BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS

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

Datasheet for the decision of 28 July 2009

Case Number: T 0848/08 - 3.5.05

Application Number: 03727702.7

Publication Number: 1512058

IPC: G06F 1/00

Language of the proceedings: EN

Title of invention:
Secure mobile wireless device

Applicant:
Nokia Corporation

Opponent:
-

Headword:
Platform security for mobile phone/NOKIA

Relevant legal provisions:
EPC Art. 56
EPC R. 139

Keyword:
"Inventive step (main request - no, 1st auxiliary request - yes after amendments)"
"Request for correction of application number in grounds of appeal- allowable"

Decisions cited:
J 0008/80, J 0010/87, J 0006/91, J 0011/92, T 0460/99

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 0848/08 - 3.5.05

D E C I S I O N
of the Technical Board of Appeal 3.5.05
of 28 July 2009

Appellant: Nokia Corporation
Keilalahdentie 2-4
FI-02150 Espoo (FI)

Representative: Wallin, Nicholas James
Withers & Rogers LLP
Goldings House
2, Hays Lane
London SE1 2HW (GB)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 27 November 2007 refusing European application No. 03727702.7 pursuant to Article 97(1) EPC 1973.**

Composition of the Board:

Chairman: D. H. Rees
Members: P. Cretaine
F. Blumer

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division announced in oral proceedings held on 7 November 2007, with reasons dispatched on 27 November 2007, refusing European Patent Application No. 03 727 702.7 on the grounds that the subject-matter of independent claims 1 and 12 of the main request did not involve an inventive step, contrary to Article 56 EPC, having regard to the disclosure of:

D1: EP-A-0 813 133.

A first auxiliary request filed during oral proceedings was not admitted into the procedure.

II. Notice of appeal was submitted on 24 January 2008. The appeal fee was paid on the same day.

III. In its cover letter to the Statement of Grounds of Appeal, filed on 7 April 2008, the appellant referred to an incorrect application number (04768808.0 instead of 03727702.7). According to the telefax letter filed by the appellant on 10 April 2008, the formalities officer for application 04768808.0, another application owned by the appellant, contacted the appellant on 9 April 2008. The appellant then contacted the formalities officer responsible for the present application. The formalities officer for the present application was said to have confirmed that the Statement of Grounds of Appeal had been transferred to the correct application, 03727702.7 and that it was deemed to have been filed on 7 April 2008.

In this telefax letter, the appellant requested that the application number indicated on the front of its letter of 7 April 2008 be corrected under Rule 139 EPC, first sentence, as it was an "error in transcription" as referred to in Rule 139 EPC.

IV. The board issued an invitation to oral proceedings scheduled to take place on 28 July 2009 accompanied by a communication. In the communication the board indicated its intention to allow the correction of the application number under Rule 139 EPC.

V. In response to the board's negative preliminary assessment of the claims submitted with the Statement of Grounds of Appeal the appellant filed, in its letter of 26 June 2009, the following new sets of claims to replace the requests on file:

Main request: claims 1 to 13;
1st Auxiliary Request: claims 1 to 13;
2nd Auxiliary Request: claims 1 to 12;
3rd Auxiliary Request: claims 1 to 12;
4th Auxiliary Request: claims 1 to 12.

VI. At the oral proceedings, which took place as scheduled on 28 July 2009, the appellant filed claims 1 to 11 of a further new 1st Auxiliary Request replacing the 1st Auxiliary Request on file and requested that the decision under appeal be set aside and a patent be granted on the basis of the Main Request as filed with letter dated 26 June 2009, or, subsidiarily, on the basis of the 1st Auxiliary Request as filed during oral proceedings before the board, or, subsidiarily, on the

basis of any of the 2nd to 4th Auxiliary Requests as filed with letter dated 26 June 2009.

The appellant also filed the following document:

D3: ANDREW S. TANENBAUM: "Modern Operating Systems", 2nd edition, Prentice-Hall, Upper Saddle River (NJ, USA) 2001, PP.645-653.

The further documents on which the appeal is based, i.e. the text of the description and the drawings, are as follows:

description, pages:

1-2, 5-19 as originally filed;
3, 4, 4A as filed in connection with the Main Request, the 2nd Auxiliary Request, the 3rd Auxiliary Request and the 4th Auxiliary Request with letter of 26 June 2009;
3, 4, 4A as filed in connection with the 1st Auxiliary Request during oral proceedings.

drawings, sheets:

1/2 to 2/2 as filed with entry into the regional phase before the EPO.

VII. *Main Request*:

Claim 1 reads as follows:

"A secure mobile wireless device for a single user in which native executable code is installed, the device including:
a plurality of protected resources; and

a plurality of servers; wherein
access to each said protected resource is provided by a corresponding server;
the native executable code is assigned a set of capabilities which define a/the protected resource(s) on the device which the native executable code can access; and
access to said protected resources is policed by said corresponding servers on the basis of the capabilities assigned to the native executable code."

Claim 12 is a method claim corresponding to claim 1.

Claim 13 reads as follows:

"An operating system adapted to run on a secure mobile wireless device and for causing the device to operate in accordance with the method of claim 12."

1st Auxiliary Request:

Claim 1 reads as follows:

"A secure mobile wireless device for a single user in which native executable code is installed, the device including:
a plurality of protected resources;
a plurality of servers; and
a trusted computing base having a kernel; wherein
access to each said protected resource is provided by a corresponding server;
the native executable code is assigned a set of capabilities which define a/the protected resource(s)

on the device which the native executable code can access;
said corresponding servers are arranged to police access to said protected resources on the basis of the capabilities assigned to the native executable code;
the capabilities are stored in a location that is only accessible to the trusted computing base; and
the kernel is arranged, for each client-server communication, to pass the client capabilities to said server."

Claim 11 is a method claim corresponding to claim 1.

In view of the outcome of the appeal the wording of the further requests is irrelevant.

VIII. At the end of the hearing the board announced its decision.

Reasons for the Decision:

1. *Admissibility / Correction under Rule 139 EPC*

1.1 The board notes that the time limit for filing the Statement of Grounds of appeal expired on 7 April 2008. On the same day, shortly after 17:00, the Statement of Grounds of Appeal with reference to the incorrect application number was filed by telefax. The board does not see any contradiction between the summary of facts, as given by the appellant (see above, Summary of Facts and Submissions, point III), and the information derivable from the file.

1.2 Any confirmation by the formalities officer that she had transferred the Statement of Grounds of Appeal to the correct file and that it was deemed to have been filed on 7 April 2008 has no legal effect. Requests for an amendment under Rule 139 EPC may be filed with respect to any "document filed with the European Patent Office" in any proceedings before the EPO, including appeals proceedings (see, for example, T 460/99). In the present case, there is no doubt that the written (erroneous) Statement of Grounds satisfies these conditions.

1.3 For the purposes of Rule 139 EPC, a mistake may be said to exist in a document filed with the EPO if the document does not express the true intention of the person on whose behalf it was filed (J 8/80, OJ EPO 1980, 293, point 4). The applicant needs to prove that a mistake has been made, what the mistake was and what the correction should be. In cases where the making of the alleged mistake is not self-evident and in cases where it is not immediately evident that nothing else would have been intended than what is offered as the correction, the burden of proving the facts must be a heavy one (see J 8/80, OJ EPO 1980, 293, point 6).

1.4 The board accepts that a mistake has been made (i.e., the reference to the wrong application number) and that the correction requested by the appellant reflects the true intent of the appellant. Even though the Statement of Grounds of Appeal referred to the wrong application number, its text clearly referred to the present application, and the internal reference number and keyword ("10019 EP - Capabilities") was the same as used on the Notice of Appeal (which carried the correct

application number). As the requested correction does not concern the description, the claims or the drawings (in which case Rule 139 EPC, second sentence, would apply), the correction may be admissible even if the true intent of the appellant is not derivable from the erroneous communication.

1.5 Rule 139 EPC does not compel the EPO to permit the correction of errors of any kind at any time but gives the EPO the authority to permit certain types of correction at its discretion, which also means that corrections can be made dependent on conditions (J 6/91, OJ EPO 1994, 349, point 5.3). The pertinent case law regularly takes into account whether the requested correction may adversely affect the public interest (J 11/92, OJ EPO 1995, 25; J 6/91, OJ EPO 1994, 349), whether the correction could constitute a procedural abuse (for example, to give effect to a change of the applicant's mind, see J 8/80, OJ EPO 1980, 293, point 6) and whether the request for correction was delayed (J 10/87, OJ EPO 1989, 323).

1.6 In the present case, the board does not see that the interests of third parties could have been affected. As the request for correction was filed only three days after the four month time limit under Article 108 EPC expired, third parties could not reasonably make any dispositions based on the assumption that no admissible appeal was filed. The board cannot see any link to a possible procedural abuse, and the board is satisfied that the request for correction was filed without any delay.

1.7 Since the conditions for a correction are met and as the board does not see any reason why its discretion should not be exercised in the appellant's favour, the request for correction is allowed and the corrected version of the letter dated 7 April 2008 (as filed by telefax on 10 April 2008) is deemed to have been filed on 7 April 2008. The appeal is admissible.

2. *Main Request - Inventive step:*

2.1 Prior art

2.1.1 D1 discloses a scheme for downloading signed content onto a computer. The signed content may be an executable code and the signature on the content describes the security credentials of the creator of the code and the computer resource requirements of the code. The access of the downloaded code to the resources is managed, in the computer, by a security manager (secure content usage system) which, on the basis of the credentials and resource requirements of the code, assigns capabilities to the code; the security manager uses the capabilities to grant and regulate access by the code to the computer resources. Examples of computer resources are mentioned on column 3, lines 28-31. Examples of executable codes are mentioned on column 3, lines 10-11.

2.1.2 The appellant acknowledged, in a letter to the examining division dated 1 October 2007, in the statement of grounds of appeal, in the statement of the inventor filed in response to the summons and during the oral proceedings, that an early version of the Symbian Operating System (OS) was known and installed

in mobile phones before the priority date of the present application. The Symbian OS is designed for mobile wireless devices and is a server based operating system wherein servers running on the device provide services and resources to applications, both within the operating system and at a user level, which require them. For example, a file server provides access to the data storage system, a phone server (ETEL) provides access to the cellular phone stack, a window server provides access to the display, etc... The arrangement is based on a client-server model, with client programs that require access to the phone functionality passing requests via the kernel Inter-Process Communications (IPC) process to the individual servers, which then act on request. The mobile phones equipped with the early version of Symbian OS were closed platforms, on which native code was installed on manufacture, and no further software could then be installed by the user during use, thereby avoiding the problem of malicious code being installed and using the phone functions.

The board considers that the above-mentioned prior art of a mobile wireless device using the early version of Symbian OS represents the closest prior art since it requires less structural and functional modifications to arrive at the claimed invention than the prior art disclosed in D1.

2.2 The subject-matter of claim 1 differs from this closest prior art in that the resources are protected by having a set of capabilities assigned to a native executable code installed on the device which define the protected resources on the device which the native executable code can access and in that access to said protected

resources is policed by the corresponding servers on the basis of the capabilities assigned to the native executable code.

The technical effect of these differences is that the resources of the device are accessed only by codes having being assigned appropriate capabilities.
The objective technical problem may thus be defined as how to protect the resources of the mobile wireless device against malicious unauthorized native executable codes.

The skilled person trying to solve that problem would come across document D1 which relates to resource access by executable codes in a computer system, based on the use of capabilities which are assigned to the codes and checked by a security manager which centrally grants and regulates access to the resources (column 6, lines 38-40, column 7, lines 17-21). By applying the teaching of D1 to a device using the early version of the Symbian OS, the skilled person would arrive at a device wherein capabilities are assigned to a native executable code installed in the device, as defined in claim 1, but wherein access to the resources is centrally policed. Distributing a task between several entities is however common practice and an obvious alternative in the field of programming, in order to avoid a single point of failure and to balance the computing load. By distributing the capabilities checking task, the skilled person would choose the most straightforward implementation which consists in performing the capabilities check in the entities already provided in the device for accessing resources,

i.e. in the servers of the Symbian OS, thereby arriving to a device as defined in claim 1.

Thus, the subject-matter of claim 1 of the main request does not involve an inventive step.

Similar arguments apply to the corresponding method of claim 12 and the corresponding computer program claim 13.

2.3 The appellant argued that D1 does not relate to native executable codes but to Java applets which are downloaded to a computer. The board accepts that D1 relates to the download of non-native executable codes(such as Java applets, OLE or SOM codes which are the code types mentioned in D1) which need to be interpreted (or compiled) before being executed by the operating system of the computing device and that the security manager of D1 assigns capabilities to such codes at the time they are downloaded, i.e. installed, in the computing device (column 4, lines 8-10). However the board judges that the teaching of D1 in respect of the scheme of assigning capabilities by the security manager to the downloaded code is not specific to the nature of the executable code (Java, OLE and SOM are just mentioned as examples) but would be considered by the skilled person to apply to all kinds of executable codes.

The appellant further argued that D1, although it uses the term "capabilities", does not define capabilities in the sense of claim 1, i.e. as privileges assigned to an executable code which define the protected resources the code is allowed to access, but merely define how

much of the resources (e.g. memory space) may be used by the executable code. The Board is not convinced by this argument and notes that the passage at column 6, lines 38-50 discloses that the security manager implements a range of security policies, based on the capabilities, including the simple policy "no access, complete access". This corresponds to the definition of a capability used throughout the description of the present application. The board therefore considers that the capabilities described in D1 fall unambiguously within the meaning used in claim 1 of the application.

According to the appellant, even if the skilled person would combine the early version of Symbian OS with D1, he would not implement a decentralised solution in the servers of Symbian OS but rather a centralised one since D1 does not relate to a server based operating system and describes a centralised security manager. The board considers that the distribution of the capabilities check in the Symbian OS servers is an obvious step for the skilled person since it is always desirable for a programmer to associate a function (in the present case the resource access provided by the Symbian OS servers) with the corresponding authorisation (in the present case the capabilities check).

The appellant also argued that the commercial success of the phones equipped with the Symbian OS according to the alleged invention should be used as a secondary indication which points to the presence of inventive step. Firstly the board is not convinced that the alleged commercial success derives from the technical features of claim 1 alone, as is required by the

established case law of the boards of appeal to take commercial success into account as a secondary indication of inventive step. Secondly, the board judges that, even if commercial success deriving from the features of claim 1 were proven, the technically relevant examination of the subject-matter of claim 1 (see point 2.2 above) would nonetheless be in itself sufficient to establish the lack of inventive step.

3. *1st auxiliary request:*

Claim 1 of the 1st auxiliary request differs from claim 1 of the main request in specifying that the device includes a trusted computing base TCB having a kernel, that the capabilities are stored in a location that is only accessible to the TCB, and that the kernel is arranged for each client-server communication to pass the client capabilities to said server.

The arguments presented in point 2 regarding claim 1 of the main request apply similarly with respect to the identical features.

In addition to the differences presented in point 2.2 above the subject-matter of claim 1 of the 1st auxiliary request differs from the closest prior art represented by a mobile wireless device equipped with the early version of Symbian OS in that the capabilities are:
- stored in a location which is only accessible to a TCB and,
- for each client-server communication, passed to the server by the kernel of the TCB.
These features provide the technical effects that the capabilities, once installed on the device, cannot be

changed without authorisation to access the TCB, and that servers can be certain that the capabilities they received are correct since directly passed by the kernel of the TCB, the most trusted part of the OS. These features therefore solve the problem of protecting the capabilities against corruption both when stored in the device and when passed to the servers.

None of the documents on file disclose or suggest in combination the storing of capabilities in a location only accessible to the TCB and the passing of client capabilities for each client-server communication by the kernel of the TCB.

Applying the teaching of D1 to the prior art Symbian OS as argued for the main request would result in the capabilities being stored in the servers, some of which may possibly be accessed by code executing outside the TCB.

The only document on file which addresses the problem of protection of the capabilities is D3. D3 describes three methods of protecting capabilities from tampering:
- a tagged architecture using a tag bit indicating whether a memory word contains a capability or not, and which can be modified only by the operating system;
- cryptographic protection of capabilities stored in user space;
- storing of capabilities inside the operating system.
However, D3 does not disclose or suggest to apply the storing of capabilities in the operating system to a server-based operating system; furthermore, D3 teaches

that a process has to request capability from the operating system whereas in claim 1, for each client-server communication, the kernel passes the capabilities to the server without having the server needing to make a call to any access control manager. Further in the invention it is the server that makes the decision whether access should be granted to the resources it manages, rather than that decision being made by the operating system. The invention was plausibly argued to be consequently a simpler and more dynamically flexible arrangement.

Therefore, the subject-matter of claim 1 involves an inventive step.

Similar arguments apply to the corresponding method of claim 11.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the department of first instance with the order to grant a patent on the basis of Auxiliary Request 1 (claims 1-11) as submitted during the oral proceedings before the board, and a description to be amended.

Registrar: Chairman:

K. Götz D. H. Rees