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 8 October 2013

Case Number:	T 0297/10 - 3.5.03
Application Number:	01930988.9
Publication Number:	1303938
IPC:	H04L 29/06, H04L 29/08
Language of the proceedings:	EN

Title of invention:
Method and apparatus for interfacing a network to an external element

Applicant:
Motorola Mobility LLC

Headword:
Interfacing a network to an external element/MOTOROLA

Relevant legal provisions:
EPC Art. 56
RPBA Art. 13(1)

Keyword:
"Inventive step (main request) - no"
"Admissibility (auxiliary request) - no"

Decisions cited:
-

Catchword:
-

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Case Number: T 0297/10 - 3.5.03

DECISION
of Technical Board of Appeal 3.5.03
of 8 October 2013

Appellant: (Applicant)	Motorola Mobility LLC 600 North US Highway 45 Libertyville, IL 60048 (US)
Representative:	Openshaw, Paul Malcolm Openshaw & Co. 8 Castle Street Farnham Surrey GU9 7HR (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted 25 September 2009 refusing European patent application No. 01930988.9 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman:	F. van der Voort
Members:	A. J. Madenach
	R. Moufang

Summary of Facts and Submissions

I. The present appeal arises from the decision of the examining division refusing European patent application No. 01930988.9 on the ground that the subject-matter of claims 1 and 5 did not involve an inventive step (Articles 52(1) and 56 EPC) having regard to the disclosure of

D1: "Security in the WLTS", Jormalainen S. and Laine J., Internet citation, 30 November 1999

and common general knowledge.

II. In a reply dated 15 August 2013 to the summons dated 10 June 2013 to attend oral proceedings the appellant confirmed its main request, *i.e.* that the decision of the examining division be set aside and that a patent be granted on the basis of the set of claims as decided upon by the examining division, *i.e.* claims 1 to 9 as received on 23 February 2007, and filed a set of claims 1 to 9 as an auxiliary request.

III. Oral proceedings were held on 8 October 2013. In the course of the oral proceedings, the appellant withdrew the main request and requested that the decision under appeal be set aside and that a patent be granted on the basis of claims 1 to 9 of a new main request (which was filed as an auxiliary request with the letter dated 15 August 2013) or, alternatively, on the basis of claims 1 to 9 of a new auxiliary request as filed at the oral proceedings. At the end of the oral proceedings, after deliberation, the board's decision was announced.

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

"An apparatus for interfacing a core network (10) to a feature server (402, 502, 602, 606) external to the core network, wherein the core network (10) is interfaced to a radio access network (12) that provides wireless and date communication services to a mobile unit (14) in accordance with a wireless communication protocol, the apparatus comprising:

a service delivery element (26), wherein the service delivery element (26) is within the core network (10), the service delivery element (26) comprising at least one internal interface to couple the service delivery element (26) to other devices within the core network (10), an external interface to couple the service delivery element (26) to at least one feature server (402, 502, 602, 606) external to the core network (10), an embedded security layer (408) to authenticate the at least one feature server (402, 502, 602, 606) on the core network (10) and to provide a secure interface for the at least one feature server (402, 502, 602, 606) to the core network (10) through the external interface and a processor adapted to operate responsive to a control program stored within a memory associated with the processor; and wherein the service delivery element (26) is operable to recognize the feature server (402, 502, 602, 606), to negotiate a security level between the feature server (402, 502, 602, 606) and the core network (10), and to manage access by the feature server (402, 502, 602, 606) to the core network (10)."

Claim 1 of the auxiliary request differs from claim 1 of the main request in that between "the core network (10)" and ",and to manage" the following wording is inserted: "regarding a service that requires the execution of programmable code by the core network".

Reasons for the decision

1. *Main request: inventive step (Article 56 EPC)*

1.1 The board considers D1 to be the closest prior art for the subject-matter of claim 1.

D1 is concerned with security issues in the wireless transport layer security (WTLS) which is used in the wireless application protocol (WAP). A WAP gateway connects the wireless domain to the world wide web (WWW) (D1, sentence bridging pages 4 and 5). D1 also discloses the use of a secure sockets layer (SSL) below the hypertext transfer protocol (HTTP) layer for requests made by the WAP gateway to an origin server in the WWW (page 6, first paragraph, and Figure 3).

More specifically, D1 discloses an apparatus (gateway in Figure 3.1) for interfacing a wireless domain, *i.e.* a wireless network which includes a client (page 4, last line to page 5, first line, and Figure 3.1), to a web server external to the wireless domain.

It is implicit that the wireless network comprises, in addition to the mobile unit of the client as shown in Figure 3.1, a backbone of the wireless domain, since this is necessary in order to form a complete working wireless domain. This backbone is considered to correspond to the claimed core network. The front end of the wireless domain, which includes the mobile unit as shown in Figure 3.1, forms a radio access network that provides wireless voice and data communication services to the mobile unit in accordance with a wireless communication protocol. The web server of the WWW (see Figure 3.1) provides services like online banking and e-commerce (page 2, chapter 1, second paragraph) and is considered to correspond to the feature server of claim 1. The WAP gateway as a protocol gateway (D1, page 5, first line) corresponds to the service delivery element of claim 1 (*cf.* the present application as published, page 8, line 31, "protocol gateway"). Being connected to the wireless domain with its radio access network and the core network and given that the wireless voice and data communication services of the communication network are to be routed from the radio access network via the core network to the gateway, the gateway (*i.e.* the service delivery element in the terminology of claim 1) necessarily comprises an internal interface to couple the service delivery element to devices in the core network and an external interface to couple it to the web server (feature server in the terminology of claim 1) external to the core network (*cf.* Figure 3.1).

The WAP gateway (service delivery element) furthermore comprises an embedded security layer ("Security Layer (WTLS)" in Figure 3.2) for communications with the core network and uses a secure sockets layer (SSL) for communications with the web server (page 6, lines 2-4). Therefore, a secure end-to-end connection, *i.e.* between the client within the wireless domain and the web server, is provided (*cf. e.g.* page 6, second paragraph). The security layers (WTLS and SSL) serve to authenticate the server and to provide a secure interface for the server to the communication network through the external interface (page 7, chapter 3.3.3, first paragraph).

Further, it is implicit that the service delivery element comprises a processor responsive to a control program stored within a memory associated with the processor, in order to be able to perform the handshake protocol as explained in chapter 3.3.3.

The handshake protocol (chapter 3.3.3) further implies that the service delivery element is operable to recognise the feature server (otherwise a two-way communication would not be possible). Furthermore, it is operable to negotiate a security level between the feature server and the wireless domain. This follows from the authentication procedure (page 8, chapter 3.4) which implies that at least two security levels exist, one being "authenticated" and the other being "not authenticated". In the case of authenticated partners, the security level is furthermore determined by the strength of the keys used for encryption (page 14, chapter 4.4). The handshake protocol (chapter 3.3.3) also implies that the gateway is operable to manage access by the feature server to the communication network.

The board notes that most of the details described in D1 concern the WLTS security layer between the wireless domain and the gateway. It is however part of common general knowledge that corresponding procedures apply likewise to the SSL security layer between the gateway and the server.

1.2 The claimed apparatus differs from the apparatus of D1 in that according to claim 1 the service delivery element is within the core network, whereas in D1 it is positioned outside the network (see Figure 3.1).

1.3 However, placing the gateway (*i.e.* the service delivery element according to claim 1) within the core network is suggested in D1 as an alternative arrangement in order to increase the trust in the decryption/encryption process carried out within the WAP gateway (D1, page 6, third paragraph) and would thus, if desired, be used by the skilled person. This implementation would therefore not require the exercise of inventive skill (Article 56 EPC).

1.4 The appellant argued that D1 did not disclose a core network interfaced to a radio access network. Instead, the gateway was connected to a wireless domain which was to be considered as corresponding to the claimed radio access network.

The board disagrees. As already pointed out in point 1.1 above, a wireless domain or, equivalently, a mobile network (see D1, page 6, second paragraph) necessarily comprises, apart from the mobile devices a backbone consisting, in the case of GSM, of a base station subsystem, a switching and management subsystem and an operation and maintenance subsystem, which are coupled to the mobile devices by a radio interface and which handle the traffic inside the mobile network and the traffic going outside the mobile network. The board considers this backbone to correspond to the claimed core network and, in this case, the mobile devices to correspond to the claimed radio access network.

1.5 Further, the appellant saw a difference between the claimed service delivery element, which according to the appellant served to protect the network, and the known WAP gateway which served to protect the client and the external feature server. In particular, it was argued that, according to claim 1, authentication and negotiation were done between the server and the service delivery element, whereas the WAP gateway of D1 only served as an interface between the client and the server, which themselves negotiated.

This argument is at variance with the fact that according to D1 a security layer is formed between the WAP gateway and the mobile terminal on the one hand (page 6, first paragraph) and between the WAP gateway and the web server on the other hand (*ibidem*). This implies that the WAP gateway is the point at which the web server is recognised and its access to the core network (and ultimately to the client) is managed. Further, it is part of common general knowledge that the SSL layer below the HTTP layer negotiates a security level between the WAP gateway and the web server in a manner equivalent to that described with respect to the WTLS layer in D1.

The appellant further argued that according to claim 1 the security level is between the server and the core network, *i.e.* not between a client and the server as in D1. However, in the board's view, the client(s) form(s) the radio access network which, according to the reasoning given above, is connected via a radio interface to the core network and forms its endpoint. Therefore, if a security level between a client and the server is negotiated, it necessarily implies that a security level between the server and the core network is negotiated.

The appellant further argued that, whereas D1 discloses security between the client and the WAP gateway, the claim provided for a security level which is negotiated between the service delivery element and the feature server. This argument does however not take into account that the SSL layer ensures security between the WAP gateway and the web server (page 6, lines 2 to 4), which, as is commonly known, is negotiated between the two endpoints, *i.e.* the WAP gateway and the web server.

The appellant also pointed to the fact that according to chapter 3.3.3 (including Figure 3.4) and chapter 3.4 of D1 the handshake and authentications were only between the client and the server without involving the WAP gateway. This observation overlooks the fact that according to D1, page 5, first paragraph, all encoding and decoding, including the application of a security protocol, is done by the WAP gateway.

The appellant finally argued that D1 was about ensuring the security of data transmitted between the server and a client, including privacy, authentication and integrity of the data (chapters 2.1, 2.2 and 2.3 of D1), whereas the present invention aimed at providing scalable access of external features to the core network based on a variety of security variables negotiated by the service delivery element (page 5, lines 8 to 22 of the application as published). The board however fails to see a feature relating to the scalable access in claim 1. As far as the negotiation of a security level is concerned, it is noted that the negotiation of a security level as defined in claim 1 can be read onto the negotiation of the data security parameters (see D1, *e.g.* section 3.3.3, first line, section 3.8, lines 1 and 2, and section 4.4).

1.6 For the reasons set out above, the subject-matter of claim 1 does not involve an inventive step (Articles 52(1) and 56 EPC) having regard to the teaching of D1 and common general knowledge. The main request is therefore not allowable.

2. *Auxiliary request: admissibility (Art. 13(1) RPBA)*

2.1 According to Article 13(1) RPBA, any amendment to a party's case after it has filed its grounds of appeal may be admitted and considered at the board's discretion. The discretion shall be exercised in view of, *inter alia*, the complexity of the new subject-matter submitted, the current state of the proceedings and the need for procedural economy. Amendments sought to be made after oral proceedings have been arranged shall not be admitted if they raise issues which the board cannot reasonably be expected to deal with without adjournment of the oral proceedings (Article 13(3) RPBA). According to established case law, new claims filed at a late stage should be clearly allowable. In particular, they should not introduce new objections under the EPC and should overcome all outstanding objections under the EPC.

2.2 In the present case, the auxiliary request was filed during the oral proceedings.

Claim 1 of this request comprises the additional feature that the service delivery element is operable to negotiate a security level between the feature server and the core network "regarding a service that requires the execution of programmable code by the core network" (see point IV above).

According to the appellant, the additional feature derives from page 4, lines 14 to 23, of the application as published.

The board notes however that the cited passage does refer to a service that requires the execution of programmable code, but is not concerned with the negotiation of a security level. Further, security negotiation is for the first time mentioned at page 10, lines 8 to 11 in connection with establishing a secure link between an external element and the core network. No security level is however mentioned in this context and the link to the cited passage at page 4 remains unclear.

Further, the cited passage relates to external application program interfaces (APIs) which interface services and functional components and are linked to internal APIs via the services delivery element (page 4, lines 9 to 11 of the application as published). Therefore, this paragraph is more about linking external and internal APIs than about the negotiation of a security level between a feature server and the core network.

Further, whereas the negotiation of a security level had previously been claimed to be between the feature server and the core network, it is now claimed with regard to a service. No original disclosure for this amendment was given.

The amendment to claim 1 according to the auxiliary request thus gives rise to objections under Article 123(2) EPC.

2.3 In view of the above and considering the advanced stage of the proceedings as well as the need for procedural economy, the board exercised its discretion under Article 13(1) and 13(3) RPBA and did not admit the auxiliary request to the proceedings.

3. There being no allowable request, it follows that the appeal is to be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

G. Rauh F. van der Voort