Internal distribution code:

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

Datasheet for the decision of 26 April 2023

Case Number: T 1813/19 - 3.5.06

Application Number: 09782681.2

Publication Number: 2344972

IPC: G06F21/00

Language of the proceedings: EN

Title of invention:
MALWARE DETECTION METHOD AND APPARATUS

Applicant:
WithSecure Corporation

Headword:
Malware detection/WITHSECURE

Relevant legal provisions:
EPC Art. 56, 84
RPBA Art. 12(4)

Keyword:
Claims - clarity (no)
Inventive step - (no)

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Case Number: T 1813/19 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 26 April 2023

Appellant: (Applicant)	WithSecure Corporation Tammasaarenkatu 7 00180 HELSINKI (FI)
Representative:	Berggren Oy P.O. Box 16 Eteläinen Rautatiekatu 10A 00101 Helsinki (FI)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 8 February 2019 refusing European patent application No. 09782681.2 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	M. Müller
Members:	M. Domingo Vecchioni
	K. Kerber-Zubrzycka

Summary of Facts and Submissions

I. The appeal is against the decision of the examining division, dated 8 February 2019, to refuse European patent application No. 09782681.

II. The examining division refused the application on the basis that the claims according to a main request and first and second auxiliary requests did not fulfill the requirement of inventive step, Article 56 EPC, starting from the following document:

D6: US 6,928,550 B1 (J.-F. Le Pennec et al.) 9 August 2005

Claim 1 according to the first auxiliary request was also found to infringe the requirements of Article 123(2) EPC.

III. Notice of appeal was filed on 11 April 2019, the appeal fee being paid on the same day. With the grounds of appeal, filed on 7 June 2019, the appellant requested that the decision of the examining division be set aside and that a patent be granted on the basis of a main request or one of two auxiliary requests, all filed with the statement of grounds of appeal. Oral proceedings were conditionally requested.

The main request and the second auxiliary request are the same as those underlying the decision under appeal.

IV. In a communication pursuant to Article 15(1) RPBA sent on 9 February 2023 together with a summons to oral proceedings, the board provided its preliminary opinion on

the appeal. The claims according to all requests appeared not to meet the requirements of Articles 84 and 56 EPC.

V. With a reply received on 31 March 2023, the appellant indicated that it would not attend the oral proceedings and requested a decision according to the state of the file, without commenting in substance on the board's preliminary opinion.

VI. The oral proceedings were thereupon cancelled.

VII. Independent claim 1 according to the main request reads as follows:

"A malware detection method implemented within a computer and comprising:

for a given electronic file, determining if the file is associated with a valid digital signature using a trust verification system of an operating system of the computer (S4); and

if it is, then verifying that the signature belongs to a trusted source (S8), wherein the trusted source authored or published the file and created the signature, and if so then excluding said file from a malware scan (S10), and if the signature cannot be verified as belonging to a trusted source then including said file in the malware scan (Sll);

wherein said digital signature relies upon a public key infrastructure and the step of verifying that the signature belongs to a trusted source comprises maintaining a database of trusted public keys, identifying a public key used to verify the digital signature, and determining if the public key is contained in the database of trusted public keys."

VIII. Independent claim 1 according to auxiliary request 1 reads as follows:

"A malware detection method implemented within a computer by means of an anti-virus application and comprising:

for a given electronic file, determining if the file is associated with a valid digital signature using a trust verification system of an operating system of the computer (S4), by making a call to an embedded Trust Verification Application Programming Interface, API, of the operating system; and

if it is, then verifying that the signature belongs to a trusted source (S8), wherein the trusted source authored or published the file and created the signature, and if so then excluding said file from a malware scan (S10), and if the signature cannot be verified as belonging to a trusted source then including said file in the malware scan (Sll);

wherein said digital signature relies upon a public key infrastructure and the step of verifying that the signature belongs to a trusted source comprises maintaining a database of trusted public keys within the computer including receiving public keys from a service provider, identifying a public key used to verify the digital signature, and determining if the public key is contained in the database of trusted public keys."

IX. Independent claim 1 according to auxiliary request 2 reads as follows:

"A malware detection method for detecting malware on a computer and comprising:

maintaining a database of trusted public keys in the computer, said step of maintaining comprising,

identifying at a network based service, public keys belonging to a public key infrastructure architecture and which are used to digitally sign electronic files,

verifying that these public keys belong to a trusted source, and

securely sending the trusted public keys to the computer;

for a given electronic file, determining if the file is associated with a valid digital signature using a trust verification system of an operating system of the computer (S4); and

if it is, then verifying that the signature belongs to a trusted source (S8), wherein the trusted source authored or published the file and created the signature, and if so then excluding said file from a malware scan (S10), and if the signature cannot be verified as belonging to a trusted source then including said file in the malware scan (Sll);

wherein the step of verifying that the signature belongs to a trusted source comprises identifying a public key used to verify the digital signature, and determining if the public key is contained in the database of trusted public keys."

Reasons for the Decision

The application

1. The application relates to the detection of malware, e.g. a virus, in a computer.

2. A conventional approach involves an anti-virus software on the computer scanning files on the basis of a database of known virus signatures. In another approach, a hash of the file is computed and compared

with a list of hash values of trusted files provided by the anti-virus provider. In both approaches, the database of virus signatures or the list of trusted files are large, they consume a significant amount of memory and must be maintained (page 1, line 5 to page 3, line 17, of the description).

3. The application proposes that files be trusted - and thus excluded from a malware scan - if they have been "supplied, published or authored" by a "trusted source", i.e. a source considered trustworthy by the anti-virus provider. This is realised as follows.

For a given electronic file, a first check is performed, involving determining whether the file is "associated" with a "valid digital signature". The signature may be embedded in the file or the file may be listed in a catalog file that has itself been signed (page 6, lines 18-20).

If the outcome of the first check is positive, it is determined, in a second check, whether the signature belongs to a trusted source. If the outcome is again positive, the file is excluded from the malware scan.

If either the first or the second check fails, the file is included in the malware scan (which may be performed using conventional approaches).

4. The digital signature is generated using public key cryptography.

The application explains that in a conventional approach to generate and verify digital signatures, a hash value of the file is signed (encrypted) using the signer's private key. The signature may then be veri-

fied using the signer's public key. The signer's public key, together with the identity of the signer, are included in a "digital certificate", which is itself signed by a certification authority. The digital certificate may be embedded in the signed document. This enables one to retrieve the public key of the signer, to verify the signature of the file (and thereby also the file integrity) using that public key and to verify the identity of the signer (the certification authority being trustworthy; cf. page 6, line 25 to page 7, line 14).

5. In a preferred embodiment of the proposed malware detection method, the anti-virus software performs the first check, i.e. the determination of whether the file is associated with a valid digital signature, by using the "WinVerifyTrustEx" API included in the Windows operating system. The second check is performed by using a database of trusted public keys, said database being supplied and maintained by the anti-virus provider (page 6, lines 14-23; page 7, line 16 to page 8, line 8; page 8, line 19 to page 11, line 5).

6. According to the application, the proposed approach "remov[es] the burden placed on the anti-virus provider to maintain and update a trusted file list" as it will "only be required to supply and maintain a database of public keys belonging to trusted sources". The computer system does also "not need to store a list containing a large number of hash values for trusted files that are not actually on the [computer system], reducing the memory consumed by such a list and reducing the data traffic that would otherwise be required" for regularly updating the list. It further "reduces the processing burden by minimising the number of files that require a full malware scan" (page 11, lines 7-20).

Main request - Claim construction and Article 84 EPC

7. The method of claim 1 involves a first step of "determining if the file is associated with a valid digital signature using a trust verification system of an operating system of the computer". Claim 1 specifies also that the digital signature relies upon a public key infrastructure.

7.1 The determination of whether a digital signature is "valid" is understood by the board as a verification that the signature, after decryption, matches a hash of the file, as in the conventional approach to digital signature verification described on page 6, lines 28-31. This verification would confirm the integrity of the file (that it has not been altered since it was signed) and that the public key provided for the decryption of the signature corresponds to the private key that was used to sign the file. It would however not involve any determination of whether the source associated to these keys is a "trusted source" in the sense that files signed by this source may be assumed to be malware-free.

7.2 The board considers the term "trust verification system of an operating system" as used in claim 1 to be unclear, Article 84 EPC.

It is understood that this expression is meant to generalise the "WinVerifyTrustEx" function of the Windows operating system that is used in the preferred embodiment, so as not to be limited to that particular function and/or operating system (page 6, lines 16-18; page 10, lines 13-18).

While it is clear that the "WinVerifyTrustEx" function

falls within the scope of the term "trust verification system", the boundary of that scope does not appear to be sufficiently clear.

It is in particular unclear what kind of "trust" is being referred to. A first possibility would be that a "trust verification system" within the meaning of claim 1 is a system that merely provides for the verification that a digital signature is valid and that it may, for that very reason, be "trusted". Another possibility would be that the system provides a complete determination of whether a file is from a "trusted source" - in the same sense as this term is used in the application, i.e. the file may be assumed to be malware-free - and that this determination involves - but might go well beyond - performing a verification of the validity of the digital signature associated to the file.

In the following, and notwithstanding its clarity objection, the board adopts the first, broader interpretation, as the only functionality of the "trust verification system" being used in the claimed method is that of verifying the validity of a digital signature. This appears to be coherent with the functionality of the Trust Verification API of Windows that is emphasised in the description (page 6, lines 14-23). The appellant did not object to that interpretation.

8. The method of claim 1 involves a second step of "verifying that the signature belongs to a trusted source (S8), wherein the trusted source authored or published the file and created the signature".

8.1 From the claim wording, it is unclear, Article 84 EPC, whether the claimed verification involves not only

verifying (1) that the source to which the signature belongs is a "trusted source" but also (2) whether that source actually "authored or published the file and created the signature".

8.2 The description only discloses a computer-implemented verification of (1) (see e.g. page 8, lines 3-8). There is in particular no disclosure of a computer-implemented verification that the source actually "authored or published the file". The feature "wherein the trusted source authored or published the file" does thus not appear to imply any technical feature of the computer-implemented method. It may at best be considered to merely limit the claim to a particular circumstance of use, namely one in which the source having signed the file was actually its author or publisher. This is taken into account in the assessment of inventive step.

8.3 The board notes further that claim 1 does not specify which entity carries out the second step. Claim 1 does in particular not exclude that this step is also carried out by a computer program that is part of the operating system.

Main request - Article 56 EPC

9. It is common ground that document D6 is a suitable starting point for assessing inventive step of claim 1.

9.1 D6 discloses a method in which a "web/file server (101)" storing a file may request a "virus-free certificate authority server (102)" to perform a "full anti-virus checking" of the file and, if the file is found to be virus-free, to issue a "virus-free certificate"

for the file (see D6, col. 6, line 60 to col. 7, line 12; figure 1; col. 8, line 30 to col. 9, line 10).

9.2 A "client workstation (100)" downloading the file from the web/file server is then provided with the associated virus-free certificate. The anti-virus software running on the client workstation verifies the validity of the virus-free certificate. If the certificate is found to be valid, on the basis of the public key of the virus-free certification authority (VCA), the file needs no further check by the anti-virus software. Otherwise, if the file has no valid virus-free certificate, it is subjected to a conventional anti-virus check (D6, col. 9, line 17 to col. 10, line 31).

9.3 D6 explains that the aim of the method is to "speed up and improve the anti-virus processing" (D6, col. 5, lines 45-49).

9.4 D6 mentions that, preferably, the VCA generates the virus-free certificate using two different pairs of public/private keys. A first private key is used to sign a hash of the file. The signature together with a first public key, corresponding to the first private key, are included in a digital certificate which the VCA generates using a second private key corresponding to the VCA's (general) public key. The rationale for the use of two different pairs of keys is that the first pair may be given a validity period differing from that of the VCA's general pair of keys and does also not need to be as complex (D6, col. 7, lines 30-51).

D6 mentions that "[t]he VCA public key is in the workstation or if not must be retrieved through a secure channel" and that "[t]he VCA server may be

authenticated by another CA having the required public key" (D6, col. 9, lines 42-48).

9.5 The anti-virus software on the workstation authenticates first the virus-free certificate using the VCA public key, then verifies the validity of the file signature contained in the virus-free certificate using the public key that is also contained in it (D6, col. 9, lines 41-48 and 63-67).

10. D6 discloses thereby, using the wording of claim 1, "a malware detection method implemented within a computer by means of an anti-virus application", the latter one being the anti-virus software running on the workstation.

The method of D6 involves with the step of checking, by the anti-virus software, whether the signature included in the certificate is valid a step of "determining", for a given electronic file, "if the file is associated with a valid digital signature".

It involves also with the step of authenticating the virus-free certificate using the VCA public key a step of "verifying that the signature belongs to a trusted source", as it is implicit in D6 that the anti-virus software trusts the VCA. The VCA has also "created the signature".

If the file passes both verification steps, the method of D6 involves "excluding [the] file from a malware scan" and, otherwise, "including [the] file in the malware scan", as in the method of claim 1.

Finally, the digital signature in D6 "relies upon a public-key infrastructure".

11. The method of claim 1 thus differs from the method disclosed in D6 in the following:

(i) the determination that the digital signature is valid is performed "using a trust verification system of an operating system of the computer";

(ii) the verification that the signature belongs to a trusted source is carried out after the determination of the validity of the digital signature;

(iii) the verification that the signature belongs to a trusted source is carried out by "identifying a public key used to verify the digital signature" and by determining whether it is contained in a database of trusted public keys that is being "maintained";

(iv) the fact that trusted source has "authored or published the file".

12. Differentiating features (i) and (iii) correspond to differentiating features A and B identified by the examining division (decision under appeal, point 12) and the appellant (statement of grounds of appeal, page 2).

The examining division argued that these were juxtaposed features not producing a synergetic effect, which could thus be separately examined (decision under appeal, point 12).

The appellant contested this finding, arguing that "feature A [feature (i)] when implemented alone will both verify a signature and generate an indication of trust, but that indication of trust is limited and under the control of the OS provider and the CAs" and

that "[b]y introducing feature B [feature (iii)], the claimed invention allows a third party to be responsible for public key verification, solving the problem identified with feature A [feature (i)]" (statement of grounds of appeal, page 3).

13. The board agrees with the examining division and considers that distinguishing features (i)-(iv) are not functionally interrelated so as to achieve any synergistic technical effect and that they may therefore be separately examined for inventive step. It is in particular noted that any of the measures specified by these features could be implemented independently of the others.

14. The board is not convinced by the appellant's argumentation for the following reasons.

Feature (i), interpreted as explained at point 7.2 above, does not go beyond specifying that the verification of the digital signature is carried out by a component of the operating system. It does not imply the provision of any "indication of trust" by the operating system, where "trustworthy" would refer to being malware-free, as apparently argued by the appellant.

Furthermore, as noted at point 8.3 above, claim 1 does not exclude that the two verification steps are implemented completely as part of the operating system. The claim does not specify or imply the involvement of any "third party" that would be distinct from the operating system (OS) supplier of a certification authority (CA), as argued by the appellant.

15. Re feature (iii)

Starting from D6, it would be obvious to a skilled person that the virus-free certification service offered by the VCA could as well be offered by various VCAs. This would require the anti-virus software to have access to the public keys of VCAs that are to be trusted, e.g. in the form of a database of trusted VCAs with their public keys, maintained and made accessible or supplied to the workstation by the provider of the anti-virus software. This would lead to feature (iii).

The board is therefore not convinced by the appellant's argument that the skilled person would not have been motivated to modify the teaching of D6 to include a step of checking if the VCA's public key is in a database of trusted public keys (statement of grounds of appeal, page 4).

16. Re feature (iv)

This feature limits the claimed method to a special circumstance of use without any associated technical effect and cannot therefore support an inventive step.

In any case, it is obvious in the context of the method of D6 in view of the following considerations. A VCA may itself make electronic files available for download. It would be obvious to provide also for such files a virus-free certificate. When a workstation would verify the virus-free certificate, the identified source would be a trusted source that, incidentally, has authored or published the file, hence feature (iv).

17. Re feature (ii)

No technical effect appears to be achieved by the particular order in which the two verification steps are

carried out as the decision to exclude the file from malware detection requires in any case, in D6 as well as in claim 1, that the file passes both verification steps. Hence, no inventive step can be acknowledged on the basis of feature (ii).

18. Re feature (i)

18.1 As acknowledged in the present application (page 6, lines 14-23, page 8, line 31 to page 9, line 2, page 10, lines 13-15), at the relevant date, the Windows operating system provided functionality for assessing the trustworthiness of electronic files based on associated digital signatures, such as via the "Trust Verification API" and the "WinVerifyTrustEx" function. The existence of this functionality will have been part of the common general knowledge of a person skilled in the field of computer security given the notoriety of the Windows operating system.

18.2 Starting from D6, a first obvious consideration for a skilled person would thus have been that the method disclosed therein could similarly be implemented as part of an operating system, i.e. that the functionality of the anti-virus software, including the two verification steps, could be integrated in the operating system. Feature (i) would thereby be realised and is thus obvious already for that reason. This is independent of whether any of features (ii)-(iv) is also adopted for the reasons given above.

18.3 Furthermore, it would also have been obvious to a skilled person to consider whether existing implementations of cryptographic routines might be re-used. Where the operating system provides for implementation of basic cryptographic operations, such as verifying

the validity of a digital signature, it would have been an obvious option to consider using that implementation for this step of the method disclosed in D6. This is an alternative line of argumentation leading to the conclusion that the provision of feature (i) is obvious.

19. The appellant argued in the statement of grounds of appeal that "[t]he inventors have recognised that, for many files, the author or publisher of files will be security checking and signing files with their own keys (provided to them by a CA)", that one "cannot rely on this 100%, as an author or publisher's certificate may be compromised or the author or publisher may themselves start to generate malware, which may go undetected by the CAs and the OS supplier", and that therefore a "whitelist [...] containing certificates that we know to be trusted" is generated, e.g. "using crowd-sourced data".

The board does not find this argument relevant as it is not concerned with what would have been obvious or not obvious to a skilled person starting from D6, instead of what may have been the inventors' starting point. Furthermore, this argument relies on a number of features which are not present in claim 1.

20. It follows that claim 1 of the main request does not involve an inventive step, Article 56 EPC, starting from D6.

Auxiliary request 1

21. Claim 1 of auxiliary request 1 differs from claim 1 of the main request in the following underlined features:

(a) "a malware detection method implemented within a

computer by means of an anti-virus application",

(b) "for a given electronic file, determining if the file is associated with a valid digital signature using a trust verification system of an operating system of the computer (S4), by making a call to an embedded Trust Verification Application Programming Interface, API, of the operating system",

(c) "maintaining a database of trusted public keys within the computer including receiving public keys from a service provider".

22. Compared with claim 1 of the auxiliary request 1 on which the decision under appeal was based, present claim 1 differs only in the wording of the first step, which reads in that previous request as follows:

"for a given electronic file, making a call to an embedded Trust Verification Application Programming Interface, API, of an operating system of the computer to determine if the file is associated with a valid digital signature using a trust verification system (S4)".

The examining division objected to this wording under Article 123(2) EPC as it introduced the possibility that the signature would not be validated by the operating system itself but by another entity called by the operating system. Claim 1 was also objected to under Article 56 EPC for essentially the same reasons as the main request.

23. The board exercised its discretion under Article 12(4) RPBA 2007 to admit auxiliary request 1 as it addresses

the objection under Article 123(2) EPC without changing the subject-matter to be examined for inventive step.

24. The board considers that the amendments have a basis in the application as filed (for (a): see page 6, line 5, and figure 1; for (b): see page 8, line 31 to page 9, line 4, and page 10, lines 13-15; for (c): see page 7, lines 26-27) and that the examining division's objection under Article 123(2) EPC is thus overcome.

25. Claim 1 fails however to meet the requirements of Article 84 EPC for the reasons provided at points 7 to 8.2 above in respect of the main request.

26. Furthermore, the expression "an embedded Trust Verification Application Programming Interface, API, of the operating system" is unclear, Article 84 EPC. From the description (page 6, lines 16-18, and page 10, lines 13-15), it appears to refer to a specific API existing in the Windows operating system. Claim 1 is however not limited to that operating system and the claim does also not appear to be limited to that specific API. Like for the expression "trust verification system", it is not clear what the boundaries of the scope of the term "Trust Verification Application Programming Interface, API" are supposed to be. This renders claim 1 unclear, Article 84 EPC.

27. As regards inventive step, the board considers that the objection against claim 1 of the main request still applies to claim of auxiliary request 1, in particular in view of the line of argumentation described at point 18.3 above, which provides for the added features (a) and (b). Feature (c) was already covered by the argumentation in point 15 above.

Auxiliary request 2

28. Claim 1 of auxiliary request 1 differs from claim 1 of the main request in that the claimed method comprises the following steps:

"maintaining a database of trusted public keys in the computer, said step of maintaining comprising,
- identifying at a network based service, public keys belonging to a public key infrastructure architecture and which are used to digitally sign electronic files,
- verifying that these public keys belong to a trusted source, and
- securely sending the trusted public keys to a computer"

instead of the related features which were contained at the end of claim 1 of the main request.

29. The objections under Article 84 EPC against claim 1 of the main request (points 7 and 8 above) apply similarly against claim 1 of auxiliary request 2.

30. The objection under Article 56 EPC against claim 1 of the main request applies as well against claim 1 of auxiliary request 2.

The new features have been essentially covered by the argumentation in point 15 above. In the case of multiple VCAs providing virus-free certificates, the provider of the anti-software (whether an independent software vendor or the OS supplier if the anti-virus functionality is to be implemented as part of the operating system) would regularly update its database of trustworthy VCA and would verify their public keys (to be included in the database) on the basis of

digital certificates issued for the VCAs by another certification authority (see D6, col. 9, lines 46-48).

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

L. Stridde Martin Müller

Decision electronically authenticated