**Internal distribution code:**

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

# Datasheet for the decision of 6 February 2018

**Case Number:** T 1170/12 - 3.5.01

**Application Number:** 08802613.3

**Publication Number:** 2286376

**IPC:** G06Q10/00

**Language of the proceedings:** EN

**Title of invention:**
METHOD AND APPARATUS FOR ENABLING ACCESS TO CONTACT INFORMATION

**Applicant:**
III Holdings 1, LLC

**Headword:**
Rights object / III HOLDINGS

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

**Keyword:**
Late-filed request - justification for late filing (no - change of ownership or representation is no justification)
Inventive step - (no - rights object is obvious implementation of non-technical requirement)

**Decisions cited:**
T 0641/00

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 1170/12 - 3.5.01**

# D E C I S I O N
# of Technical Board of Appeal 3.5.01
# of 6 February 2018

| | |
|---|---|
| **Appellant:** (Applicant) | III Holdings 1, LLC<br>2711 Centerville Road, Suite 400<br>Wilmington, DE 19808 (US) |
| **Representative:** | Ablett, Graham Keith<br>Ablett & Stebbing<br>7-8 Market Place<br>London, W1W 8AG (GB) |
| **Decision under appeal:** | **Decision of the Examining Division of the European Patent Office posted on 20 January 2012 refusing European patent application No. 08802613.3 pursuant to Article 97(2) EPC.** |

**Composition of the Board:**

| | |
|---|---|
| **Chairman** | P. Scriven |
| **Members:** | A. Wahrenberg |
| | P. Schmitz |

## Summary of Facts and Submissions

I. The appeal is against the decision of the Examining Division, refusing European patent application 08802613.3 for lack of inventive step (Article 56 EPC).

II. The Examining Division considered inventive step starting from either D2 (US 2006/0075231 A) or a general-purpose distributed information system. Both assessments lead to the same conclusion: that the subject-matter of the independent claims of the main and first auxiliary request did not involve an inventive step.

III. In the statement setting out the grounds of appeal, the appellant requested that the decision to refuse the application be set aside and that a patent be granted on the basis of a main request or a first auxiliary request, both filed with the notice of appeal, the main request corresponding to the first auxiliary request before the Examining Division.

IV. In a communication accompanying a summons to oral proceedings, the Board set out its preliminary observations on the case. The Board tended to agree with the Examining Division that controlling access to contact information was, as such, a non-technical aim. The Board was, however, of the opinion that the encryption scheme defined in claim 1 of the main and first auxiliary requests did not follow directly from any non-technical requirement specification, and agreed with the appellant that D2 disclosed a different encryption scheme. Nonetheless, the Board considered the claimed encryption scheme to be part of the skilled

person's common general knowledge, since it was disclosed in the textbook:

D11: Schneier, Bruce.: "Applied Cryptography: Protocols, Algorithms and Source Code in C, Second Edition", 1995, John Wiley & Sons, chapters 3 and 8.3.

Therefore, the Board gave a negative opinion on inventive step.

V. With a letter dated 8 January 2018, the appellant filed an amended main request and an amended first auxiliary request. The previous main and first auxiliary request were maintained and relabeled as auxiliary requests numbers 2 and 3.

VI. Claim 1 of the main request reads:

*A device (301) for restricting access, by a receiving device, to data fields (701-704) of a data set which is transmitted to that receiving device, the device comprising:*

*means for selecting a said receiving device (302);*

*means for selecting a data set to be transmitted to the selected receiving device;*

*a rights management unit (112) operable:*

*to select, for the selected receiving device, one or more usage permissions (710, 715) of particular data fields (701-704) of the selected data set, and*

*to generate a rights object wherein the selected usage permissions (710, 715) for the selected receiving*

*device (302) are comprised in the generated rights object and are in a form such that a rights management unit of the selected receiving device (302) is enforced to use the selected data set only in accordance with the selected usage permissions (710, 715);*

*means for associating the generated rights object with the selected data set; and*

*means for transmitting (103) the associated rights object to the selected receiving device;*

*wherein the data set comprises contact information having a plurality of contact details as the data fields (701-704).*

VII. Claim 1 of the first auxiliary request differs from the main request by the addition of the following text as the penultimate feature in claim 1:

*"and means to encrypt the rights object using a rights encryption key and to include information to enable the selected receiving device to decrypt a received encrypted data set;"*

VIII. Claim 1 of the second auxiliary request reads:

*A method of enabling access to contact information, the method being performed on a transmitting device (301), the method comprising the steps of:*

*- providing, at the transmitting device (301), a rights object associated with contact information (702-704) for contacting a recipient (301), the contact information (702-704) comprising at least one contact detail selected from the group comprising a telephone*

*number, a cellular phone number, an email address, and an internet based user identification;*

*- transmitting the rights object from the transmitting device (301) to a receiving device (302); and*

*- encrypting the contact information (702-704) and transmitting the encrypted contact information (702-704) from the transmitting device (301) to the receiving device (302);*

*wherein the rights object is such that by receiving said rights object, the receiving device (302), having access to said contact information (702-704), is enabled to contact the recipient (301), and wherein the rights object comprises at least one permission (710) or restriction for displaying a contact detail comprised in said contact information (702-704),*

*wherein the rights object comprises information for decrypting the contact information, and*

*wherein the rights object is encrypted using a rights encryption key.*

IX. Claim 1 of the third auxiliary request differs from the second auxiliary request by the replacement of the final clause by:

*wherein the rights object is encrypted using a rights encryption key such that only a rights management unit (112) of the receiving device (302) can decrypt the encrypted rights object.*

X. The Board held oral proceedings. Nobody was present on behalf of the appellant, as announced by letter in advance.

XI. The appellant's arguments, insofar as relevant to the Board's decision, can be summarised as follows:

There had been a change in both ownership and representation since the filing of the grounds of appeal. For this reason, the Board should adopt a flexible approach in exercising its discretion under Article 13(1) RPBA. The amendments were a genuine attempt to overcome the objections in the Board's communication.

Claim 1 of the amended main request was more restricted compared to previously filed claims. It therefore represented convergent subject-matter.

D2 did not disclose a rights object comprising information for *decrypting* the electronic business card. The electronic certificate in D2 included a public key used for *encrypting* data or for verifying an electronic signature. Furthermore, D2 did not disclose that the electronic certificate itself was encrypted. This would not even make sense, because the electronic certificate did not contain any secret information.

The digital signature, on the other hand, was encrypted using the secret key of the user, but it did not include any information for *decrypting* the business card. Therefore, it could not be read onto the claimed "rights object".

The rights object was a data structure having specific characteristics; it was used to implement a digital

rights management (DRM) scheme. Thus, even if the desire to disclose or not disclose certain personal data was non-technical, this did not imply that the data structure was also non-technical.

The independent claims defined a two-fold encryption scheme, in which the contact information was encrypted, the information for decrypting contact information was combined with at least one permission or restriction so as to form the rights object, and the rights object was encrypted using a rights encryption key. Such an implementation was not rendered obvious by D2 or standard cryptographic operations.

By placing both the content encryption key and the at least one permission or restriction in the same rights object, which was encrypted, it was possible to tie the rights to a DRM agent of the receiving device. This ensured that the permissions or restrictions were respected.

XII. The appellant's final request was that the decision under appeal be set aside and that a patent be granted on the basis of the main request or auxiliary request 1, both filed with the letter of 8 January 2018, or auxiliary requests 2 or 3 which were filed (as the former main request and auxiliary request 1, respectively) with the notice of appeal.

## Reasons for the Decision

1. *Background*

1.1 The invention is about controlling access to contact information, such as a telephone number or an e-mail address. The contact information may be in the form of an electronic business card as shown in Figure 7A of the application as published. When a person (called the "recipient" in the application) exchanges contact information with another person, he may want to control how the other person can use the information. For example, the recipient (i.e. the person who will be contacted) may want the other person to be able to see his work phone number but not his private number.

1.2 The application purports to solve this problem by providing a "rights object" comprising at least one "permission" or "restriction" for using the contact information. The application defines the rights object in general terms as being such that, by receiving the rights object, a receiving device having access to the contact information is enabled to contact the recipient (see paragraph [0006] of the published application).

1.3 Figure 7B shows an example of a rights object for the electronic business card in Figure 7A. It comprises a permission to display the name of the recipient, but no permission to display the phone numbers or VoIP ID. The rights object also contains some constraints. The means of contacting the recipient is restricted to SMS, and the number of times the recipient can be contacted is limited to 2.

1.4 The application sets out that the rights object is managed by a "rights management unit" of the receiving device. The rights management unit of the receiving device ensures that, when receiving the rights object and the contact information, the contact information is only used as defined by the permissions or restrictions in the rights object (paragraph [0042]).

1.5 The application, furthermore, describes that the contact information may be encrypted (paragraphs [0006], [0047], and [0055]). In the second and third auxiliary requests, the rights object comprises information (a key) for decrypting the contact information and the rights object itself is encrypted using a "rights encryption key".

2. *Main request*

2.1 According to Article 12(2) RPBA, the statement setting out the grounds of appeal shall contain the appellant's complete case. Any amendment after that may be admitted and considered at the Board's discretion (Article 13(1) RPBA).

The discretion shall be exercised in view of *inter alia* the complexity of the new subject matter submitted, the current state of the proceedings, and the need for procedural economy (Article 13(1) RPBA). Another established criterion that a Board may consider when exercising discretion under Article 13(1) RPBA is whether the amended subject-matter converges with or diverges from the subject-matter previously claimed (Case Law of the Boards of Appeal of the European Patent Office, 8th edition 2016, chapter IV, section

E.4.4.4).

2.2 A change of ownership or representation does not normally justify late amendments or a divergence from subject-matter previously claimed (Case Law of the Boards of Appeal of the European Patent Office, 8th edition 2016, chapter IV, section E.4.6.1). The new owner takes over the application in the state that it is in at the time of transfer of ownership. The EPO and the public must be able to rely on the steps taken by an applicant, even if the application is subsequently transferred, or the applicant changes representative.

2.3 The Board carried out a preliminary study based on the then pending main request (now second auxiliary request), for which the two-fold encryption, using a first key for the business card and a second key for the rights object, was presented as the pivotal issue.

2.4 The current main request, as well as switching from a method of enabling access to a device for restricting access in claim 1, does not involve encryption. There is little or no overlap between the two versions of claim 1, and the arguments from the statement setting out the grounds of appeal no longer apply. These are all reasons against admitting the main request.

2.5 The appellant argued that the amendments were a genuine attempt to overcome the objections set out in the Board's communication.

While the suitability of the amendments for overcoming objections is a relevant criterion (Case Law of the Board's of Appeal of the European Patent Office, chapter IV, section E.4.4.3), not every amendment that addresses an objection is admissible. In particular,

one that opens up a new discussion may not be.

2.6 As set out above, the Board sees a number of reasons for not admitting the main request. The Board sees no reason that justifies its admission at a relatively late stage in the appeal proceedings. Therefore, the Board does not admit the main request (Article 13(1) RPBA).

3. *First auxiliary request*

3.1 The reasons for not admitting the main request are equally valid for the first auxiliary request, because claim 1 of the first auxiliary request builds on claim 1 of the main request, and although it does mention encryption, the scheme is not the same as in claim 1 of the previous main request.

Claim 1 of the first auxiliary request comprises the feature *"means to encrypt the rights object using a rights encryption key and to include information to enable the selected received device to decrypt a received encrypted data set"*. In the Board's view, this is not the same as including the information for decrypting the contact information in the rights object and encrypting the information for decrypting the contact information (a first key) using a second key.

For these reasons, the Board does not admit the first auxiliary request (Article 13(1) RPBA).

*4. Second auxiliary request*

4.1 The second auxiliary request corresponds to the main request as filed with the notice of appeal and to the first auxiliary request before the Examining Division.

4.2 The Examining Division considered that the subject-matter of claim 1 would have been obvious over D2. The division argued that the rights object in claim 1 differed from the "electronic certificate" and from the "digital signature" in D2 by (i) the at least one permission or restriction, and by (ii) the information for decrypting the contact information being comprised in it. These differences did not involve an inventive step, because (i) did not provide any technical contribution, and because (ii) was an obvious alternative to the encryption scheme in D2.

The Examining Division considered that it would have been obvious to encrypt the business card in D2 using a secret key and to decrypt it using the corresponding public key in the electronic certificate. D2 was said to provided a hint towards that in paragraph [0081].

4.3 The Board is not persuaded that D2 can be read that way. It is not at all clear that the secret key mentioned in paragraph [0081] is part of a key pair comprising the public key in the electronic certificate, for the following reasons:

According to paragraph [0081], the electronic business card may be encrypted by the 3DES algorithm using a secret key. 3DES is a symmetric algorithm, meaning that the electronic business card has to be decrypted using the same secret key.

Furthermore, the public key in the electronic certificate seems to be used for verifying the digital signature (paragraph [0082]). Thus, it appears that it paired with the secret key for generating the digital signature (paragraph [0080]), which is not the same as the secret key in paragraph [0081].

4.4 The Board notes that D2 suggests, in paragraph [0063], that the 3DES algorithm may be carried out by using a public key. This teaching puts the whole meaning of 3DES into question. Therefore, the Board considers that D2 is unclear and unsuitable as starting point for assessing inventive step.

4.5 The Examining Division also considered inventive step over a general-purpose distributed information system. The Board agrees that that is a reasonable starting point. However, the Board considers the electronic business card described in the published application to be closer to the invention as defined in claim 1. The application starts from the scenario of transmitting such an electronic business card to a receiving device (see paragraph [0003]).

4.6 The subject-matter of claim 1 differs from this scenario by:

the contact information being encrypted;

the rights object comprising:
- at least one permission or restriction;
- information for decrypting the contact information; and

the rights object being encrypted using a rights encryption key.

4.7 The Board agrees with the Examining Division that controlling access to information is not, as such, a technical aim, and that the technical contribution is provided by the implementation of the non-technical aim using technical means. In accordance with the COMVIK-approach (see T 641/00 - Two identities/COMVIK, OJ 2003, 352), only those features that provide a technical contribution can contribute to inventive step. The non-technical features may appear in the problem formulation as a requirement to be met.

4.8 The Examining Division considered whether the at least one permission or restriction in claim 1 contributed to the technical implementation and found that it did not do so. The Board agrees. Claim 1 defines the at least one permission or restriction as some information comprised in the rights object. The actual enforcement of the permission or restriction must be ensured by the rights management unit of the receiving device, which is outside the scope of claim 1. Thus, the at least one permission or restriction as defined in claim 1 is just some information describing the recipient's contact preferences. This is no more technical than the contact information itself. Moreover, the recipient's contact preferences may, for non-technical reasons, be just as sensitive as the contact information to which they apply.

4.9 The remaining features of claim 1 define a scheme in which the contact information is encrypted, and the key for decrypting the contact information is transmitted to the receiving device in a rights object. The encryption protects the contact information from access by third parties. However, since anyone having access to the decryption key can decrypt the contact information, the transmission of the decryption key

needs to be protected. For that reason, the rights object is encrypted using a second key. This has the result that the at least one permission or restriction comprised in the rights object is also protected.

4.10 Therefore, the Board considers that the technical problem solved by subject-matter of claim 1 is how to protect the contact information and the at least one permission or restriction from access by third parties.

4.11 The skilled person is someone familiar with data transmission and the security issues that may arise. That person knows about symmetric encryption and the problems that arise when the key itself has to be transmitted. A well-known solution to that problem is to use a key-encryption key for encrypting the data encryption key. That is common general knowledge in the art, as shown by D11 (see, for example, the third paragraph of section 8.3).

4.12 The encryption scheme described in D11 is universal in the sense that it can be applied to any type of data. Therefore, the skilled person would have used it for protecting the contact information and the at least one permission or restriction as defined in claim 1 of the second auxiliary request.

4.13 The appellant argued that, by placing both the data encryption key and the at least one permission or restriction in the same rights object, which was encrypted using a second key, it was possible to tie the rights object to a rights management unit of the receiving device. This particular arrangement ensured that the permission or restriction was respected.

4.14 The appellant's arguments do not persuade the Board. As already concluded above, the enforcement of the permission or restriction is outside the scope of claim 1. The skilled person faced with the problem of providing secure transmission of the contact information and the at least one permission or restriction would have to choose some sort of data structure. He could provide the data encryption key and the at least one permission or restriction as one "object". He could also transmit (and encrypt) the different data pieces separately. These are different possibilities that the skilled person would consider, without using any inventive skill.

4.15 In conclusion, the Board finds that the subject-matter of claim 1 of the second auxiliary request does not involve an inventive step (Article 56 EPC).

5. *Third auxiliary request*

5.1 Claim 1 of the third auxiliary request adds, over the second auxiliary request, the feature that the rights object is encrypted such that only a rights management unit of the receiving device can decrypt the encrypted rights object.

5.2 The Board considers this feature to be already implied by the features of the second auxiliary request, because the purpose of encryption is to establish a secure channel. The receiving device must have suitable means for decrypting the rights object, otherwise the invention would not make any sense.

5.3 Therefore, the third auxiliary request lacks inventive step (Article 56 EPC) for the same reasons as the second.

**Order**

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

The appeal is dismissed.

The Registrar: The Chairman:

T. Buschek P. Scriven

Decision electronically authenticated