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

# Datasheet for the decision of 11 May 2011

**Case Number:** T 0286/07 - 3.5.06

**Application Number:** 01986160.8

**Publication Number:** 1402330

**IPC:** G06F 1/00

**Language of the proceedings:** EN

**Title of invention:**
Method and apparatus for delegating digital signatures to a signature server

**Applicant:**
Oracle International Corporation

**Opponent:**
-

**Headword:**
Delegating digital signatures/ORACLE

**Relevant legal provisions:**
-

**Relevant legal provisions (EPC 1973):**
EPC Art. 84, 111(1)

**Keyword:**
"Claim 1 - clarity (no, ambiguous)"
"Decision re appeals - remittal (yes)"

**Decisions cited:**
-

**Catchword:**
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

**Case Number:** T 0286/07 - 3.5.06

# D E C I S I O N
**of the Technical Board of Appeal 3.5.06**
**of 11 May 2011**

**Appellant**: Oracle International Corporation
500 Oracle Parkway
Redwood Shores, CA 94066 (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 14 August 2006 refusing European patent application No. 01986160.8 pursuant to Article 97(1) EPC 1973.**

**Composition of the Board:**

**Chairman:** D. H. Rees
**Members:** A. Teale
W. Sekretaruk

## Summary of Facts and Submissions

I. This is an appeal against the decision dispatched on 14 August 2006 by the examining division to refuse European patent application No. 01 986 160.8 in the form according to the main request submitted in the oral proceedings on 15 November 2005. According to the reasons for the appealed decision, claim 1 according to the main request lacked inventive step, Article 56 EPC 1973, in view of the following document:

D1: EP 1 030 282 A1.

However the application according to the auxiliary request submitted in the same oral proceedings met the requirements of the EPC.

II. A notice of appeal was received on 31 August 2006 in which the appellant requested that the decision be set aside and a patent granted on the basis of the main or the auxiliary request submitted on 15 November 2005. The appellant also made an auxiliary request for oral proceedings. The appeal fee was paid on 7 September 2006.

III. With a statement of grounds of appeal received on 8 December 2006 the appellant submitted amended description pages and claims to amend the main request and requested that the decision be set aside and the application remitted to the examining division for allowance on the basis of the (amended) main request or the auxiliary request. If the main request were to be refused, then the appellant requested oral proceedings.

IV. In an annex to a summons to oral proceedings the board *inter alia* raised a clarity objection, Article 84 EPC 1973, against claim 1 of both the main and the auxiliary request.

V. In a submission received on 7 April 2011 the appellant requested that the case be remitted back to the examining division and that the board give an early indication on this point before the oral proceedings. The appellant also confirmed that the main request was based on the following application documents:

**Description**:
pages 1, 2 and 5 to 11 as published
pages 3 and 4, received on 8 December 2006.

**Claims**:
1 to 17, received on 8 December 2006.

**Figures**:
1/4 to 4/4 as published.

VI. In a communication of the registry dated 12 April 2011 the board informed the appellant that the oral proceedings would take place as announced.

VII. Oral proceedings took place on 11 May 2011 at which the appellant withdrew the auxiliary request and requested that the decision under appeal be set aside and that the case be remitted to the examining division for further prosecution on the basis of the main request filed 8 December 2006. At the end of the oral proceedings the board announced its decision.

VIII. Claim 1 according to the main request reads as follows:

"A method for facilitating the delegation of operations involved in providing digital signatures to a signature server (140), the method comprising: receiving a request for a digital signature from a user (105) at the signature server, the request including an item to be signed on behalf of the user by the signature server; authenticating the user at the signature server; determining whether the authenticated user is authorized to sign the item by communicating with an authority server (143) that is separate from the signature server; looking up a private key for the user at the signature server; signing the item with the private key for the user; and returning the signed item to the user so that the user can send the signed item to a recipient."

The claims according to the main request also comprise a claim 9 to a computer program for performing the method according to any preceding claim and an independent apparatus claim 10.

## Reasons for the decision

1. *The admissibility of the appeal*

In view of the facts set out at points I to III above, the board finds that the appeal is admissible.

2. *The context of the invention*

2.1 The invention relates to a distributed computing system comprising servers linked by networks and, in particular, to the digital signature of a data item, for instance an electronic form provided by an application running on an application server outside the user's organisation, to initiate a commercial transaction.

2.2 To ensure the non-repudiation of the transaction, the form is provided with a digital signature using a private key belonging to an authorized user. Instead of authorization being the responsibility of the application server outside the organisation, this task is delegated to a signature server within the organisation. The authorization policy of the organisation is stored on a database which may be stored on a separate authority server within the organisation (see figure 1).

2.3 The authorization policy defines which members of the organisation are authorized to sign using specific signatures. For instance, the officers of a corporation may be authorized to sign with a private key for the corporation, whereas other employees of the corporation may only be able to sign with their own private keys. The authorization policy may also define a maximum transaction value for a user. According to page 3, lines 34 to 37, of the (amended) description, "In one embodiment, determining whether the user is authorized to sign the item prior to signing the item involves looking up an authorization for the user based upon an identifier for the user as well as an identifier for an

application to which the user will send the signed item." Since the authorization policy information is stored within the organisation, the organisation can react quickly to update user authorizations in the light of personnel changes, such as employees leaving the organisation or employees changing role within the organisation, perhaps only temporarily.

2.4 According to the application (see figure 2), the user receives a form concerning the commercial transaction from an application running on an application server outside the organisation. The user completes the form and sends it to the signature server for signature. The signature server first authenticates the user, meaning that the signature server determines, for instance by prompting the user to enter a password, whether the user is who the user claims to be. Then the signature server consults the authorization policy to determine whether the user is authorized to sign the form. If so, then the form is signed with the appropriate private key and returned to the user for sending to the application.

3. *Clarity of claim 1, Article 84 EPC 1973*

3.1 In the annex to the summons to oral proceedings the board stated that claim 1 seemed to be unclear in that it set out an object to be achieved, namely determining whether the authenticated user was authorized to sign the item, without setting out those features necessary for achieving this object. In particular, it was ambiguous whether claim 1 required that authorization depend on the particular item to be signed or whether it was to be understood more broadly as requiring that

the authenticated user be authorized to sign items *per se*, for instance because they were the company CEO (see page 2, lines 16 to 18, of the description).

3.2 The appellant has responded by disputing whether claim 1 is ambiguous and arguing that the board's argumentation merely demonstrates that the claim wording is broad enough to cover various possible implementations, the boards of appeal having repeatedly emphasized that the clarity of a claim is not diminished merely by its breadth. In other words, the appellant has argued that the broader possible interpretation of claim 1 is the only possible one, this interpretation covering not only item-dependent authorization but also item-independent authorization.

3.3 The appellant's arguments have not persuaded the board that the expression in claim 1 "determining whether the authenticated user is authorized to sign the item" cannot reasonably be interpreted in two ways: firstly, that authorisation depends on the user and not on the item (item-independent) and, secondly, that authorisation depends both on the user and the item (item-dependent). The description provides a basis for both interpretations. The sentence bridging pages 7 and 8 refers to officers of a corporation signing for the corporation, there being no restriction to specific items (item-independent authorization). Page 3, lines 34 to 37, refers to authorization depending upon an identifier for the user and an identifier for the application to which the user will send the signed item (item-dependent authorization).

3.4 Hence the board finds that claim 1 is ambiguous and thus unclear, Article 84 EPC 1973. Consequently, as a precondition for being successful in the examination proceedings, the claim has to be amended accordingly. The board has taken the broader interpretation of claim 1, as argued by the appellant, in considering the differences between the subject-matter of claim 1 and the disclosure of D1 below.

4. *The disclosure of document D1*

4.1 D1 concerns the signing of a message with a private key which is not kept by the user but by a signature server. According to the first embodiment (see figures 1 and 2 and paragraphs [0061] to [0098]), the user sends an ID, authentication dynamic signature data and a message to be signed to the signature preparing server 10; see paragraph [0062]. This recalls registered authentication dynamic signature data and a private key from control data base 12 containing information on users and their private keys (see paragraph [0065]) and uses dynamic signature verifying section 14 to check the authentication dynamic signature data provided by the user. If the user is authenticated then the message and private key are sent to the encryption operation section 18 for the message to be signed using the private key; see paragraph [0074]. Transactions are controlled by the dynamic signature encryption key control system 16 which sends a copy of the signed message to the user; see paragraph [0079].

4.2 It is common ground between the board and the appellant that the comparison in D1 by the dynamic signature verifying section 14 of the authentication dynamic

signature data provided by the user with that registered in the control data base 12 (see figures 1 and 2 and paragraphs [0071] to [0073]) constitutes the claimed "authentication" of the user, in the sense of confirming that a user is who the user claims to be.

4.3 The question of whether D1 discloses determining whether a user is authorized to sign an item has been disputed. According to the appealed decision (see reasons, point 1.2), the encryption of the user's message by encryption operation section 18 if the dynamic signature verifying section 14 determines that the request for a digital signature is legitimate (see D1 paragraph [0074] and figure 1) satisfied the claimed expression "authorization". The appellant has disputed this interpretation of D1, arguing that the decision equates authorization with authentication and that authorization, in the sense of checking whether the user is permitted to perform a particular task, is not known from D1.

4.4 The board agrees with the appellant that paragraph [0074] of D1, referring to the dynamic signature key control section 16 in figure 1, does not disclose checking whether the user is permitted to perform a particular task and therefore does not disclose authorization.

4.5 However in the oral proceedings the board pointed out that D1 disclosed the user sending an ID, authentication dynamic signature data and a message to be signed to the signature preparing server 10; see paragraph [0062]. It was implicit in D1 that the signature preparing server 10 would check whether the

user ID was valid, meaning that the signature preparing server would check to see whether the user was authorized to use the system, this authorization check occurring before the user was authenticated by comparing the stored authentication dynamic signature data with that entered by the user. The appellant has not disputed this interpretation of D1, but has pointed out that, according to claim 1, user authorization is checked after the user has been authenticated.

4.6 Hence, in terms of claim 1 of the main request, D1 discloses a method for facilitating the delegation of operations involved in providing digital signatures to a signature server, the method comprising: receiving a request for a digital signature from a user at the signature server, the request including an item to be signed on behalf of the user by the signature server; authenticating the user at the signature server; [before authenticating the user] determining whether the user is authorized to sign the item; looking up a private key for the user at the signature server; signing the item with the private key for the user and returning the signed item to the user so that the user can send the signed item to a recipient.

4.7 It is thus common ground between the board and the appellant that the subject-matter of claim 1 (interpreted broadly; see point 3.4 above) differs from the disclosure of D1 in that:

i. the step of determining whether the user is authorized to sign the item occurs after the user has been authenticated at the server, the

authorization check occurring before authentication in D1, and

ii. it is determined whether the authenticated user is authorized to sign the item by communicating with an authority server that is separate from the signature server.

4.8 Regarding the requirements of Article 56 EPC 1973, the reasons for the appealed decision are not valid with respect to these differences. Thus the appeal is allowed.

5. *Remittal, Article 111(1) EPC 1973*

5.1 Following the examination as to the allowability of the appeal, the board shall decide on the appeal. The board of appeal may either exercise any power within the competence of the department which was responsible for the decision appealed or remit the case for further prosecution.

5.2 The board's interpretation of D1, in particular concerning the question of the authorization of the user to sign the item, differs significantly from that upon which the appealed decision was based. Indeed the changed factual situation may require further documents to be taken into account in any re-assessment of patentability. Therefore the board exercises its discretion and remits the case to the first instance for further prosecution.

## Order

## For these reasons it is decided that:

The decision under appeal is set aside.

The case is remitted to the examining division for further prosecution.

The Registrar: The Chairman:

K. Götz D. H. Rees