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 2012

Case Number: T 1367/08 - 3.5.06

Application Number: 05021028.5

Publication Number: 1643339

IPC: G06F 1/00

Language of the proceedings: EN

Title of invention:
Method and system for restricting the use of an application
program

Applicant:
SYSMEX CORPORATION

Opponent:
–

Headword:
Restricting use of an application program / SYSMEX

Relevant legal provisions:
EPC Art. 123(2)

Relevant legal provisions (EPC 1973):
EPC Art. 56

Keyword:
"Inventive step (no - main, first, second and fourth auxiliary
requests)"
"Added subject-matter (yes - third auxiliary request)"

Decisions cited:
–

Catchword:
–

EPA Form 3030
C7800.D

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Europäisches
Patentamt

European
Patent Office

Office européen
des brevets

Beschwerdekammern   Boards of Appeal   Chambres de recours

Case Number: T 1367/08 **-** 3.5.06

D E C I S I O N
of the Technical Board of Appeal 3.5.06
of 27 June 2012

Appellant: SYSMEX CORPORATION
(Applicant)   5-1, Wakinohama-Kaigandori 1-chome
                        Chuo-ku
                        Kobe-shi
                        Hyogo 651-0073   (JP)

Representative: Hoffmann Eitle
                        Patent- und Rechtsanwälte
                        Arabellastraße 4
                        D-81925 München   (DE)

Decision under appeal: **Decision of the Examining Division of the**
                            European Patent Office posted 18 February 2008
                            refusing European patent application
                            No. 05021028.5 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman: D. H. Rees
Members: S. Krischer
                   W. Sekretaruk

Summary of Facts and Submissions

I.   The appeal is directed against the decision of the
      examining division, posted on 18 February 2008, to
      refuse the application 05021028.
      The reason for the refusal was lack of inventive step
      over document:

      D2   US 5 550 968 A, 27 August 1996.

II.   A notice of appeal was received on 18 April 2008. The
      fee was received the same day. A statement of the
      grounds of appeal was received on 20 June 2008. Sets of
      claims for a main and two auxiliary requests were filed.
      Oral proceedings were conditionally requested.

III. The board issued a summons to oral proceedings, raising
      objections with respect to inventive step.

IV.   In a letter dated 24 May 2012, the appellant filed a
      third and a fourth auxiliary request.

V.   Oral proceedings were held on 27 June 2012. At their
      end, the chairman announced the board's decision.

VI.   The appellant requests to set the decision aside and to
      grant a patent on the basis of a main request filed
      with the grounds (claims 1-17 as filed with the
      attachment, not as formulated on page 1 of the grounds,
      i.e. including the replacement of "client computer" by
      "user computer" in line 2), a first or second auxiliary
      request filed with the grounds (each request with
      claims 1-17), a third or a fourth auxiliary request
      filed with the letter dated 24 May 2012 (third request
      with claims 1-20; fourth request with claims 1-18).

The further text on file is: the description page 1 as
filed during oral proceedings on 1 February 2008,
pages 2-31 as filed with letter dated 8 November 2007,
and the drawing sheets 1-18 as originally filed.

VII.   Claim 1 of the main request reads as follows:

"1. A method for restricting the use of functions of an
application program installed on a user computer for
being used for processing measurement results of a
measuring apparatus, comprising the steps of:

receiving input of authentication information used to
authenticate a user;

authenticating the user based on the received
authentication information;

acquiring use authority information related to the
authenticated user from a database that stores use
authority information that indicates authority to use
objects configuring the application program; and

setting use restrictions regarding the functions of the
application program for the authenticated user based on
the acquired use authority information comprising the
steps of:

searching objects configuring the application program;

determining whether or not the user has use authority
of the objects of the search result based on the use
authority information; and

setting any object as non-usable when it has been determined that the user does not have use authority of the object."

VIII.   Claim 1 of the first auxiliary request differs from claim 1 of the main request only in the "acquiring" step (additions in *italics*):

"acquiring use authority information related to the authenticated user from a database that stores *user information that indicates the authenticated user and* use authority information *for the authenticated user* that indicates authority to use objects configuring the application program, *the objects processing measurement results of the measuring apparatus*"

IX.   Claim 1 of the second auxiliary request reads as follows (additions to the main request in *italics*):

"1. A method for restricting the use of functions of an application program installed on a user computer for being used for processing measurement results of a measuring apparatus, comprising the steps of:

receiving input of authentication information used to authenticate a user;

authenticating the user based on the received authentication information;

once acquiring use authority information related to the authenticated user from a database that stores use

authority information that indicates authority to use
objects configuring the application program;

*storing the acquired use authority information in a
buffer;* and

setting use restrictions regarding the functions of the
application program for the authenticated user based on
the acquired use authority information comprising the
steps of:

searching objects configuring the application program;

determining whether or not the user has use authority
of the objects of the search result based on the use
authority information *stored in the buffer;* and

setting any object as non-usable when it has been
determined that the user does not have use authority of
the object."

X.   Claim 1 of the third auxiliary request reads as follows
       (additions to the main request in *italics*):

"1. A method for *changing user authority of a user for*
an application program installed on a user computer *and*
used for processing measurement results of a measuring
apparatus, comprising the steps of:

       receiving, *by the user computer,* input of
authentication information used to authenticate a user;

       authenticating, *by an authentication server,* the
user based on the received authentication information;

when a user authentication is successful,
acquiring*, by the user computer,* use authority
information related to the authenticated user from a
database *of the authentication server, the database
storing* use authority information that indicates
authority to use *controls* configuring *a screen
displayed by* the application program;

setting*, by the user computer,* use restrictions
regarding the *controls configuring the screen displayed
by* the application program for the authenticated user
based on the acquired use authority information;

*receiving, by the user computer, an instruction to
change the use authority information stored in the
database, when the authenticated user is allowed to use
a control for changing the use authority information
stored in the database;*

*sending the instruction from the user computer to
the authentication server; and*

*changing, by the authentication server, the use
authority information stored in the database according
to the instruction received from the user computer.*"

XI.   Claim 1 of the fourth auxiliary reads as follows:
        (additions to the main request in *italics*):

        "1. A method for *changing user group authority
        information for* an application program installed on a
        user computer *and* used for processing measurement
        results of a measuring apparatus, comprising the steps
        of:

receiving, *by the user computer,* input of
authentication information used to authenticate a user;

authenticating, *by an authentication server,* the
user based on the received authentication information;

when a user authentication is successful,
acquiring, *by the user computer,* use authority
information related to the authenticated user from a
database *of the authentication server, the database
storing* use authority information that indicates
authority to use *controls* configuring *a screen
displayed by* the application program;

setting, *by the user computer,* use restrictions
regarding the *controls configuring the screen displayed
by* the application program for the authenticated user
based on the acquired use authority information;

*receiving, by the user computer, an instruction to
change the user group authority information stored in
the database, when the authenticated user is allowed to
use a control for changing the user group authority
information stored in the database;*

*sending the instruction from the user computer to
the authentication server; and*

*changing, by the authentication server, the user
group authority information stored in the database
according to the instruction received from the user
computer*

*wherein the step of setting the use restrictions
comprises the steps of:*

searching *controls* configuring the application
program;

determining whether or not the user has use
authority of the *controls* of the search result based on
the use authority information; and

setting any *control* as non-usable when it has been
determined that the user does not have use authority of
the *control*."

Reasons for the Decision

1.   *Admission of the third and fourth auxiliary requests*

One effect of the amendments incorporated in these
requests is to clarify claim 1 by replacing the overly
broad expression "object" by "control" (see the summons,
section 4.1.4) and by adding to each step which
computer executes the step (user computer or
authentication server). Given this improved clarity and
since the requests do not raise issues too complex for
the board to handle in the oral proceedings, they are
admitted into the procedure (Article 13(1) Rules of
Procedure of the Boards of Appeal).

2.   *Original disclosure of the third auxiliary request*

"A method for changing user authority of a user"
(claim 1, line 1) is not originally disclosed. The
description as originally filed only discloses storing
and changing the "use authority" of a user *group*, and
not of a single user, see page 32, lines 15-19, 25-27;
figures 17, 18 with user group names; for the

"authority" data to be changed in TBL3 of database DB2
see figure 9 with the control names (F33) and the user
group fields (F34 to F311) and page 19, line 18 to
page 20, line 6 (in particular page 19, line 25: "for
storing the use authority of controls for each user
group").

The appellant argued during the oral proceedings that a
user group name "user1" (page 20, line 1; figure 9
(F310)) would imply that only one user named "user1" is
in that group. The board agrees to the extent that
independent of the fact whether the user group "user1"
really comprises only one user, it is clear that a
group *can* comprise only one member. However, even a
one-member user group is a user group, and not a user.
A user group has a different technical implementation
than a user and has different technical capabilities;
e.g. a one-member user group can be extended to two
members, whereas a user cannot.

The appellant further argued that page 31, lines 5-8
disclosed "processes for ... changing the content of
the database DB2 can be performed from the user
authentication tab 71a". This implied the ability to
change the "use authority" per user. However firstly,
the board considers that the skilled person would
understand a user "authentication tab" as serving for
authentication purposes, and not for *authorisation* ones.
Secondly, this tab is also three times called a "user
information tab" (page 30, line 33; page 31, line 1;
and figure 17 (71a)). The board considers that the
skilled person would understand this to be its correct
name, especially since the user information displayed
on this tab is "assigned user group, logon ID, user

name, default database, expiration data and the like"
(page 31, lines 2, 3). There is no mention of the
authorisation of a control. Thirdly, the above cited
expression "changing the content of the database DB2"
does not unambigiously disclose that *all* content of DB2
can be changed.

Thus, the board is not convinced by the appellant's
arguments and concludes that claim 1 of the third
auxiliary request does not satisfy the requirements of
Article 123(2) EPC.

3.   *Inventiveness*

3.1   Main request

3.1.1   In the appealed decision, claim 1 is refused for lack
        of inventive step over document D2. The claim refused
        is identical to claim 1 of the present main request
        with the exception of replacing "client computer" by
        "user computer".

        The only difference between claim 1 as refused and the
        disclosure of D2 is identified in the decision as the
        use of the application program for processing
        measurement results of a measuring apparatus. The
        generic method of D2 is said to be applicable without
        any modification to measuring apparatuses.

3.1.2   The appellant takes the view that there are other
        differences. In the grounds of appeal, it is stated on
        pages 8-9, section 1.1 that D2 does not disclose the
        feature of setting use restrictions regarding the
        functions of the application program and that "D2 deals
        with restriction of access to data to be displayed and

not to restriction of access to functionalities"
(page 9, paragraph 3).

3.1.3   However, the board considers that displaying data is
        one example of a functionality of a program, so that in
        restricting which data are to be displayed D2 does
        indeed deal with restrictions to program
        functionalities and hence discloses the setting of use
        restrictions regarding the functions.

3.1.4   Furthermore, the actual disclosed embodiments of
        "restricting the use of functions" of claim 1, line 1
        relate only to the setting of so-called "objects" as
        non-usable (claim 1, last step). These "objects" are
        controls of a GUI window, according to the grounds,
        page 5, dash 4, line 5 and according to original
        description page 29, lines 15-25. In the latter passage,
        it is said that the controls of the main windows are
        searched and those controls which are flagged as
        disabled are displayed in light colour and do not
        response to user mouse clicks.

3.1.5   Document D2 discloses restricting access to controls of
        a GUI (abstract, line 1). It shows controls which are
        usually called "text boxes" (figures 3, 4) as in the
        sole elaborated example. The access to these text boxes
        is not only for reading their displayed content, but
        may also be for modifying it, see D2, column 6,
        lines 63-67 (*italics style* added):

        "The GUI 40 includes a window or panel 42 which
        provides *access to* a database or *software
        application* which maintains employee records. The
        panel 42 is utilized to permit employees to access

and/or *update* certain categories of employee
information *via some of the controls ...*"

By obscuring these controls, reading and updating is
prevented.

This is also confirmed in the grounds, page 12,
paragraph 7 ("restrict access to viewing or ...
modifying the data itself").

3.1.6   Document D2 defines controls as follows (column 1,
line 28):

"A control is a visual element within a GUI which
may be manipulated by a user to interact with data.
Icons and objects are examples of controls."

Thus, the controls of D2 may also be icons which
clearly may represent a function of a program to be
executed ("display" or "modify") when the icon is
clicked with the help of the mouse.

It follows that the board has no reason to interpret
the well-known technical term "controls" as used in D2
in a different sense than in the application. In both
cases, it is used in the commonly known sense.

Thus, this is not a difference between the disclosure
of D2 and what is claimed.

3.1.7   In the grounds, page 9, section 1.2 it is argued
that there is a further difference in that D2 does not
disclose the step of "searching objects configuring the
application programs" (first sentence), since "D2
merely states that it is determined whether a window

includes one or more controls" (page 10, line 1). And
further that "the controls of D2 are merely related to
access of information <u>displayed</u> in a window and are
different from the objects <u>configuring</u> the application
program and providing functionalities to the
application" (lines 2-5).

3.1.8   In assessing this argument the board first notes that
in D2, during the creation of a window, all controls
are checked if they are to be displayed with or without
obscuration (column 3, lines 32-44).

3.1.9   As to the statement that the controls in D2 would not
allow to *configure* a program, but only to *access*
information displayed in a window (and possibly change
it), it is necessary to construe what "configuring the
application program" (claim 1) actually means in the
context of the application. The description uses the
word "configure" in a way which is unusual for computer
scientists or programmers (page 33, line 24):

> "In window systems ..., systems controlled by
> graphical user interface (GUI) components
> configuring the screen, such as buttons, scroll
> bars, list boxes, menus (...) and the like
> configuring the window are standard."

This means that the *screen* or the *window* is configured
by GUI controls, and not the *application program* in the
sense of, for example, providing parameters
representing a user's preferred settings. "Configured"
is used in the application in the sense of "*formed*" or
"*built*". The board notes in further support that
figure 12 also does not show any particular
configuration elements for the measuring apparatus.

Nor could the board find any passage in the description
suggesting that the GUI controls *configured the
application program* in any sense other than simply
populating a window.

3.1.10 The passage supporting the feature of claim 1 of
"searching objects configuring the application program"
is the following (from page 24, lines 29 on):

> "the CPU 31a searches the control included in the
> window (step S112), selects one control from among
> the controls of the search result (step S113), and
> references the use authority data stored in the
> buffer area to check the set value of the user
> authority of this control (step S114). ... Then the
> CPU 31a determines whether or not use authority
> have been checked for all controls of the search
> result (step S117), and when there is a control
> that has not been checked (step S117: NO), the CPU
> returns the process to step S113."

See also figure 11 (S112).

This means that *every* control of the window is
"searched". Thus, the "objects configuring the
application program" searched in claim 1 would be *all
the controls building [the GUI of] the application
program*. And that is what D2 does, as noted above. Thus
again the board agrees with the appealed decision that
this is not a distinguishing feature. In the oral
proceedings the appellant maintained the view that the
claimed "search" was not carried out in D2, but could
not point out any concrete disclosure in the
application which would contradict the board's
interpretation. In the board's view, the only

distinction between the application and D2 on this
point is a different choice of words to describe the
same functionality.

3.1.11 As to the statement in the grounds, page 11,
paragraph 5 that D2 does not belong to the same
technical field as the invention, the board is of the
opinion that both D2 and the application mainly belong
to the technical field of GUI design, in particular
concerned with use restrictions of GUI controls. That
the application also belongs to the field of
application "(medical) particle measuring apparatuses"
(description page 2, paragraph 2 and page 8, line 12)
does not seem to be of any relevance since the board
cannot find any feature in claim 1 that is influenced
by that field of application (except "for being used
for processing measuring results of a measuring
apparatus" from line 2 on). The board agrees with the
appealed decision that it would not require an
inventive step to adapt the teaching of D2 to "(medical)
particle measuring apparatuses", nor indeed to any
computer-controlled device having a user interface and
multiple users who should have different kinds of
access to the functionality of the program controlling
the device.

3.1.12 The appellant argued during the oral proceedings that
the application would provide security checks on two
levels (namely the authentication of the user and the
authorisation of the authenticated user for each
control) whereas D2 merely discloses a password check
for each secured control (see figure 5B), without
authenticating the user. The board is not convinced by
this argument since the embodiment in D2, column 9,

lines 54-60 (not that of figure 5B, which relates to a different embodiment) discloses both an authentication (called registration) and an authorisation check:

> "The attributes of the security control subclass relative to each secure control then check to see whether the registered user making the request is authorized to view the secure control information (Step 146). This may be accomplished by checking the user identification of the user running this session against a list of authorized user identifications."

Thus, the two-level security check is not a distinguishing feature.

3.1.13 In the oral proceedings the appellant maintained that in D2 there is a (possibly different) password for each control, which has to be supplied in some way every time that control is included in a new window. The board considers that this is not only intrinsically implausible but that this interpretation is directly contradicted by the passage just cited.

3.1.14 This all confirms that the only difference between claim 1 and D2 is the use of the application program for processing measurement results of a measuring apparatus. However, the board cannot recognise that the generic method of D2 has to be adapted in order to be applied to measuring apparatuses. Nor is inventive to have the idea of doing so.

3.1.15 Therefore, claim 1 of the main request is not inventive, in violation of Article 56 EPC 1973.

3.2   First auxiliary request

3.2.1   Compared with the main request, claim 1 of the first
        auxiliary request contains the following added wording
        in *italics* (all in the third step):

            "acquiring use authority information related to the
            authenticated user from a database that stores *user
            information that indicates the authenticated user
            and* use authority information *for the authenticated
            user* that indicates authority to use objects
            configuring the application program, *the objects
            processing measurement results of the measuring
            apparatus*"

3.2.2   During oral proceedings, the appellant stated that the
        aim of this request was to clarify the expressions "use
        authority information" and "objects".

3.2.3   The added wording does not contribute any new technical
        feature to claim 1. It is implicit that every database
        from which use authority information related to the
        authenticated user is acquired has to store information
        about the user. Furthermore, the technical environment
        of the method (i.e. a measuring apparatus) is also
        already present in the main request.

3.2.4   Therefore, claim 1 of the first auxiliary request is
        not inventive, in violation of Article 56 EPC 1973, for
        the same reasons as for the main request.

3.3   Second auxiliary request

3.3.1   The additional features of the second auxiliary request
        relate to the well-known principle of buffering data

from a storage with a long access time (e.g. a database) in a storage with a short access time (e.g. the RAM). This is a routine measure belonging to the general knowledge of a programmer.

3.3.2 During oral proceedings, the appellant argued that the skilled person would not buffer passwords, since this decreased the security of the system. However, in the cited embodiment of D2, there are not passwords to be buffered, but "lists of authorized user identifications" (see column 9, line 59). Thus, there is nothing to teach away from applying this routine measure to the system of D2.

3.3.3 Therefore, claim 1 of the second auxiliary request is not inventive, in violation of Article 56 EPC 1973.

3.4   Fourth auxiliary request

3.4.1 The only substantive differences between claim 1 of this request and claim 1 of the main request are that the authority information stored in the database can be changed and that the authority information relates to user groups and not to single users. These differences cannot be found (at least not explicitly) in D2. They also do not interact with each other, nor with the difference between claim 1 of the main request and D2, namely the processing of measurement results.

3.4.2 The appellant argued during oral proceedings that these differences increased the flexibility of managing the authorisations without the need for reprogramming when the authorisations are to be changed.

3.4.3   However, the board considers the differences as obvious
        solutions to the everyday problem of managing
        authorisations in computers. In particular, storing
        authorisation data persistently is needed when the
        authorisation lasts longer than the current program run.
        Databases or files are well-known as persistent storage
        means. For example, the operating system UNIX uses a
        password file for the login authorisations which is
        changeable by the so-called superuser. Furthermore,
        authorisations for files in UNIX can be given for a
        user group.

3.4.4   In response the appellant argued during oral
        proceedings that a doctor would have to take over the
        role of the superuser in the present case of a medical
        measurement apparatus. A doctor would not have the
        technical knowledge to safely open an editor in order
        to change the password file or to change a file
        authorisation. However, the claim does not specify how
        the "authority information" is changed, so that this
        argument has no force. The board further notes that it
        is anyway commonplace to provide "easy" interfaces to
        facilitate operations which would otherwise be complex,
        for the benefit of inexperienced users.

3.4.5   Thus, claim 1 of the fourth auxiliary request is not
        inventive, in violation of Article 56 EPC 1973.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

B. Atienza Vivancos   D. H. Rees

C7800.D