

**Internal distribution code:**

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

**Datasheet for the decision  
of 21 June 2022**

**Case Number:** T 1026/17 - 3.5.01

**Application Number:** 06842769.9

**Publication Number:** 2038828

**IPC:** G06Q30/00

**Language of the proceedings:** EN

**Title of invention:**

A PROCESS FOR SECURING TENDERING SYSTEM

**Applicant:**

KOHLI, Jitendra

**Headword:**

Securing a tendering system/KOHLI

**Relevant legal provisions:**

EPC Art. 56

RPBA 2020 Art. 13(2)

**Keyword:**

Inventive step - mixture of technical and non-technical features - bidder created pass-phrases (no - not technical) - main request and auxiliary request I (no)  
Auxiliary request II late filed during oral proceedings - not admitted

**Decisions cited:**

T 0641/00

**Catchword:**

In the Board's judgement it is part of the non-technical requirement specification to keep keys (be it analog or electronic keys) away from people one does not trust. This does not require technical considerations of a technically skilled person. The Board does not consider this to be a technical difference, but to be an administrative consideration within the sphere of a business person when contemplating a secure tender process. It is not regarded as a technical innovation, but a natural choice for the bidders to use individual keys, keep the keys back as long as possible and furnish them as late as possible. And even if this was considered technical, it would, in the Board's view, be obvious to do so.

Furthermore, the Board considers that implementing a functionality in the networked e-tender system corresponding to D1 would be, at the claimed level of generality, obvious in view of the above business related requirement specification. The Board notes that the implementation is claimed in functional terms and neither the claim nor the application as a whole provide details on how encryption/decryption is achieved on a technical level. The application apparently relies in this respect on the skilled person's common general knowledge. The Board notes in this regard that if providing necessary software and data structures were beyond the skilled person's skills, the invention would not be sufficiently disclosed (Article 83 EPC).

Even if the appellant is correct that using different keys for different bidders is a difference over D1, this would in the Board's view imply - in the light of bidders creating their own individual keys for unlocking/decrypting being obvious - that the keys of different bidders are different, too. Therefore creating individual keys/pass-phrases would inherently require the use of multiple keys for implementation.

(See points 4.2 to 4.4 of the reasons)



**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 1026/17 - 3.5.01

**D E C I S I O N**  
**of Technical Board of Appeal 3.5.01**  
**of 21 June 2022**

**Appellant:** KOHLI, Jitendra  
(Applicant) 6 Jain Mandir Road,  
Opposite Shivaji Stadium  
New Delhi 110 001 (IN)

**Representative:** Kuhnen & Wacker  
Patent- und Rechtsanwaltsbüro PartG mbB  
Prinz-Ludwig-Straße 40A  
85354 Freising (DE)

**Decision under appeal:** **Decision of the Examining Division of the  
European Patent Office posted on 22 November  
2016 refusing European patent application No.  
06842769.9 pursuant to Article 97(2) EPC.**

**Composition of the Board:**

**Chairman** W. Chandler  
**Members:** M. Höhn  
Y. Podbielski

## **Summary of Facts and Submissions**

I. This appeal is against the decision of the examining division, refusing European patent application No. 06842769.9 pursuant to Article 97(2) EPC *inter alia* on the ground of lack of inventive step (Article 56 EPC) with regard to prior-art publication:

D1: RONG DU ET AL: "Designing Secure E-Tendering Systems", TRUST, PRIVACY AND SECURITY IN DIGITAL BUSINESS LECTURE NOTES IN COMPUTER SCIENCE; LNCS, SPRINGER, BERLIN, DE, vol. 3592, August 2005 (2005-08), pages 70-79, ISBN: 978-3-540-28224-2.

II. In the statement setting out the grounds of appeal, the appellant requested that the appealed decision be set aside and that a patent be granted on the basis of the main request or auxiliary requests I to III as submitted with the statement setting out the grounds of appeal. Oral proceedings were requested as an auxiliary measure.

III. In a first communication the Board expressed its preliminary opinion that all requests lacked inventive step (Article 56 EPC). Objections under Articles 83 and 123(2) EPC in the contested decision were maintained.

IV. In a reply dated 18 January 2021, the appellant submitted a new main request and auxiliary requests I to III. Oral proceedings were requested as an auxiliary measure, preferably in the form of a videoconference.

V. The Board summoned for oral proceedings. In an annex to the summons the Board maintained the preliminary

opinion that all requests lacked inventive step (Article 56 EPC).

VI. Oral proceedings were held on 21 June 2022 as a videoconference. In the course of the oral proceedings auxiliary requests II and III were withdrawn and a new auxiliary request II was filed. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the main request or auxiliary request I filed with letter dated 18 January 2021 or auxiliary request II filed during the oral proceedings. After due consideration of the appellant's arguments the Chairman announced the decision.

VII. Independent claim 1 according to the main request reads as follows:

"1. A process for conducting electronic tendering over a secure portal server in a networked computer system including clients comprising secure and open means for the bidder and the buyer in a predetermined time locked event and including the following steps:

pre-authentication of the bidder/buyer by means of digital signatures, providing access to the resources of the secure portal server via the networked computer system,

tendering of bids represented by digital data over the secure portal server, integrally evaluating and awarding the bids,

wherein that the tendering of bids includes

online configuring of tendering rules by digitally signing electronic security and tendering policy agreement and an initiating tender floating process modules,

at a client, electronically encrypting bids using bidder created pass-phrase(s), digitally signing of the electronically encrypted bids, and submission using cryptographic protocol,

at the secure portal server, receiving digitally signed and electronically encrypted bids using a cryptographic protocol and storing the received digitally signed and electronically encrypted bids in a time-locked manner so that stored bids are not accessible till a specified date and time have elapsed, and till all the duly authorized tender-opening officers are present online on the system and have recorded their presence on the system with digital signatures,

starting an online tender opening event at the portal server which can be attended electronically and simultaneously by authorized officers of the buyer and authorized representatives of bidders from remote locations as permitted by the rules configured for that tender, and

furnishing the pass-phrase by a concerned authorized bidder for decrypting the respective stored digitally signed and electronically encrypted bid by the attending authorized buyer during the online tender opening event, and

evaluating the bids with parameters permitted as per the rules configured for that tender."

Claim 1 of the first auxiliary request adds to the end the additional feature that "the process further includes providing an electronic attendance register with digital signatures of all authorized participants during the online tendering opening event".

Claim 1 of the second auxiliary request further includes "digitally counter-signing of each opened bid, and generating of downloadable comparative charts generated based on salient points of each bid as submitted to ensure further transparency and non-tampering of opened bids during the online tendering opening event".

## **Reasons for the Decision**

### 1. The invention

The application addresses the problem that tendering processes, comprising actions such as inviting bidders to quote their bids, opening the tenders at a certain date, evaluating the bids and placing an order, are essentially manual processes, which are time consuming, and prone to mistakes and unfair practices. Current systems are alleged to do bidding with rudimentary and restricted features without appropriate security and transparency related features and are found to be unable to appropriately address the issue of variation in the tendering policy, procedures and rules amongst various government organisations globally (see page 1, line 24 to page 2, line 20 of the description).

The invention provides an automatic system for electronically conducting the complete process of

tendering/procurement by government and professional corporate organizations on the Internet/Intranet.

Main request

2. Inventive step - Article 56 EPC

The claimed invention according to independent claim 1 comprises a mix of both technical and non-technical aspects.

2.1 In the Board's view the process of tendering, the associated underlying data such as bids, evaluating and awarding bids or rules configured for a tender and required by the service are business requirements. Such requirements can, in line with the Comvik approach (T 641/00 - *Two identities/COMVIK*), be included in the problem formulation. They are not normally relevant for an assessment of inventive step, since they do not provide a technical contribution.

2.2 In the Board's judgement, the following features of claim 1 form part of the non-technical requirement specification and do not contribute to the technical character:

- conducting tendering over a secure portal comprising secure and open means for the bidder and the buyer in a predetermined time locked event,
  - pre-authentication of the bidder/buyer,
  - tendering of bids over the secure portal, integrally evaluating and awarding the bids,
- wherein that the tendering of bids includes
- configuring of tendering rules and tendering policy agreement and an initiating tender floating process,



at a bidder, signing and sealing/locking of the bids (analogous to a sealed or locked compartment), and submission,

- at the secure portal, receiving signed and sealed bids and storing the received bids in a time-locked manner so that stored bids are not accessible until a specified date and time have elapsed, and until all the duly authorized tender-opening officers are present and have recorded their presence,
- starting a tender opening event at the portal which can be attended simultaneously by authorized officers of the buyer and authorized representatives of bidders from remote locations (e.g. by phone) as permitted by the rules configured for that tender, and
- unlocking the respective stored signed and sealed bid by the attending authorized buyer during the tender opening event, and
- evaluating the bids with parameters permitted as per the rules configured for that tender.

These aspects of claim 1 fall into the sphere of the non-technical business person and are given to the technically skilled person for implementation.

2.3 The technical aspects of the claimed invention are that the tendering process is conducted electronically over a networked computer system involving a portal server and clients. The bids are represented by digital data which is digitally signed and electronically encrypted using a cryptographic protocol.

2.4 Prior art document D1 is considered to be the closest prior art and discloses all of the above mentioned features of claim 1, technical and non-technical ones. D1 explicitly discloses a secure e-tendering system and addresses the need for integrity, confidentiality,

authentication and non-repudiation in e-tendering communications using digitally signed messages (see section 2). In particular, it discloses the consideration of time integrity by closing/opening time issues of an E-Tender Box (see section 2.2) thereby addressing the need for handling the electronic tendering in a time locked manner according to claim 1.

In order to protect the confidentiality of submitted tenders until the pre-accorded opening time, the e-tender box opening time is controlled according to an encryption-based access control mechanism to protect against the main security threat posed by inside attackers to the e-tender box. Since the tender/offer is encrypted and stored before the opening time, even if an insider manages to get access to the submitted tender files, no information will be revealed. The control of a decryption key releasing time can be achieved by many technologies such as time vault service using pairing based encryption (see middle of page 73 of D1). As one embodiment of these "many technologies" D1 discloses a Trusted Third Party (TTP) issuing certificates and cryptographic keys, which also acts as a secure time server (STS) for time synchronisation and time controlled key release (see D1, page 76, paragraphs 3 to 5). Tender submissions are digitally signed and the close of tender stage covers the close of the tender box at a time specified by the principal. Documents submitted by tenderers are then released to the principal for evaluation. The principal will request a key to decrypt the offers from the STS. The STS will only release the key when the tender box is to be opened at or after the tender closing time. After the submission deadline, the principal can evaluate the tenders, i.e. bids (see D1, page 76, paragraphs 3 and 4).

3. The appellant pointed out that D1 stated "...The amount of money and resources involved in many tendered projects may tempt insiders to collude. Ensuring the security of the e-tendering process is paramount." (last 3 lines on page 1). However, D1 did not achieve 100% security of the encrypted bid. It was essentially a distribution of the insiders from one organisation to two organisations. If collusion could be done with one organisation, it could also be done with two organisations. There was nothing that prevented collusion between two organisations. The technical effect, as claimed by D1 itself was only "reducing the chances of collusion" (see section 4, page 78, paragraph 3).

The main object of the present invention was to provide a "process for securing tendering system" (line 28, page 2 of the description). The technical effect of the claimed invention was the total elimination of collusion, as would be evident to a person skilled in the art.

The final technical effect (of ensuring full confidentiality through technical processes), varied depending on which method of encryption was used. Merely using encryption was not enough. D1 did not specify which encryption method it was using. The proposed method in D1 (even though not explicitly defined), was likely to be asymmetric-key. The indicators for this were on page 76, section 3.3. "The STS performs two functions, time synchronisation and time-controlled key release for accessing submitted tenders." Only a single key was being released for accessing all tenders. This would be possible only with an asymmetric key, and not symmetric key. Further, this

key was stored in the server (i.e. STS), and not with the bidder. The final technical effect of D1 was that full-confidentiality could not be achieved, as collusion could occur with administrators of STS.

The invention in claim 1 differed in that bidder-generated passphrase(s) (symmetric key) were used for encryption at the client-end, and the same was used for decryption. There was no dependency for a decryption-key on either the buyer (referred to as Principal in D1), or a third-party. The decryption-key remained with the bidder until the opening. Hence the risk of collusion was totally eliminated.

4. The Board has doubts that the term "pass-phrase(s)" used in claim 1 is disclosed in the application as a symmetric key. Nowhere in the application documents is there a reference to symmetric encryption. Even the term "pass-phrase" is found only twice in the description as filed (on page 17, lines 11 and 16). It is not even explicitly disclosed that a furnished pass-phrase is used for decryption. While the Board accepts that using the pass-phrase for decryption is implicit in the application, it cannot be interpreted as a symmetric key. The application documents do not give details how exactly encryption/decryption is achieved and do not backup the appellant's argumentation in this regard. In the Board's view the claimed invention would equally work with a pair of keys/pass-phrases, one used for encryption and the other for decryption. What is necessary is that the pass-phrase for decryption is furnished by a concerned authorized bidder according to claim 1.

- 4.1 The Board accepts that there is a difference between D1 and the claimed subject-matter as to where the key is

generated. While in D1 the key(s) come from the Trusted Third Party TTP, according to claim 1 the key(s) come from the bidder ("bidder created"). The underlying problem is to keep the keys/pass-phrases confidential as long as possible.

4.2 In the Board's judgement it is part of the non-technical requirement specification to keep keys (be it analog or electronic keys) away from people one does not trust. This does not require technical considerations of a technically skilled person. The Board does not consider this to be a technical difference, but to be an administrative consideration within the sphere of a business person when contemplating a secure tender process. It is not regarded as a technical innovation, but a natural choice for the bidders to use individual keys, keep the keys back as long as possible and furnish them as late as possible. And even if this was considered technical, it would, in the Board's view, be obvious to do so.

4.3 Furthermore, the Board considers that implementing a functionality in the networked e-tender system corresponding to D1 would be, at the claimed level of generality, obvious in view of the above business related requirement specification. The Board notes that the implementation is claimed in functional terms and neither the claim nor the application as a whole provide details on how encryption/decryption is achieved on a technical level. The application apparently relies in this respect on the skilled person's common general knowledge. The Board notes in this regard that if providing necessary software and data structures were beyond the skilled person's skills, the invention would not be sufficiently disclosed (Article 83 EPC).

- 4.4 Even if the appellant is correct that using different keys for different bidders is a difference over D1, this would in the Board's view imply - in the light of bidders creating their own individual keys for unlocking/decrypting being obvious - that the keys of different bidders are different, too. Therefore creating individual keys/pass-phrases would inherently require the use of multiple keys for implementation.
- 4.5 During the oral proceedings the appellant referred to an Expert Opinion of the European Commission. The arguments presented in this regard, however, cannot change the outcome of the Board's analysis as this opinion gives background information, but is not concerned with the issue of technicality.
- 4.6 The Board therefore concludes that the subject-matter according to claim 1 does not involve an inventive step over the disclosure of D1 in view of the skilled person's common general knowledge.

Auxiliary request I

5. The Board considers the additional feature of claim 1 of this request, i.e. an electronic attendance register with digital signatures, to be an obvious implementation of a further non-technical requirement specification, which is dictated by the administrative tendering process. The Board does not consider the fact that the opening event is a meeting to be of technical relevance. In the same way as a traditional tendering process it is regarded as notorious to keep track of who is present in the room and participates in the bidding.

A computer expert provided with the complete description of the non-technical abstract administrative concept including the additional feature, would have considered the claimed implementation obvious in view of the normal skills and the general knowledge of computer programming. The use of digital signatures is regarded as obvious for the same reasons as set out above.

The Board therefore concludes that the subject-matter according to claim 1 of this request also does not involve an inventive step over the disclosure of D1 in view of the skilled person's common general knowledge.

Auxiliary request II

6. Admissibility (Article 13(2) RPBA 2020)

This auxiliary request was filed during the oral proceedings and represents an amendment to the appeal case under Article 13(2) RPBA 2020. Thus, this request is late filed and may only be admitted at the Board's discretion as in principle such late filed requests are not taken into account unless there are exceptional circumstances, which have been justified with cogent reasons.

The appellant argued that the request was filed as reaction to the discussion during the oral proceedings that the opening event does not further improve the whole system. The Board is not convinced. The additional features of claim 1 according to this request are directed to providing feedback of information about opened bids by counter-signing and

providing comparative charts and only come into play after the opening event. This does not answer to aspects discussed during the oral proceedings and has not been addressed before by arguments, neither during appeal nor in the first instance proceedings. The Board does not see any exceptional circumstances which would have prevented the appellant from introducing such features earlier than at the end of the oral proceedings.

Therefore the late filing of this request has not been justified by the appellant and it was not admitted into the appeal proceedings.

## Order

### **For these reasons it is decided that:**

The appeal is dismissed.

The Registrar:

The Chairman:



T. Buschek

W. Chandler

Decision electronically authenticated