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 17 September 2008

Case Number: T 1583/05 - 3.5.01

Application Number: 99945107.3

Publication Number: 1210789

IPC: G06F 17/60, G06T 1/00, H04N 1/32

Language of the proceedings: EN

Title of invention:
Method and device for inserting and authenticating a digital signature in digital data

Applicant:
NEC CORPORATION

Opponent:
-

Headword:
Inserting digital signatures/NEC

Relevant legal provisions:
-

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

Keyword:
"Novelty (no)"

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 1583/05 - 3.5.01

D E C I S I O N
of the Technical Board of Appeal 3.5.01
of 17 September 2008

Appellant: NEC CORPORATION
7-1, Shiba 5-chome,
Minato-ku
Tokyo (JP)

Representative: Vossius & Partner
Siebertstrasse 3
81675 München (DE)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 5 August 2005 refusing European application No. 99945107.3 pursuant to Article 97(1) EPC 1973.**

Composition of the Board:

Chairman: S. Steinbrener
Members: R. R. K. Zimmermann
A. Pignatelli

Summary of Facts and Submissions

I. European patent application 99 945 107.3, titled a method and device for inserting and authenticating a digital signature in digital data, claimed priority from a US patent application filed in 1999.

II. In the examination proceedings the applicant made various attempts to overcome objections raised by the examining division, which finally refused the application at the end of oral proceedings. According to the reasons for this decision given in writing and posted on 5 August 2005, the requests then on file were not acceptable for added subject-matter and lack of clarity in the claims.

III. Against the refusal of the application, the appellant (applicant) lodged an appeal on 17 October 2005. He paid the appeal fee on the same date. By a letter dated and received on 15 December 2005, the appellant filed an amended set of claims and a statement setting out the grounds of appeal.

IV. The Board summoned the appellant to oral proceedings on 17 September 2008. In a communication sent with the summons, the Board expressed doubts regarding allowability of the appeal. In particular, it indicated that the prior art seemed to anticipate the invention as claimed, referring to the following documents:

D4: EP-A-0 883 284

D12: J. Kelsey et al: "An Authenticated Camera", Proceedings, Annual Computer Security Applications Conference, 9-13 December 1996, pages 24-30.

V. In reply to the summons, the appellant filed an amended set of claims (main request) by letter dated 13 August 2008, and in the oral proceedings on 17 September 2008, a further amended set of claims (auxiliary request), the respective claim 1 reading as follows:

Main request:
"1. A method for inserting data into digital data for subsequent authentication of the digital data, the method comprising the steps of:
inserting data comprising a public key for a digital signature into a predetermined bits portion of the digital data;
transmitting the digital data including the inserted data to a recipient; and
authenticating, by the recipient, the digital data based on the inserted data."

Auxiliary request:
"1. A method for inserting a public key used for decrypting a digital signature into digital data, the method comprising the steps of:
assigning a predetermined bits portion of the digital data for the public key;
inserting the public key into the predetermined bits portion of the digital data; and
transmitting the digital data comprising the inserted public key to a recipient, so as to enable subsequent authentication, by the recipient, of the digital data based on the inserted public key."

VI. In the oral proceedings before the Board, the matter was discussed with the appellant. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the main request filed with the letter of 13 August 2008 or the auxiliary request filed during the oral proceedings.

VII. According to the appellant, the claimed invention was patentable over the prior art. The invention was designed to overcome several drawbacks of the prior art. For example, for applications involving digital cameras using a public key encryption system for image authentication, the user had to have knowledge of the corresponding public key in order to authenticate the image. However, there were potentially millions of such devices in existence. The invention solved this problem by using predetermined bits portion to hold the corresponding public key of the device.

Document D12 described protocols for an authenticated camera that allowed people to verify that the digital image was taken by a specific camera at a specific time and at a specific place. However, there was no discussion in this document of inserting a public key for a digital signature into a predetermined bits portion of digital data, for example the image data taken by the camera.

Similarly in document D4, the public key appeared to be transmitted separately from the encrypted digital data.

The invention was thus novel and inventive over the prior art documents cited in the proceedings.

VIII. After deliberation at the end of the oral proceedings, the Board announced the decision on the appeal.

Reasons for the Decision

1. The appeal is admissible.

2. The appeal, however, is not allowable since none of the appellant's requests is acceptable for reasons of lack of novelty of the subject-matter of the respective claim 1.

2.1 Claim 1 of the main request defines a method for inserting data into digital data for subsequent authentication of the digital data.

Prior art document D12 discloses a method for authenticating the images taken by a specific camera. It is based on protocols allowing the verification of the digital images taken at a specific time and place (see e.g. the abstract and sections 1.1 and 1.3 at page 24 f.). The protocols require an initial authorisation of the camera, a set of operations to take the images, and a final authentication during which digital data, the message M_5 including the image data, is transmitted from the camera to a recipient, the base station.

This digital signal M_5 defined at page 28, right-hand col., section 3 f. is a concatenation of a public key C_{B1}, a signature M_2, the authenticated images A_1, ..., A_n, and a digital signature $Sign_{SKc}(M_4,X_n)$. Contrary to

the arguments of the appellant, there are data, namely X_n, which comprise the public key $C_{B1,}$ implicitly inserted into a predetermined bits portion of the message M_5, and which is used for decrypting a digital signature, e.g. M_0 and M_2 (see sections 1 and 3 at page 27), and for authenticating digital data.

In fact, the base station forms a message M_6 when it is "satisfied that the set of images is authentic" (see page 28, right-hand column, section 4).

It follows that document D12 fully anticipates the subject-matter of claim 1 of the main request.

2.2 Claim 1 of the auxiliary request is an attempt, as confirmed by the appellant, to overcome objections raised by the Board regarding clarity of the claims. It defines that the public key be inserted into the predetermined bits portion of the digital data instead of referring to data comprising a public key as the main request does. The amendments are thus indeed not suitable to add anything in substance which was not already present in claim 1 of the main request.

The difference in wording does therefore not confer novelty to the claimed subject-matter. In document D12, as with all public key schemes, the public key C_{B1} is used for decrypting a digital signature, e.g. the message M_2 (see page 27, right-hand col. section 3.). As already pointed out above, the message M_5 is a concatenation of the public key C_{B1}, the message M_2, A_1, etc. so that the public key C_{B1} can be considered to be inserted into the message M_5 in order to enable subsequent authentication by the recipient as claimed.

It is thus clear that the method of claim 1 of the auxiliary request is still fully anticipated by document D12.

3. In summary, none of the requests complies with the requirement of novelty as set out in Article 54 (1) and (2) EPC 1973. The requests are thus not acceptable so that the appeal cannot be allowed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

T. Buschek S. Steinbrener