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 18 September 2013

Case Number: T 0754/09 - 3.5.01

Application Number: 04803857.4

Publication Number: 1697886

IPC: G06Q 10/00

Language of the proceedings: EN

Title of invention:
Systems and methods for enabling anonymous reporting of business activities

Applicant:
SAP AG

Headword:
Anonymous reporting/SAP

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

Keyword:
"Inventive step (no - obvious and non-technical implementations, respectively, of non-technical requirements)"

Decisions cited:
T 0641/00, T 1227/05, T 1784/06

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 0754/09 - 3.5.01

D E C I S I O N
of the Technical Board of Appeal 3.5.01
of 18 September 2013

Appellant: (Applicant)
SAP AG
Dietmar-Hopp-Allee 16
69190 Walldorf (DE)

Representative:
Richardt Patentanwälte GbR
Wilhelmstraße 7
65185 Wiesbaden (DE)

Decision under appeal:
Decision of the Examining Division of the European Patent Office posted 15 December 2008 refusing European patent application No. 04803857.4 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman: S. Wibergh
Members: K. Bumes
P. Schmitz

Summary of Facts and Submissions

I. The appeal is against the decision of the examining division to refuse European patent application No. 04803857.4, entitled "*Systems and methods for enabling anonymous reporting of business activities*", for lack of inventive step (Article 56 EPC 1973).

II. According to the examining division, a technical problem resided only in the computer implementation of an administrative protocol which allowed a user to file a complaint in an anonymous fashion and nevertheless to prove authorship of the complaint at a later stage. Without relying on any prior art document, the technical components for ensuring anonymity (proxy-servers; data encryption) were considered well-known.

The skilled computer programmer or systems analyst would readily implement administrative constraints on a well-known client-server system using straightforward computer programming and data encryption techniques. No surprising or unexpected technical effect derived from this commonplace client-server application to an administrative task.

III. The appellant requests that the decision under appeal be set aside and a patent be granted on the basis of its final main request filed at oral proceedings which the Board held (18 September 2013) according to an auxiliary request.

Claim 1 reads:

"1. A method for submitting a report on a business activity, the method comprising:

receiving, at a first server, from a user device complaint data to identify at least one questioned business activity, wherein the user device is logged onto the first server using first identifying information associated with a user of the user device;

forwarding the complaint data from the first server to a second server, the first server being anonymously logged onto the second server, wherein the first server is a web server and wherein the second server is an application server;

encrypting the complaint data and

providing by the second server a confirmation code to a source of the complaint data to indicate that the complaint data was received by the second server, wherein providing confirmation further comprises providing a key configured to decrypt the encrypted version of the complaint data,

decrypting by the user the encrypted complaint data and verify [sic] that the user is the author of the complaint data."

IV. According to the appellant's submissions in the statement setting out the grounds of appeal, the starting point of the problem-solution analysis should be a prior art document (from the International Search Report, for example) since the examining division's references were not considered as notorious in the sense of the case law (T 1242/04, point 9.2; T 690/06, point 8).

The objective technical problem was how to provide a method of anonymously reporting complaint data such that a later manipulation of the complaint data was effectively prevented. The encryption of complaint data

and the provision of a confirmation message comprising the encryption key were not part of an administrative protocol but of a technical solution which had to be considered as a whole.

V. In an annex to the summons, the Board communicated its preliminary opinion that claim 1 seemed to rephrase requirements dictated by US law (A1, paragraphs 003 to 007). Insofar the claim seemed to define subject-matter in obvious functional terms of a non-technical problem to be solved. Using a decryption key as a confirmation code (based on A1, paragraph 045) seemed to imply only an undisclosed and obvious technical effect (memory saving).

VI. In response to the Board's summons, the appellant emphasised the aspect that a web server was used to pass the complaint data anonymously from an identified (non-anonymous) user device to an application server (embodiment according to A1, Figure 2). The appellant reiterated its analysis of the prior art documents cited in the International Search Report in order to augment its argumentation in favour of an inventive step.

VII. At the oral proceedings held before the Board, the appellant stated that the method according to claim 1 solved two partial problems:
- how to achieve anonymous reporting over a computer-implemented communications network;
- how to provide the anonymous user with a means to prove his/her authorship.

Regarding the first partial problem, the appellant disputed that a server logged anonymously onto another server was notorious prior art.

Regarding the second partial problem, feeding back a decryption key as a confirmation item was a technical feature since the confirmation at the same time enabled the user to verify his/her authorship, thus enhancing efficiency in memory usage, for example. Moreover, encryption was recognised as a technical means for a technical purpose (data security).

As the final paragraph of claim 1 required the verification to be actually carried out, the claim aimed not only at the possession of confirmation information for a potential further use but specified how that single item of information (a decryption key) was used to efficiently implement both a confirmation and a verification means. This approach was not obvious from prior art documents or common general knowledge.

Reasons for the decision

1. The application, filed as international application PCT/EP2004/014234, claims a priority date of 16 December 2003 and was published as

A1: WO-A1-2005/059785.

It relates to systems and methods for enabling anonymous reporting of questionable business activities (A1, paragraph 002), as required by US law enacted on 30 July 2002 (A1, paragraphs 003 to 006). If an anonymous whistle-blower requests protection under that act, he/she has to prove authorship of the reported

complaint (A1, paragraphs 007 and 010).

In its most general aspect, the application proposes an anonymous log-on facility and a feedback procedure for confirming that the complaint data has been received by an application server (A1, original claim 1; Figure 1). In a more specific embodiment (original claim 3; Figure 2), anonymity may be achieved by logging a first server (web server) anonymously onto a second server (application server).

The confirmation may be provided to the user in the form of a complaint code or, as claimed, in the form of a key configured to decrypt an encrypted version of the complaint data. The user may use the decryption key at a later stage to verify his/her authorship of the complaint data (A1, paragraphs 044/045; original claims 13 and 14).

Article 56 EPC 1973 - Inventive step

2. The Board does not set out from a server architecture already comprising an anonymous log-on feature but from a general network of servers, which was undoubtedly well-known to everybody working in the field of computers. No documentary evidence is required to prove the existence of such a basic computer architecture.

3. In the light of Article 52(1)(2)(3) EPC, Article 56 EPC 1973 requires a non-obvious technical contribution (see e.g. T 641/00-*Two identities/COMVIK*, OJ EPO 2003, 352; T 1784/06-*Classification method/COMPTEL*).

Non-technical constraints, such as legal requirements, cannot contribute to an inventive step and, thus, do

not have to be proven to be known. In any case, the present application (A1, paragraph 003) states that the requirements of the *Sarbanes-Oxley Act* (US legislation) existed on 30 July 2002, i.e. before the priority date claimed by the application.

4. The application addresses the following non-technical requirements.

4.1 Anonymous, confidential reporting of questionable business activities should be enabled (A1, paragraphs 002 to 005).

4.2 If an anonymous user ("whistle-blower") requests protection under said US law, he/she has to prove authorship of the reported complaint (A1, paragraph 007).

5. Regarding the non-technical requirements, the technical problem to be solved (and, thus, the examination for an inventive step) relates only to their implementation.

In the Board's judgement, the implementation --- as far as disclosed at all --- relies on obvious technical considerations of a skilled person.

5.1 Where an anonymous data transfer is required, it is self-evident that at least one link in the communication chain must work in an anonymous manner. Claim 1 (paragraph 3) specifies that the anonymising function is provided between the first server and the second server (Figure 2 of A1) but the application does not mention any advantage of choosing that particular place. Nor does it disclose any technical detail for

achieving the desired anonymous log-on (the "*default user*" according to paragraph 0043 is apparently only a predetermined pseudonym) or for overcoming any particular technical problem in doing so.

5.2 Regarding the requirement of confidentiality, the general idea of encrypting the complaint data (paragraph 4 of claim 1) constitutes a notorious approach for protecting data content from unauthorised third parties who might have access to a transmission channel.

Claim 1 (and the application as a whole) fails to specify a non-obvious use of encryption.

5.3 The method of claim 1 (final two paragraphs) enables a proof that the user has transmitted specific data:

(a) the receiver of the complaint data (i.e. the second server) feeds back a confirmation code to the source of the data;

(b) the user's authorship is verified by checking that the confirmation code works as a key to decrypt an encrypted version of the complaint data.

Providing confirmation feedback from the receiver to the sender is a general aspect of usual acknowledgements of receipt. The application presents confirmations in the form of a decryption key or in the form of a code or number as largely equivalent means of proof (A1, paragraphs 010, 039, 041, 044, 045).

Decryption is a mathematical method which serves a technical purpose in a technical system where cryptography is used for data security.

However, in claim 1, the decryption operation is used for proving the authorship of a document, which is a non-technical, legal problem. Therefore, the intrinsically non-technical, mathematical method of decryption cannot derive a technical character from the problem solved (T 1227/05-*Circuit simulation/INFINEON*, point 3.1, OJ EPO 2007, 574). Thus, providing and using the decryption key for fulfilling a legal verification task does not enter into the examination for an inventive step.

5.4 A synergistic technical effect put forward in the appeal procedure relates to a saving of memory which might be achieved (at an undefined place in the system) as the decryption key is also used as a confirmation feedback to the whistleblower.

The Board notes that the application as filed does not address any memory saving and does not set out any circumstances in which such a saving might be actually achieved. Thus this alleged, undisclosed advantage cannot be considered for inventive step.

6. Therefore, the Board judges that the method of claim 1 does not involve an inventive step (Article 56 EPC 1973).

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

T. Buschek S. Wibergh