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 0808/14 - 3.4.03

Application Number: 05024336.9

Publication Number: 1669955

IPC: G07F19/00

Language of the proceedings: EN

Title of invention:
System and method of bootstrapping a temporary public-key infrastructure from a cellular telecommunication authentication and billing 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:

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 0808/14 - 3.4.03

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

Appellant: (Applicant)	Nokia Technologies Oy 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 26 November 2013 refusing European patent application No. 05024336.9 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. 05 024 336 on the grounds that the subject-matter of claim 1 of the main request did not involve an inventive step within the meaning of Article 56 EPC. Auxiliary requests 1-3 were not admitted into the procedure pursuant to Rule 137(3) 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 13.35;

description:
- pages 3 and 4 as filed during oral proceedings,
- pages 1, 2, 5-20 as originally filed; and

drawings sheets 1-12 as originally filed.

III. The following documents are referred to:

D1: FR 2 779 896 A
D1a: AU 1999 34978 A1.

IV. Claim 1 reads as follows:

"A method of ordering, paying for, and delivering goods and services using a mobile station, comprising: accessing through a telecommunications infrastructure (30) a gateway by the mobile station and transmitting

an identification code for the mobile station to the gateway;
verifying the identity of the mobile station by the gateway by accessing an authentication center and comparing variables computed by the mobile station and variables computed by the gateway;
verifying the legitimacy of the gateway by the mobile station by comparing variables computed by the gateway with variables computed by the mobile station;
requesting a digital certificate by the mobile station through the telecommunications infrastructure (30) from the gateway to be used to order and pay for a product or service from a seller;
receiving a digital certificate at the mobile station from the gateway when the identity of the mobile station has been verified by the gateway;
requesting by the mobile station a product or service from the seller; and
transmitting through a different communications infrastructure (35) a digital signature by the mobile station accompanied by the digital certificate for a signature verification key as payment to said seller."

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 discussed *inter alia* whether the requests on file met the requirements of Article 76(1) EPC 1973, Article 123(2) EPC and Article 84 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 divided from parent application EP 01 955 476 (with publication number EP 1 397 787, being derived from WO 02/21464 A2).

2.2 Claim 1 is chiefly based on a combination of claims 1, 12 and 13 of the parent application as filed. In the opinion of the Board it would be evident to the skilled reader that the claimed dependency of originally filed parent claim 13 (i.e. "recited in claim 11") is an error, and should actually read "recited in claim 12". This is clear from the fact that the additional feature of claim 13 concerns a step to be carried out "when the identity of the mobile station and the gateway have been verified"; verification of the gateway being defined in claim 12, but not in claim 11 or in any claim on which claim 11 depends.

2.3 Fig. 1 depicts a communication infrastructure 30 (by means of which the mobile station and the gateway communicate), and a communication infrastructure 35 (by means of which the mobile station and the seller communicate). While it might be argued that the passage describing these communication infrastructures (page 6, lines 12-18) does not exclude possible embodiments in which communication infrastructures 30 and 35 could be the same, it would be clear to the skilled reader that they are, in general, different communication infrastructures, as reflected in present claim 1. Dependent claims 2-7 are essentially based on the dependent claims 2-6 and 9 of the parent application as filed. Hence, the requirements of Article 76(1) EPC 1973 are met.

2.4 Method claims 1-13 of the present application as filed are identical to those of the parent application as filed, and the descriptions and drawings are identical. Hence, the requirements of Article 123(2) EPC are met.

3. *Inventive Step*

3.1 The document D1/D1a, disclosing a method for making a secure remote payment for goods or services using a "mobile radiotelephone", has been consistently seen as the closest prior art by both the Examining Division and the appellant-applicant, and the Board sees no reason to question this. At the request of the appellant, the English language version D1a is used.

3.2 The method of claim 1 of the present application differs from the method of D1a at least in the following features:

(a) *"verifying the legitimacy of the gateway by the mobile station by comparing variables computed by the gateway with variables computed by the mobile station";*

(b) *"requesting a digital certificate by the mobile station through the telecommunications infrastructure (30) from the gateway to be used to order and pay for a product or service from a seller";*

(c) *"receiving a digital certificate at the mobile station from the gateway when the identity of the mobile station has been verified by the gateway";*

(d) *"transmitting through a different communications infrastructure (35) a digital signature by the*

mobile station accompanied by the digital certificate for a signature verification key as payment to said seller."

3.3 According to the method of D1a, a mobile telephone 1 provides access to a gateway 10 via a radio communications network 5, and, via the gateway, to a payment server 4 and a sales server 8, which are connected to an open computer telecommunications network such as the internet.

The method according to D1a involves firstly a subscriber identification and authentication step 62, so that "the payment server manager is assured that the buyer is a bona fide member of the radio communications network to which the payment server is connected." This step may involve sending an electronic signature generated in the mobile telephone to a management centre 6 of the network, which checks it by comparing it with a signature calculated locally (page 10, lines 19-34; page 11, lines 5-30).

This is followed by a buyer authentication step 63, so that "the payment server manager is assured that the buyer is authorized to pay for the purchased goods and/or services." This step may also involve the generation and transmission of a (second) electronic signature by the mobile phone to be checked in the payment server 4, or alternatively in the management centre 6 or a control centre (page 11, line 31 to page 12, line 29).

Once this step is successfully completed, the payment server manager "can then authorize payment or make compensation movements between the buyer's account 2 and the supplier's account 7" (page 11, lines 34-36; page 13, line 34 to page 14, line 1). The authorisation

is communicated to the supplier's sales server 8 (page 13, lines 7-13) to confirm purchase of goods or services requested by the buyer from the sales server of the supplier (page 12, line 32).

In summary, according to D1a, all communications go through a closed type radio communications network 5 (see Fig. 1 and page 2, lines 7-9). The identification, authentication and payment authorisation steps take place as part of a single transaction during which the mobile radiotelephone 1 is in contact with the radio communications network 5, and electronic signatures sent by the mobile phone are checked during this transaction.

3.4 The method claimed in the present application differs considerably from that of D1a. According to features (b)-(d), a mobile station requests and (subject to successful identification and verification) receives a digital certificate through the telecommunications infrastructure linking the mobile station to the gateway. Subsequently, to authorise a purchase, this certificate is transmitted by the mobile station to a seller (hence, it is implicit that the digital certificate received from the gateway is stored on the mobile station) together with a digital signature. In this way the seller may use the digital certificate to check the digital signature (see Fig. 8, step 870).

3.5 As indicated in the application, the technical problem may be seen as reducing the burden upon the mobile telephone infrastructure. Since the digital signature and digital certificate are transmitted directly from the mobile station to the seller "through a different communications infrastructure", "the mobile station 20 need only be authenticated by the mobile telephone

infrastructure for billing and authentication 90 upon startup", which "imposes a minimal burden upon the telecom mobile telephone infrastructure for billing and authentication 90" (page 19, third paragraph, last sentence).

3.6 While the use of a digital certificate to check a digital signature is well known in the art *per se* (see paragraph bridging pages 2 and 3), the Board sees nothing in the available prior art which would render obvious the issuing, on request, of a digital certificate by a communications gateway to a mobile station, or the subsequent transmission of a signature by the mobile station to a seller, together with the digital certificate for signature verification.

3.7 Moreover, distinguishing feature (a), which defines the step of verifying the legitimacy of the gateway by the mobile station, represents a further difference over D1a. Within the context of the present invention, this step is required to "verify that the gateway is authorized to issue the digital certificate" (see page 3, last paragraph, third sentence). The Board concurs with the appellant that the skilled person would not have any incentive to incorporate such a feature into the method of D1a, which employs an entirely different architecture in which no certificate is issued.

3.8 The Board therefore judges that, in the light of the available prior art, there is no basis for concluding that the claimed features (a)-(d) would be obvious to a skilled person, and hence that the subject-matter of claim 1 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 13.35;

description:
- pages 3 and 4 as filed during oral proceedings,
- pages 1, 2, 5-20 as originally filed; and

drawings sheets 1-12 as originally filed.

The Registrar: The Chairman:

S. Sánchez Chiquero G. Eliasson

Decision electronically authenticated