Internal distribution code:

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

Datasheet for the decision of 19 November 2013

Case Number: T 1035/08 - 3.5.01

Application Number: 02721194.5

Publication Number: 1400053

IPC: G06Q20/00

Language of the proceedings: EN

Title of invention:
DISTRIBUTED QUANTUM ENCRYPTED PATTERN GENERATION AND SCORING

Applicant:
VISA INTERNATIONAL SERVICE ASSOCIATION

Headword:
Distributed risk analysis/VISA

Relevant legal provisions:
EPC Art. 84, 56

Keyword:
Clarity - processing on encrypted data, risk analysis (no)
Inventive step - distributed risk analysis (no - business method with no apparent inventive implementation)

Decisions cited:

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Case Number: T 1035/08 - 3.5.01

D E C I S I O N
of Technical Board of Appeal 3.5.01
of 19 November 2013

Appellant: (Applicant)	VISA INTERNATIONAL SERVICE ASSOCIATION 900 Metro Center Boulevard Foster City, CA 94404 (US)
Representative:	Eisenführ, Speiser Patentanwälte Rechtsanwälte PartGmbB Johannes-Brahms-Platz 1 20355 Hamburg (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 15 January 2008 refusing European patent application No. 02721194.5 pursuant to Article 97(1) EPC 1973.**

Composition of the Board:

Chairman: S. Wibergh
Members: W. Chandler
P. Schmitz

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division to refuse the European patent application No. 02721194.5. It concerns a method of assessing financial fraud.

II. The examining division decided that claim 1 of the sole request did not involve an inventive step because it was essentially a mere automation, using notorious computer hardware, of an administrative method, namely assessing the risk of a financial transaction.

III. In the statement of grounds of appeal, the appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the claims filed on 10 September 2007, i.e. the refused request. An auxiliary request was to remit the case to the examining division with the same claims. The appellant also requested oral proceedings.

IV. In the communication accompanying the summons to oral proceedings, the Board tended to agree with the examining division's reasons and pointed out additional problems under Article 84. Moreover, since it was not apparent how the fraud risk was assessed from the encrypted data or exactly how this processing was distributed between the client and the server, there was a possible objection under Article 83 EPC.

V. In the reply, the appellant gave no arguments and stated that it did not intend to attend the oral proceedings.

VI. At the oral proceedings, held in the appellant's absence, the Board deliberated and decided on the above-mentioned requests.

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

"A method of assessing a financial fraud risk within a distributed client/server system, said method comprising:
receiving (702) first and second financial transactions from transactional information sources at a central computer system;
generating (710) first features for said first financial transaction at said central computer system;
generating (710) second features for said second financial transaction at said central computer system;
determining (718) feature changes between said first features and said second features at said central computer system;
encrypting (730) said feature changes at said central computer system;
transmitting (734) said encrypted feature changes from said central computer system to a client computer system and storing said encrypted feature changes in a local key database;
receiving (806) a local, current financial transaction at a client computer system;
encrypting (810) said current transaction at said client computer system;
generating (810) local features from said encrypted current transaction at said client computer system;
applying (814) said local features to said local key database and determining whether an alert has resulted, said local key database being in communication with a key engine; and

performing (818) a risk analysis for said local, current transaction by said key engine so as to produce a risk score, whereby the risk associated with said current financial transaction is assessed in a distributed manner."

Reasons for the Decision

1. The appellant explained the invention as follows:

Prior art fraud detection systems attempted to detect fraud by processing transactional data at a central server. Additional data, located at the source of the transaction ("at-source" data), was not normally transmitted to the central server for processing and thus a complete risk assessment could not be performed. In other words, performing risk scoring at a single, central location generally did not enable all of the available detail regarding that transaction to be included in the risk assessment.

For example, if a central scoring location received transactional data indicating a $5,000 purchase of computer equipment, there was no additional data received indicating whether a single item was purchased or whether five $1,000 computers were purchased (even though the purchase of five computers would be considered riskier). Other examples of at-source data that were typically not sent to a central location to be included in a risk assessment included Web browser information, a TCP/IP address, an e-mail address, server information, etc. The question was then how to include this remote, at-source data, in the assessment of risk of a financial transaction.

One solution might have been to send all at-source data from the remote locations to a central server for processing. This approach was the one that a skilled person would most likely have pursued. However, this approach was problematical in that it could be difficult to arrange for all the data to be transmitted centrally, the types of data could change thus requiring the central server to adapt to new data fields, and data privacy issues could emerge when sensitive information was being sent to a central site over a network.

The invention was based on the realisation that the best way to solve this problem was to perform processing and scoring of the transactional data both centrally and on local client computers. Because additional at-source information (that might be sensitive) was now being used at distributed locations to assess risk (and because certain information would be sent from a central location to a distributed location), the data was encrypted and *processing was performed on the encrypted data*, thus eliminating the possibility of releasing sensitive information. It was further realised that because the data was being processed both centrally and at distributed client locations, *novel techniques for processing the data* could be used. It was through a combination of these techniques that the presently claimed invention addressed the technical problem posed.

For example, claim 1 required that the first and second financial transactions were received at a central computer system. These transactions represented a financial transaction for a particular account and a previous transaction for that account. Features were generated for each transaction and the changes between

these features were then determined at the central server. The use of features (or characteristic variables) was a known technique of assessing risk based upon sets of data. Before these feature changes were transmitted to a client computer system for further processing they were encrypted to prevent the release of a any sensitive information.

2. In the light of this explanation, the only potentially novel parts of the invention appear to be the ideas of a distributed determination of the risk, encrypting the feature changes and sending them to the client and determining the risk from encrypted data. Indeed this is confirmed by the appellant's formulation of the alleged technical problem as "how to use at-source type data in the calculations in a secure manner and in a distributed system".

3. However, as the Board set out in its communication, it is not clear from claim 1 how this problem is solved. In particular, the claim gives only a functional specification, but no details of how the processing is performed on the encrypted data or any details of the other "novel techniques" referred to above. Similarly, it is not clear from the penultimate feature how the local features are "applied" to the encrypted feature changes from the central computer system stored in the local key database. It is also not clear what the "alert" represents, or how it is subsequently used in the process. Finally, it is not clear - not even from the application as a whole - how a risk analysis of the last feature can be performed from this data. The appellant did not provide any explanation of these features and did not attend the oral proceedings. Consequently, the Board has no reason to change its

view. Accordingly, claim 1 is not clear (Article 84 EPC).

4. Moreover, these unclarities give all the more weight to the examining division's conclusion that the description does not indicate what specific technical problems might arise that would require an inventive step to overcome.

5. Thus, the Board cannot see any prejudicial error in the examining division's conclusion that the subject-matter of the invention does not involve an inventive step (Article 56 EPC 1973). In particular, that "financial transactions" have no technical character as they are clearly part of a method of doing business, which is excluded. The same goes for the object of the claim, namely assessing financial fraud risk. It is agreed that the computer system and the encryption function are technical, but notorious.

6. The appellant synthesises the effect of the remaining features into the above-mentioned alleged technical problem of "how to use at-source type data in the calculations in a secure manner and in a distributed system". However, in the Board's judgement, this is still not a technical problem because "the calculations" referred to simply relate to deriving the non-technical risk assessment. Put another way, the invention seems to stop short at deriving financial information without being part of any technical process.

7. The appellant highlights three dangers of determining whether a claimed feature has technical character or not, namely acontextual assessment, isolated assessment, and prejudicial triggering. The Board

agrees to some extent with these comments, but cannot agree that any of these have played a role in the decision under appeal.

8. As an example of the latter, the appellant gave an analogy with the invention of a telephone. If the telephone were invented today and claimed as a "method of communication between remote users", there would be no discussion of technical versus non-technical features. On the other hand, if it were claimed as "a method of communication between business persons", there would be an analysis of the technical character of the features and the claim would be at risk. This would be wrong since the invention was the same in both cases, the latter in fact defining those using the invention more narrowly. However, in the Board's view, apart from the fact that it is hard to imagine how a telephone could be claimed as a “method of communication”, the analogy does not seem to hold because if the method involved inventive technical considerations, it would still be good if the business persons were omitted. In contrast, the present invention does not seem to have any point if not in connection with risk assessment.

9. Accordingly, starting from common general knowledge, as the examining division did, the subject matter claimed is also not inventive (Article 56 EPC 1973).

10. As the request is not allowable, there is no reason to remit the case to the examining division to consider the further cited documents, so that the appeal must be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

T. Buschek S. Wibergh

Decision electronically authenticated