Internal distribution code:

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

Datasheet for the decision of 12 March 2018

Case Number: T 1322/12 - 3.5.06

Application Number: 07100377.6

Publication Number: 1818850

IPC: G06F21/24

Language of the proceedings: EN

Title of invention:
Techniques for attesting to content

Applicant:
Apple Inc.

Headword:
Attesting to content/APPLE

Relevant legal provisions:
EPC 1973 Art. 84

Keyword:
Claims - clarity (no)

Decisions cited:

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

Catchword:

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

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

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 1322/12 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 12 March 2018

Appellant: (Applicant)	Apple Inc. 1 Infinite Loop Cupertino, CA 95014-2084 (US)
Representative:	Barnfather, Karl Jon Withers & Rogers LLP 4 More London Riverside London SE1 2AU (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 30 December 2011 refusing European patent application No. 07100377.6 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Sekretaruk
Members:	A. Teale
	M. Müller

Summary of Facts and Submissions

I. This is an appeal against the decision, dispatched with reasons on 30 December 2011, to refuse European patent application No. 07 100 377.6 on the basis that the subject-matter of claim 1 did not involve an inventive step, Article 56 EPC, in view of the following document:

D1: US 6 848 048 B1.

II. A notice of appeal and the appeal fee were received on 14 February 2012. The appellant requested that the decision be overturned in its entirety, that a patent be granted or that the case be remitted to the first instance for further prosecution or to appoint oral proceedings.

III. In a statement of grounds of appeal, received on 30 April 2012, the appellant made an auxiliary request for oral proceedings before the board.

IV. In an annex to a summons to oral proceedings the board set out its provisional opinion *inter alia* that claim 1 of the main request was unclear, Article 84 EPC 1973.

V. With a letter received on 12 February 2018 the appellant submitted amended claims according to first, second and third auxiliary requests and amended pages of the description.

VI. In a letter received on 28 February 2018 the appellant's representative stated that he had been instructed not to attend the oral proceedings and would appreciate a telephone call from the Board in the event

of rejection of any of the requests based on "relatively straightforward objections".

VII. On 9 March 2018 the board, via its registry, sent the appellant a fax stating that the board could not see any simple amendment which could lead to grant. The appellant had not withdrawn the request for oral proceedings, and they would take place as scheduled.

VIII. Oral proceedings took place on 12 March 2018 in the absence of the appellant, as announced in advance. At the end of the oral proceedings the board announced its decision.

IX. The application is being considered in the following form:

Description (all requests): pages 1, 3 to 6 and 8 to 13, as originally filed, and pages 2 and 7, received on 12 February 2018.

Claims:
Main request: 1 to 26, received on 2 November 2011.
First auxiliary request: 1 to 26, received on 12 February 2018.
Second auxiliary request: 1 to 24, received on 12 February 2018.
Third auxiliary request: 1 to 23, received on 12 February 2018.

Drawings: pages 1 to 4, as originally filed.

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

"A computer-implemented method, comprising: receiving (110,310) content in a message disseminated on a computer network from a sender; acquiring (120) a

signed version of a message digest for the content, wherein the message digest was generated (320) by an identity service on behalf of the sender and the identity service signs the message digest on behalf of the sender, the identity service being a trusted and reliable third-party known to a recipient or principal, wherein by signing the message digest on behalf of the sender, the mere presence of the signature, once validated, serves as an attestation to the recipient that the content is authentic and from the sender; validating (130,350,360) the signed version of the message digest for purposes of assuring the recipient that the content and the sender are each authentic before the recipient accesses the content; and processing a particular policy (140) in response to validating the signed version of the message digest, wherein the particular policy is resolved in response to whether the content was validated, whether a signature that the identity service signed the message digest with was validated, or whether both the content and the signature were validated, and wherein the particular policy is identified via a policy identifier that is included in metadata, and wherein the metadata is included (321) with the message digest, and the metadata includes usage limitations with respect to the content, and wherein a recipient process configures the particular policy to provide unique processing in response to the sender."

The claims according to this request also comprise an independent claim 18 to a system and an independent claim 25 to a computer program.

XI. Claim 1 according to the first and second auxiliary requests reads as follows:

"A computer-implemented method, comprising: receiving (110,310), by a recipient service, content in a message disseminated on a computer network from a sender, using a sender service, to a recipient using the recipient service; acquiring (120) a signed version of a message digest for the content, wherein the sender has been authenticated by an identity service and the message digest was generated (320) and signed (320) by the identity service using a signature associated with the identity service, on behalf of the sender, the identity service being a trusted third-party knowable to the recipient service, wherein by the identity service signing the message digest the identity service attests to the recipient service that the content is authentic and the content is from the sender; validating (130,350,360) the signed version of the message digest for purposes of assuring the recipient that the content and the sender are each authentic before the recipient accesses the content, wherein validating the signed version of the message digest includes verifying that the signature associated with the message digest is associated with a trusted third-party signing service or the identity service; processing a particular policy (140) in response to validating the signed version of the message digest, wherein the particular policy is resolved in response to whether the content was validated, whether a signature that the identity service signed the message digest with was validated, or whether both the content and the signature were validated, and wherein the particular policy is identified via a policy identifier that is included in metadata, and wherein the metadata is included (321) with the message digest, and the metadata includes

usage limitations with respect to the content, and wherein a recipient process configures the particular policy to provide unique processing in response to an identity of the sender; and transmitting for presentation the content to the recipient in response to verifying that the content is authentic and the content is from the sender."

The claims according to the first and second auxiliary requests also comprise an independent claim 18 to a system, and the claims according to the first auxiliary request further comprise an independent claim 25 to a computer program.

XII. Claim 1 according to the third auxiliary request differs from that according to the first and second auxiliary requests only in the insertion of the following paragraph before the ultimate paragraph, commencing "processing a particular policy ...":

"wherein validating (130) further includes reproducing (131) an independent version of the message digest and comparing that independent version to the acquired version, and if equal and if a signature associated with the signed message digest is verified, then determining the content from the sender is authenticated."

The claims according to this request also comprise an independent claim 17 to a system.

Reasons for the Decision

1. The admissibility of the appeal

In view of the facts set out at points I to III above, the appeal fulfills the admissibility criteria under the EPC and is consequently admissible.

2. Summary of the invention

2.1 The application concerns attesting to (i.e. certifying) the authorship of content contained in a message sent from an author (sender) to a recipient via a computer network; see paragraphs [0001 and 0003]. This is particularly important in the case of email, since the "From" field can be easily falsified, known as "spoofing". The invention solves this problem using a trusted third party, termed an "identity service" (IS), to sign a message digest (MD) of the content of the message. According to paragraph [0057], third sentence, the message digest is a hash of the message content.

2.2 In a first embodiment (see, for instance, figure 3; step 310 and paragraph [0044]), the message digest is produced by the sender and then sent to the identity service which signs it. The claims however relate to a second embodiment (see paragraph [0045] and paragraph [0048], last sentence) in which the message digest is not produced by the sender. Instead, the message itself is sent to the identity service which not only signs the message digest but also computes it first. The message transmitted from the sender to the recipient contains content, metadata and an Authorship Attestation Certification (AAC), the AAC containing the signature of the identity service and a message digest of the content. According to the description, the AAC

serves as an "attestation as to the authenticity of content sent from a sender and received by a recipient"; see paragraph [0016].

2.3 Figure 2 illustrates the steps carried out at the sender's computer by the "sender service" (see paragraphs [0033 to 0040]), and figure 3 illustrates the steps taken by the identity service; see paragraphs [0042 to 0052]. The sender service first authenticates itself (211) to the identity service and then submits the content data to the identity service; see figure 2; steps 220 and 221. The identity service responds (see steps 320 and 330) with an Authorship Attestation Certificate (AAC) together with metadata (222) identifying the identity service, setting out usage limitations associated with the content of the message and identifying a policy to which the recipient is to adhere when receiving the content; see paragraph [0038]. The sender then sends the message, containing the content, metadata and AAC, to the recipient.

2.4 Figure 1 shows the steps taken by the "recipient service" at the recipient's computer; see paragraphs [0019 to 0032]. The recipient service receives the message (step 110) and, before it is viewed by the recipient, validates the signed message digest (step 130), for instance by comparing an internally generated message digest with that derived from the message (step 131). If the two message digests are equal, then the recipient "may at least assume that the content has not been tampered with"; see paragraph [0024]. According to paragraph [0025], to exclude the possibility that "the content may not have originated from the sender that it is purported to be coming from" the recipient service verifies that the signature associated with the message digest is that of a known trusted identity service.

Thus the signature and the message digest "combine to attest to the authenticity of the content from the sender".

2.5 Based on the results of this validation, the steps of the policy are applied ("resolved" in the terms of claim 1); see step 140 and paragraph [0026]. One such policy is that the content is assumed to be authentic in response to the signature included with the signed message digest; see step 150. Put another way, "the mere presence of the signature from that trusted identity service serves as an attestation that the content is from the purported sender"; see paragraph [0027], last sentence. The recipient process (understood by the board to be part of the recipient service) may configure the policy to provide unique processing in response to a particular sender; see paragraph [0031].

3. The board's interpretation of the application, including claim 1 of all requests

3.1 As stated in its preliminary opinion, the board understands the invention in the context of Public Key Infrastructure (PKI) to use asymmetric encryption. The appellant has not disputed this interpretation.

3.2 Hence the board understands the "signature" produced by the identity service to be the message digest, computed by the identity service, encrypted using the identity service's private key.

3.3 Likewise, the board understands the step by the recipient service of validating the signed message digest (see figure 1; steps 130 and 131 and paragraphs [0023 to 0025]) to be a single test by which the

internally generated message digest, computed by the recipient service, is compared to that obtained by decrypting the signature contained in the AAC using the identity service's public key. If they are equal, then it is established that the message content has not been changed since it was submitted to the identity service for signature.

4. Clarity, Article 84 EPC 1973

4.1 The feature of "assuring the recipient"

4.1.1 Claim 1 according to the main and all three auxiliary requests sets out the step of "validating [...] the signed version of the message digest for [the] purposes of **assuring the recipient** that the content and the sender are each authentic before the recipient accesses the content" (emphasis by the board). The board understands establishing that the sender is authentic to mean establishing that the sender is the one indicated in the message. Sender and content are thus understood by the board to be "authentic" if neither the "From" field nor the message has been tampered with.

4.1.2 The board finds that there is no technical basis for successful validation being capable of assuring the recipient in this way, since it does not establish the identity of the sender of the message. This, in the board's understanding of the invention, would, for instance, require that the message contain the senders's signature in the form of a message digest encrypted using the sender's private key and a corresponding validation step by the recipient service of decrypting that signature using the sender's public key. Claim 1 of all four requests does not set out

features which would allow the recipient to verify that the stated sender of a message is indeed the sender; the recipient simply has to take this on trust from the identity service.

4.1.3 The appellant has argued that claim 1 does not require that the message digest be signed with the sender's private key and has referred to step 110 ("Receive content in a message from a sender") in figure 1 and corresponding paragraph [0021] in the description as evidence that the stated sender of the message is indeed the sender. In the board's opinion, these disclosures only show that the message has passed via the sender. As the board pointed out in its preliminary opinion (point 6.2), in view of the signature by the identity service, the recipient can only be certain that the message content has been submitted to the identity service. The recipient cannot however verify that the stated sender was indeed the sender of the message.

4.1.4 The appellant has also argued that "the mere presence of a signature validated by the identity service assures the recipient that the content of the message is authentic and from the sender" and that "the identity service attests to the recipient service that the content is authentic and the content is from the sender". As stated above, the board cannot find a technical basis for this assurance/attestation in the features set out in claim 1 of all four requests.

4.1.5 The appellant has argued that the identity service may authenticate the sender, either previously or when a message is sent, using a variety of credentials. The board does not dispute that the identity service can verify that the sender is who he/she claims to be.

However, even if, as claim 1 of all requests sets out, the recipient trusts the identity service, claim 1 of all requests sets out the method steps taken by the recipient. These cannot be limited by steps previously taken by the identity service.

4.1.6 Hence the step of validating the signed version of the message digest for the purposes of assuring the recipient, set out above, sets out an effect of the claimed subject-matter but no features capable of providing this effect, thus rendering claim 1 of all four requests unclear.

4.2 The feature of validating the content, the signature or both

4.2.1 Claim 1 of the main and all three auxiliary requests sets out the step of resolving a policy in response to "whether the content was validated, whether a signature that the identity service signed the message digest with was validated, or whether both the content and the signature were validated". The board takes the view that claim 1 implies that the signature can be validated separately from the content in two separate tests. In the board's view, as the two tests are inseperable, the cited step makes claim 1 of all four requests unclear.

4.2.2 The appellant has argued that the message digest can contain metadata indicating a policy of what to do with a message that fails one of the two tests. The board is not persuaded by this argument because the validation step 130 ("validate the signed version of the message digest") is a single test with a single result, namely whether or not the locally computed message digest is equal to that derived by decrypting the signature using

the identity service's public key. While it is true that the test involves several intermediate steps (discussed in the provisional opinion), for instance computing a local message digest and decrypting the signature, this does not mean that the test delivers more than a single boolean result, namely true or false. Hence the three results of the validation test (validating the content, the signature or both), set out in claim 1 of all four requests, contradict the disclosure in the description and drawings according to the board's understanding of the invention, set out in its provisional opinion (see point 6.4), rendering claim 1 of all four requests unclear.

4.3 The board consequently finds that claim 1 according to the main and first to third auxiliary requests does not overcome the clarity objections, Article 84 EPC 1973, raised in the annex to the summons.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated