Internal distribution code:
(A) [ ] Publication in OJ
(B) [ ] To Chairmen and Members
(C) [ ] To Chairmen
(D) [x] No distribution

Datasheet for the decision of 10 July 2009

Case Number:	T 1624/06 - 3.5.05
Application Number:	99305731.4
Publication Number:	0977397
IPC:	H04L 9/08
Language of the proceedings:	EN

Title of invention:
Method for transferring sensitive information using initially unsecured communication

Applicant:
LUCENT TECHNOLOGIES INC.

Opponent:
-

Headword:
Transferring sensitive information/LUCENT

Relevant legal provisions:
EPC Art. 123(2)

Relevant legal provisions (EPC 1973):
EPC Art. 54, 56

Keyword:
"Main request - novelty (no)"
"First auxiliary request- inventive step (no)"
"Second auxiliary request - Added subject-matter (yes)"

Decisions cited:
-

Catchword:
-

Case Number: T 1624/06 - 3.5.05

DECISION
of the Technical Board of Appeal 3.5.05
of 10 July 2009

Appellant:

LUCENT TECHNOLOGIES INC.
600 Mountain Avenue
Murray Hill
NJ 07974-0636 (US)

Representative:

Sarup, David Alexander
Alcatel-Lucent Telecom Limited
Unit 18, Core 3, Workzone
Innova Business Park
Electric Avenue
Enfield EN3 7XU (GB)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted 23 May 2006 refusing European application No. 99305731.4 pursuant to Article 97(1) EPC 1973.

Composition of the Board:

Chairman: D. H. Rees
Members: P. Cretaine
G. Weiss

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division dispatched 23 May 2006, refusing European patent application No. 99305731.4. The decision was based on the ground that independent claims 1 and 10 did not meet the requirements of Article 54(1) and (2) EPC 1973 since their subject-matter was known from the following prior art document:

D1: PARK C-S: "ON CERTIFICATE-BASED SECURITY PROTOCOLS FOR WIRELESS MOBILE COMMUNICATION SYSTEMS" IEEE NETWORK: THE MAGAZINE OF COMPUTER COMMUNICATIONS,IEEE INC. NEW-YORK,US, vol. 11, no. 5, 1 September 1997, pages 50-55, XP000699941 ISSN: 0890-8044

II. Notice of appeal was submitted on 19 July 2006 and the appeal fee was paid on the same day. In the statement setting out the grounds of appeal dated 12 and received 13 September 2006, the appellant (applicant) implicitly requested that a patent be granted on the basis of the claims on which the appealed decision had been based (claims 1-17, main request). In addition the appellant submitted an auxiliary set of claims (claims 1-14, first auxiliary request).

III. In a communication accompanying a summons to oral proceedings, the board gave a preliminary opinion that the subject-matter of claim 1 according to the main request was disclosed in D1 and that the subject-matter of claim 1 according to the auxiliary request did not involve an inventive step when starting out from D1 as closest prior art.

In addition the board raised similar objections based on the following prior art document, cited in the examination procedure:

D2: BELLER M J ET AL: "PRIVACY AND AUTHENTICATION ON A PORTABLE COMMUNICATIONS SYSTEM" PROCEEDINGS OF THE GLOBAL TELECOMMUNICATIONS CONFERENCE. (GLOBECOM),US,NEW-YORK, IEEE, 2 December 1991, pages 1922-1927, XP000313732, ISBN: 0-87942-697-7.

The board further gave its reasons why the appellant's arguments were not convincing.

IV. In a letter of response to the summons submitted on 5 June 2009, the appellant announced that it would not attend the oral proceedings, and requested that they be cancelled and that procedure be continued in writing.

The appellant provided further arguments in support of the novelty and inventive step of the main and auxiliary requests and submitted a second auxiliary set of claims (claims 1-10, second auxiliary request).

V. Oral proceedings were held on 10 July 2009 in the absence of the appellant.

After due deliberation on the basis of the submissions and requests dated 12 September 2006 and 5 June 2009, the board announced its decision.

VI. The appellant's requests are as follows:

that the decision under appeal be set aside and that a patent be granted based, as a main request, on claims 1 to 17 as originally filed (with the numbering of claim 12 corrected as requested) or, as a first auxiliary request, on claims 1 to 14 filed with the statement setting out the grounds of appeal or, as a second auxiliary request, on claims 1 to 10 filed with a letter received 5 June 2009.

The further text on which this decision is based is:

description pages 1 to 13 as originally filed, and
drawing sheets 1/2 and 2/2 as originally filed.

VII. Claim 1 of the main request reads as follows:

"A method for transferring sensitive information to a first party using initially unsecured communication, comprising:
(a) receiving, at said first party, a public key of a second party;
(b) producing an encryption result by performing keyed encryption on at least a first random number using said public key;
(c) transferring said encryption result from said first party to said second party;
(d) transferring authorizing information to said second party over a first encrypted and authenticated communication channel established using said first random number; and
(e) receiving sensitive information from said second party over a second encrypted and authenticated communication channel established using said first random number".

Independent claim 10 of the main request reads as follows:

"A method for transferring sensitive information from a first party using initially unsecured communication channel, comprising:
(a) outputting a public key of said first party;
(b) receiving, at said first party, an encryption result from a second party, said encryption result being a result of performing keyed encryption on at least a first random number using said public key of said first party;
(c) decrypting said encryption result to obtain said first random number;
(d) receiving authorizing information from said second party over a first encrypted and authenticated communication channel established using said first random number; and
(e) transferring sensitive information to said second party over a second encrypted and authenticated communication channel established using said first random number if said authorizing information is acceptable".

Claims 1 and 9 of the first auxiliary request differ from claims 1 and 10 of the main request in that the first channel is a *voice channel* and the second channel is a *control channel*.

Claim 1 of the second auxiliary request reads as follows (amendments vis-à-vis the main request in italics):

"A method for transferring sensitive information to a first party using initially unsecured communication, comprising:
(a) receiving, at said first party, a public key of a second party *and a certificate of said public key*;
(a1) authenticating the network by verifying authenticity of the public key of the network on the basis of said certificate;
(b) producing an encryption result by performing keyed encryption on at least a first random number *and an identifier for said first party* using said public key;
(c) transferring said encryption result from said first party to said second party, *the encryption result being used to authenticate the first party*;
(d) transferring authorizing information to said second party over a first encrypted and authenticated communication channel established using said first random number, *the first communication channel being a voice communication channel*; and
(e) receiving sensitive information from said second party over a second encrypted and authenticated communication channel established using said first random number, *the second communication channel being a control channel".*

Independent claim 6 of the second auxiliary request reads as follows:

"A method for transferring sensitive information from a first party using initially unsecured communication channel, comprising:
(a) outputting a public key of said first party *and a certificate of said public key*;

(b) receiving, at said first party, an encryption result from a second party *if said second party authenticated the network*, said encryption result being a result of performing keyed encryption on at least a first random number *and an identifier for said second party* using said public key of said first party;
(c) decrypting said encryption result to obtain said random number *and said identifier for said second party*;
(d) receiving authorizing information from said second party over a first encrypted and authenticated communication channel established using said first random number, *the first communication channel being a voice channel*; and
(e) transferring sensitive information to said second party over a second encrypted and authenticated communication channel established using said first random number if said authorizing information is acceptable, *the second communication channel being a control channel*."

Reasons for the Decision

1. Admissibility

The appeal is admissible.

2. Non-attendance of oral proceedings

In its letter of 5 June 2009 the appellant announced that it would not be represented at the oral proceedings and requested that the procedure be continued in writing. The board considered it to be expedient to maintain the set date for oral proceedings. Nobody attended the hearing on behalf of the appellant.

Article 15(3) RPBA stipulates that the board shall not be obliged to delay any step in the proceedings, including its decision, by reason only of the absence at the oral proceedings of any party duly summoned who may then be treated as relying only on its written case.

The appellant also had to expect that the board would discuss the appellant's newly filed second auxiliary request in respect of its compliance with, inter alia, Article 123(2) EPC, as it had been warned in the board's communication.

Thus, the board was in a position to take a decision at the end of the hearing.

3. Main request - novelty (Article 54 EPC 1973)

3.1 D1 relates to mutual authentication and session key exchange protocols for establishing secure communications between the network infrastructure and a mobile station in wireless mobile communication systems, thereby enabling the transfer of sensitive information, i.e. information which should be protected against eavesdropper, from the network to the mobile.

In particular, the passage on page 52, right-hand column, lines 13 to 45, discloses a method comprising, in combination, all the steps of the method of claim 1, whereby the mobile station MS corresponds to the first party of claim 1 and the home network HN corresponds to the second party:

- the home network HN has its own certificate $cert_{HN}$, which includes a public key (lines 22-23) $p_{HN,}$ and broadcasts it; it is therefore implicitly disclosed that the mobile station receives the public key of the home network, according to step (a) of claim 1.

- then a session key k_S is randomly chosen by the mobile station, encrypted with p_{HN} and sent to the network (lines 40-42): steps (b) and (c) are thus disclosed in D1.

- the MS's certificate $cert_{MS}$ is also sent encrypted with the session key k_S from the mobile to the network (lines 42-43):

. the MS's certificate enables the network HN to authenticate the mobile (lines 44-45);

. furthermore the MS's certificate contains a current expiration date $date_{ms}$ which indicates the time limit for validity of the certificate, i.e. the mobile user's solvency, and which could be set to the same as the billing period (see on page 54, right-hand column, lines 1-13): therefore $cert_{MS}$ contains, inter alia, *authorizing information* for granting network access privileges to the mobile;

. the MS can authenticate the HN (page 52, line 38) and verify its public key p_{HN}: the session key k_S being chosen by the mobile and being sent to the network encrypted with this public key, the uplink communication channel from the mobile MS to the network HN using this secret session key represents *a first encrypted and authenticated communication channel* established using the session key.

Step (d) of claim 1 is thus disclosed in D1.

- the downlink communication channel from the network HN to the mobile MS using the secret session key k_S represents *a second encrypted and authenticated channel* established using said session key; the aim of the protocols defined in D1 being to provide secret communication over the traffic channel between a network and an MS (D1, page 51, left-hand column, lines 39- 47), it is implicit from D1 that *sensitive information* is received by the MS from the HN over said downlink channel when the solvency of the mobile has been verified, i.e. when the mobile has been authorized: step (e) of claim 1 is therefore also disclosed in D1.

All the steps of claim 1 according to the main request being disclosed in combination in D1, its subject-matter is not novel and does not meet the requirements of Article 54 EPC 1973.

The subject-matter of claim 1 of the main request can also be read onto the disclosure of D2, particularly on page 1925, in the paragraph titled "Minimal Public-Key Solution: MSR" and the corresponding figure 3, which discloses the following steps:

- the portable receives the public key Nj of the network (step (1) of figure 3): this corresponds to step (a) of claim 1

- the portable picks a random session key x, encrypts it with the public key of the network, and sends it to the network (steps (2) and (3) of figure 3): this corresponds to steps (b) and (c) of claim 1.

- the portable sends its identity i and its certificate c encrypted with session key x to the network: the portable being equipped with the certificate at service-subscription time (page 1923, right-hand column, paragraph 4.1) or at service initiation (page 1925, right-hand column, lines 6-7) for authentication purposes, it is implicit that the certificate represents authorizing information for verifying network access privileges of the mobile; step (d) of claim 1 is thus disclosed in D1.

- the portable receives information from the network, encrypted with the session key (page 1922, left-hand column, lines 51-53): this corresponds to step (e) of claim 1.

Independent claim 10 contains steps corresponding to the steps of claim 1, but expressed in terms of a communication of data seen from the network point of view. Thus, its subject-matter is equally not novel.

3.2 The appellant has argued that D1 simply corresponds to a security protocol similar to the CFT security protocol described with respect to figure 2 of the specification and that, as a consequence, D1 does not disclose both **encrypting and authenticating** the communication channel prior to the transmission of authorizing information.

The board however observes that in D1 a secret session key has been established between the mobile and the network. In the board's judgment, a channel using this session key as an encryption key is per definition an authenticated channel. The certificate MS, which includes the authorizing information, is transmitted encrypted with session key k_s from the mobile to the network: the channel on which the authorizing information is transmitted is thus both encrypted, using k_s, and authenticated, since k_s is a secret session key between the mobile and the network party. In the same way, the downlink channel (network to mobile) is an authenticated channel since it also uses k_s as an encryption key.

The appellant also identified a second alleged point of difference, namely that two encrypted and authenticated communication channel are specified in claim 1 of the main request. The board considers that it is normal in the art to consider uplink and downlink channels to be separate, so that D1 also discloses two channels.

In his letter of 5 June 2009 in response to the communication accompanying the summons, the appellant further argued that the MS's certificate is not transferred over an encrypted and authenticated channel since, according to lines 57-59 on page 52 of D1, it can be "exposed". The board notes that this passage relates to the exposition of the certificate **inside the network after it has been decrypted**, i.e. after it has been transferred to the network, and is therefore irrelevant for examining if the first channel is encrypted and authenticated.

The appellant also argued in his letter of 5 June 2009, that the "authentication information" of D2 is not transferred over an encrypted and authenticated channel since the portable sends its identity i over a **non-authenticated** channel. The board notes however that the identity i and certificate are transferred encrypted with the key x from the portable to the network; x being a secret session key shared by the portable and the network, a channel using this key for encryption is an authenticated channel, as stated above in respect of D1.

4. First auxiliary request- inventive step (Article 56 EPC 1973)

The method of claim 1 according to the auxiliary request differs from the method of claim 1 according to the main request and from the disclosure of D1 (or D2) in that:

- in step (d) the first channel is further defined as being a *voice channel*

- in step (e) the second channel is further defined as being a *control channel*.

In a wireless mobile communication system, the existing channels may be divided in two categories: traffic channels, conveying speech (voice channels) or data (data channels), and control channels, conveying signaling information (data). The choice of a channel depends on the kind of information the parties (mobile and network) desire to exchange.

The protocols of D1 and D2, in particular the ones defined on page 52 of D1 and page 1925 of D2, enable a mobile and a network to share a secret session key. Although D1 and D2 do not explicitly define the kind of channels which could be protected using the session key, it is implicit that any channel between the mobile and the network using encryption based on this session key is an encrypted and authenticated channel, irrespective of the kind of information it conveys, i.e. irrespective of whether it is a traffic channel (either data or voice channel) or a control channel.

In the board's judgment, starting from D1 or D2, the problem underlying claim 1 according to the auxiliary request is to enable the transfer of an authorizing information which is a voice (speech) signal and of a sensitive information which is a signaling signal. The skilled person looking for a solution to this problem would obviously choose for each information the kind of channel which is provided in the communication system and which is the most adapted, i.e. he would choose a voice channel for a voice information and a control channel for a signaling information. The choice of transferring authorization information over a voice channel is, in the board's judgment, a mere design option.

Contrary to the appellant's arguments, the board sees no particular advantage in being able to convey the authorization information over a voice channel - it would be equally easy to enter credit card information via a keyboard and transfer it over a data channel. In the same way, transferring sensitive information over a control channel is an obvious selection between two possibilities (traffic or control channel), which the skilled person will perform depending on the content of the sensitive information. For instance, an A-key of a mobile network could be transferred on a control channel.

Thus, the method of claim 1 according to the auxiliary request does not appear to involve an inventive step (Article 56 EPC 1973).

Independent claim 9 according to the auxiliary request contains steps corresponding one to one to the steps of claim 1 according to the auxiliary request, but expressed in terms of a communication of data seen from the network point of view. Thus, its subject-matter also does not involve an inventive step.

5. Second auxiliary request:

5.1 Objection under Article 123(2) EPC

This request has been submitted by the appellant in response to the communication accompanying the summons.

The appellant did not identify the basis for the amendments in the originally filed application.
In particular, claim 1 adds to the originally filed claim 1 in steps (b) and (c) that the encryption result of a keyed encryption on *an identifier for the first party* and a first random number, using the public key of the second party, is *being used to authenticate the first party.* The feature of authenticating the first party using said encryption result is however not disclosed in the originally filed application.
The description in paragraph 28 merely defines that the network (second party) obtains the identification number ID (identifier) of the mobile (first party) and the session key (first random number) by decrypting the encryption result with its private key. The obtained identification number is used by the network for associating a particular A-key to the mobile (see paragraph 34).

The description and claims as originally filed therefore merely describe that the first party (mobile) is identified but do not disclose that the first party is authenticated, i.e. that its identity is verified.

It is however common knowledge of a person skilled in the art of mobile telephony that authentication of a subscriber phone is a procedure which goes further than the simple identification of the subscriber phone by its identification number. In particular both the GSM and the IS-41, which were respectively the European and North American standards commonly used at the priority date of the present application (the IS 41 being moreover mentioned in the description), use cryptographic procedures involving secret keys for authenticating the mobile phone to the network.

For these reasons the board considers that claim 1 according to the second auxiliary request does not meet the requirement of Article 123(2) EPC.

5.2 Clarity and inventive step

The board would like to make the following comments in respect of clarity and inventive step of the subject-matter of claim 1.

In step (a1), claim 1 recites "authenticating the network" although the term "network" has no antecedent definition in the claim, thereby rendering the subject-matter of the claim unclear (Article 84 EPC 1973).

Even if the terms "network" in step (a1) and "authenticate" in step (c) were replaced by, respectively, the terms "second party" and "identify" to remove the deficiencies under Articles 84 and 123(2) EPC, the board considers that the subject-matter of claim 1 would not involve an inventive step.

In that respect, the following features, that claim 1 of the second auxiliary request add to claim 1 of the main request, are either already known from D1 or represent common measures with no inventive merit on themselves:

- in step (a), the reception, by the first party, of a certificate of the public of the second party is implicitly disclosed in D1 (page 52, right hand column, line 37: "The home network HN broadcasts its certificate cert_{HN}.");

- step (a1) is implicitly disclosed in D1 (page 52, lines 38-39: "The MS can authenticate the HN by verifying... to s_{CA}.");

- in step (b) an identifier for the first party is sent encrypted with the second party's *public key* to the second party, whereas in D1 the identifier ID_{MS} of the mobile is included in the certificate and sent encrypted with the *session key* to the network. The appellant argued that sending an identifier enables the network to associate an A-key with the mobile. This technical effect is also achieved by the scheme of D1. Moreover, using the network's public key instead of the session key for encrypting the identifier appears to be an obvious alternative for the skilled person having both keys at its disposal.

- in steps (d) and (e) the added features of having a voice and control channel, as, respectively, the first and second communication channel, are also present in steps(d) and (e) of the first auxiliary request; for the same reasons as explained above in respect of the first auxiliary request, the board concludes that the skilled person would, without the exercise of inventive skill, include these features in the method according to claim 1.

6. There being no further request, the appeal has to be dismissed.

Order

For this reasons it is decided that:

The appeal is dismissed.

Registrar:	Chairman:
K. Götz	D. H. Rees