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

Datasheet for the decision of 13 January 2012

Case Number: T 1216/08 - 3.5.06

Application Number: 00950637.9

Publication Number: 1303802

IPC: G06F 1/00

Language of the proceedings: EN

Title of invention:
System and method of verifying the authenticity of dynamically connectable executable images

Applicant:
Rovi Solutions Corporation

Headword:
Authenticating a program image/ROVI

Relevant legal provisions (EPC 1973):
EPC Art. 54(1)(2), 56

Keyword:
"Novelty - yes"
"Inventive step - yes"

Case Number: T 1216/08 - 3.5.06

DECISION
of the Technical Board of Appeal 3.5.06 of 13 January 2012

Appellant:	ROVI SOLUTIONS CORPORATION 2830 De La Cruz Boulevard Santa Clara, CA 95050 (US)
Representative:	Needle, Jacqueline Beck Greener Fulwood House 12 Fulwood Place London WC1V 6HR (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted 31 January 2008 refusing European patent application No. 00950637.9 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman:	D. H. Rees
Members:	M. Müller C. Heath

Summary of Facts and Submissions

I. The appeal lies against the decision of the examining division to refuse the European patent application no. 00950637.9.

II. The decision was delivered in writing on 31 January 2008 as a so-called decision according to the state of the file and for its reasons made reference only to the communication dated 30 October 2007. This communication cited, *inter alia*, the following documents

D1: EP 0 778 520 A
D2: WO 00/14631

and objected that the independent claims lacked novelty over D2.

III. A notice of appeal was received on 31 March 2008 and the appeal fee was paid on the same day. On 30 May 2008, a statement of grounds of appeal was received.

IV. The appellant argued that the examining division was wrong in not allowing the application with the application documents on file and thus implicitly requested that the decision under appeal be set aside and that a patent be granted.

V. With summons to oral proceedings, the board raised objections as to lack of clarity and lack of conciseness. On the assumption that these could be overcome, however, the board expressed its intention to remit the application to the examination division with an order to grant.

VI. In response, the appellant filed amended claims and description pages and requested that a patent be granted on the basis of the following documents:

description, pages

1-4	as filed with letter of 8 December 2011
5-11	corresponding to pages 3-9 as published and renumbered as requested on 24 June 2005

claims, no.

1-30	as filed with letter of 8 December 2011

drawings, no.

1/6-6/6	as published

In view of the board's intention to remit the application the appellant also announced not to be represented at the oral proceedings.

VII. Claim 1 reads as follows:

"A system for determining the authenticity of a program image (100) having one or more pointers that are in need of fixing up by a program loader (208), the system comprising a validator (204) arranged to:

generate at a first point in time a reference digital signature based upon a selected content of the program image (100); and

generate at a second point in time an authenticity digital signature based on said selected content of the program image, wherein the validator is further arranged to compare the reference digital signature with the authenticity digital signature to determine the authenticity of the program image,

characterised in that said selected content of the program image excludes each pointer located within said content that is in need of fixing up by a program loader."

Claim 23 reads as follows:

"A method of determining the authenticity of a program image having one or more pointers that are in need of fixing up by a program loader, the method comprising:

at a first point in time generating a first reference digital signature based upon a selected content of the program image,

at a second point in time generating an authenticity digital signature based upon said selected content of the program image; and

comparing the authenticity digital signature with the reference digital signature to determine the authenticity of the program image,

characterised in that the method further comprises:

identifying pointers within the program image (100) that are in need of fixing up by a program loader; wherein

the selected content of the program image excludes each pointer located within said content that is in need of fixing up by a program loader."

VIII. The oral proceedings were held as summoned in the appellant's absence. At the end of the oral proceedings, the chairman announced the decision of the board.

Reasons for the Decision

The Invention

1. The invention deals with the authentication of software in a dynamic loading environment (description as published, p. 1, lines 20-21). It is known to calculate an electronic signature for the image of a given program (a "disk image", see p. 1, line 12) so that by authenticating that signature later it can be determined whether the program image was changed. If the program image normally does not change a failure to authenticate the signature may be taken to indicate that the program image was tampered with and should, hence, be rejected as insecure. This approach fails however if the program image contains pointers which are legitimately modified during program loading and linking (p. 1, lines 17-19; page 5 as published, lines 13-17). To address this problem, the invention proposes to determine in a given program image the "pointers that are in need of fixing up" and to sign, instead of the entire program image, only "selected content of the program image" excluding these pointers (see *e.g.* present claim 1).

Article 84 and Rule 29(2) EPC 1973, and Article 123(2) EPC

2. The description and the original claims consistently refer to an "executable image" which contains pointers to be fixed up and which is electronically signed excluding these pointers.

2.1 In the present claims and the amended description pages the term "executable image" was replaced by "program image". On amended page 4 a short explanation was added to the effect that the term used in the claims differs from the term used in the description but that they are meant to be equivalent.

2.2 It is unambiguous from the description (see *e.g.* p. 1, lines 7-22) that the "executable image" refers to the image of a computer program, hence a "program image". It is also directly and unambiguously evident for the skilled person (*e.g.* from the independent claims) that what the description refers to as an "executable image" is executable only to the extent to which pointers "in need of fixing up" have actually been "fixed up" (p. 1 as published, lines 14-16). The board hence considers that the replacement of the term "executable image" by "program image" and the new paragraph on page 4, as well as the corresponding amendment to claim 18, do not extend beyond the application as originally filed.

2.3 Claim 23 was amended to specify that the "selected content" of the program image which is electronically signed excludes not just some but "each pointer ... in need of fixing up". This adapts claim 23 to original claim 1.

2.4 The other amendments to the claims constitute reformulations without any change in substance. The board is thus satisfied that amended claims 1-30 comply with the requirements of Article 123(2) EPC.

3. The amended claims contain a single independent system claim 1 and a single corresponding independent method claim 23. The conciseness objection pursuant to Rule 29(2) EPC 1973 is thus moot. The board is also

satisfied that the amended claims are clear, in compliance with Article 84 EPC 1973.

The Prior Art

4. Document D2 is concerned with chip cards which allow the dynamic loading and linking of additional program modules (p. 1, lines 6-8). D2 observes that the dynamic linking is too demanding of memory to be executed on-card (p. 2, lines 28-31) but that it would compromise security if the linking would take place in the card terminal (p. 2, lines 15-20). In this context D2 mentions the problem that the chip card cannot check a statically predefined signature of the program in question because the linking process must resolve the symbolic references (p. 2, lines 22-26). Therefore, it is proposed to split the linking process into a complex prelinking step which leaves for the second step only the resolution of the symbolic references; Only the second step will be performed on card (cf. p. 5, lines 16-23; p. 8, lines 26-29). D2 discloses that after the prelinking "the code" can be signed, and that the signed code will be linked and verified on card (p. 8, lines 29-32).

5. Document D1 is concerned with maintaining the guaranteed integrity of a verified architecture-neutral program ANP (e.g. written in Java) when on the other hand the program should be compiled so as to increase execution speed (p. 2, lines 3-5 and 29-40). The solution according to D1 is to package an architecture neutral program ANP (*i.e.* source code) together with its compiled version in an architecture specific - *i.e.* compiled - version ASP and three signatures (see p. 6,

lines 25-36 and fig. 3), namely the signature of the program provider (the "original party", OrigParty, index OC) applied to the ANP and the signatures of the compiler (index C) and the "compiling party" (CompParty, index CP), respectively, applied to the ASP.

Novelty

6. The appellant argues (grounds of appeal, p. 4) that D2 would not anticipate the claimed invention because D2:

a) is not concerned with the authenticity of an executable image,
b) has no reference to pointers that need to be fixed up,
c) does not generate a digital signature based upon the content of an image
d) does not generate an authenticity digital signature based upon the content of an executable image,
e) does not compare the two signatures, and
f) does not disclose the generation of a signature from content from which the pointers requiring fixing up have been excluded.

Since the term "executable image" was replaced by "program image" in order to clarify the claims without changing their scope the board assumes the appellant to maintain with regard to the amended claims that D2

a') is not concerned with the authenticity of a program image as claimed, and
d') does not generate an authenticity digital signature based upon the content of a program image as claimed.

7. The board disagrees with the appellant as regards features a/a' and b-e.

7.1 *Re. b:* The board concurs with the examining division that the symbolic references which the program loader resolves according to D2 read on the "pointers that are in need of fixing up" according to the invention.

7.2 *Re. a/a' and c:* The board agrees that the *term* "authentication" is not used literally in D2. However, the *concept* of authentication is disclosed in D2. Authentication of code means verification that a piece of code is the expected one. Thus where D2 addresses the problem that code might be manipulated between the terminal and the card (p. 2, lines 18-20) the skilled person would clearly understand this as a reference to code authentication.
Furthermore, the "code" signed according to D2 (cf. page 8, lines 30-31) requires only final linking (cf. p. 5, lines 19-21) before it can be executed on the card and therefore is a program image in the sense of the independent claims which also contains pointers "in need of fixing up" before it can be executed.
Therefore, the digital signature generated for the code according to D2 also qualifies as an "authenticity digital signature based upon the content of a program image" as claimed.

7.3 *Re. d/d' and e:* On page 8 (lines 29-31) D2 does not specify any details about the signature or the verification process. It is clear, however, in the board's view that the signature verification referred to on page 8 is meant to implement the signature verification discussed on page 2 (esp. lines 22-26) because D2

proposes the two-step linking process specifically in order to enable the signature verification which traditional linking does not allow (p. 3, lines 16-21). D2 discloses that a statically predefined signature of the program cannot be checked if and because the linking process changes the program (*loc. cit.*). For the skilled person this statement implies that the desired verification involves the comparison of two signatures as claimed.
Thus the board concurs with the examining division that D2 discloses features d (resp. d') and e, too.

8. The board however agrees with the appellant as regards feature f.

8.1 The board understands the examining division's argument to be as follows (see communication of 30 October 2007, point 3.1, item e):

i) The "code" signed after the prelinking process of D2 (see p. 8, lines 30-31) must be identified with the term "object code" as used elsewhere in D2 (see p. 6, last par. and fig. 1). Because the "object code" according to D2 is clearly distinct from the symbolic references this argument implies that D2 discloses signing only "selected content exclud[ing the] pointer[s] ... in need of fixing up".

ii) The examining division further argues (*loc. cit.*, last sentence) that the problem defined in D2, namely that changed modules cannot be verified, would not be solved if the object code including the symbolic references were signed.

8.2 The board disagrees with both considerations.

i) D2 does not imply the identification of the terms "code" and "object code". In the board's view, the skilled person would identify the term "der Code" in the phrase "Nach dem prelink Prozeß kann der Code signiert werden" (p. 8, lines 29-30) with the entire output of the prelinking process (including the symbolic reference) rather than only the "object code" (excluding the references).

ii) D2 discusses the problem that verification of program signatures is impossible when it requires the comparison of a program before linking with a program after linking (p. 2, lines 22-26). As a solution for this problem D2 discloses the option to run the entire linker on-card. This would allow, as is implied by D2, the verification of the original program against the loaded program before linking. This option is dismissed in D2 because it would exceed the memory resources available on the card. The prelinking process according to D2 produces object code packaged with symbolic references which remain to be resolved in the second linking step. D2 discloses that the signed code will be linked and verified "during" the loading process (p. 8, lines 30-32). In the board's view, the skilled person would understand that this phrase refers to linking and verification as two logically distinct steps performed during loading. On this understanding, the signed code could be verified on the card *before* the final linking step.
Therefore, the problem of D2 is indeed solved when the entire output of the prelinking process is

signed. Thus the interpretation according to point i) is not in conflict with the problem addressed by D2.

8.3 The board therefore concludes that by virtue of feature f the subject matter of independent claims 1 and 23 is new over D2 in the sense of Article 54(1)(2) EPC 1973.

8.4 According to D1 the electronic signatures are generated on the basis of a program before or after compilation (ANP and ASP; cf. p. 4, lines 50-52; p. 6, lines 3-5 and 12-14). More specifically, the digital signature is based on a hash function calculated "on the data bits of the ANProgram code" or the "ASProgram code" (cf. p. 4, lines 52-54; p. 6, lines 5-6 and 14-19). The skilled person would understand this as meaning that the electronic signatures are generated from the entire programs rather than only from selected content, let alone from content selected by exclusion of pointers. Hence, the subject matter of claims 1 and 23 is also new over D1 by virtue of feature f.

Inventive Step

9. Although the decision was only based on lack of novelty as far as the independent claims were concerned, the board deems it appropriate in the present case to exercise its power under Article 111(2) EPC and to consider inventive step as well.

10. Document D2 constitutes the most pertinent document on file because it also addresses the problem of authenticating an electronically signed program in the context of linking.

10.1 The solution according to D2 provides that code authentication is possible on the card up until the final linking step but not after that. This is sufficient to authenticate a program loaded onto the card before it is run and to run only programs which have not been tampered with before loading (p. 2, lines 15-20).

10.2 Beyond D2, by virtue of feature f the claimed invention enables code authentication also after final linking or even after the program has been executing for some time (cf. application as published, p. 1, lines 21-23 and p. 9, lines 17-19). Feature f hence further increases the security of the system according to D2.

10.3 While increased security is an obvious desirable in general, D2 does not specifically disclose the need for code authentication after linking (p. 2, lines 15-20). This omission is consistent with the apparent assumption in D2 that the chip card itself is safe (see e.g. p. 2, lines 26-27). The board thus considers that D2 contains no prompt to increase the security by enabling run-time code authentication on the chip card, nor does it suggest to achieve this by means of feature f. Also D1 cannot, in the board's view, suggest this feature because D1 does not even disclose the general authenticating problem in the context of linking.

10.4 In the board's judgement thus the subject matter of claims 1 and 23 is not obvious over D2 alone or in combination with D1.

10.5 In the board's judgment thus claims 1 and 23 are based on an inventive step over the prior art to hand in the sense of Article 56 EPC 1973.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The application is remitted to the department of first instance with the order to grant a patent based on the following application documents:

description, pages	
1-4	as filed with letter of 8 December 2011
5-11	corresponding to pages 3-9 as published and renumbered as requested on 24 June 2005
claims, no.	
1-30	as filed with letter of 8 December 2011
drawings, no.	
1/6-6/6	as published

The Registrar: The Chairman:

B. Atienza Vivancos D. H. Rees