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

Datasheet for the decision of 12 July 2012

Case Number: T 1582/07 - 3.4.03

Application Number: 03773831.7

Publication Number: 1552484

IPC: G07F 7/10, G06F 17/60, G06F 1/00

Language of the proceedings: EN

Title of invention:
Facilitating and authenticating transactions

Applicant:
Vodafone Group PLC

Headword:
-

Relevant legal provisions:
EPC Art. 123(2)

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

Keyword:
"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

Case Number: T 1582/07 - 3.4.03

D E C I S I O N
of the Technical Board of Appeal 3.4.03
of 12 July 2012

Appellant: (Applicant)
Vodafone Group PLC
Vodafone House
The Connection
Newbury
Berkshire RG14 2FN (GB)

Representative:
Harries, Simon George
Vodafone Group Services Limited
Vodafone House
The Connection
Newbury
Berkshire RG14 2FN (GB)

Decision under appeal:
Decision of the Examining Division of the European Patent Office posted 13 April 2007 refusing European patent application No. 03773831.7 pursuant to Article 97(1) EPC 1973.

Composition of the Board:

Chairman: G. Eliasson
Members: V. L. P. Frank
T. Bokor

Summary of Facts and Submissions

I. This is an appeal from the refusal of application 03 773 831 for the reason that the claims of the main and auxiliary requests 1, 2 and 6 to 7 contained undisclosed subject-matter (Article 123(2) EPC) and that the subject-matter of claim 1 of the main and auxiliary requests 1 to 5 and 8 did not involve an inventive step (Article 56 EPC 1973).

II. At the oral proceedings before the board the appellant applicant requested that the decision under appeal be set aside and that a patent be granted in the following version:

Description, pages:
1-3, 10-11, 22 as filed during oral proceedings,
7 as filed with letter dated 6 April 2005,
4-6, 8-9, 12-21, 23-45 as published.

Claims:
1-21 as filed during oral proceedings.

Drawings:
Sheets 1/12-12/12 as published.

III. The independent claims of this request read:

"1. A method for carrying out an authentication process for authenticating a subsequent transaction with an application services part (22) by any one of a plurality of users using a data processing apparatus (10) incorporating a transaction manager (14), including the step

during the authentication process of operatively associating with the data processing apparatus (10) a selected one of a plurality of authentication storage means (12) respective to the users, each authentication storage means (12) storing predetermined authentication information and being registered with a common telecommunications system (16) for which the users have respective mobile terminals, the application part (22) being separate from the telecommunications system (16) and controlled by a third party, and the step of carrying out the authentication process via a communications link (19) with the common telecommunications system (16), the authentication process being carried out by a security services part (18) of the telecommunications system (16) and involving the use of the predetermined authentication information stored by the selected one authentication storage means (12), the authentication process further including generating a session key that is transmitted by the security services part (18) of the telecommunications system to the applications services part (22), and also transmitting the session key from the transaction manager (14) in an application request to the application services part (22) and wherein the application services part (22) compares the session keys prior to proceeding with the transaction, the predetermined authentication information stored by each authentication storage means (12) corresponding to information which is used to authenticate that user’s mobile terminal in relation to the telecommunications system (16) but the

authentication process for authenticating the transaction by that user with the data processing apparatus (10) not requiring use of that user's mobile terminal."

"13. A system including an application services part (22) and data processing apparatus (10), incorporating a transaction manager (14), in combination with a selected one of a plurality of authentication storage means (12) which are respective to users and are each for storing predetermined authentication information relating to the carrying out of an authentication process for authenticating a subsequent transaction with the application services part (22) by the users with the data processing apparatus (10), the system further including common telecommunications system (16), the authentication storage means (12) all being operable to be registered with the common telecommunications system (16) for which the users have respective telecommunications handsets, the application services part (22) being separate from the telecommunications system (16) and controlled by a third party, the authentication storage means (12) when operatively associated with the data processing apparatus (10) being operative to carry out the authentication process via a communications link (19) with the common telecommunications system (16), the authentication process being carried out by a security services part (18) of the common telecommunications system (16) and involving the use of the predetermined information stored by the selected one authentication storage means (12),

the authentication process further including generating a session key that is transmitted by the security services part (18) of the telecommunications system (16) to the application services part (22) and wherein the transaction manager (14) is operable to transmit the session key in an application request to the application services part (22), and wherein the application services part (22) is operable to compare the session keys prior to proceeding with the transaction, the predetermined authentication information stored by each authentication storage means (12) corresponding to information which is used to authenticate that user's telecommunications handset in relation to the telecommunications system (16) but the authentication process for authenticating the transaction by that user with the data processing apparatus (10) not requiring use of that user's telecommunications handset."

IV. The following prior art document is cited in this decision:

D3: US 6 075 860 A.

V. The examining division found that the introduction of the features:

i) "not requiring use of that user's telecommunications handset nor requiring the telecommunications handset to be actually authenticated",

ii) "telecommunications handset", and
iii) "registrable"

extended the subject-matter of the claims beyond the content of the application as filed (Article 123(2) EPC).

The examining division further found that the method of claim 1 of the main request (as well as that of claim 1 of the auxiliary request 3) differed from the disclosure of document D3 in that in the latter there was no explicit reference to a transaction. The examining division interpreted the term "transaction" on the basis of the application's description as meaning the downloading of data and found that the method of authenticating a user disclosed in D3 would be used by a skilled person for downloading data, i.e. performing a "transaction", without involving an inventive step (reasons, points 5 to 8).

Claim 1 of auxiliary request 8 introduced, in addition to the features of claim 1 of the auxiliary request 3, additional features related to the use of a session key. The examining division considered that these features addressed a second problem, namely controlling and following up a transaction, besides the first problem of authenticating a transaction by a SIM card. The use of session keys, as an identifier to keep open a running session was however a well known principle in Internet programming and general implementation of computer applications in general. No inventive activity could thus be recognized in the agglomeration of the known SIM authentication with the general practice of

generating and using a session key in a commercial communication link (reasons point 10).

VI. The appellant applicant argued essentially as follows:

Undisclosed subject-matter:

– Feature (i): The application explained how a user's handset was authenticated with a telecommunications network using a SIM. In the same way the SIM could be used in or in association with data processing apparatus or a computer so that the same form of authentication process could be carried out - in accordance with the embodiment. Such an embodiment was described in relation to Figure 1, while the authentication process was described in relation to the flow chart of Figure 2. Clearly, the process described on pages 9 and 10 of the specification described an authentication process using the SIM and the data processing apparatus. It was clear that the user’s handset was not involved in this process and that the user’s handset was not authenticated using the authentication information used in the embodiment to authenticate the transaction with the data processing apparatus. Therefore, it was submitted that there was proper basis for the text objected to by the examining division.

– Feature (ii): Basis for the use of the term *"telecommunications handset"* could be found, for example, on page 6 at lines 16 to 29 of the application. Clearly, the handset described there was a telecommunications handset. This was implicit to any person skilled in the art.

Inventive step:

– By specifying that the application services part was separate from the common telecommunications system and was controlled by a third party, the nature of the entities present in the present invention, and the nature of the transaction, was further emphasized and distinguished from that of document D3. The claims were directed to the technical problem of providing improved authentication security for a transaction performed by a data processing apparatus of a user with an application services part of a third party. The solution was to use SIM-type authentication data to authenticate a transaction between a user's data processing apparatus and the application service part without using a mobile terminal, the authentication being performed via a communication link with a telecommunication system having authenticating means. Document D3 was not concerned with authentication of a transaction. D3 used SIM data to establish a secure communication channel between a computer and network server. What happened after establishment of the secure communication channel was not the subject matter of D3. Document D3 was not concerned with the same problem as the present invention and did not disclose the claimed arrangement. The case law required the prior art to actually include a prompt or pointer to the invention to demonstrate lack of inventive step.

Reasons for the Decision

1. The appeal is admissible.

2. *Amendments*

2.1 The present invention relates to a method (claim 1) and a system (claim 13) for authenticating a subsequent transaction between a user and a third party through the use of the security services of a telecommunication system to which the user (or more precisely the user's authentication storage means) is registered. This is achieved by associating authentication storage means (eg a conventional Subscriber Identity Module or SIM) with the user's data processing apparatus (eg a personal computer) and carrying out the authentication process with the telecommunication system through a communication link. The telecommunication system generates after the successful authentication of the SIM a session key which is transmitted to both the user's personal computer and to the third party. The user's personal computer then forwards the session key to the third party together with the transaction's request. Prior to carrying out the transaction, the third party compares both keys, the one received from the telecommunication system and the one forwarded by the user. In this manner the security and authentication infrastructure of the telecommunication system is used and the third party is freed from the task of providing an authentication infrastructure itself.

The corresponding embodiment of the invention is disclosed on pages 9 to 11 and Figures 1 and 2 of the

application. The claims of the request submitted during the oral proceedings before the board are essentially based on the claims of auxiliary request 8 defended before the examining division.

2.2 From the three features objected by the examining division as offending against Article 123(2) EPC only the first two remain in the claim, i.e. the feature of *"not requiring use of that user's mobile terminal"* and *"telecommunications handset"* (in claim 13). The feature *"registrable"* was replaced by *"registered"* as requested by the examining division (reasons, point 1(c)) and the board finds that this objection is now rendered moot.

2.3 It has thus to be assessed whether the feature *"not requiring use of that user's mobile terminal"* is directly and unambiguously derivable from the application as filed.

In fact, the examining division objected to the feature *"not requiring use of that user's telecommunications handset nor requiring the telecommunications handset to be actually authenticated"*. However, the board understands this objection as equally applying to the feature *"not requiring use of that user's mobile terminal"*, since the objection to the feature *"telecommunications handset"* was cast as a separate objection and it appears that the examining division raised the objection of added subject-matter separately for each one of both negations (*"not requiring … nor requiring …"*).

2.3.1 A user's mobile terminal (or a user's handset) using a SIM as authentication storage means can be

authenticated with a mobile or cellular telecommunications network, such as a GSM (Group Special Mobile) or 3G (Third Generation) network. In this authentication process the network sends a challenge to the handset incorporating the SIM, in response to which the SIM calculates a response and transmits it back to the network which checks it against its own information for that user or subscriber in order to complete the authentication process.

According to the application, the SIM can be used in the same way in or in association with the data processing apparatus or computer so that the same form of authentication process can be carried out (page 6, last paragraph). *"In or in association with"* the computer includes the possibility (ie in association with) that the handset is linked to the computer and the authentication process takes place through the handset. The application however clarifies that *"in association with"* foresees the use of a *"dongle"* which allows wired or wireless communication with the personal computer, rendering the use of the handset unnecessary (page 9, 3rd paragraph).

2.3.2 The application thus discloses that the authentication process can be performed without requiring the handset to be used, as it is foreseen to use the SIM in or in association with the personal computer, ie by placing it directly in the computer or in a dongle. The feature *"not requiring use of that user's mobile terminal"* thus does not convey information to the skilled person or even the general reader that is not directly and unambiguously derivable from the application as filed.

Although cast in the negative, this feature is a positive feature of the invention.

2.3.3 The board is for these reasons satisfied that the feature *"not requiring use of that user's mobile terminal"* does not contravene the requirements of Article 123(2) EPC.

2.4 The examining division also objected to the use of the expression *"telecommunications handset"* as not having been disclosed in the application as filed.

2.4.1 The application however discloses on page 6, start of last paragraph, that *"the smart card is a Subscriber Identity Module or SIM of the type used in and for authenticating the user of handsets in a mobile or cellular telecommunications network …"*.

The board considers that a skilled person would directly and unambiguously recognize one of the *"handsets in a mobile or cellular telecommunications network"* as a *"telecommunications handset"*.

2.4.2 The board is thus satisfied that the feature *"telecommunications handset"* does not contravene the requirements of Article 123(2) EPC.

2.5 The amendments made to the description adapt the description to the claims.

3. *Inventive step (Article 56 EPC 1973)*

3.1 Document D3 is considered as the closest prior art document available. It discloses a method and a system

for authenticating an authorized user of a remote terminal 102 (e.g. a portable computer) as an authorized user of a computer network 104. To this effect the remote terminal is coupled to a wireless modem 110 for facilitating a wireless communication channel with the computer network. The authorized user places an authentication card 118 (eg a SIM) containing a mobile subscriber identifier and authenticated encryption keys in a card reader 116 which is operably coupled to the remote terminal. The card reader 116 may be physically integrated into the remote terminal 102 or may be coupled to or integrated with wireless modem 110. To facilitate the authentication process both the authorized user and the network server must possess compatible mobile subscriber identifiers and authentication encryption keys. The network server maintains these values in a resident database, while the authorized user maintains these data on the SIM (abstract; column 3, line 46 to column 4, line 15; column 5, line 56 to column 6, line 41; column 8, lines 20 to 30; Figure 1).

In D3 the computer network 104 can be considered to be equivalent to the telecommunications system 16 of the present application.

After successful completion of the authentication process the authorized user of the remote terminal is recognized as an authorized user of the computer network and allowed access to its resources (eg databases, CPU use, etc).

3.2 The method of claim 1 differs from this conventional method in that

(a) the authentication process is for authenticating a subsequent transaction with an application services part being separate from the telecommunications system and controlled by a third party,

(b) the authentication process generates a session key that is transmitted by the telecommunications system to the third party's application services part,

(c) the session key is also transmitted from the user's data processing apparatus in an application request to the third party's application services part, and in that

(d) the third party compares both session keys prior to proceeding with the transaction.

3.3 The technical problem addressed by these features can be formulated as how to authenticate a transaction between a user and a party without burdening the party with the security infrastructure required for the authentication process.

3.4 The solution proposed by the application consists in using the security and authentication infrastructure already in place of a telecommunication system for authenticating a registered user to that system and allowing a third party to benefit from it. This is achieved by generating a session key after successful authentication and transmitting the session key independently to the user and to the third party, so

that the third party can validate the user's application request by comparing the session key accompanying the request with the one obtained from the telecommunications system.

3.5 The board does not agree with the reasoning of the examining division that the authentication process and the generation of the session key addressed independent technical problems, since all the features identified above under point 3.2 relate directly to the authentication of the transaction between the user and the third party.

3.6 No prior art document discloses to use the security services of a telecommunications system for allowing a third party to authenticate a transaction with one of the users of the telecommunications system. In particular, there is no evidence to the board that session keys – in the sense as understood by the examining division – would be received by the third party via two different and independent routes and that the third party would compare the two session keys prior to validating the transaction.

3.7 The board finds for these reasons that the method of claim 1 involves an inventive step within the meaning of Article 56 EPC 1973.

3.8 The system of claim 13 comprises the third party's application services part, the user's data processing apparatus in combination with the authentication storage means and the common telecommunication system and the capabilities required for implementing the method of claim 1. It involves an inventive step for

the same reasons given in relation to the method of claim 1.

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:

Description, pages:
1-3, 10-11, 22 as filed during oral proceedings,
7 as filed with letter dated 6 April 2005,
4-6, 8-9, 12-21, 23-45 as published.

Claims:
1-21 as filed during oral proceedings.

Drawings:
Sheets 1/12-12/12 as published.

Registrar Chair

S. Sánchez Chiquero G. Eliasson