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 November 2018

Case Number: T 0075/17 - 3.5.06

Application Number: 10708607.6

Publication Number: 2406712

IPC: G06F9/445, G06F21/00, H04L29/08, H04L29/06

Language of the proceedings: EN

Title of invention:
METHOD FOR TRANSMITTING AN NFC APPLICATION AND COMPUTER DEVICE

Patent Proprietor:
NXP B.V.

Opponent:
Giesecke & Devrient GmbH

Headword:
Transmitting an NFC application/NXP

Relevant legal provisions:
EPC Art. 56

Keyword:
Inventive step (all requests) - no

Decisions cited:
G 0003/14

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 0075/17 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 6 November 2018

Appellant: (Opponent)	Giesecke & Devrient GmbH Patent und Lizenzen Prinzregentenstrasse 159 81677 München (DE)
Representative:	Bornhäuser, Frank Giesecke & Devrient GmbH Patent- und Lizenzabteilung Prinzregentenstrasse 159 81677 München (DE)
Respondent: (Patent Proprietor)	NXP B.V. High Tech Campus 60 5656 AG Eindhoven (NL)
Representative:	Krott, Michel NXP B.V. Intellectual Property & Licensing High Tech Campus 60 5656 AG Eindhoven (NL)
Decision under appeal:	**Decision of the Opposition Division of the European Patent Office posted on 31 October 2016 rejecting the opposition filed against European patent No. 2406712 pursuant to Article 101(2) EPC.**

Composition of the Board:

Chairman	W. Sekretaruk
Members:	M. Müller
	G. Zucka

Summary of Facts and Submissions

I. The appeal is against the decision of the opposition division, dispatched with reasons dated 31 October 2016, to reject the opposition against European patent No. 2 406 712 because none of the grounds for opposition prejudiced the maintenance of the patent as granted.

II. The opponent (appellant) appealed this decision and requested that the decision be set aside and the patent be revoked (see the notice of appeal dated 28 December 2016 and the statement of grounds of appeal dated 15 February 2017) for lack of novelty or inventive step (Articles 54, 56 and 100(a) EPC) over the document

D4: GSMA, "mobile NFC technical guidelines - Version 2.0", November 2007.

In contrast to the initial notice of opposition, the appellant no longer challenged the patent under the grounds for opposition under Article 100(b) and (c) EPC or in view of other documents except D4.

III. The proprietor (respondent) replied by letter dated 23 June 2017 and requested that the appeal be rejected and that the patent be maintained as granted, or, alternatively, on the basis of claims according to one of three auxiliary requests filed with that letter.

IV. In an annex to a summons to oral proceedings, the board informed both parties of its preliminary opinion that claim 1 of all requests lacked inventive step over D4.

V. In response to the summons, with a letter dated 5 October 2018, the respondent filed amended claims according to auxiliary requests 2-4.

VI. Claim 1 of the patent reads as follows:

"A method for transmitting an NFC application, comprising the steps of:

establishing, by means of a proxy, a secure channel between a Trusted Service Manager and an NFC device via a computing device comprising the proxy and via an RFID reader of the computing device, the RFID reader having reading and writing capabilities, and

channeling, by utilizing the proxy, to the NFC device an NFC application intended for the NFC device and received at the computing device from the Trusted Service Manager through the secure channel,

receiving the NFC application at the NFC device utilizing an NFC interface of the NFC device."

Claim 1 of auxiliary request 1 corresponds to claim 1 as granted with the addition of the following step, inserted between the steps of "establishing" and "channeling":

"... exchanging keys stored on a memory of the NFC device and associated with the NFC device and/or a user of the NFC device between the NFC device and the Trusted Service Manager utilizing the proxy and the reader for establishing the secure channel, ..."

Claim 1 of auxiliary request 2 is identical to claim 1 of auxiliary request 1, except that the following phrase is added to the step of "establishing":

"... wherein the proxy is part of the computing device and the computing device is connected to or comprises the RFID reader ..."

Claim 1 of auxiliary request 3 is identical to claim 1 of auxiliary request 2, except for the addition of a further phrase to the step of "establishing", namely:

"... and wherein the RFID reader does not comprise the proxy ...".

Claim 1 of auxiliary request 4 is identical to claim 1 of auxiliary request 3 except for the following additions made at its end:

"... wherein the computing device is a point of sale, a home computer, or a PDA,
wherein the NFC device is a mobile phone, a plastic card, or a non-connected NFC device,
wherein the NFC application is a transport application, a payment application, a loyalty application, an event ticket, or a governmental application, and
wherein the NFC application comprises reloading or revocation".

All the requests further contain an independent computing device claim formulated by reference to the independent method claim 1.

VII. Oral proceedings were held on 6 November 2018 as scheduled. At the end, the chairman announced the decision of the board.

Reasons for the Decision

The invention

1. The application generally relates to a way of "transmitting an NFC application" to an NFC device such as a mobile phone (see the application as originally filed, e.g. page 1, lines 3-4, 11-12, and 23-24).

1.1 NFC devices are used for contactless services such as ticketing in public transportation (see page 4, lines 20-27).

1.2 For transmitting NFC applications to an NFC device, it is disclosed as known to utilise a "Trusted Service Manager" (TSM) which communicates with a proxy on the mobile phone "over the air" (OTA), e.g. via GSM (lines 17-28).

1.3 The declared object of the invention is "to provide an alternative method to transfer an NFC application to an NFC device" (lines 33-34).

1.4 As a solution, it is proposed that the TSM "establish a secure channel" to the NFC device "via" a computing device "comprising" a "proxy" and an RFID reader with "reading and writing capabilities" (see e.g. page 2, lines 5-7 and 24-25). The proxy is an "application" which "run[s] on the computing device", i.e. a piece of software (see page 2, lines 18-19). As to its function, it is only said that "due to the proxy the" TSM "can communicate with the NFC device in a secure manner" (lines 22-23). As to its location, it is disclosed that the proxy can be part of a "point of

sale" or any other "computing device" such as "a PC or a PDA, which are connected to or comprise a RFID reader" (see page 5, lines 18-20).

Claim construction

2. The claims of all requests use terminology, the precise meaning of which may not be immediately evident. It must therefore be determined how the skilled person would understand these claims before an assessment is possible of whether the claimed subject-matter is new or inventive over the prior art.

2.1 The board appreciates that lack of clarity is not a ground for opposition and thus cannot normally be objected to in opposition (see G 3/14). However, as the Enlarged Board has pointed out, issues related to clarity may nonetheless have to be addressed in opposition because "the uncertain boundaries of a claim [...] may play a role when arguing the various grounds for opposition" (see G 3/14, point 80 (g) of the reasons).

2.2 A central feature of claim 1 in all requests is the feature "establishing, by means of a proxy, a secure channel between a" TSM "and an NFC device via a computing device comprising the proxy and via an RFID reader of the computing device, the RFID reader having reading and writing capabilities". The following questions arise in construing this phrase:

a) What is a "secure channel"?
b) Are the claimed "NFC device" and the "computing device" separate from each other?
c) How do the "proxy" and the "RFID reader" in the "computing device" relate to each other?

2.3 Claim 1 of all requests refers to an "RFID reader having reading and writing capabilities". It must be determined

d) how the RFID reader is limited by having, in particular, "writing capabilities".

2.4 Claim 1 of all requests specifies that it is an "NFC application" which is transmitted. Hence, it must also be determined

e) what, in general, is an "NFC application" and how is claim 1 limited by the reference to an "NFC application".

3. The board takes the following view.

3.1 *Re a)* In claim 1 of the main request, no features are specified that might make a channel secure.

3.1.1 The description discloses that the channel may be secured by exchanging keys between the NFC device and the TSM (see page 3, lines 1-5, and page 5, lines 3-7). This feature has been incorporated into claim 1 of all auxiliary requests. As regards the main request, the board finds that the claimed "secure channel" cannot be identified with just any channel but instead requires that some - undefined - measures are taken to protect privacy of the transmitted content.

3.1.2 This issue need not be discussed further, however, because the board has come to the conclusion that the specific security measure end-to-end key exchange according to the auxiliary requests does not render the claims inventive (see below).

3.2 *Re b)* Conventional use of language dictates that the "computing device", "via" which a channel to the "NFC device" is established, and the "NFC device" itself must be distinct.

3.3 *Re c)* The proxy and the RFID reader are different already because they are pieces of software and hardware, respectively.

3.3.1 Apart from that, claim 1 of the main request and auxiliary request 1 merely refers to the "computing device comprising the proxy" and to the "RFID reader of the computing device", which, in the board's judgment, does not exclude that the proxy "runs on" the RFID reader. The same applies to claim 1 of auxiliary request 2 because it subsumes the option that the "proxy is part of the computing device" and the "computing device [...] comprises the RFID reader".

3.3.2 Claim 1 of auxiliary requests 3 and 4 specifies explicitly that "the RFID reader does not comprise the proxy". According to the respondent, this feature is disclosed in figure 2. During the oral proceedings, the original disclosure of this feature was not challenged (Article 123(2) EPC).

3.4 *Re d)* The description mentions the RFID reader as "having reading and writing capabilities" in several places but does not explicitly define the "writing" capabilities. It is evident that the RFID reader must be able to send information to the NFC device, namely the NFC application. The appellant pointed out that, normally, the skilled person would not assume that the RFID reader could "write" directly into the local memory of the receiving NFC device and that the description does not disclose that it did. From that

perspective, "writing" would have to be construed as "sending". The respondent did not challenge this interpretation and the board agrees. The board also notes that the claimed invention (all requests) does not make use of any "writing capabilities" of the RFID reader except for "channeling", i.e. sending, the NFC application to the NFC device.

3.5 *Re e)* The description specifies NFC applications mostly in terms of function, for instance as "a transport application, a payment application, a loyalty application, an event ticket or a governmental application" (see page 4, lines 20-23 of the original description, and claim 1 of auxiliary request 4). Moreover, original claim 8 specifies that "the NFC application [...] comprises reloading or revocation", whereas the original description (see page 3, lines 20-21, and again claim 1 of auxiliary request 4) refers to "actions related to issuing the NFC application to the NFC device, including reloading or revocation". The respondent explains that reloading and revocation essentially mean the updating and deletion of an NFC application (see its letter of 5 October 2018, page 8, paragraph 2).

3.5.1 According to the respondent, it follows from the description that NFC applications must be construed as "complex", i.e. large, "software applications" with high data security requirements (*loc. cit.*).

3.5.2 The board does not agree that the description implies a particular minimal size for the NFC applications to be transmitted. Whether an NFC application implies high data security requirements can be left open in view of what follows.

The prior art

4. D4 is one of a "series of technical guidelines intended to support NFC standardisation and technology implementation activities" developed by several mobile network operators cooperating in a GSM Association initiative (see page 1, paragraph 1 and paragraph 3 from the bottom).

4.1 D4 discloses the over-the-air (OTA) provisioning of "NFC Services" (see e.g. page 40, section 7.2.2.1, and page 41, section 7.2.3.2) via a "Trusted Service Manager" to NFC devices such as mobile phones (see figures 1, 9, 11, 12 and 15 and figure 7 on page 29 of the appendix; page 8, section 2, introduction; page 34 *et seq.*, section 7.1.3; page 38, section 7.1.3.3). D4 discloses the use of encryption in this context (see, for instance, figure 12). D4 also mentions several earlier systems, in particular Mifare (= MIKRON Fare Collection), FeliCa (= Felicity Card) and EMV (= Europay, MasterCard, Visa), which were typically used for payment and transport applications (see for instance section 8.5.1, appendix, page 21).

4.2 D4 discloses several alternatives for the transmission of data and applications (page 41, section 7.2.3.2). One of them, SMS, although being disclosed for "Midlet installation", is said to be unsuitable for the transport of "heavy applications", i.e. applications larger than 1kb, because an individual SMS (then) contained only 140 bytes of data (see page 41, paragraphs 1 and 4). "Commands", however, such as "install, install for make selectable and [i]nstall for personalisation can be easily encapsulated in SMS" (page 41, paragraph 2; but see also page 40, section 7.2.2.2).

4.3 As another alternative, the option "Through NFC reader" is disclosed (see page 41, paragraph 9, just before section 7.2.3.3). This paragraph states that "commands are encapsulated in HTTP, sen[t] to a Proxy application in an NFC reader" and then "sent over Radio Frequency (RF) field to the UICC", i.e. the universal integrated circuit card, on the mobile device. It is also stated that "The use of this transport channel is based on the same process as OTA management".

Novelty and inventive step

5. The appellant's objection to claim 1 of the patent as granted turns, in particular, on the disclosure of the above-mentioned section "Through NFC reader" in D4 (page 41). During the oral proceedings, the appellant stressed that this passage had to be read in the context of the entire document D4. In particular, it argued that the reference to "the same process as OTA management" in that passage implied, *inter alia*, encrypted end-to-end communication between the service provider and the UICC (by reference, in particular to figure 12), and the mention of "commands" had to be construed as subsuming entire applications.

6. The board considers that the skilled person would understand this passage and its context as follows.

6.1 The NFC reader is disclosed as a component separate from the UICC because they are connected via RF. For the same reason, the NFC reader is at least suggested to be separate from the mobile phone, which contains the UICC. If both were contained in the mobile phone, it would seem more plausible to use a wired connection. The NFC reader qualifies as a "computing device", because it executes a "proxy application". The commands

must be construed as those mentioned above in section 7.2.2, in particular in section 7.2.2.2 on page 40. D4 does not disclose, clearly and unambiguously, that the communication between the NFC reader and the UICC must be secured by encryption. In particular, it is not evident what precisely the reference to the "same process as OTA management" means in this respect.

6.2 From that perspective, D4 discloses a method for transmitting "commands" by establishing a channel between the TSM and an NFC device, via a "computing device comprising [a] proxy". As the proxy is part of the channel, it may also be said that the channel is established "by means of [the] proxy".

6.3 The board also takes the view that the "NFC reader" in the cited passage of D4 subsumes the "RFID reader" as claimed, following here the appellant's argument that "NFC" is based on "RFID".

7. In the decision under appeal, three differences between claim 1 as granted and D4 are assumed (see point 3.3 of the reasons), namely

i) a secure channel via a[n] RFID reader;
ii) an RFID reader having reading and writing capabilities;
iii) transmitting an NFC application to the NFC device using the established secure channel.

7.1 The respondent stated that a further difference is

iv) that the proxy is not comprised in the RFID reader.

7.2 The board agrees with differences i) and iii) but does not agree that ii) constitutes a difference (see point 9 below). As argued above, the board also does not accept difference iv) for the main request.

7.3 The board also considers that the mentioned differences do not interact with each other in a surprising manner, so that their inventive merit may be assessed separately. Specifically, channel security (feature i)) is an issue irrespective of what is being transmitted (feature iii)), and no non-trivial effect of separating proxy and RFID reader could be determined at all.

Main request

8. *Re i*) Even though D4 may not disclose the channel to be secure, the board concurs with the appellant that the context of D4 at least suggests the relevance of securing the provisioning channel by encryption. Beyond that, however, the achievement of channel security by encryption was well-known long before the priority year 2009 of the present application.

8.1 The board thus concludes that the skilled person would find it obvious, as a matter of common practice, to secure the transmission channel to address common transmission risks (in this regard, see also the grounds of appeal, the paragraph bridging pages 1 and 2).

8.2 Even if it might sometimes "make sense", as the respondent puts it (see its letter, page 6, paragraph 2), to afford less protection to "commands" than to entire applications, it would still be obvious to protect the transmission of commands too. Tampering,

for instance, with an installation command, may have very undesirable consequences.

9. *Re ii)* The respondent accepts that the NFC reader of D4 has reading capabilities and claims that it need not have "writing capabilities". It must, however, at least have "sending capabilities" to transmit the commands. In view of the above analysis, the board thus concludes that the NFC reader must be construed as having "reading and writing capabilities" within the meaning of claim 1.

10. *Re iii)* D4 discloses that SMS, each containing at most 140 bytes, "is not suitable for the loading of heavy applications (above 1kb)". This at least suggests that there are applications which are larger than a single SMS but for which SMS still is "suitable".

10.1 The board agrees with the respondent that D4 does not exclude the possibility that the applications are transported over a different channel than the commands (see the respondent's letter, page 6, paragraph 2, and page 9, paragraph 3).

10.2 In contrast to such a scenario, it would be a simplification in terms of speed and technical complexity if it were made possible, as claimed, to transport entire "NFC applications" over the same channel as the commands.

10.3 The board finds it obvious for the skilled person to consider this option at least for the small applications mentioned above. It does not withstand this conclusion if the channel via the NFC reader were disclosed in D4 only as a "minor option" (see the

respondent's letter, section 4.1.1.3, esp. page 7, last paragraph).

11. In summary, the board concludes that claim 1 of the patent lacks inventive step over D4.

Auxiliary request 1

12. Claim 1 of auxiliary requests 1-4 contains the additional feature of "exchanging keys stored on a memory of the NFC device and associated with the NFC device and/or a user of the NFC device between the NFC device and the Trusted Service Manager utilizing the proxy and the reader for establishing the secure channel".

13. In this context, the board first notes that asymmetric encryption was commonly known in the art well before 2009.

13.1 In asymmetric encryption, the sender encrypts a message with the receiver's public key and the receiver decrypts it using its private key.

13.2 This is end-to-end encryption. Intermediate devices passing on an encrypted message are unaffected, particularly if - as the NFC reader in the D4 - they are not interested in the transmitted content.

13.3 As the receiver of an encrypted message needs its private key for decryption, it is an obvious option for that key to be stored in the receiving device. The board also considers it as an obvious option to store the corresponding public key alongside the private key and to make it available to the sender when needed.

13.4 The board thus concludes that claim 1 of auxiliary request 1 also lacks inventive step over D4 and common knowledge in the art (Article 56 EPC).

Auxiliary request 2

14. Claim 1 of auxiliary request 2 further requires that the "proxy is part of the computing device and the computing device is connected to or comprises the RFID reader". As explained above (point 3.3.1), this language is considered not to change claim 1 in substance. The board thus concludes that claim 1 of auxiliary request 2 also lacks inventive step over D4 and common knowledge in the art (Article 56 EPC).

Auxiliary request 3

15. Claim 1 of auxiliary requests 3 and 4 further specifies that "the RFID reader does not comprise the proxy".

15.1 During the oral proceedings, the respondent stated that the separation of RFID and proxy increased the flexibility of the solution of D4 because it did away with the requirement that the UICC had to be kept in radio distance to the "computing device".

15.2 However, even if separate, claim 1 still requires both RFID reader and proxy to be part of the same computing device. Hence, the required proximity between the NFC device and the computing device as claimed remained dictated by the RFID reader comprised in the computing device. The separation of proxy and RFID reader thus does not achieve the alleged flexibility.

15.3 The respondent did not propose any other effect achieved by the claimed separation of the RFID device and proxy, nor can the board think of any. The board therefore judges that this feature is an obvious modification of the system of D4 within the competence of the person skilled in the art.

Auxiliary request 4

16. Claim 1 of auxiliary request 4 specifies that

A) "the computing device is a point of sale, a home computer, or a PDA",
B) "the NFC device is a mobile phone, a plastic card, or a non-connected NFC device",
C) "the NFC application is a transport application, a payment application, a loyalty application, an event ticket, or a governmental application", and
D) "the NFC application comprises reloading and revocation".

16.1 *Re A)* On the understanding that, according to D4, the NFC device (i.e. the "computing device" as claimed) need not be integrated in the mobile phone (see point 6.1 above), it would be obvious to "put it elsewhere", i.e. integrate it in some other suitable device. In the board's judgment, all three claimed alternatives are obvious alternatives. Further, the description does not place importance on this choice. Moreover, the incorporation of the claimed "computing device" in, for instance, a "home computer", does not affect the claimed "method of transmitting an NFC application", in particular not the nature of the "NFC application" or the implied security requirements.

16.2 *Re B)* The UICC of D4 must already be construed as a "plastic card".

16.3 *Re C) and D)* Indicating, in vague terms, the purpose and functions of the NFC application does not, in the board's judgment, imply any specific technical feature of the NFC application or the message of transmitting one in a way which could change the preceding inventive-step analysis.

16.4 The board thus concludes that claim 1 of auxiliary request 4 also lacks inventive step over D4 and common knowledge in the art (Article 56 EPC).

General remark

17. The respondent complained in its letter of 5 October 2018 that the board had not used the problem-solution approach in its preliminary opinion, but had "merely comment[ed] on different ones of the distinguishing features separately and mention[ed] the term 'obvious'" (see page 13, last paragraph). The problem-solution approach, however, required that "the distinguishing features that provide a technical effect in combination [had] to be considered in combination with each other" (page 14, paragraph 1). As stated in point 7.1, however, the respondent could not convince the board of the alleged synergy of the distinguishing features. Therefore, it is sufficient according to the problem-solution approach to consider separately which problem each of the distinguishing features solves. The above analysis does this (see in particular, points 8.1, 8.2, 10.2 and 10.3).

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.
2. The European patent is revoked.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated