Internal distribution code:

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

Datasheet for the decision of 2 August 2016

Case Number: T 0899/11 - 3.5.06

Application Number: 05101068.4

Publication Number: 1586976

IPC: G06F1/00

Language of the proceedings: EN

Title of invention:
Distributed dynamic security for document collaboration

Applicant:
Oracle International Corporation

Headword:
Security for document collaboration/ORACLE

Relevant legal provisions:
EPC 1973 Art. 56

Keyword:
Inventive step - main request (no) - auxiliary request (yes) background art in a document potential starting point for the inventive-step assessment even in view of its disadvantages

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 0899/11 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 2 August 2016

Appellant: (Applicant)	Oracle International Corporation 500 Oracle Parkway, M/S 5 op 7 Redwood Shores, CA 94065 (US)
Representative:	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 22 November 2010 refusing European patent application No. 05101068.4 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Sekretaruk
Members:	M. Müller
	S. Krischer

Summary of Facts and Submissions

I. The appeal lies against the decision of the examining division, with reasons dispatched on 22 November 2010, to refuse European patent application No. 05 101 068.4 for lack of compliance with Article 123(2) EPC. In an *obiter dictum* section the decision gave reasons why the claimed invention lacked inventive step over

D1: US 5 787 175 A.

II. Notice of appeal was filed on 31 January 2011, the appeal fee being paid on the same day. A statement of grounds of appeal was filed on 15 March 2011. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the documents on file.

III. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that the claimed invention lacked inventive step over D1, Article 56 EPC 1973.

IV. In response to the summons, with a letter dated 1 July 2016 the appellant filed amended claims 1-21 and 1-19 according to a main request and an auxiliary request, respectively.

V. Oral proceedings were held on 2 August 2016, during which the appellant filed amended claims 1-17 and amended description pages 6, 7 and 15 according to a "2nd aux request", and withdrew the pending auxiliary request. It requested, as a main request, that a patent be granted on the basis of claims 1-21 as filed with letter of 1 July 2016 or, as the only auxiliary request, on the basis of claims 1-17 labelled "2nd aux

request" as filed on 2 August 2016 and the following further application documents:

description, pages
1, 2 as filed on 25 September 2007,
6, 7, 15 as filed on 2 August 2016,
3-5, 8-14, 16, 17 as originally filed, and
drawings, sheets
1/3-3/3 as originally filed.

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

"A computer-implemented method for managing security associated with document collaboration, comprising

associating collaborators with different encrypted versions of a symmetric key, wherein decrypted versions of the symmetric key permit access to a document, and

using an identity service as one of the collaborators, to interact with documents and collaborators and manage document access and security,

characterized in that the identity service is added as one of the collaborators, and performs the steps of;

identifying (210) a collaborator associated with a document, when the collaborator lacks an encrypted version of a symmetric key needed to access the documents or lacks a proper key needed to decrypt that symmetric key;

verifying (220) that a community list associated with the document, and the collaborator, permits the collaborator to enter into a dynamic trusted relationship between the collaborator and the document, and in response to the verifying;

acquiring (230) a dynamic public key from or on behalf of the collaborator;

decrypting (240) the symmetric key which grants access to the document by the identity service using its own private key-public key pair; and

encrypting (250) the symmetric key with the dynamic public key."

The main request also contains an independent system claim 13, the wording of which is immaterial for this decision.

Claim 1 of the auxiliary request reads as follows:

"A computer-implemented method for managing security associated with document collaboration, comprising:

maintaining a list of collaborators, including an identity for each collaborator,

associating the collaborators on the list with different encrypted versions of a symmetric key, wherein each collaborator's version of the symmetric key is encrypted with the public key for that particular collaborator, wherein decrypted versions of the symmetric key permit access to a document, and wherein the list of collaborator identities and their associated encrypted versions of the symmetric key is embedded within or linked or indexed to the document,

using an identity service as one of the collaborators, to interact with documents, collaborators and lists of collaborators to manage document access and security,

characterized in that the identity service is added as one of the collaborators for the document and is identified in the list of collaborators for the document, and performs the steps of;

identifying (210) a collaborator associated with a document, when the collaborator lacks an encrypted version of a symmetric key needed to access the

documents or lacks a proper key needed to decrypt that symmetric key;

verifying (220) that a community list associated with the document, and the collaborator, permits the collaborator to enter into a dynamic trusted relationship between the collaborator and the document, and in response to the verifying,

acquiring (230) a dynamic public key from or on behalf of the collaborator;

decrypting (240) the encrypted version of the symmetric key which grants access to the document by the identity service using its own private key-public key pair; and

wherein once the identity service has the decrypted symmetric key, it re-encrypts (250) the symmetric key with the collaborator's newly provided dynamic public key;

wherein the identity service notifies the collaborator that it is free to acquire the needed symmetric key from the document, and the collaborator accesses the document, acquires the encrypted version of the symmetric key, uses its new dynamic public key to decrypt the encrypted version of the symmetric key, and uses the symmetric key to access the content or services of the document,

and wherein if a new collaborator is being added to or removed from the list of collaborators that can access the document, the identity service further:

generates a modified version of the symmetric key, and

updates the encrypted versions of the modified symmetric key for each of the collaborators in the list of collaborators."

Independent system claim 11 of the auxiliary request corresponds closely to claim 1 and reads as follows:

"A dynamic collaborative document security system for managing security associated with document collaboration, comprising:

a list of collaborators, including an identity for each collaborator, wherein the collaborators on the list are associated with different encrypted versions of a symmetric key, wherein each collaborator's version of the symmetric key is encrypted with the public key for that particular collaborator, wherein decrypted versions of the symmetric key permit access to a document, and wherein the list of collaborator identities and their associated encrypted versions of the symmetric key is embedded within or linked or indexed to the document;

an identity service included as one of the collaborators for the document, configured to interact with documents, collaborators and lists of collaborators to manage document access and security,

characterized in that the identity service is identified in the list of collaborators for the document, and is configured to perform the steps of;

identifying (210) a collaborator associated with a document, when the collaborator lacks an encrypted version of a symmetric key needed to access the documents or lacks a proper key needed to decrypt that symmetric key;

verifying (220) that a community list associated with the document, and the collaborator, permits the collaborator to enter into a dynamic trusted relationship between the collaborator and the document, and in response to the verifying,

acquiring (230) a dynamic public key from or on behalf of the collaborator;

decrypting (240) the encrypted version of the symmetric key which grants access to the document by

the identity service using its own private key-public key pair; and

once the identity service has the decrypted symmetric key, re-encrypting (250) the symmetric key with the collaborator's newly provided dynamic public key;

notifying the collaborator that it is free to acquire the needed symmetric key from the document,

wherein the collaborator is configured to access the document, acquire the encrypted version of the symmetric key, use its new dynamic public key to decrypt the encrypted version of the symmetric key, and use the symmetric key to access the content or services of the document,

and wherein if a new collaborator is being added to or removed from the list of collaborators that can access the document, the identity service is further configured to:

generate a modified version of the symmetric key, and

update the encrypted versions of the modified symmetric key for each of the collaborators in the list of collaborators."

VII. In its letter of 1 July 2016 (points 2.5, 3 and 3.1) the appellant referred to the fact that Article 123(2) EPC was the "sole formal ground of rejection for the Decision" whereas the *obiter dictum* in the decision contained a new objection against the pending claims that "had not been the subject of any objection in the Summons". Since the decision was delivered in the appellant's absence, it was suggested that this might be a "potential issue under Article 113(2) EPC" (Article 113(1) EPC apparently being meant). No further explanation was given as to what the "issue" was

considered to be and why the examining division might have violated the appellant's right to be heard.

VIII. At the end of the oral proceedings, the chairman announced the decision of the board.

Reasons for the Decision

Article 113(1) EPC 1973

1. During the oral proceedings, the appellant did not elaborate further on its written suggestion (see the letter of 1 July 2016, point 3.1) that the *obiter dictum* in the decision under appeal might "represent a potential issue under Article 113" EPC and, specifically, requested neither remittal of the case for further prosecution nor reimbursement of the appeal fee under Rule 103 EPC. Since the board is also not of the opinion that the behaviour of the examining division showed a fundamental deficiency under Article 11 RPBA or a substantial procedural violation under Rule 103(1)(a) EPC, this issue requires no further discussion.

The invention

2. The application is concerned with secure collaborative work on or with "documents" which, as the description explains, can be any file, resource, directory or service (page 1, and page 3, last paragraph).

2.1 The application refers to a data structure called a "community list" which may be associated with a document or a collaborator or both and defines potentially

trusted collaboration "relationships" (page 4, paragraph 2; page 11, penultimate paragraph).

2.2 A "collaborative document" is encrypted with a symmetric key and associated with a list of current collaborators, for each of which a "version" of the symmetric key is provided, encrypted with the collaborator's public key (page 6, paragraphs 2 and 3). The collaborators and their associated encrypted keys are maintained in a list (*loc. cit.*, page 7, paragraph 2) and kept in association with the document as its metadata (page 7, paragraph 3).

2.3 An "identity service" is disclosed that manages additions to or removals from the list of collaborators and which provides a new collaborator with a new key if needed (see e.g. page 8, 3rd and 4th paragraphs). The application makes a point of adding the "identity service" itself as a collaborator (see e.g. page 8, 2nd paragraph; page 11, 2nd paragraph). The identity service provides a new key to a new collaborator by decrypting its own version of the symmetric key and re-encrypting it with the collaborator's public key. The fact that the identity service is itself treated as a collaborator makes sure that the document's metadata lists it amongst the collaborators and provides it with its associated encrypted "version" of the document key (page 12, paragraph 1).

2.4 Whenever a collaborator is added or removed, a new symmetric key is generated, the document is re-encrypted with the new symmetric key and the new symmetric key is re-encrypted for each collaborator with its respective public key (see page 8, paragraph 3, and page 13, paragraph 2). The collaborators need

not be made aware of this re-encryption (see esp. the cited paragraph, last three lines).

2.5 It is disclosed - albeit not claimed - that a symmetric key may "include[] all valid identifications which can access the document" (page 6, lines 9 to 11) and that when the list of collaborators changes a new key must be generated (see page 13, lines 8 to 12). This appears to be the reason why a new symmetric key is generated whenever group membership changes, and in particular also when a new collaborator joins the group. However, it is not disclosed how the symmetric key is generated to "include" identifications.

The prior art

3. D1 deals with controlling collaborative access to work group documents by the users of a computer system.

3.1 D1 discloses in its background section that known work group systems encrypt the documents, typically using symmetric DES encryption, and make the DES key available to all group members (see esp. column 4, lines 1-3, and column 4, line 52 to column 5, line 1, but also column 12, lines 43 to 47)). When, as regularly happens, a member leaves the group the problem of how to revoke that person's access privileges arises (column 4, lines 44-51, and column 5, 1-4). As a solution, it is known to re-encrypt the document with a new key so that the old key becomes useless to the former group member. The new key will however have to be distributed to the remaining group members, which is in itself a security risk (column 5, lines 5-17).

3.2 Addressing this security problem, D1 proposes the following solution. For each group member (i.e. each

current "collaborator"), an entry (called a "member definition") in a document "prefix" (column 12, lines 15 to 23) is provided, including a member identifier and the document key encrypted with the member's public key (column 12, lines 32 to 47). The prefix may or may not actually be part of the document file (*loc. cit.*).

3.3 All access requests are managed by an "access controller" (see figure 2, no. 44). When a user requests access to a document, the controller checks whether the user is contained in the list of member definitions (column 16, lines 16 to 37, and column 14, line 62 to column 15, line 11) and, if so, tries to obtain the member's private key. If this succeeds, the document key can be decrypted for that member and access is enabled (see column 16, lines 30 to 33, 51 to 55 and 60 to 65). The copy of the private key is then destroyed (column 16, line 63 to column 17, line 4).

3.4 An essential property of this solution is that the re-encryption of documents can be avoided because the document key never leaves the access controller. In other words, no group member ever receives the document key and thus cannot keep it after leaving the group. To make this possible, however, members have to hand over their private keys to the controller for decryption.

3.5 Deleting a member from the group is straightforward: only the member definition must be deleted, no new encryption is needed (column 15, lines 60 to 62).

3.6 It is disclosed that (initially, at least) only the "founding member has the authorization" to change group membership (column 14, lines 52 to 58). It is again up to the access controller to verify that a member

requesting a group change is authorised to do so (column 15, lines 34 to 36).

Suitable starting points for the inventive-step assessment

4. The board considers that D1 provides two suitable starting points for the assessment of inventive step, the system summarized in the background section (esp. column 4, line 44 to column 5, line 17) and the solution proposed in D1 to overcome the deficiency of the known system (see column 6, line 3 *et seq.*). For brevity, these will be referred to below as the "background" and the "invention" of D1, respectively.

4.1 The appellant challenged the suitability of the background of D1 as a starting point because D1 disclosed it merely "as a negative", i.e. in terms of its disadvantages, and in order to justify the invention as an attempt to overcome them. In this sense, D1 as a whole taught away from its background, which, therefore, the skilled person starting from D1 would not use as a basis for further developments.

4.2 The board disagrees with the appellant's assertion that the skilled person would be deterred from starting from the background of D1 merely because D1 focused on how to overcome its disadvantages and thus "taught away" from it.

4.3 Although the known system in the background section of D1 is described with a focus on one of its disadvantages, it is still the disclosure of a known system. As a matter of principle, this disclosure thus constitutes prior art for the present invention as well.

4.4 The board is, however, aware of the fact that the background contains only very little detail about the known system.

The main request

5. The subject-matter of claim 1 differs from the background of D1 in the majority of its features. Specifically, the background of D1 does not disclose

a) what happens when a member is added to a group,
b) the use of the community list for this purpose,
c) the symmetric key being protected using asymmetric encryption (key pairs), or
d) that the identity service is added as one of the collaborators.

5.1 *Re a)* D1 states that it is "not unusual" for group members to be added or removed over time (see column 4, lines 44-45). As a matter of necessity, any new member must be provided with the latest valid symmetric key. The skilled person would be aware that this individual "key distribution" is open to the same kinds of attacks as the distribution of newly generated keys (see column 5, lines 13-15).

5.2 *Re b)* The board considers it to be an obvious administrative requirement that individual users may not be authorised to gain access to a "collaborative document". For instance, it may be the administrative policy in a company to limit access to a document to the employees of a particular department. Given this requirement (see T 641/00, headnote II), it would be obvious to refer to a list of eligible employees so as to verify a new member's authorisation before the handing out the document access key. Furthermore, it

would be obvious for the skilled person to automate the enforcement of this policy.

5.3 *Re c)* In the board's view, it is well-established in the art that asymmetric encryption is used to secure the distribution of symmetric keys and, more specifically, that a symmetric key is transmitted to each authorised party after encryption with that party's public key. This general assumption is not disclosed in the prior art to hand, although it is consistent with the fact that the invention of D1 also discloses the encryption of symmetric keys with the members' public keys (column 13, lines 63-65). The appellant did not challenge this assumption.

5.3.1 Due to this common knowledge, the mention of the security problem of key distribution in the background of D1 would prompt the skilled person to use asymmetric key encryption. This implies the steps of "associating collaborators with different encrypted versions of a symmetric key" (claims page 18, lines 5-6), of "acquiring (230) a dynamic public key from or on behalf of the collaborator" (line 17) and of "encrypting (250) the symmetric key with the dynamic public key".

5.3.2 It does not, however, imply the step of "decrypting (240) the symmetric key which grants access to the document by the identity service using its own private key-public key pair".

5.4 *Still re c)* This remaining difference solves the problem of protecting the symmetric key at the component responsible for key generation and distribution. The board takes the view that it would be obvious as a security measure to store the symmetric key in encrypted form. The need to decrypt the

symmetric key before key distribution would follow as a matter of necessity. The appellant pointed out that it would be unusual to use asymmetric encryption for protecting a locally stored key. The board agrees but considers that this choice might be unusual but would still be obvious if it happened to be convenient in the circumstances.

5.5 *Re d)* Claim 1 implies that the identity service will, "as one of the collaborators", be associated with an "encrypted version of a symmetric key" but leaves open how this association is achieved and where the keys are held. The "notion of "using an identity service as one of the collaborators" is not defined. As a consequence, the board considers that this "using" feature must be interpreted to mean no more than its only apparent consequence, namely that the component responsible for key distribution is provided with a private key-public key pair and an encrypted version of the symmetric key. As just argued, however, the latter is, in the board's view, an obvious solution to the problem of protecting the symmetric key.

5.6 In summary, the board finds that the subject-matter of claim 1 of the main request lacks inventive step over the background of D1, Article 56 EPC 1973.

The auxiliary request

6. The board is satisfied that the amended claims comply with Article 123(2) EPC.

6.1 The problem with the dynamic public key being acquired only "from" rather than "from or on behalf of the collaborator" (see summons, point 5.2) is moot because the latter version now claimed was originally disclosed

in claim 9. The problem with the claim potentially making reference to several different community lists (summons, point 5.1) is likewise no longer pertinent, because only one such list is now claimed.

6.2 The list of collaborators including collaborator identities is disclosed on page 6, lines 4-6 (all references in this passage being to the application as originally filed). The individually encrypted versions of the symmetric key are disclosed on page 6, lines 16-21, and that they may be part of the list of collaborators is disclosed on page 7, lines 10-12. The list being "embedded or linked or indexed to the document" is disclosed on page 7, lines 22-28, and on page 14, lines 7-8. That a new symmetric key is generated and the corresponding re-encryption is performed whenever a member is added or removed is disclosed on page 3, lines 3-5, on page 8, lines 17-26, and on page 13, lines 8-18. From the fact that the collaborators need not be informed about the change (lines 16-18) it follows that the re-encrypted keys must be stored somewhere. In the board's judgement the skilled person would read this as implying that the re-encrypted keys will be stored in the list of collaborators.

7. The board further considers that the amended claims comply with Article 84 EPC. The only objection in this respect which the board raised in its summons to oral proceedings, namely what it meant for a document to maintain a list (summons, point 5.3), is moot since the the document is no longer claimed as the subject of the maintaining step.

8. The list of collaborators being "embedded within or linked or indexed to the document" (claim 1, lines 11-12) implies, in the board's judgement, that

the list of collaborators is more than a mere logical - i.e. conceptual - reference to the totality of all pertinent collaborator identities and encrypted symmetric keys. Rather, the skilled person would understand the list of collaborators to be a separate data structure or service which, albeit not necessarily located at the identity service, is "central" with respect to the collaborators - and the identity service as one of them.

8.1 Claim 1 specifies that the collaborator acquires the newly encrypted symmetric key "from the document" and that it "accesses the document" before "acquir[ing] the encrypted version of the symmetric key". Given that the rest of the claim is unambiguous about the fact that the encrypted keys are contained in the list of collaborators, the skilled person would understand this statement to mean that the newly encrypted key is retrieved from this list.

8.2 The further requirement of claim 1 that the symmetric key and its encrypted versions are modified in the list of collaborators whenever a new collaborator is added to or removed from the group, implies that collaborators, in order to access a document, will have to refer to the list of collaborators repeatedly, in particular not only once when they are added to the list.

Inventive step over the background of D1

9. In addition to differences a) to d) as discussed above, the subject-matter of claim 1 of the auxiliary request requires further features which are not discussed in the brief background section of D1. Specifically, the background of D1 does not disclose

e) a list of collaborators,
f) comprising encrypted versions of the symmetric key,
g) and including the "identity service" with its own encrypted version of the symmetric key, or
h) that a new symmetric key is also generated when a new collaborator is *added* or *removed*.

9.1 In the background of D1, some "list" of group members (i.e. collaborators) is required to make possible the key distribution mentioned. An obvious implementation of feature c) however would not require that the encrypted keys be kept in a shared location, let alone including that of the identity service as a collaborator.

9.2 In view of the fact that the provision of asymmetric encryption (feature c) is already a difference between the background of D1 and claim 1, the board judges that features e) to g) in combination are not also obvious from the background of D1 alone. Also the problem of providing "a single centralized access control mechanism" mentioned in D1 (see column 5, lines 32-34) does not prompt the skilled person to provide a list of encrypted symmetric keys according to feature e) to g).

9.3 The board is aware that a list according to features e) and f) is known from the invention of D1 (see column 12, lines 43-45). However, it is of the opinion that the skilled person could have, but would not have, without exercising inventive step, extracted this individual feature from the detailed invention of D1 and incorporated it into the background section of D1.

9.4 In summary, the board is of the opinion that claim 1 of the auxiliary request is inventive over the background of D1, Article 56 EPC 1973.

Inventive step over the invention of D1

10. Claim 1 of the auxiliary request differs from the invention of D1 at least in the following features.

i) The collaborators according to the claimed invention retrieve the valid encrypted version of the symmetric key from the list of collaborators which is "embedded or linked or indexed to the document". Thereby, they get access to the symmetric key "permit[ting] access to [the] document." In contrast, in the system of D1 the symmetric key never leaves the access controller.

ii) A new symmetric key is generated whenever a new member (or collaborator) is added to or removed from the group. In contrast, because the symmetric key never leaves the access controller, it need not be regenerated even if a member leaves the group. Regeneration of the symmetric key when a group member joins the group is nowhere disclosed or suggested in D1.

iii) The identity service, responsible for the generation of the encrypted keys, is "added as one of the collaborators", i.e. the identity service accesses the same data structure to retrieve its version of the symmetric key as the collaborators use in order to access the document. In D1, the access controller, which is separate and different from the group members, is responsible for encrypting the symmetric key for the collaborators. D1 does not disclose or suggest, however, that the access controller, in order to do that, had to decrypt its version of the symmetric key. In other words, it is not excluded by D1 that the access controller has access to the symmetric key in plain text.

11. An effect of differences i) and ii) is that the collaborators retain control over their private keys (which, in D1, must be made available to the access controller) but at the price of giving the collaborators access to the symmetric key and, hence, of having to regenerate the symmetric key if group membership changes.

11.1 It is central to the invention of D1 that the symmetric key never leaves the access controller and therefore need not be regenerated when group membership changes. In fact and as explained in the background section of D1, the system of D1 was specifically designed to make regeneration of the symmetric key superfluous while, at the same time, remaining able to exclude former group members from accessing the collaborative document.

11.2 From this perspective, an effect of differences i) and ii) is to forego the advantages for which the system of D1 was specifically designed. The board is of the opinion that the skilled person, based on the teaching of D1 alone, would not have had any motivation to modify the invention of D1 in such a fundamental way. Moreover, the board is not aware of any clue in the prior art to hand that would have prompted the skilled person to do it.

11.3 Therefore, the board comes to the conclusion that the invention according to claim 1 of the auxiliary request was not obvious over D1 to the person skilled in the art, and therefore involves an inventive step over D1, Article 56 EPC 1973.

12. The same reasoning applies to the independent system claim which is, mutatis mutandis, identical to system claim 11.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.
2. The case is remitted to the examining division with the order to grant a European patent with the following documents:

claims
1-17 as filed on 2 August 2016;
description, pages
1, 2 as filed on 25 September 2007,
6, 7, 15 as filed on 2 August 2016,
3-5, 8-14, 16, 17 as originally filed; and
drawings, sheets
1/3-3/3 as originally filed.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated