

**Internal distribution code:**

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

**Datasheet for the decision  
of 8 January 2019**

**Case Number:** T 0478/15 - 3.4.03

**Application Number:** 11170659.4

**Publication Number:** 2369545

**IPC:** G06Q20/00

**Language of the proceedings:** EN

**Title of invention:**

System and method of secure authentication and billing for goods and services using a cellular telecommunication and an authorization infrastructure

**Applicant:**

Nokia Technologies Oy

**Headword:**

**Relevant legal provisions:**

EPC 1973 Art. 56, 76(1)  
EPC Art. 52(1), 123(2)

**Keyword:**

Amendments - added subject-matter (no)  
Inventive step - (yes)

**Decisions cited:**

**Catchword:**



**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 0478/15 - 3.4.03

**D E C I S I O N**  
**of Technical Board of Appeal 3.4.03**  
**of 8 January 2019**

**Appellant:** Nokia Technologies Oy  
(Applicant) Karaportti 3  
02610 Espoo (FI)

**Representative:** Style, Kelda Camilla Karen  
Page White & Farrer  
Bedford House  
John Street  
London, WC1N 2BF (GB)

**Decision under appeal:** **Decision of the Examining Division of the  
European Patent Office posted on 16 October 2014  
refusing European patent application No.  
11170659.4 pursuant to Article 97(2) EPC.**

**Composition of the Board:**

**Chairman** G. Eliasson  
**Members:** S. Ward  
C. Heath

## Summary of Facts and Submissions

I. The appeal is against the decision of the Examining Division refusing European patent application No. 11 170 659 on the grounds that the claimed subject-matter did not meet the requirements of Article 76(1) EPC, did not involve an inventive step within the meaning of Articles 52(1) and 56 EPC, and was not clear (Article 84 EPC).

II. At the end of the oral proceedings held before the Board the appellant requested that the decision under appeal be set aside and that a patent be granted in the following version:

claims 1-7 of the main request as filed during oral proceedings at 15.25;

description:

- pages 1-4 and 8-36 as originally filed,
- pages 7, 37-43 filed with letter dated 20 March 2012;
- page 5 as filed during oral proceedings at 15.33 (page 6 being deleted); and

drawings sheets 1-12 as originally filed.

III. The following documents are referred to:

- D1: WO 02/21464 A2
- D3: O'MAHONY D ET AL: ELECTRONIC PAYMENT SYSTEMS FOR E-COMMERCE, ARTECH HOUSE, NORWOOD, MA,, US, 2001, pages 45 - 48.

IV. Claim 1 reads as follows:

*"1. A method, comprising:*

accessing (310) by a mobile station (20) a gateway (60) and transmitting an identification code to the gateway; verifying the identity of the mobile station by the gateway by accessing an authentication centre and comparing variables computed by the mobile station and variables computed by the gateway; verifying (330, 340) by the mobile station the legitimacy of the gateway by comparing variables computed by the mobile station and variables computed by the gateway; creating a shared signing key (SK); requesting (360, 370) by the mobile station a signature verification address from the gateway for facilitating the mobile station to pay for a service provider (50); receiving (390, 400, 420) by the mobile station the requested signature verification address from the gateway when the identity of the mobile station has been verified by the gateway; requesting (710) by the mobile station a product or service or access or a right from the service provider; receiving (730) by the mobile station an invoice for the requested product or service or access or right from the service provider; and in response to determination (740) that the invoice is correct, transmitting (750) by the mobile station a digital signature created using the shared signing key and accompanied by the signature verification address as approval of the invoice for the product or service or access or right to the service provider; and verifying the digital signatures by a signature verification service (65) at the signature verification address using the shared signing key (SK)."

- V. With the summons to oral proceedings, the Board sent the appellant a communication under Article 15(1) RPBA setting out its provisional views. The Board indicated

*inter alia* that it was doubtful whether the main request on file met the requirements of Article 76(1) EPC 1973. The question of inventive step was also discussed.

## **Reasons for the Decision**

1. The appeal is admissible.
2. *Article 76(1) EPC 1973 and Article 123(2) EPC*
  - 2.1 The present application is a divisional application based on the earlier application EP 03 722 897 (published as EP 1 509 863, and corresponding to the European phase of WO 03/096140), which will be referred to as the parent application.
  - 2.2 Claim 1 is essentially based on a combination of claims 1, 13 (verifying the legitimacy of the gateway) and 14 (requesting a signature verification address) of the parent application as filed. The features relating to receiving and checking the invoice are based on paragraph [0054], sixth and seventh sentences, paragraph [0058] and Figs. 6 and 7 of the parent application as filed. The objections raised under Article 76(1) EPC 1973 in the Board's communication pursuant to Article 15(1) RPBA have been overcome by amendment. Dependent claims 2-7 are essentially based on dependent claims 2-7 of the parent application as filed. Hence, the requirements of Article 76(1) EPC 1973 are met.
  - 2.3 All claims (1-24) of the parent application as filed are repeated as paragraphs labelled "Subject-matter 1"

to "Subject-matter 24" in the description of the present application as filed. The remainder of the description is essentially identical to that of the parent application as filed, and the figures of the two applications are also identical. The entire content of the parent application as filed is therefore comprised in the present application as filed, and hence, in the light of the conclusion of the previous paragraph, the requirements of Article 123(2) EPC are met.

3. *Inventive Step*

3.1 The appellant considers D1 to be the closest prior art (which was also the position taken by the Examining Division in the communication of 13 March 2014, although no specific prior art was cited in the reasoning of the contested decision). The Board sees no reason to differ.

3.2 The essential difference between the present invention and the method of D1 resides in the use of a signature verification service at a signature verification address to verify the digital signature of the mobile station using a shared signing key.

Specifically, claim 1 differs from D1 in defining the following features (emphasis added by the Board):

- (a) *creating a **shared signing key** (SK);*
- (b) *requesting (360, 370) by the mobile station a **signature verification address** from the gateway for facilitating the mobile station to pay for a service provider (50);*

- (c) receiving (390, 400, 420) by the mobile station the requested **signature verification address** from the gateway when the identity of the mobile station has been verified by the gateway;
- (d) in response to determination (740) that the invoice is correct, transmitting (750) by the mobile station a digital signature created using the shared signing key and accompanied by the **signature verification address** as approval of the invoice for the product or service or access or right to the service provider; and
- (e) verifying the digital signatures by a **signature verification service** (65) at the **signature verification address** using the **shared signing key (SK)**.

3.3 It appears from the contested decision that some aspects of the claimed subject-matter were considered to be non-technical ("merely of administrative relevance", see Reasons for the decision, point 4.1). However, the above features (a)-(e) which distinguish claim 1 from D1 relate to a choice of cryptographic method (shared signing key) and a choice of how, and by whom, the digital signature used for payment authorization should be verified. These are not commercial choices, but technical choices to be made by a person skilled in cryptography and the technology of secure electronic payments. The Board is therefore satisfied that the features (a)-(e) which distinguish claim 1 from D1 are technical features.

3.4 According to the application, the invention provides *inter alia* a solution to the problem of allowing "a user or consumer to pay for goods and services" while



preventing hackers and criminals from making "purchases which are charged to the legitimate user" (paragraph [0008]). The appellant does not argue that the method of the present invention is necessarily superior to that of the closest prior art, but argues that it "provides an alternative solution to that of D1" (statement of grounds of appeal, point 3.3.10). The Board can accept that this is a reasonable technical problem on which to base the analysis of inventive step (see *Case Law of the Boards of Appeal*, 8th Ed. 2016, I.D.4.5).

- 3.5 The question, therefore, is whether, having regard to the prior art, it would be obvious for the skilled person to modify D1 by incorporating the technical features (a)-(e) to solve the above problem.
  
- 3.6 According to the method of D1, the mobile station's public key (or "public signature verification key", see paragraph bridging pages 2 and 3) is used to generate a digital signature which may serve to approve charges made in the purchase of goods and services (page 9, lines second paragraph, second and third sentences), and the public key, as certified by the digital certificate issued by the gateway, may be used by the seller to verify the signature (see e.g. claims 1 and 5).
  
- 3.7 By contrast, according to the invention defined by claim 1 of the present application, a shared signing key is created, which the mobile station uses to create a digital signature, and the shared signing key is transmitted to the signature verification service (implicit in the final feature of claim 1) to constitute a shared secret. To authorise payment, the mobile station transmits the digital signature together

with the signature verification address (the address of the signature verification service) to the service provider, and the digital signature is then verified (on behalf of the service provider) by the signature verification service at the signature verification address using the shared signing key.

In the opinion of the Board, the feature that the digital signature is verified by the signature verification service using the shared signing key can only be reasonably understood to mean that the signing key is *not* shared with the service provider and that the service provider cannot therefore verify the signature. If this were not the case, the claim would not appear to make technical sense, as signature verification could be performed by the service provider using the shared key, and the signature verification service would serve no purpose.

3.8 The Board accepts that public key cryptography and shared secret key cryptography are well established alternative approaches, the advantages and disadvantages of each being equally well-known, as suggested in the contested decision (see Reasons for the decision, points 4.2 and 5).

3.9 Hence, it might be argued that it would be obvious to replace the step in D1 in which the digital certificate is transmitted to the seller (service provider) so that the seller may verify the signature using the public key with a step in which a shared secret key is (securely) transmitted to the seller so that the seller may verify the signature using the shared secret key.

However, even if such a measure would be obvious to the skilled person, it would not lead to the method of the

present invention. According to claim 1, the digital signature is verified not by the service provider, but by a signature verification service, at an address which is transmitted to the service provider together with the signature.

By this means the claimed method eliminates the potential security risk involved in communicating a shared key to a service provider (a risk which would increase each time a buyer wished to purchase goods and services from a new provider). Hence, in arranging for a signature verification service to perform the signature verification using the shared signing key, the invention provides a secure alternative to the method of D1.

3.10 On the basis of the available prior art, the Board does not see how it could reasonably be denied that the claimed method involves an inventive step, since none of the cited documents disclose the distinguishing technical features (a)-(e) listed above. It is true that D3 discloses consulting an "on-line directory service" (page 46, first paragraph), but this is in order to obtain the certificate which certifies the sender's public key. Thus, what is disclosed is a variation within the field of public key infrastructure, which provides no pointer to the solution of the present invention.

3.11 As a final point, the Board takes the view that the argument of the Examining Division that the claimed solution would provide security only to the buyer and not to the seller is, even if true, not relevant. As stated by the appellant, the "claimed invention is not concerned about the security at the seller end of the transaction at all but aims to provide protection for

the buyer" (statement of grounds of appeal, point 3.3.2). Whether the claimed solution would solve other problems, or offer all of the same benefits as the public key scheme of D1, is irrelevant.

- 3.12 The Board therefore concludes that the subject-matter of claim 1 would not be obvious to the skilled person on the basis of the available prior art, and hence involves an inventive step within the meaning of Article 52(1) EPC and Article 56 EPC 1973.

## Order

### For these reasons it is decided that:

1. The decision under appeal is set aside.
2. The case is remitted to the department of first instance with the order to grant a patent in the following version:

claims 1-7 of the main request as filed during oral proceedings at 15.25;

description:

- pages 1-4 and 8-36 as originally filed,
- pages 7, 37-43 filed with letter dated 20 March 2012;
- page 5 as filed during oral proceedings at 15.33 (page 6 being deleted); and

drawings sheets 1-12 as originally filed.

The Registrar:

The Chairman:



S. Sánchez Chiquero

G. Eliasson

Decision electronically authenticated