(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 October 2008 (23.10.2008)

PCT

(10) International Publication Number
WO 2008/125736 A1

(51) International Patent Classification:
H04L 12/56 (2006.01)

(21) International Application Number:
PCT/FI2008/050189

(22) International Filing Date: 15 April 2008 (15.04.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20075260 17 April 2007 (17.04.2007) FI

(71) Applicant *(for all designated States except US)*: **TELIASONERA AB** [SE/SE]; Sturegatan 1, S-10663 Stockholm (SE).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **KORHONEN, Jouni** [FI/FI]; Mutkatie 2 A 4, FI-11100 Riihimäki (FI).

(74) Agent: **KOLSTER OY AB**; ISO Roobertinkatu 23, P.O.Box 148, FI-00121 Helsinki (FI).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

[Continued on next page]

(54) Title: QUALITY OF SERVICE SIGNALING

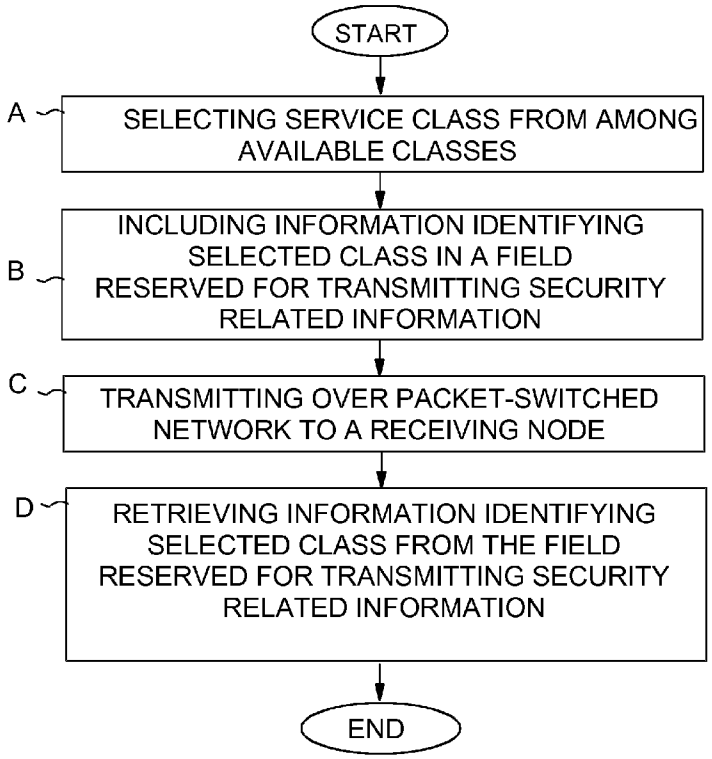

FIG. 1

(57) Abstract: The invention relates to a method of implementing quality of service signaling in a packet-switched communication system (3), comprising selecting (A) a quality of service class from among a set of predetermined available classes, including (B) information identifying the selected class in a field of a packet (4), and transmitting (C) said packet (4) over the packet switched communication system (3). In order to save available bandwidth, the step of including (B) information identifying the selected class in a field of a packet (4) is carried out by including said information in a field reserved for transmitting security related information.

WO 2008/125736 A1

— *of inventorship (Rule 4.17(iv))*

Published:
— *with international search report*

Quality of service signaling

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to QoS (Quality Of Service) signaling between nodes in a communication network, and in particularly to a new way of carrying out such signaling.

2. Description of Prior Art

QoS signaling is typically carried out in packet-switched networks, for instance, in order to provide different priorities to different users or data flows, or to guarantee a dataflow a certain level of performance. Prior art solutions implement QoS signaling between network nodes as signaling during, after or before signaling carried out for other purposes, such as signaling relating to security, for instance. As the available bandwidth between nodes is typically restricted, a continuous need exists to optimize the use of the available bandwidth in such a way that as much of the bandwidth as possible can be used for transmitting payload data. Therefore, a drawback with the prior art QoS signaling is that it consumes bandwidth.

SUMMARY OF THE INVENTION

An object of the present invention is to solve the above mentioned drawback and provide a new way of implementing QoS signaling. This object is achieved with a method as defined in independent claim 1, a node as defined in independent claim 6, and a node as defined in independent claim 11.

The invention is based on the idea of incorporating QoS signaling into the transmission of security related information. Thus, a situation in which a separate bandwidth is reserved in order to transmit QoS information between nodes of a packet-switched network can be avoided. Instead, an available bandwidth already reserved for transmitting security related information can be utilized also for QoS signaling. Such a solution makes it possible to save the available bandwidth for other purposes.

Preferred embodiments of the method and nodes of the invention are disclosed in the attached dependent claims.

BRIEF DESCRIPTION OF DRAWINGS

In the following, the present invention will be described in closer detail by way of example and with reference to the attached drawings, in which

Figure 1 is a flow diagram of an embodiment of the invention,

Figure 2 illustrates two nodes according to an embodiment of the invention, and

Figure 3 illustrates an Authentication Header which can be utilized in an embodiment of the invention.

DESCRIPTION OF AT LEAST ONE EMBODIMENT

Figure 1 is a flow diagram of an embodiment of the invention. The embodiment illustrated can be utilized in a packet-switched network where the protocol used is IKEv1 (Internet Key Exchange), IKEv2 (Internet Key Exchange), Mobile IPv4 (Internet Protocol) or Mobile IPv6 (Internet Protocol), for instance.

In block A it is assumed that predetermined service classes have been defined in order to make it possible to select a desired QoS for a dataflow. Qos (Quality of Service) refers to control mechanisms that can provide different priorities to different users or data flows, or guarantee a dataflow a certain level of performance in accordance with requests from an application program. Several alternative prior art solutions exist for controlling traffic in a network in order to obtain a desired QoS for the different data flows, and also several alternative ways of defining QoS classes. In the following, it will by way of example be assumed that seven predetermined QoS classes have been defined such that class 1 means the best available QoS and class 7 means the worst available QoS.

In block A, a service class is selected for a dataflow from among the available seven classes. In the following example it will be assumed that service class 2 is selected.

In block B, information identifying the selected class is included in a field reserved for transmitting security related information. One alternative is

to utilize a field reserved for a Security Parameter Index (SPI). An SPI is a pointer that refers to a session key and an algorithm used to ensure a secure data connection between two nodes. A sending node uses the SPI to identify and select the Security Association (SA) to be used for securing a packet. An SA may include cryptographic keys, initialization vectors or digital certificates. A receiving node uses the SPI to identify and select the encryption algorithm and key to be used for decrypting a received packet.

An alternative is to have predetermined values of the SPI reserved for QoS signaling via standardization, for instance. In such a case, seven SPI values can be reserved for this purpose, starting from value N+1 and ending with value N+7. In this case, the value of N is selected in such a way that a conflict with SPI values already previously reserved for other purposes is avoided. For instance, SPI values 1 to 255 are reserved for other purposes in Mobile IP, which means that N has to be 255 or greater to avoid a conflict with these reserved values. In this example, a selection of service class 2 therefore means that the SPI value N+2 is included as the information identifying a selected class.

Another alternative is to utilize dynamically allocated SPI values for QoS signaling. In such a case, the nodes participating in the communication utilize a predetermined algorithm to determine the SPI values used for QoS signaling. One alternative is to utilize a Hash function (such as SHA1, Secure Hashing Algorithm) or a random function (such as PRF, Pseudo Random Function, of NIST, National Institute of Standards and Technology) in connection with a predetermined input, such as a subscriber identity or a service identifier. In this connection, the input should be unique to the participating nodes. In this way, the previously mentioned number N can be generated with the function utilizing the input (N = get_nn_bits(function(input))). The best QoS class 1 is allocated the value N+1 and the worst available service class is allocated the value N+7.

In order to ensure that the dynamically allocated QoS values do not conflict with SPI values which have been previously reserved for other purposes, the utilized algorithm can be arranged to recalculate N in a predetermined way if a conflict occurs. Such a recalculation can be carried out by continuously increasing the value of N with one (N=N+1) until a conflict is avoided for all values N+1...N+7, by recalculating N with an alternative

function, or by recalculating N with an alternative input (subscriber identifier, service identifier, etc.). Naturally in order to function properly, both nodes participating in the communication need to implement the same algorithm with the same input when they carry out the calculations and recalculations to determine the SPI values dynamically allocated to the QoS values for the datastream in question.

In block C, the packet including the field containing the information identifying the selected QoS class is transmitted from the transmitting node to the receiving node via the packet-switched network.

In block D, information identifying the selected class is retrieved from the field reserved for security related information. In an implementation where predetermined values of the SPI are reserved for QoS signaling, the value itself directly indicates the QoS class for the receiving node. In the above example, the value N+2 indicates the service class 2 to the receiving node. If, however, dynamically allocated SPI values are used to indicate the QoS class, the receiving node needs to carry out the calculation explained in connection with block B in order to first determine the value of N, and after this the receiving node is able to determine that the retrieved value N+2 indicates service class 2.

Figure 2 illustrates two nodes according to an embodiment of the invention. Nodes 1 and 2, such as a host and a gateway, communicate with each other over a packet-switched communication network 3.

The nodes 1 and 2 can communicate with each other via a wired or wireless connection. One alternative is that the node 1 is a mobile station, such as a mobile station communicating via a WLAN connection (Wireless Local Area Network), and that the node 2 is a Home Agent, in other words a router on a mobile stations home network that maintains information about the current location of the mobile station. Other nodes arranged in the network 3 between the nodes 1 and 2 may participate in transmitting the packets 4 between the nodes 1 and 2. One example of such a participating node is a base station handling the traffic over the radio interface with node 1.

Nodes 1 and 2 correspond to prior art nodes, however, they have been programmed to implement QoS signaling as has been explained in connection with Figure 1.

According to the present invention, a simple negotiation about the QoS class for packets transmitted from node 1 to node 2 can be implemented. In such a case, node 1 is configured to include information indicating a selected QoS service class in packets 4 transmitted to node 2, as has been explained in connection with Figure 1. However, if node 2 determines that the selected QoS class is not appropriate, it includes information indicating which service class node 2 determines to be an appropriate service class in the packets 4 transmitted from node 2 to node 1. In that case, node 1 is configured to be responsive to the service class indicated in the packets received from node 2, in which case it starts to implement the service class indicated by the packets received from node 2.

Figure 3 illustrates an Authentication Header which can be utilized in an embodiment of the invention. An Authentication Header (AH) contains a 32 bit field for a Security Parameter Index (SPI), which according to the present invention can be utilized for QoS signaling, as has been explained in connection with Figure 1. As the SPI is widely available, also lover levels (such as wireless radio) can retrieve the information indicating the selected QoS class and utilize it when controlling data flows.

It is to be understood that the above description and the accompanying figures are only intended to illustrate the present invention. It will be obvious to those skilled in the art that the invention can be varied and modified also in other ways without departing from the scope of the invention.

CLAIMS:

1. A method of implementing quality of service signaling in a packet-switched communication system (3), comprising

selecting (A) a quality of service class from among a set of predetermined available classes,

including (B) information identifying the selected class in a field of a packet (4), and

transmitting (C) said packet (4) over the packet-switched communication system (3), c h a r a c t e r i z e d in that

said step of including (B) information identifying the selected class in a field of a packet (4) is carried out by including said information in a field reserved for transmitting security related information.

2. A method according to claim 1, c h a r a c t e r i z e d in that said field reserved for transmitting security related information is a field reserved for a Security Parameter Index.

3. A method according to claim 1 or 2, c h a r a c t e r i z e d in that

each quality of service class has been assigned a fixed value identifying the class, and

said fixed value assigned for the selected class is included (B) as said information indicating the selected class.

4. A method according to claim 1 or 2, c h a r a c t e r i z e d in that said method comprises

calculating a value indicating the selected class by utilizing a predetermined algorithm and predetermined parameters, and

including (B) said calculated value as said information indicating the selected class.

5. A method according to claim 4, c h a r a c t e r i z e d in that said method comprises

comparing said calculated value with predetermined reserved values which are reserved for other purposes, and

re-calculating said calculated value in a predetermined way prior to including said value as said information indicating the selected class, until said calculated value corresponds with no one of said reserved values.

6. A node (1) for a packet-switched network, said node being configured to

include information indicating a selected quality of service class in a field of a packet (4), and

transmit said packet (4) via said packet-switched network (3) to another node (2), c h a r a c t e r i z e d in that said node is configured to

carry out said inclusion of information indicating a selected quality of service class in a field reserved for transmitting security related information.

7. A node (1) according to claim 6, c h a r a c t e r i z e d in that said field reserved for transmitting security related information is a field reserved for a Security Parameter Index.

8. A node (1) according to claim 6 or 7, c h a r a c t e r i z e d in that said information indicating a selected quality of service class consists of a predetermined fixed value assigned to the selected quality of service class.

9. A node according to claim 6 or 7, c h a r a c t e r i z e d in that said node (1) is configured to

calculate a value indicating the selected class by utilizing a predetermined algorithm and predetermined parameters, and

include said calculated value as said information indicating the selected class.

10. A node according to claim 7, c h a r a c t e r i z e d in that said node (1) is configured to

compare said calculated value with predetermined reserved values which are reserved for other purposes, and

re-calculate said calculated value in a predetermined way prior to including said value as said information indicating the selected class, until said calculated value corresponds with no one of said reserved values.

11. A node (2) for a packet-switched network, said node being configured to:

receive a packet (4) transmitted via a packet-switched network (3) from another node (1), and

retrieve information indicating a selected quality of service class from a field of said received packet (4), c h a r a c t e r i z e d in that said node (2) is configured to

carry out said retrieval of information indicating a selected quality of service class from a field reserved for transmitting security related information.

12. A node (2) according to claim 11, characterized in that said field reserved for transmitting security related information is a field reserved for a Security Parameter Index.

13. A node (2) according to claim 11 or 12, characterized in that said information indicating a selected quality of service class consists of a predetermined fixed value assigned to the selected quality of service class.

14. A node according to claim 11 or 12, characterized in that said node (2) is configured to utilize a predetermined algorithm and said retrieved information for calculating the selected quality of service class.

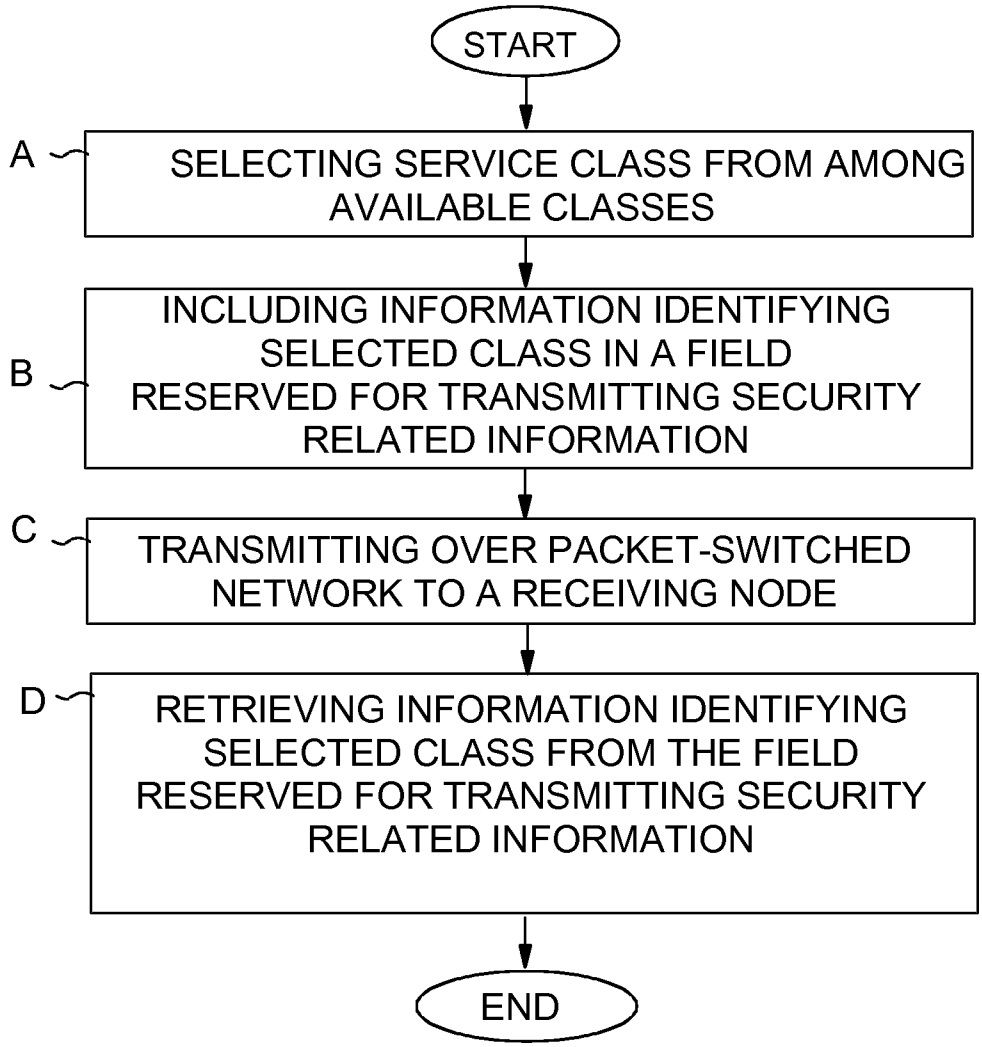
START
A
SELECTING SERVICE CLASS FROM AMONG AVAILABLE CLASSES
B
INCLUDING INFORMATION IDENTIFYING SELECTED CLASS IN A FIELD RESERVED FOR TRANSMITTING SECURITY RELATED INFORMATION
C
TRANSMITTING OVER PACKET-SWITCHED NETWORK TO A RECEIVING NODE
D
RETRIEVING INFORMATION IDENTIFYING SELECTED CLASS FROM THE FIELD RESERVED FOR TRANSMITTING SECURITY RELATED INFORMATION
END

FIG. 1

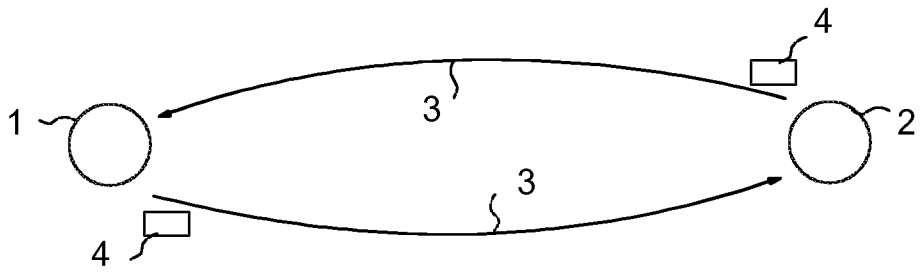
4
3
1
2
3
4

FIG. 2

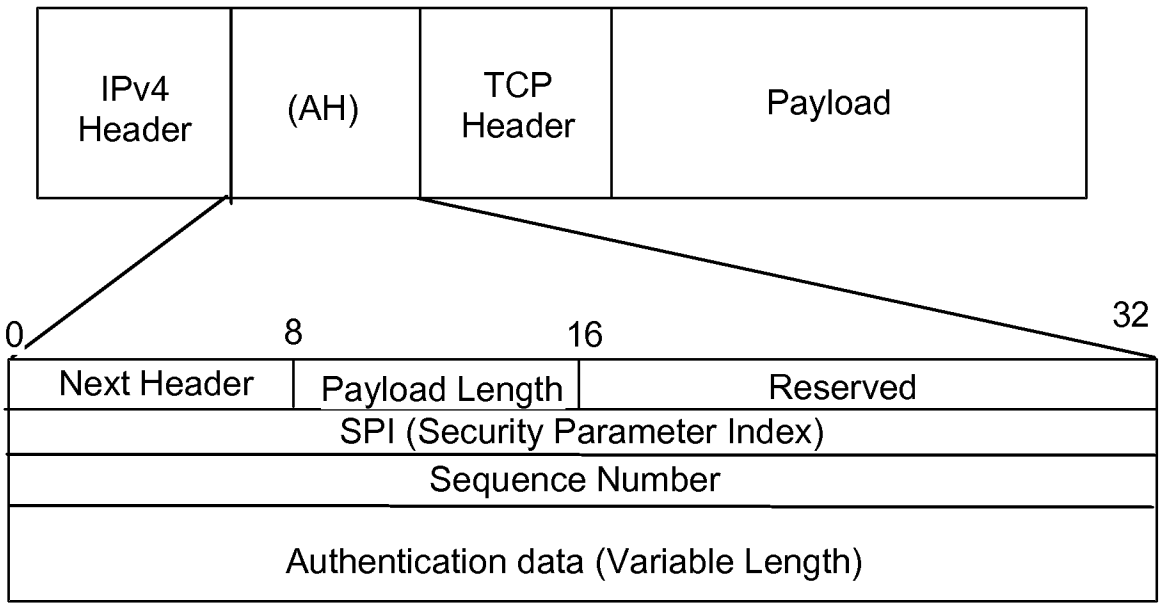
IPv4 Header
(AH)
TCP Header
Payload
0
8
16
32
Next Header
Payload Length
Reserved
SPI (Security Parameter Index)
Sequence Number
Authentication data (Variable Length)

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2008/050189

A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC8: H04L, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

FI, SE, NO, DK

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI, INSPEC, IPCOM, ELSEVIER, IEEE Xplore

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7136382 B1 (SHARMA, M. et al.) 14 November 2006 (14.11.2006), column 4, line 50 - column 5, line 30	1-14
A	FINEBERG, V. 'A Practical Architecture for Implementing End-to-End QoS in an IP Network', IEEE Communicatons Magazine, January 2002, IEEE Service Center, Piscataway, US, pages 122-130, page 126, left column, first paragraph	1-14
A	US 2003/0039210 A1 (JIN, J. et al.) 27 February 2003 (27.02.2003), abstract	1-14
A	US 2007/0076599 A1 (AYYAGARI A. et al.) 05 April 2007 (05.04.2007), abstract, paragraph [0007]	1-14
A	US 6658003 B1 (SUGAI K. et al.) 02 December 2003 (02.12.2003), abstract	1-14
A	WO 99/48310 A1 (NOKIA TELECOMMUNICATIONS OY et al.) 23 September 1999 (23.09.1999), abstract	1-14

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 July 2008 (18.07.2008)	24 July 2008 (24.07.2008)

Name and mailing address of the ISA/FI
National Board of Patents and Registration of Finland
P.O. Box 1160, FI-00101 HELSINKI, Finland
Facsimile No. +358 9 6939 5328

Authorized officer
Seppo Ojala

Telephone No. +358 9 6939 500

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/FI2008/050189

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
US 7136382 B1	14/11/2006	None	
US 2003/0039210 A1	27/02/2003	US 2005111360 A1	26/05/2005
US 2007/0076599 A1	05/04/2007	GB 2430834 A	04/04/2007
US 6658003 B1	02/12/2003	FR 2794319 A1 JP 2000244574 A	01/12/2000 08/09/2000
WO 99/48310 A1	23/09/1999	AT 378785T T US 6728208 B1 EP 1064800 A1 AU 2838999 A FI 980617 A	15/11/2007 27/04/2004 03/01/2001 11/10/1999 20/09/1999

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2008/050189

CLASSIFICATION OF SUBJECT MATTER

Int.Cl.
H04L 12/56 (2006.01)