Internal distribution code:

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

Datasheet for the decision of 24 June 2019

Case Number: T 1383/14 - 3.5.05

Application Number: 01974579.3

Publication Number: 1325582

IPC: H04L9/00, H04L12/22, H04Q7/38

Language of the proceedings: EN

Title of invention:
TECHNIQUES FOR HIDING NETWORK ELEMENT NAMES AND ADDRESSES

Applicant:
Nokia Technologies Oy

Headword:
Network addresses hiding/NOKIA

Relevant legal provisions:
EPC Art. 54, 56, 84, 123(2)

Keyword:
Novelty - main request (yes)
Inventive step - main request (yes)
Claims - clarity (yes)
Amendments - added subject-matter (no)

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 1383/14 - 3.5.05

D E C I S I O N
of Technical Board of Appeal 3.5.05
of 24 June 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 29 January 2014 refusing European patent application No. 01974579.3 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chair	A. Ritzka
Members:	P. Cretaine
	D. Prietzel-Funk

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division, posted on 29 January 2014, refusing European patent application No. 01974579.3. A main request and first and second auxiliary requests were refused for lack of compliance with the requirements of Article 123(2) EPC, lack of clarity (Article 84 EPC) and lack of novelty
(Article 54 EPC) having regard to the disclosure of

D4: G. Montenegro, "Firewall Support for Mobile IP", Internet draft, IETF, 27 January 1998.

An objection under Article 56 EPC was further raised against the main request in case the clarity objection against this request were overcome. This objection was based on the combination of D4 with

D5: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Architecture for an All IP network (3G TR 23.922 version 1.0.0)", October 1999.

An objection under Article 83 EPC was further raised against the first auxiliary request.

II. Notice of appeal was received on 28 March 2014, and the appeal fee was paid on the same day. The statement setting out the grounds of appeal was received on 3 June 2014. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the main request or first to third auxiliary requests, all requests as submitted with the statement setting out the grounds of appeal. The

appellant also requested oral proceedings in the event that the main request should not be allowed.

III. A summons to oral proceedings was issued on 17 January 2019. In a communication annexed to the summons, the board gave its preliminary opinion on the case. In its view, the main request met the requirements of Article 123(2) EPC. The board suggested to the appellant a slight amendment to independent claims 1 and 9 of the main request in order for this request to meet the requirements of Article 84 EPC, and the requirements of Articles 54 and 56 EPC with regard to D4 and D5. The board indicated that it would then be in a position to cancel the oral proceedings and remit the case to the examining division with the order to grant a patent on the basis of the main request.

IV. By letter of response dated 28 February 2019, the appellant filed an amended main request consistent with the board's suggestion.

V. The board informed the appellant by a notification dated 18 March 2109 that the oral proceedings had been cancelled.

VI. Claim 1 according to the main request reads as follows:

" Method, comprising:
providing a message generated by a network entity in a first network to be delivered to a target network entity in a second network, which is a hidden network with respect to said first network, wherein said message comprises first and second parts;
routing (1.-5.) said message generated by said network entity in said first network to a contact point of said

second network in accordance with said first part of said message; and
routing (7.-12.) said message generated by said network entity in said first network from said contact point to said target network entity in said second network in accordance with said second part of said message;
wherein said first part of said message comprises a first name usable for routing said message to said contact point,
wherein said second part of said message comprises an encrypted second name, wherein said second name is always in encrypted form outside of said second network, wherein said encrypted second name is decrypted by said contact point of said second network before it is used, and the second name is usable for routing only within said second network, and
wherein said target network entity is a S-CSCF."

The main request comprises a further independent claim (claim 9) directed to a corresponding apparatus.

Due to the outcome of the appeal proceedings, there is no need to detail the claims of the auxiliary requests.

Reasons for the Decision

1. Admissibility of the appeal

The appeal complies with Articles 106 to 108 EPC (see point II above) and is therefore admissible.

2. Main request - Article 123(2) EPC

The board agrees with the appellant that the features of claim 1 objected to under Article 123(2) EPC in the impugned decision are supported by the application documents as originally filed.

In that respect the feature that the second name is always encrypted outside the second network has been amended to specify that the second name is always in encrypted form outside the second network. This feature corresponds to one of the two mechanisms used to hide a network mentioned in the penultimate paragraph of page 7, wherein an indirect reference to the hidden network is partially encrypted to hide the name of the target network element. In the language of claim 1, the part of the indirect reference which is encrypted is designated as second name. Further, in the third full paragraph on page 11, it is described that the contact point ensures that, with respect to outgoing messages, i.e. messages from the second, hidden, network to the first network, all names of the hidden networks are in the format of a name address pair where the second part is encrypted. Moreover, in the fourth full paragraph on page 11, it is specified that if the receiver is outside the hidden network, i.e. the receiver receives an outgoing message from the hidden network, the name pair format with the second part encrypted is used. Therefore, it is unambiguously disclosed in the description as originally filed that the second name is always in encrypted form outside of the second network.

The feature that the encrypted second name is decrypted only by the contact point of the second network, objected to by the examining division, is no longer present in independent claims 1 and 9.

The feature that the target entity is a S-CSCF is supported by the passage starting in the last paragraph of page 3. It is described therein that a S-CSCF can be hidden by identifying it with an address pair in which the second part is the encrypted address of the S-CSCF itself. Further, the third paragraph on page 13 describes that the name of the S-CSCF is encrypted at the contact point for outgoing messages and decrypted at the contact point for incoming messages. It thus clearly teaches that a S-CSCF can be a target network entity within the meaning of claim 1.

Dependent claim 8, objected to by the examining division, is clearly supported by the originally filed dependent claim 18.

Claims 3 and 4, now dependent on claim 1, are supported by originally filed dependent claims 4 and 5.

Claim 10, dependent on claim 9, is supported by originally filed dependent claim 23.

For these reasons, the board is satisfied that the claims of the main request meet the requirements of Article 123(2) EPC.

3. Main request - Article 84 EPC

The impugned decision objected that the "data used for routing the message (outgoing) in the second network" was an essential feature which was lacking in independent claims 1 and 9.

The claims are directed to a method and apparatus for routing a message from a network entity in a first network to a target network entity in a second network,

by using a contact point of the second network, the aim of the invention being to hide the address of the target network entity within the second network to the network entity in the first network. The claims first define a routing of the message from the entity in the first network to the contact point and then a routing of the message from the contact point to the target network entity. Routing schemes between network entities on different networks, based on addressing schemes, are well known in the art. In claims 1 and 9, the first and second names represent the address of the target network entity needed for routing the message. In order to achieve the above-mentioned technical effect, the part of the address of the target network entity which is used for routing within the second network is known by the network entity in the first network only in encrypted form and has to be decrypted by the contact point. Thus, the features which are necessary to achieve the technical effect, the so-called essential features as defined in the case law of the boards of appeal, are not the features related to the routing per se, but the features related to the hiding, by encryption, of the second name of the target network entity and which are well defined in the independent claims. Further, since the claims are directed to the routing of a message from the first network to the second network, i.e. of an incoming message in the terminology used in the application, there is no need to define in the claims how the network entity in the first network has got the knowledge of the second name in encrypted form through reception of a message sent from the contact point, i.e. of an outgoing message in the terminology used in the application.

Moreover, the wording "said target network entity is a S-CSCF" in independent claims 1 and 9 is clear, contrary to what is stated in the impugned decision, since defining a physical entity by the function it performs, in the present case a "Serving Call State Control Function", is a well-established practice in the field of network communications.

For these reasons, the board holds that the claims of the main request meet the requirements of Article 84 EPC.

4. Main request - Novelty and inventive step

The impugned decision objected that the subject-matter of claims 1 and 9 was already disclosed in D4.

D4 is an internet specification for mobile IP. It describes mechanisms for allowing a mobile node out on a public sector of the internet to negotiate access past a firewall and construct a secure channel into its home network (see page 2, lines 7 to 10). The home network represents a private network separated by a firewall from the general internet, or public network, so that its addresses may not be routable by the general internet (see page 4, lines 17 to 24). Traffic from the mobile node to the firewall of the home network may be encrypted and authenticated (see page 8, section 4.2, first paragraph). The mobile node's current address (i.e. in the visited public network) is known from the firewall, since the mobile node always initiates contact (see page 10, lines 12 to 16). When roaming on the public internet, the mobile node can reach addresses internal to the private network, i.e. its home network, by encapsulating the packets in a secured header and sending them to the firewall (see

page 11, lines 14 to 16; page 14, lines 16 to 19). A data packet from the mobile node via the firewall to a correspondent node in the private network has the format shown at the top of page 22: the "Inner IP Hdr" field contains the correspondent node's address in the private network which is sent encrypted by the mobile node to the firewall. The firewall decrypts this address and provides a packet which is sent from the firewall to the correspondent node (see page 22, lines 14 to 19).

The impugned decision identified the public internet and the home network of the mobile node in D4 as the first network and the second network of claim 1, respectively. The impugned decision also identified the correspondent's node address contained in the "Inner IP Hdr" field of D4 as the second name of claim 1. This address is known by the mobile node and encrypted by it only at the time the mobile node desires to send a message to the correspondent node. Since the mobile node of D4 is roaming in the public internet, this address is present in a non-encrypted form outside the home network. Thus, the subject-matter of claim 1 differs from the disclosure of D4 at least in that the second name is always in encrypted form outside the second network. Further, the feature that the target network entity is a S-CSCF, is not disclosed in D4. The subject-matter of claim 1 is thus new (novel) with regard to the disclosure of D4 (Article 54 EPC).

The technical effect of these distinguishing features is that the address of a S-CSCF in the second network is always protected by encryption in the first network. A network entity in the first network is thus not able to have knowledge of the address of a S-CSCF of the second network.

The objective technical problem can thus be formulated, as proposed by the appellant, as how to improve the privacy of an entity in the second, hidden network.

In D4, the mobile node can have access to the unencrypted correspondent node address. The aim of the encryption in D4 is to protect this address from being revealed to other entities in the first network when it is transmitted from the mobile node to the firewall. The address, however, is stored unprotected in the mobile node. D4 is thus not concerned with the above-mentioned problem. Therefore, the skilled person would not get any pointer from D4 to solve the problem in the claimed manner. Further, even if the skilled person were considering to combine D4 with D5, they would not arrive at the subject-matter of claim 1 since D5 does not mention any encryption.

The appellant further plausibly argued that the method according to claim 1 does enable entities in the first network to access the services provided by a S-CSCF server of the second network by receiving, upon service request the encrypted IP address of the S-CSCF server. However, an operator of the first network controlling the entities in said first network is not able to determine the topology of S-CSCF servers of the second network by learning their IP addresses. This represents a definitive improvement in terms of network privacy.

For these reasons, the subject-matter of claim 1 involves an inventive step (Article 56 EPC). Independent claim 9 comprises the same features as claim 1 but in terms of a claim for an apparatus. Claim 9 therefore meets the requirements of Article 56 EPC.

Claims 2 to 8 and 10 to 11 are dependent claims and, as such, also meet the requirements of Article 56 EPC.

5. Conclusion

The board judges that the claims according to the main request meet the requirements of Articles 54, 56, 84 and 123(2) EPC.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the examining division with the order to grant a patent on the basis of the following documents:
   - claims 1 to 11, filed as main request by letter dated 28 February 2019;
   - description:
     - pages 7 to 14 and 17 as originally filed,
     - pages 1, 15 and 16 filed by letter dated 24 March 2003,
     - pages 2 and 5a filed by letter dated 30 May 2008,
     - page 6 filed during oral proceedings on 8 July 2009,
     - page 2a introduced by the examining division with communication dated 27 July 2009,
     - pages 3 to 5 filed by letter dated 15 February 2013
   - drawing sheets 1/10 to 10/10 as originally filed.

The Registrar: The Chair:

K. Götz-Wein A. Ritzka

Decision electronically authenticated