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 February 2014

Case Number:	T 0913/10 - 3.5.06
Application Number:	01981819.4
Publication Number:	1374063
IPC:	G06F12/14
Language of the proceedings:	EN

Title of invention:
METHOD AND APPARATUS FOR AUTOMATIC DATABASE ENCRYPTION

Applicant:
Oracle International Corporation

Headword:
Distinct administrator roles/ORACLE

Relevant legal provisions:
EPC 1973 Art. 56
RPBA Art. 13(1)

Keyword:
Inventive step - (no)
Late-filed request - admitted (no)

Decisions cited:
T 0641/00

Catchword:

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

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 0913/10 - 3.5.06

DECISION
of Technical Board of Appeal 3.5.06
of 19 February 2014

Appellant: Oracle International Corporation
(Applicant)
500 Oracle Parkway
Redwood Shores, CA 94065 (US)

Representative: Davies, Simon Robert
D Young & Co LLP
120 Holborn
London, EC1N 2DY (GB)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted on 4 December 2009 refusing European patent application No. 01981819.4 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman: D. Rees
Members: M. Müller
W. Sekretaruk

Summary of Facts and Submissions

I. The appeal lies against the decision of the examining division, with written reasons dispatched on 4 December 2009, to refuse the European patent application no. 01981819.4 for lack of an inventive step in view of the document

D2: WO97/49211.

II. An appeal was lodged on 13 January 2010 and the appeal fee was paid the following day. A statement of grounds of appeal was filed on 7 April 2010. It was requested that the decision under appeal be set aside and a patent be granted based on the main or the auxiliary request as subject to the decision.

III. With a summons to oral proceedings, the board addressed the question of how the terminology in the claims had to be construed, especially as regards the term "role". The board expressed the opinion that one common use of the term "role" in the field of databases related to "responsibilities and privileges in an organisation without implying any implementation or implementation support by or in a computing system" (see point 5.2). On request by the appellant the board provided two documents to establish this opinion, *inter alia*

D3: Cox T B, "White Paper: The role of the database administrator", ComputerWeekly.com, 12 March 2000.

Based on its favoured interpretation, the board further expressed its tendency to confirm the finding of the decision that the claimed matter lacked an inventive step over D2, Article 56 EPC 1973. The board also raised an objection under Article 123 (2) EPC against both requests.

IV. In response to the summons, the appellant filed four new sets of claims as new main and 1st to 3rd auxiliary requests while maintaining the previous two requests as 4th and 5th auxiliary requests. The appellant also filed a statement by the inventor Rick Wessman regarding the skilled person's understanding of the term "role" as used in the application.

V. During oral proceedings, after the main and the first auxiliary had been discussed, the appellant withdrew the 2nd to 5th auxiliary requests and filed the further auxiliary request to grant a patent based on claim 4 of the 1st auxiliary request.

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

"A method for managing encryption within a database system that is managed by a database administrator, wherein encryption is performed automatically and transparently to a user of the database system, wherein users of the database system are managed by a user administrator, the method comprising:

receiving a request to store data in a column (226) of a database (118) in the database system, wherein the column is designated as an encrypted column;

in response to receiving the request, automatically encrypting data using an encryption function (204), wherein the encryption function uses a key stored in a keyfile (120) managed by a security administrator, said keyfile containing keys and corresponding key identifiers for encrypting and decrypting data, wherein the keyfile is stored as an encrypted file in the database system; and storing data in the database using a storage function (208) of the database system;

wherein the key identifier associated with the encrypted column is stored within the database as metadata (222) associated with a table (218) containing the encrypted column; and

wherein the security administrator, the database administrator, and the user administrator are distinct roles within the database system."

Claim 1 of the 1st auxiliary request corresponds to claim 2 of the main request, *i.e.* to claim 1 of the main request with the addition of the following text:

"... the method further comprising:

receiving a request to retrieve data from the encrypted column of the database system:

if the request to retrieve data is received from the database administrator, preventing the database administrator from decrypting encrypted data;

if the request to retrieve data is received from the security administrator, preventing the security administrator from decrypting encrypted data;

if the request to retrieve data is received from an authorized user of the database system, allowing the authorized user to decrypt encrypted data."

Claim 1 of the further request coincides with claim 1 of the 1st auxiliary request to which are added the additional features of claims 3 and 4 which read as follows:

"3. The method of claim 1, wherein managing the keyfile includes:

creating the keyfile;

establishing a plurality of keys to be stored in the keyfile;

establishing a relationship between a key identifier and the key stored in the keyfile;

storing the keyfile in an encrypted file in the database system; and

moving an obfuscated copy (116) of the keyfile to a volatile memory within a server associated with the database system.

4. The method of claim 3, further comprising establishing encryption parameters for the encrypted column, wherein the encryption parameters include encryption mode, key length, and integrity type, by:

entering encryption parameters for the encrypted column manually; and

recovering encryption parameters for the encrypted column from a profile table in the database system."

The main and 1st auxiliary requests contain an apparatus claim corresponding closely with the respective independent method claim 1. As regards the further auxiliary request, the exact wording of all claims other than claim 1 was left open, pending the board's decision about its admissibility.

VII. At the end of the oral proceedings, the chairman announced the board's decision.

Reasons for the Decision

The invention

1. The application generally relates to the security of database systems. More specifically, it is concerned

with measures to protect data stored in a database against unauthorized access while securing the possibility for the database administrator (DBA) to maintain the database.

1.1 According to the application it was known in the art to encrypt and decrypt sensitive data at the user's end and to store only encrypted data in the database. This made it impossible for a malevolent DBA to access the sensitive data in plain text but required that user applications had to be able to encrypt and decrypt information (see original application, p. 2, 2nd par.).

1.2 The application proposes to manage encryption within the database but to split the database administration tasks over different administrators so that access to sensitive data by any of them can be prevented.

1.3 Specifically, the application refers to a "database administrator" (DBA), a "security administrator", and a "user administrator" (henceforth: SA and UA), and illustrates their responsibilities in broad terms and by example: The DBA may be "performing services such as data backup, data recovery, storage allocation, and the like", the SA "manages the encryption system" which "encryption includes, but is not limited to managing [a] keyfile and specifying which columns of tables in [the] database ... are encrypted", and the UA "grants privileges to user[s] ... for accessing [the] database" (p. 5, lines 23-30).

1.4 The application discloses that "within the database system" the three administrators "are distinct roles" and that "[a] person selected for any one of these roles may not be selected to perform any of the other roles". Figure 1 of the application which, according to the description (p. 5, lines 7-8) illustrates a database system according to an embodiment of the invention depicts the three administrators with people icons. The application proposes that the three administrators "are not authorized users and, therefore, are prevented from decrypting and receiving encrypted data stored within the database" (p. 10, lines 6-9).

1.5 The application further discloses that the database contains metadata storing encryption parameters which include, *inter alia*, key identifiers referring to the key with which individual database columns are encrypted. The keys themselves and their key identifiers are held in a keyfile. According to figure 1 the keyfile is part of the database system but accessible from the database server and separate from the database.

The prior art

2. Document D2 discloses a database system comprising several databases, especially one called O-DB storing the actual data records in encrypted form and one called IAM-DB storing what is called a "data element protection catalogue". In the O-DB, every data element is linked to a data element type - the column of a database (see the table on p. 5) - and the IAM-DB contains, for each individual such type, "one or more protection attributes" which "state rules of how to process the corresponding data element values", especially when "a user wants to read a certain data element", notably an "authorised" one (p. 4, lines 1-13; p. 5, line 29 - p. 6, line 16, p. 10, lines 3-8 and 15-32). For instance, the IAM-DB may define the "degree of encryption" for individual data elements (p. 14, line 21 - p. 15, line 12). It is also disclosed that the data element protection catalogue may make "callings to information stored

in some other place" (see p. 5, lines 8-12). It is disclosed that the data element protection catalogue may itself be encrypted (see p. 7, lines 23-25) and it is further disclosed that the IAM-DB may only be accessed by an "authorised IAM operator", "i.e. a person responsible for security", and that O-DB and IAM-DB are preferably physically separated from each other (p. 10, lines 20-26, p. 20, lines 26-28).

The decision under appeal and the central contentious issue

3. The decision under appeal found that D2 disclosed all features of the then claimed matter except two (reasons 2.2). One of them related to a "message digest" which is no longer contained in any of the present independent claims and therefore not pertinent for this appeal. Regarding the other, the decision stated that D2 did not disclose "that all administrators are persons having not interchangeable roles" but it was found that this feature "is not of a technical nature" and that "[t]he distribution of roles to persons does not involve any technical consideration" and does not imply any "security consideration in the sense of a technical secure machine" (reasons 2.4).

3.1 In their analysis of D2, the examining division had made reference to "the program driving the database O-DB and processing requests from users" to establish that D2 disclosed the database administrator (see decision, reasons 1.1, lines 2-3). The appellant argued that the decision was incorrect in equating the "database administrator" of claim 1 with a *program* (see *e.g.* grounds of appeal, point 5.1; see also the statement of Rick Wessman, penult. par.) and inconsistent for, at the same time, interpreting the security administrator as a *person* (point 5.3).

3.2 During oral proceedings the appellant conceded that the allocation of people to "roles" within the database system might be considered a non-technical activity but insisted that roles were not persons but system-defined and that this implied that "roles [were] of a technical nature" (see *e.g.* grounds of appeal, points 6 and 6.2).

3.3 Independent of what precisely the examining division may have had in mind when relating the claimed DBA to a program it is clear that the decision turns on what the correct interpretation of the terms "role" and "administrator" in the claims and in view of the application as a whole is. The board agrees with the decision that the inventive step assessment of the claimed invention depends on this question. In the following, hence, the board will address this question first.

Construction of the claims

4. The board tends to agree with the appellant (see grounds of appeal, points 2-3) that the term "role" is used, in the context of computing systems such as operating or database systems, to denote a set of privileges or permissions which can be allocated to one or more users. For example, in operating systems it is known to have a privileged administrator role and a less-privileged user role. The appellant refers to this as the "conventional two-level hierarchy" (see grounds of appeal, e.g. point 8).

5. However, the board is of the opinion that there are other possible and reasonable interpretations of this term in the relevant technical field. Specifically, the term "role" is also used to describe privileges and responsibilities *in an organisation*. Hence, the term

role as such also does not imply any system support by or in a computing system, let alone any specific such support. For instance an IT expert may, as part of his job, take over the responsibility for database administration in a company and, in this sense, the "role" of database administrator, or this administrator role may rotate amongst staff of the IT department. D3 supports this view by stating, in its first substantial paragraph, that "[t]he DBA role naturally divides into three major activities: ongoing maintenance of production databases, ..., planning, design, and development of new databases applications, or major changes to existing applications, ... and management of an organisation's data and metadata. One person may perform all three roles, but each is profoundly different".

5.1 The appellant concedes that the term "role" may be overloaded but insists that the invention clearly involves system support for the three administrator roles" (see the statement of Rick Wessman, 3rd and 5th pars.). In an attempt to establish this, the claims now state that the three administrators "are distinct roles within the database system".

5.2 At least as regards the main request, the board is not convinced that this language excludes the possibility of construing the administrator roles as referring to persons separate from the computing system, in view of the fact that figure 1 of the application depicts the administrators as persons and as part of the database system. Claim 1 of the 1st auxiliary request specifies that a request to retrieve data is not granted if it is received from "the database administrator" or "the security administrator". For the purpose of this decision the board accepts that the skilled person would read this as implying that the DBA and the SA have "computer identities" different from each other and from other users which the system can identify and distinguish. For the sake of argument, the board also accepts this understanding for claim 1 of the main request.

6. Beyond that, however, the independent claims remain vague.

6.1 They specify that the database system "is managed by" a DBA, that the users "are managed by" a UA, and that the keyfile "is managed by" a SA without specifying exactly what this "managing" implies. The claims however leave undefined not only the powers of the individual administrators, but also - and in particular - the limits of these powers.

6.2 The appellant argues that the privileges granted to the SA are taken away from the DBA. The skilled person would understand this from the conventional meaning of roles in database systems. Specifying this explicitly would require a "negative limitation" which was "generally regarded as undesirable" by the EPO, as expressed in the Guidelines for Examination C-III 4.20, and it would be "pointless" - in view of the security problem addressed by the application - "to define separate roles within the system ... and then to give [one] all the privileges of the [other]" (see grounds of appeal, point 9.6).

6.3 The board disagrees with these arguments. Firstly, it is noted that overlapping privileges are not excluded by the existence of different system-defined roles: For instance the conventionally known system administrator has strictly more privileges than an ordinary user. Secondly, the cited section in the Guidelines - apart from the fact that they do not bind the boards - does not express an outright prohibition of negative limitations but allows them under certain conditions. Thirdly, the board disagrees that having overlapping roles would be "pointless": For example, management of the security features of a system might be given to an SA so as to relieve the DBA from this part of the work without requiring the DBA to give up this responsibility entirely. The SA role might thus serve to manage the workload without any intended security gain.

6.4 Finally, even the security concern does not, in the board's view, make entirely pointless a separation of responsibilities without system enforcement. For instance, information or access rights may be spread over different people with the obligation not to share them under a threat of disciplinary sanctions in case of a breach of these obligations, but compliance with these obligations may not be enforced by the system. Still short of enforcing the obligations, the system might automatically remind users about the limits of their rights and/or log user's actions so as to be able to prove any misconduct that may have happened.

7. In view of the foregoing the board adopts the interpretation that the three administrators as claimed are defined by the different sets of tasks they have to perform and the administrator *roles* correspond to some kind of distinguishable computer identities. The precise scope of the sets of tasks is not defined or whether different sets of tasks overlap with each other, nor is it claimed how it may be enforced, if at all, that no administrator exceeds its competences.

7.1 The board dismisses the appellant's suggestion that these terms must be interpreted in a more limited way based on a conventional use of the term in the art, stressing that the interpretation of the claims must be based on what is explicitly or implicitly disclosed in the application but cannot take into account what is merely obvious for the skilled person when reading the claims or the application.

7.2 Under these circumstances the board concludes that nothing in the claims or in the description can dispel the reasonable possibility that the definition of tasks to be distributed over three administrators is merely an organisational and hence non-technical issue, notwithstanding that it relates to a technical entity such as a database system, and that the claims must hence be assessed further based on this interpretation.

Inventive step, Article 56 EPC 1973

Main request

8. The system of D2 allows the identification of at least an "authorized IAM operator" and "authorized users" (see p. 10, lines 7 and 25). No further operators or users are explicitly disclosed (difference 1). The IAM operator is "responsible for security" and in particular the IAM-DB containing the data element protection catalogue. D2 does not mention a key list, what it might contain or where it might be stored. Especially, D2 does not disclose that the data element protection catalogue contains or relates to the keys used for decryption of the user data (difference 2).

8.1 Regarding the latter, difference 2, the board considers that decryption is a necessary part of the processing required when a user requests to access an encrypted data element. Moreover, it is an obviously security-related operation. Noting further that the data element protection catalogue defines the "degree of encryption" (see p. 14, line 26), the board deems it obvious as a matter of data organisation that the decryption keys are held in a keyfile in the database system which is contained in or accessible through the data element protection catalogue. The board considers it obvious, too, that the data element types refer to the keys by reference and hence that "key identifier[s]" are used and appear in the keyfile. Finally, encryption of a keyfile is considered obvious from the disclosure that the data element protection catalogue may be encrypted as a whole.

8.2 Regarding the former, difference 1, the board notes that according to established jurisprudence of the boards of appeal, where the claim refers to an aim to be achieved in a non-technical field, this aim may legitimately appear in the formulation of the problem as part of the framework of the technical problem that is to be solved, in particular as a constraint that has to be met (see T 641/00, OJ EPO 2003, 352; headnote 2, 2nd sentence). The board thus considers that the objective technical problem addressed by difference 1 is to modify D2 so as to support the distribution of tasks amongst the DBA ("manage the database system"), the SA ("manage the keyfile") and the UA ("manage the users").

8.3 The appellant argued during oral proceedings that the required distinction between three administrator roles were incompatible with the system of D2. Since all processing of accessed user data had to be processed according to the data element protection catalogue under the control of the IAM operator, it would be impossible to prevent the IAM operator from accessing sensitive user data (as explicitly required by the independent claims of the auxiliary request). The appellant also suggested that user management had to be construed as part of the data element protection according to D2 and could not easily be defined as a separate responsibility within the system of D2.

8.4 The board disagrees. The determination of whether a user - or, indeed, the IAM operator - is authorized precedes any data access and is thus naturally independent of any data element protection. Also, an authorized IAM operator managing the data element protection catalogue is not automatically an authorized user which would as such be allowed to access the data elements.

8.5 If the IAM operator of D2, as being the obvious "responsible" for a "keyfile", is identified with the required SA, this boils down to the requirement of having additional roles for the database management (beyond security issues, *e.g.* as regards the O-DB) and for user management. Since D2 can already distinguish between users and the IAM operator, the board deems that it would have been straightforward for the skilled person to add support for the identification of further "administrators" as required.

8.6 Therefore, the board comes to the conclusion that the subject matter of claim 1 according to the main request is an obvious implementation of an organisational requirement within the system of D2 and thus lacks an inventive step in the sense of Article 56 EPC 1973.

1st auxiliary request

9. The independent claims of the auxiliary request make reference to a request to retrieve data from an encrypted column and specify that this request is granted in that decryption of the encrypted data is allowed if the

request is from an authorized user but prevented if it is from "the database administrator" or the "security administrator".

9.1 The primary effect of these features is to make sure that data is only decrypted by the pertinent authorized user which, *per se*, the board deems to be known from D2 (see p. 10, lines 3-8) but which is also obvious from the nature and purpose of encryption.

9.2 The system of D2 is capable of distinguishing between an authorized IAM operator and authorized users. While it is not disclosed in D2 how this distinction is made it would be an obvious option, in the board's view, to implement the IAM operator as a special "user" with the required privileges. Moreover, the board considers it obvious that all three administrators required by the above problem are mapped to different users within the system of D2. In the board's view it would be an obvious option not to give authorization to these special users to read individual users' data if it were desired to prevent them to read such data.

9.3 The board therefore concludes that also claim 1 of the 1st auxiliary request lacks an inventive step over D2, Article 56 EPC 1973.

<u>The further auxiliary request</u>

10. Article 13 (1) RPBA gives the board discretion not to admit any amendment to a party's case after it has filed its grounds of appeal, in view of *inter alia* the complexity of the new subject-matter, the current state of the proceedings and the need for procedural economy.

10.1 The further auxiliary request was not only filed after the grounds of appeal but indeed after several hours of discussions about the main and 1st auxiliary request during the oral proceedings.

10.2 The incorporation of the additional features of claims 3 and 4 into claim 1 of the 1st auxiliary request is meant to specify in more detail the tasks of the SA and thus to clarify the intended meaning of "managing the keyfile". The board appreciates that this means to address the board's concern that the precise responsibilities of the SA were not defined in the independent claims of the other requests (see above point 6.1).

10.3 However, the additional features only specify the tasks of the SA in positive terms but neither implies any limitation of the powers of the DBA nor any system support for enforcing the distribution of tasks between amongst the administrators (see also point 6.1). *Prima facie* at least the amendment is thus insufficient to change the board's interpretation that the claims do not imply such system support (see point 7) and hence to change the board's position on inventive step in this respect.

10.4 Since D2 does not disclose a keyfile, let alone its processing, the additional features appear not to be known from D2. It is *a priori* possible that at least some of these features, separately or in combination, might be found to establish an inventive step over D2 alone, even though this point was not specifically argued by the appellant. Even if so, however, it would *prima facie* appear this would have to be for reasons substantially different from those that were discussed during the appeal proceedings up to this point. Moreover, even if it were found that the amended claim was inventive over D2 alone, it would then become necessary to consider the available prior art documents other than D2. Thus, the further request constitutes a substantial change of the appellant's case which, if admitted, would raise questions which the board deems to be inappropriately complex at this late stage of the procedure.

10.5 Thus the board exercises its discretion under Articles 13 (1) RPBA and does not admit the further auxiliary request.

11. There being no admissible and allowable request, the appeal has to be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

Beschwerdekammern des Europäischen Patentamts ✦ Boards of Appeal of the European Patent Office ✦ Chambres de recours de l'Office européen des brevets

S. Sánchez Chiquero D. Rees

Decision electronically authenticated