Internal distribution code:

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

Datasheet for the decision of 15 March 2019

Case Number: T 1114/14 - 3.4.03

Application Number: 03737550.8

Publication Number: 1476856

IPC: G07F19/00

Language of the proceedings: EN

Title of invention:
METHODS AND SYSTEMS FOR VALIDATING THE AUTHORITY OF THE HOLDER OF A DIGITAL CERTIFICATE ISSUED BY A CERTIFICATE AUTHORITY

Applicant:
Oracle International Corporation

Headword:

Relevant legal provisions:
EPC Art. 52(1)
EPC 1973 Art. 56, 84

Keyword:
Inventive step - main request, first and second auxiliary requests (no)
Claims - clarity - third and fourth auxiliary requests (no)

Decisions cited:
T 1411/08

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Case Number: T 1114/14 - 3.4.03

D E C I S I O N
of Technical Board of Appeal 3.4.03
of 15 March 2019

Appellant: (Applicant)	Oracle International Corporation 500 Oracle Parkway Redwood Shores, CA 94065 (US)
Representative:	Gill Jennings & Every LLP The Broadgate Tower 20 Primrose Street London EC2A 2ES (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 1 October 2013 refusing European patent application No. 03737550.8 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	T. M. Häusser
Members:	M. Papastefanou
	C. Heath

Summary of Facts and Submissions

I. The appeal is against the decision of the examining division refusing the European patent application No. 03 737 550.8 (published as WO 03/067536 A2) on the ground that claim 1 of the sole request before it did not involve an inventive step.

II. The appellant (applicant) requested that the decision under appeal be set aside and that a patent be granted on the basis *"of the claims of the application on which the first instance decision to refuse the application is based"*, as its Main request. The board understands that these claims are the claims filed with the appellant's (applicant's) letter dated 17 February 2009. As an auxiliary measure, the appellant requested that a patent be granted on the basis of one of the First to Fourth Auxiliary requests, which were filed with the statement of the grounds of appeal.

III. In a communication pursuant to Article 15(1) of the Rules of Procedure of the Boards of Appeal (RPBA) which followed the summons to oral proceedings, the board communicated its preliminary non-binding opinion according to which the subject-matter of claim 1 of the Main, First, Second and Fourth Auxiliary requests did not involve any inventive step. Claim 1 of the Third and Fourth Auxiliary requests did not meet the requirement of clarity according to Article 84 EPC 1973. In addition, the board raised objections against the presence of multiple independent claims of the same category in the claim sets of all requests, which was considered to be against the requirements of Rule 29(2) EPC 1973, as these claims did not appear to fall under

the exceptions foreseen in Rule 29(2) EPC 1973.

IV. The appellant did not contest the board's preliminary opinion but informed the board that it would not be attending the oral proceedings, which were thus held in the appellant's absence. No other submissions were made by the appellant. At the end of the oral proceedings the chairman announced the decision.

V. Claim 1 of the **Main request** has the following wording:

A method for a financial services provider to securely process corporate payment requests over a computer network (108), comprising the steps of:
issuing a primary digital certificate (114) to a primary certificate holder of a corporation, the primary certificate being configured to authorize the primary certificate holder to designate a plurality of holders of secondary digital certificates that are derivative from the primary certificate, each of the primary and plurality of secondary certificates including unique identifying information and an indication of authority of the holder of the certificate that includes a predetermined maximum payment that the holder of the certificate is authorized to validate and an identification of payees for which the certificate holder is authorized to validate payments, an authority defined in each of the secondary digital certificates being comparatively more limited than an authority defined in the primary digital certificate;
collecting (S506) pending corporate payment requests for clearing against an account of the corporation;
periodically (S506) generating a pending payment statement (202) that includes the collected pending payment requests;

requiring (S507) that each of the collected pending payment requests be validated by an authenticated secondary certificate holder having the authority to validate the payment requests up to the predetermined maximum payment and for the identified payees included in the indication of authority of the secondary certificate issued to the authenticated secondary certificate holder;
clearing (S508) only validated corporate payment requests of the pending payment statement against the corporate account.

VI. Claim 1 of the **First Auxiliary request** comprises the following feature, which is inserted before the last feature (*"clearing (S508)..."*):

"authenticating the secondary certificate holders seeking to validate pending payment requests by firstly requiring the collection and analysis of biometric data of secondary certificate holders and comparing said collected biometric data with previously collected biometric data stored in a database and secondly requiring the certificate holder to present the secondary certificate, and checking against an on-going database record of issued, expired, revoked or changed certificates that the secondary certificate is valid, current and uncorrupted; and"

VII. Claim 1 of the **Second Auxiliary request** has the following wording:

A method for a financial services provider to securely process corporate payment requests over a computer network (108), comprising the steps of:
issuing a primary digital certificate (114) to a primary certificate holder of a corporation, the

primary certificate being configured to authorize the primary certificate holder to designate a plurality of holders of secondary digital certificates that are derivative from the primary certificate, each of the primary and plurality of secondary certificates including unique identifying information and an indication of authority of the holder of the certificate that includes a predetermined maximum payment that the holder of the certificate is authorized to validate and an identification of payees for which the certificate holder is authorized to validate payments, an authority defined in each of the secondary digital certificates being comparatively more limited than an authority defined in the primary digital certificate;

collecting (S506) pending corporate payment requests for clearing against an account of the corporation;

periodically (S506) generating a pending payment statement (202) that includes the collected pending payment requests, wherein the pending payment statement generating step generates the pending payment statement (202) at a regular interval;

requiring (S507) that each of the collected pending payment requests be validated by an authenticated secondary certificate holder having the authority to validate the payment requests up to the predetermined maximum payment and for the identified payees included in the indication of authority of the secondary certificate issued to the authenticated secondary certificate holder;

receiving a list of validated corporate payment requests from an authenticated certificate holder of the corporation and clearing only those corporate payment requests against the corporate account that are listed in the received list of validated corporate payment requests;

clearing (S508) only validated corporate payment requests of the pending payment statement against the corporate account.

VIII. Claim 1 of the **Third Auxiliary request** is worded as follows:

A method for a financial services provider to securely process corporate payment requests over a computer network (108), comprising the steps of:
issuing a primary digital certificate (114) to a primary certificate holder of a corporation, the primary certificate being configured to authorize the primary certificate holder to designate a plurality of holders of secondary digital certificates that are derivative from the primary certificate, each of the primary and plurality of secondary certificates including unique identifying information and an indication of authority of the holder of the certificate that includes a predetermined maximum payment that the holder of the certificate is authorized to validate and an identification of payees for which the certificate holder is authorized to validate payments, an authority defined in each of the secondary digital certificates being comparatively more limited than an authority defined in the primary digital certificate;
collecting (S506) pending corporate payment requests for clearing against an account of the corporation;
periodically (S506) generating a pending payment statement (202) that includes the collected pending payment requests, wherein the pending payment statement generating step generates the pending payment statement (202) at a regular interval;
requiring (S507) that each of the collected pending payment requests be validated by an authenticated

secondary certificate holder having the authority to validate the payment requests up to the predetermined maximum payment and for the identified payees included in the indication of authority of the secondary certificate issued to the authenticated secondary certificate holder, wherein the requiring step includes a step of validating the collected pending payment requests of the pending payment statement (202) at least partially programmatically and wherein the requiring step validates each pending payment requests in the pending payment statement by (202) by matching the payment request with a corresponding payment request in an accounting system of the corporation;
receiving a list of validated corporate payment requests from an authenticated certificate holder of the corporation and clearing only those corporate payment requests against the corporate account that are listed in the received list of validated corporate payment requests;
clearing (S508) only validated corporate payment requests of the pending payment statement against the corporate account.

IX. Claim 1 of the **Fourth Auxiliary request** has the following wording:

A method for a financial services provider to securely process corporate payment requests over a computer network (108), comprising the steps of:
issuing a primary digital certificate (114) to a primary certificate holder of a corporation, the primary certificate being configured to authorize the primary certificate holder to designate a plurality of holders of secondary digital certificates that are derivative from the primary certificate, each of the primary and plurality of secondary certificates

including unique identifying information and an indication of authority of the holder of the certificate that includes a predetermined maximum payment that the holder of the certificate is authorized to validate and an identification of payees for which the certificate holder is authorized to validate payments, an authority defined in each of the secondary digital certificates being comparatively more limited than an authority defined in the primary digital certificate;
collecting (S506) pending corporate payment requests for clearing against an account of the corporation;
periodically (S506) generating a pending payment statement (202) that includes the collected pending payment requests, wherein the pending payment statement generating step generates the pending payment statement (202) at a regular interval;
requiring (S507) that each of the collected pending payment requests be validated by an authenticated secondary certificate holder having the authority to validate the payment requests up to the predetermined maximum payment and for the identified payees included in the indication of authority of the secondary certificate issued to the authenticated secondary certificate holder, wherein the requiring step includes a step of validating the collected pending payment requests of the pending payment statement (202) at least partially programmatically and wherein the requiring step validates each pending payment requests in the pending payment statement by (202) by matching the payment request with a corresponding payment request in an accounting system of the corporation;
authenticating the secondary certificate holders seeking to validate pending payment requests by firstly requiring the collection and analysis of biometric data of secondary certificate holders and comparing said

collected biometric data with previously collected biometric data stored in a database and secondly requiring the certificate holder to present the secondary certificate, and checking against an on-going database record of issued, expired, revoked or changed certificates that the secondary certificate is valid, current and uncorrupted;
receiving a list of validated corporate payment requests from an authenticated certificate holder of the corporation and clearing only those corporate payment requests against the corporate account that are listed in the received list of validated corporate payment requests; and
clearing (S508) only validated corporate payment requests of the pending payment statement against the corporate account.

X. The appellant argued essentially that the claimed method consisted of a new use of known technology, which solved the technical problem of securing existing payment modalities. There was nothing in the state of the art that would motivate the skilled person to adapt the known hardware and software to provide the claimed subject matter (see points 2.23 to 2.26 of the statement of grounds of appeal).

Reasons for the Decision

1. The appeal fulfills the provisions referred to in Rule 101 EPC and is therefore admissible.

2. The duly summoned appellant did not attend the oral proceedings before the board, as it had already announced in advance. According to Rule 71(2) EPC 1973, the proceedings could continue without the appellant. In accordance with Article 15(3) RPBA, the board relied

in its decision only on the appellant's written submissions. The board being in a position to decide the case at the conclusion of the oral proceedings (Articles 15(5) and (6) RPBA), the voluntary absence of the appellant was not a reason for delaying the decision (Article 15(3) RPBA).

3. Main request

3.1 The claimed invention relates to a method and a computer system for a financial services provider to securely process corporate payment requests over a computer network. In the context of the application, "secure processing" of corporate payment requests is to be understood as requiring that the financial service provider fulfils only those payment requests that are authorised by the payer (page 4, lines 6 to 10 of the published application).

The problem the claimed invention is trying to address is how to prevent the execution of unauthorised or fraudulent payment requests. By unauthorised or fraudulent requests are meant requests, which either have not been authorised at all by the payer or that the payer has authorised only in part (i.e. with a different amount to be paid).

The method of secure processing payment requests of the application can be described essentially as follows:

A payee (corporation A) presents to the financial services provider a payment request for a sum to be paid to it by a payer (corporation B). This payment request can take several different forms: a paper check, electronic fund transfer, extensible markup language message, credit or purchase card. The

financial services provider, before executing (clearing) the payment, requires that the payer (corporation B) validates (authorises) the payment request. The payer (corporation B or an authorised employee of corporation B) checks the payment request and confirms that the request was indeed issued by the payer for the requested amount. Only when the payer validates (confirms) the payment request, the request is fulfilled (cleared) by the financial services provider and the corresponding amount is paid to the payee (corporation A).

3.2 The board sees the described validation procedure as a purely administrative (i. e. business) one. The measure taken to ensure that only authorised requests are fulfilled (request the payer to validate the requests) is not a technical measure. The measure that the financial services provider shall require the payer of a payment request, which is submitted by a payee for clearance, to validate the request before it is cleared is based on administrative/business considerations rather than on technical constraints or considerations.

This payment validation scheme can be implemented without any technical means at all, for example by an employee of the financial services provider collecting all the pending payment requests concerning a specific payer and contacting an authorised employee of the payer in order to validate the requests, for example orally.

3.3 The invention claimed in the Main request is not limited to the described business procedure as such, but rather concerns its technical implementation in a computer system.

According to claim 1 of the Main request, the validation of the requests is performed using digital certificates. For a corporation, the potential payer of payment requests, a primary certificate is issued to a specific employee. This primary certificate authorises its holder to issue secondary certificates to other employees of the corporation so that the power to validate payment requests is delegated to one or more employees. Each secondary certificate has a unique identification and defines a specific amount as limit for the payments its holder can authorise. The financial service provider collects payment requests for the specific corporation and requires that they are validated (authorised) by an authenticated and authorised holder of a secondary certificate. Only then the payment requests are fulfilled (cleared) by the financial services provider.

3.4 The technical problem the skilled person is trying to solve is therefore how to implement the given administrative payment request validation procedure.

3.5 The board considers the claimed method to be a straightforward implementation of the described payment validation procedure, which itself is a purely administrative procedure (see points 3.1 and 3.2 above). There are no apparent technical effects obtained by the claimed method besides the ones expected by the automatisation of an administrative procedure by the use of a computer system.

3.6 Although technical means are used in the claimed method (computer systems, telecommunication network, etc.), these are considered to be common place computer and network hardware parts. The application does not indicate anything different, as the "computing device

600" (see Figure 6) and all the relevant parts used in the claimed method are described as generally known and widely used general purpose hardware parts (see the section titled "HARDWARE DESCRIPTION"; page 17, line 28 to page 18, line 28 of the published application).

According to the board, these technical means fall under the so-called "notorious" knowledge (see for example T 1411/08, Catchword and Reasons 4.1, 4.2). It would therefore be evident for the skilled person to use such means when implementing the administrative procedure.

3.7 An issue that has to be addressed in the implementation of the payment validation scheme is the verification of the identity of the person validating the payment on behalf of the payer. In other words, it has to be ensured that the person validating a request on behalf of the payer is a person who is indeed authorised to do so. The application mentions the use of Public Key Infrastructure (PKI) for solving this problem (page 11, lines 9-13).

3.8 As the examining division pointed out and the appellant did not contest (see point 2.26 of the statement of grounds of appeal), the authorisation structure using digital certificates defined in the claimed method corresponds to the use of digital certificates according to the X.509v3 standard, which was publicly known by the priority date of the application.

3.9 The board considers the following to be part of common general knowledge in the field of cryptography:

An issue to be addressed when using PKI is ensuring that the holder of a public encryption key is reliably

identified in order to avoid any type of fraud that would compromise the encrypted communication. A common way to do this is the use of digital certificates. A trusted certificate issuing authority issues a digital certificate that connects (cryptographically) a specific public encryption key with the identity of its rightful owner. The digital certificate comprises further a digital signature that ensures that the certificate is a genuine certificate that has been issued by the specific issuing authority.

X509 is a standard defining the format of public key certificates. This standard describes the generation, distribution, monitoring and verification of digital certificates. It describes, among others, the use of lists of valid, modified and expired digital certificates so that each time a certificate is to be used it is verified whether it is still valid. The standard comprises also the concept of root and intermediate digital certificates, whereby a holder of a root (primary) certificate has the authority to sign intermediate (secondary) certificates, i. e. there is no need for the issuing authority to sign all the certificates since this can be delegated to selected (primary or root) certificate holders.

The X509 standard was first issued in 1988. Its third version (X509v3) was issued in 1996. It introduced the feature of certificate extensions, which provide methods for associating additional attributes with users and the public keys. This allows, for example, an organisation to add additional information in the certificate such as an employee ID into the digital certificate.

3.10 The board is, thus, of the opinion that the skilled person, a computer programmer expert in secure communication systems, faced with the technical problem of implementing the administrative payment validation scheme, would readily realise that the generally known X509v3 standard provided a possible solution.

As a standard by definition is common general knowledge, the skilled person would not need to exercise any inventive skill in selecting the specific standard in order to implement the required payment validation scheme. Any further adaptations of the standard to the specific needs of the payment validation scheme, which might include for example the definition of specific extensions related to the maximum payment amount an employee is authorised to validate, are considered to involve only trivial programming steps that the skilled person would take in an obvious manner based only on common general knowledge and the administrative requirements of the payment validation scheme.

3.11 The appellant did not contest that the claimed method was based on the X509v3 standard. It argued, however, that the claimed invention was a new use of known technology (see point 2.6 of the statement of the grounds of appeal) and that it *"solve[d] the technical problem of how to use technology to secure the existing payment modalities from fraudulent payments"* (point 2.23).

3.12 The board considers, however, as explained above, that the scheme for avoiding fraudulent payment is provided to the skilled person as a constraint to be fulfilled when given the task of devising a suitable implementation. Furthermore, the solution of the

identified problem is merely based on generally known hardware and software.

3.13 Summarising, the board is of the opinion that the claimed method amounts to an implementation of an administrative/business scheme using a generally known cryptography standard implemented through generally known (notorious) technical means. The board concludes, hence, that the subject-matter of claim 1 of the Main request does not involve an inventive step within the meaning of Article 56 EPC 1973.

4. Auxiliary requests

4.1 In claim 1 of the **First Auxiliary request** it is additionally defined that the secondary certificate holders are authenticated using biometric information and that the secondary certificate is checked against a database where all the issued, expired, revoked or changed certificates are recorded in order to establish its validity.

According to the board's opinion, the use of biometric data to authenticate users (certificate holders) of a computer network is a standard feature in user authenticating procedures and was so on the priority date of the application. Checking the validity of a digital certificate against a record of issued, expired, revoked or changed certificates is part of the X.509v3 standard.

It has to be concluded, therefore, that neither of these additional features can support the presence of an inventive step in the subject-matter of the claim 1 of the First Auxiliary request.

4.2 Compared with the Main request, claim 1 of the **Second Auxiliary request** comprises the additional features that the pending request statement is generated at regular intervals and that payments are only cleared if they appear in a list of requests validated by an authorised holder of a digital certificate.

The board considers that the generating of pending request statements at regular intervals is a straightforward technical implementation of the administrative stipulation of generating regular settlements. As such, it lies within the common knowledge of the skilled person.

Regarding the latter feature, it is considered a required feature of the administration scheme that only the payments which are properly validated are to be cleared. That these requests are presented in a list is seen as an obvious implementation feature without any technical merits.

The conclusion of the board is, hence, that the subject-matter of claim 1 of the Second Auxiliary request does not involve an inventive step, either.

4.3 Compared to the Second Auxiliary request, claim 1 of the **Third Auxiliary request** comprises the additional features that the *requiring step includes a step of validating the collected pending payment requests of the pending payment statement at least partially programmatically and that the requiring step validates each pending payment request in the payment statement by matching the payment request with a corresponding payment request in an accounting system of the corporation.*

The board notes that according to the claim feature preceding this one, it is required that *each of the collected pending payment requests be validated by an authenticated secondary certificate holder.*

There is, thus, a contradiction between the two features of the claim, since one of them defines the requirement that each of the payment requests is validated by a certificate holder and the other that this validation can is to be done at least partially automatically (programmatically) by comparison to payment requests in the accounting system of the corporation.

This contradiction creates doubts as to how the payment requests are to be validated and ambiguity regarding the definition of the matter (scope) for which protection is sought. Claim 1 of the Third Auxiliary request does not, therefore, comply with the clarity requirement according to Article 84 EPC 1973.

4.4 Compared to the Main request, claim 1 of the **Fourth Auxiliary request** comprises the additional features present in claim 1 of both the First and Third Auxiliary requests.

Following from the board's conclusion regarding claim 1 of the Third Auxiliary request (see point 4.3 above), the board is of the opinion that claim 1 of the Fourth Auxiliary request also lacks clarity within the meaning of Article 84 EPC 1973 for the same reasons as claim 1 of the Third Auxiliary request.

5. Summarising, the board concludes that claim 1 of the Main request as well as of the First and Second Auxiliary requests does not fulfill the requirement of

inventive step according to Article 52(1) EPC and Article 56 EPC 1973. Claim 1 of the Third and Fourth Auxiliary requests does not fulfill the requirement of clarity according to Article 84 EPC 1973.

Since none of the appellant's requests is allowable, the appeal must fail.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

S. Sánchez Chiquero T. M. Häusser

Decision electronically authenticated