for a "suitable" vaccine program includes
       "vaccine program information, virus information and
       capability information of the first mobile terminal".

9.1   The board notes that claim 1 does not specify how the
        "virus monitoring unit" uses these pieces of informa-
        tion. Thus it is questionable whether their inclusion in
        the claim has, *per se*, any technical effect and thus
        whether they can contribute to inventive step of the
        claimed subject-matter at all.

9.2   The description discloses (p. 8, lines 14-19) that the
        "vaccine request message" comprises "version informa-
        tion", including the virus identity, and a "capability
        field", including "operating system (OS) information" of
        the mobile terminal.

9.3   In the scenario considered above, the board considers it
        obvious that the mobile terminal requests an update in-
        dicating the version numbers (a) of the locally
        available "vaccine program" - so that the server can
        determine whether an update is needed - and (b) of the
        local operating system - so that the server can provide
        the update for the pertinent operating system. The board
        also considers it to be an obvious option for the mobile
        terminal to indicate which virus it is specifically
        interested in - for instance to save bandwidth if the
        local antivirus software is up-to-date with respect to
        the virus of interest.

9.4   Therefore, the board also concludes that claim 1 of the
        auxiliary request lacks inventive step over D4 or D5 in
        view of common general knowledge of antivirus software,
        Article 56 EPC 1973.

Summary

10.   In view of this finding it is immaterial that, as
        explained in the summons, the board comes to the same
        conclusion starting from document D1.

11.   There not being an allowable request, the appeal must be
        dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

L. Malécot-Grob   W. Sekretaruk

Decision electronically authenticated