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 11 November 2010

Case Number:	T 0264/07 - 3.5.06
Application Number:	00916148.0
Publication Number:	1163566
IPC:	G06F 1/00
Language of the proceedings:	EN

Title of invention:
Method and system for enforcing access to a computing resource using a licensing certificate

Applicant:
-

Opponent:
-

Headword:
Resource access control/SPYRUS

Relevant legal provisions:
EPC Art. 123(2)

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

Keyword:
-

Decisions cited:
-

Catchword:
-

Case Number: T 0264/07 - 3.5.06

DECISION
of the Technical Board of Appeal 3.5.06
of 11 November 2010

Appellant:

Spyrus, Inc.
5303 Betsy Ross Drive
Santa Clara
CA 95054 (US)

Representative:

Benson, Christopher
Harrison Goddard Foote
Fountain Precinct
Balm Green
Sheffield S1 2JA (GB)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted 2 October 2006 refusing European patent application No. 00916148.0 pursuant to Article 97(1) EPC 1973.

Composition of the Board:

Chairman: D. H. Rees
Members: M. Müller
M.-B. Tardo-Dino

Summary of Facts and Submissions

I. The appeal lies against the decision of the examining division, with written reasons dated 2 October 2006, to refuse the European patent application 00916148.0.

II. The decision made reference to only one document,

D1: EP 0 813 132 A2,

and came to the conclusion that the independent claims went beyond the content of the application as originally filed, in violation of Article 123(2) EPC, and that they - when limited to an interpretation that *was* originally disclosed - lacked novelty over D1, Article 54 EPC 1973.

III. An appeal was filed by fax on 1 December 2006 and the appeal fee was paid on the same day. A statement of grounds of appeal was filed on 2 February 2007 by fax. The appellant requested that a patent be granted based on claims 1-37 that had been filed on 11 September 2006 and on which the refusal was based.

IV. With letter of 20 July 2010, the board invited the appellant to oral proceedings. In an annex to the summons the board introduced additional documents from the International Search Report, in particular

D3: EP 0 828 208 A2,

and expressed the preliminary opinion that the then valid claims violated Articles 123(2) EPC and 56 EPC

1973. The board also raised objections under Article 84 EPC 1973 against some of the dependent claims.

V. With letter dated 13 October 2010, the appellant filed claims 1-37 according to a main request, claims 1-36 according to a first auxiliary request, and claims 1-33 according to a second auxiliary request.

Claim 1 according to the main request reads:

"A method of enforcing access by a computer application (210) to a computing resource (226) controlled by a trusted computing base (208), including the steps of:

generating enforcement data (222) regarding allowable usage of said computing resource;

embedding said enforcement data in a licensing attribute certificate (220);

cryptographically binding said licensing attribute certificate to said computing resource (226) using a private key;

associating said licensing attribute certificate with said computer application (210); and

authenticating in said trusted computing base (208) the use of said computing resource (226) by said computer application (210) using a public key corresponding to said private key, wherein access to the computing resource (226) is restricted to computer applications whose use of the computing resource (226) is authenticated by said trusted computing base (208)."

Claim 21 according to the main request reads:
"A system for enforcing access by a computer application (210) to a computing resource (226)

controlled by a trusted computing base (208), comprising:

means for generating enforcement data (222) regarding allowable usage of said computing resource;

means for embedding said enforcement data in a licensing attribute certificate (220);

means for cryptographically binding said licensing attribute certificate (2220) to said computing resource (226) using a private key;

means for associating said licensing attribute certificate with said computer application; and

the trusted computing base (208) being operable to authenticate the use of said computing resource (226) by said computer application using a public key corresponding to said private key; wherein the trusted computing base (208) is arranged to limit access to the computing resource (226) only to computer applications whose use of the computing resource (226) is authenticated by said trusted computing base (208)."

Claim 1 according to the first auxiliary request is identical to that of the main request except that the associating step is now specified as follows:

"associating said licensing attribute certificate with said computer application (210), wherein said associating comprises compiling (332) computer application source code (330) with said licensing attribute certificate".

Correspondingly, claim 20 of the first auxiliary request is identical to claim 21 of the main request except that the means for associating is now specified as:

"means for associating said licensing attribute certificate with said computer application, wherein the means for associating is arranged to compile computer application source code with the licensing attribute certificate (220)".

Claim 1 according to the second auxiliary request reads

"A method of enforcing access by a computer application (210) to a cryptographic computing resource (484) controlled by a trusted computing base (208), wherein the cryptographic computing resource (484) is contained within a cryptographic token (470), including the steps of:

generating enforcement data (222) regarding allowable usage of said cryptographic computing resource (484), wherein said generating comprises generating token attribute data (502) identifying cryptographic operations on the token (470) available to said computer application;

embedding said enforcement data in a licensing attribute certificate (220);

cryptographically binding said licensing attribute certificate to said cryptographic computing resource (484) using a private key;

associating said licensing attribute certificate with said computer application (210), wherein said associating comprises compiling (332) computer application source code (330) with said licensing certificate; and

authenticating in said trusted computing base (208) the use of said cryptographic computing resource (484) by said computer application (210) using a public key corresponding to said private key, wherein access to the cryptographic computing resource (484) is restricted to computer applications whose use of the cryptographic computing resource (484) is authenticated by said trusted computing base (208)."

Claim 19 according to the second auxiliary request reads as follows:

"A system for enforcing access by a computer application (210) to a cryptographic computing resource (484) controlled by a trusted computing base (208), wherein the cryptographic computing resource (484) is contained within a cryptographic token (470), comprising:

means for generating enforcement data (222) regarding allowable usage of said cryptographic computing resource (484), wherein the means for generating is arranged to generate token attribute data (502) identifying cryptographic operations on the token (470) available to said computer application (210);

means for embedding said enforcement data in a licensing attribute certificate (220);

means for cryptographically binding said licensing attribute certificate (220) to said computing resource (484) using a private key;

means for associating said licensing attribute certificate with said computer application wherein the means for associating is arranged to compile computer application source code with the licensing attribute certificate (220); and

the trusted computing base (208) being operable to authenticate the use of said cryptographic computing resource (484) by said computer application using a public key corresponding to said private key; wherein the trusted computing base (208) is arranged to limit access to the cryptographic computing resource (484) only to computer applications whose use of the cryptographic computing resource (484) is authenticated by said trusted computing base (208)."

VI. Oral proceedings took place as scheduled on 11 November 2010. The appellant maintained its requests unchanged (see point V).

Reasons for the Decision

1. The appeal is admissible as complying with the EPC admissibility requirements (see points I and III above).

2. Article 84 EPC 1973

The board is satisfied that the claims according to all requests are clear.

3. Article 123(2) EPC

3.1 Claim 1 as refused by the examining division specified that the trusted computing base would authenticate a computer application. In the art, this would be understood to mean validating that the application has not been tampered with (see *e.g.* D3, col. 13, lines 39-46), while the description only disclosed authenticating that an application was allowed to use a computing resource in a specific manner (see *e.g.* p. 12, lines 15-21). Amended claim 1 of all requests (as well as the corresponding system claims) now specifies that it is the "use of the computing resource" which "is authenticated" and so overcomes the objection.

3.2 Claim 21 as refused specified that the computing resource itself "was arranged to be accessible" by the computer application after successful authentication. This was in conflict with the disclosure that it was the trusted computing base - rather than the computer application itself - which controlled access to the computing resource. The wording now used in claim 21 of the main request (which corresponds to claims 20 and 19 according to the first and second auxiliary requests, respectively), according to which "the trusted computing base ... is arranged to limit access" remedies this deficiency.

3.3 In summary, the board has no objections under Article 123(2) EPC against any of the pending requests.

Articles 54 and 56 EPC 1973

Main request

4. During examination and in the decision, the examining division has referred to D1 as the only prior art document. The board agrees that D1 is an appropriate starting point for the assessment of novelty and inventive step in the present case.

5. Document D1 discloses a method of "enforcing access" by a computer application to a computer resource (p. 3, lines 34-39) according to "enforcement data" defining allowable usage of said computing resource ("access control list" ACL, *loc. cit.*). D1 further discloses a

certificate for the ACL (p. 3, lines 8-9) which is associated with the pertinent computer application. The certificate is signed with the private key of a certification agency so as to establish an association between the permissions of the ACL and the computing resources (p. 3, lines 6-9). D1 also discloses a trusted computing base (essentially the entire system depicted in fig. 2) which authenticates the use of the computing resource by the computer application according to the ACL (fig. 2, items 100 and 110) using the corresponding public key (p. 3, lines 27-28), so that the access to the computing resource is restricted to computer applications whose use of the computing resource is authenticated by the TCB (p. 3, lines 45-46).

5.1 The application uses the term "licensing attribute certificate" LAC instead of just "certificate". The reference to "licensing", suggesting that the access permissions according to the invention are part of a contract between vendor and customer (cf. also p. 7, line 31 - p. 8, line 6), does not limit the certificate in form or structure. Also, whether access restrictions are enforced to comply with a license agreement or in order to maintain system security does not have a bearing on how the access restrictions are enforced. Therefore, the notion "licensing attribute certificate" is, in the board's view, no more limiting than "certificate" alone.

5.2 D1 discloses that a certificate is created "for" the ACL (p. 3, lines 8-9), but suggests that the certificate and the ACL are separate from each other so that the ACL is not, as claimed, "embedded" into the certificate. The board concludes that therefore the independent claims according to all requests are new.

The description does not define the "embedding" in detail, but figure 5 of the application, depicting a typical LAC, is taken to illustrate it. Accordingly, an LAC may contain enforcement data (such as "attribute token data"), directly followed by an associated signature.

D1 discloses that the ACL and its certificate are downloaded together (p. 3, line 27). In the board's view, it is an obvious modification of D1 to combine ACL and certificate in a joint data structure, *e.g.* for simplification by limiting the number of files that must be downloaded. Storing ACL and certificate *in sequence* - as depicted in the application (fig. 5) - is, in the board's view, a fundamental choice. It is also hinted at by fig. 1 of D1 which suggests that the ACL is downloaded just before its certificate ("ACL, CERTIFICATE(ACL)").

5.3 Claim 1 specifies that the LAC should be cryptographically *bound to the computing resource*.

5.3.1 This formulation implies, according to the appellant, that the cryptographic keys are specifically related to the computing resource - *e.g.*, they may belong to the vendor of the computing resource (cf. *e.g.* claim 13 of the main request). This would further distinguish the invention from D1 according to which the keys belong to an independent certification authority.

5.3.2 The board does not share this limited interpretation. The cryptographic certification according to D1 clearly establishes a link between the ACL and the computing resource (cf. p. 3, lines 34-36). In the board's view, this is sufficient to imply that both are "cryptographically bound" to each other as claimed.

5.3.3 Even if it were assumed, *arguendo*, that claim 1 would indeed imply the use of the vendor's key, this would not, in the board's view, establish an inventive step over D1, because the use of a different key would not change the manner in which an ACL is certified, authenticated and enforced according to D1.

6. The appellant argues that the access control mechanism of D1 can be bypassed by application code that does not have an ACL, whereas this is impossible according to the invention: The independent claims require that a resource *cannot* be accessed by an application unless its use is authenticated.

6.1 Document D1 is concerned with secure execution of software downloaded from a network and discloses enforcing access restrictions specifically for such software (p. 2, lines 1-28; p. 3, lines 27-39). The board agrees with the appellant that this is meant to "protect the client and instil trust" but cannot see a conflict between doing this and enforcing a control scheme as the appellant suggests.

Software which is not downloaded from the network - but, say, installed from a vendor's CD - is not discussed in D1, but it would indeed appear to be possible from D1 that such software might be trusted and hence would not be authenticated.

6.2 However, in the board's opinion, this feature does not establish an inventive step of claim 1 for the following reasons.

6.2.1 First, from the perspective of applications downloaded from a network, D1 does disclose that resources *cannot* be accessed unless such access is authorized. The board considers that the wording of the independent claims does not rule out this perspective.

6.2.2 Second, the board considers it obvious within the context of D1 to use a "thin client" which does not run any local applications. In this scenario, *any* access to a local computing resource would originate from a downloaded application and hence fall under the security regime of D1.

6.2.3 Third, in order to further increase the security of the system of D1 it is, according to the board, an obvious option to impose the certification requirement on *all* applications rather than only the downloaded ones.

6.3 In summary, the board concludes that for any of these reasons claim l according to the main request lack an inventive step over D1.

First auxiliary request

7. Claim 1 additionally specifies that, when associating the LAC with the computer application, the computer application source code is "compiled with" the LAC.

Thereby the LAC will become "embedded" in the computer application (p. 14, lines 24-27; fig. 3b).

7.1 The LAC itself is not compiled into executable code. The notion that the application is "compiled with" the LAC can, hence, only mean that the compiler takes the LAC as an additional parameter and reproduces it in some way as part of the executable. The compiler may, for instance, operate as usual and simply attach the LAC to the executable in a final step.

7.2 D1 discloses that "[t]he program code is encapsulated ... with the certificate and an access control list (ACL)" (p. 5, lines 15-16). This encapsulated data structure is, in the board's view, indistinguishable from the output of the claimed compilation step. Moreover, whether the encapsulation step is part of or separate from compilation does not, in the board's view, have any significant technical effect that could establish an inventive step. Also the appellant did not indicate any such effect.

7.3 The board therefore concludes that claim l according to the first auxiliary request lacks an inventive step over D1.

Second auxiliary request

8. Claim 1 according to the second auxiliary request specifically refers to a cryptographic computing resource contained within a cryptographic token, and to token attribute data identifying cryptographic operations on the token available to the computer application in question.

8.1 In contrast to D1, which does not disclose cryptographic tokens or operations, D3 deals with application certification for a cryptography framework (see title). Moreover, D3 is specifically concerned with enforcing national policies regarding the use of cryptography (col. 1, line 39 - col. 2, line 6) - which, as one motivation, is also mentioned in the present application (p. 7, lines 20-30). The appellant argued that, therefore, D3 constitutes the closest prior art for the second auxiliary request.

8.2 The appellant also argued that the problem-solution-approach as generally used by the EPO would oblige the board to determine the closest piece of prior art in a first step, and to assess obviousness of the invention exclusively in view of that closest prior art. In support for this opinion, the appellant referred to the Guidelines for Examination in the EPO (*e.g.* C-IV, 9.8, in the edition of June 2005).

8.3 The appellant therefore requested that D1 be dismissed in favour of D3 as a starting point for assessing inventive step of the second auxiliary request.

9. The board accepts that not every piece of prior art is a suitable starting point for the assessment of inventive step. There may, in particular, be documents from which the skilled person cannot reasonably be assumed to start in order to solve a given problem, for example, because in a particular context the problem solved by the invention simply does not arise.

10. In the present case, document D1 has been used as a starting point for the inventive step analysis throughout the examination procedure and during the appeal procedure up to this point. To the board it is therefore natural and appropriate to consider whether D1 is still a suitable starting point for assessing inventive step of the second auxiliary request, or whether there is some particular reason for ruling it out.

11. D1 discloses a scheme for controlling that programs downloaded from a network do not exceed their permissions when accessing local resources. The term "resources" is used broadly in D1, and meant to cover logical as well as physical resources (*e.g.* system calls as well as peripheral storage devices; p. 3, lines 34-39). Hence, D1 anticipates application of its control scheme to all kinds of resources.

11.1 The board considers that cryptographic resources as claimed, *i.e.* cryptographic operations on a cryptographic token, are *per se* well-known in the art. This opinion was expressed during oral proceedings and was not disputed by the appellant. Nonetheless it is pointed out that the prior art section in D3 supports this fact: It is disclosed, *inter alia*, that companies use cryptography to protect privacy and data integrity in their internal communication, that cryptography (and the supporting technology) has even become a matter of national interest (col. 2, lines 8-10) and that cryptographic tokens *per se* were known in the art (cf. esp. col. 1, lines 16-24; col. 2, lines 16-22 and lines 32-36; col. 3, lines 19-33; and figs. 1-2).

11.2 The board also considers it obvious that the client systems according to D1 may offer cryptographic resources as claimed, and that programs downloaded from a network may want to access these resources (*e.g.* an email client or home banking software).

11.3 Such circumstances would, naturally, require adaptation of the control scheme according to D1 to this specific kind of resource. The board therefore concludes that D1 is, indeed, a suitable starting point for the present invention.

11.4 The actual adaptation of D1 to deal with cryptographic resources as claimed would be straightforward for the person skilled in the art. Therefore, the board concludes that claim 1 according to the second auxiliary request also lacks an inventive step over D1.

12. This conclusion is not invalidated by the possibility that D3 might be "closer" to the invention than D1. Hence, there is no point in investigating further whether or not this actually is the case, even if the standard presentation of the problem-solution-approach suggests otherwise. This question may thus be left open.

13. In summary, as there are no allowable requests, the appeal must be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar:	The Chairman:
B. Atienza Vivancos	D. H. Rees