Internal distribution code:

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

Datasheet for the decision of 4 October 2016

Case Number: T 2425/13 - 3.5.06

Application Number: 04023384.3

Publication Number: 1536306

IPC: G06F1/00

Language of the proceedings: EN

Title of invention:
Proximity authentication system

Applicant:
NXP B.V.

Headword:
Proximity authentication system/NXP

Relevant legal provisions:
EPC 1973 Art. 56
EPC R. 103(1)(a)
RPBA Art. 11

Keyword:
Inventive step - (no)

Decisions cited:
T 1742/12

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Catchword:

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Case Number: T 2425/13 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 4 October 2016

Appellant: (Applicant)	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 Examining Division of the European Patent Office posted on 26 July 2013 refusing European patent application No. 04023384.3 pursuant to Article 97(2) EPC.**

Composition of the Board:

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

Summary of Facts and Submissions

I. The appeal lies against the decision of the examining division, with reasons dispatched by letter of 26 July 2013, to refuse European patent application No. 04 023 384.3 for lack of inventive step over

D3: US 6 088 450 A.

II. Notice of appeal was filed on 7 October 2013, the fee being paid on the same day. A statement of grounds of appeal was filed on 27 November 2013 along with three sets of claims 1-15, 1-10 or 1-8 according to a main and two auxiliary requests. The appellant requested that the decision under appeal be set aside and that a patent be granted based on one of these sets of claims in combination with the application documents on file, and that the appeal fee be reimbursed pursuant to Rule 103(1)(a) EPC, because the decision was insufficiently reasoned, Rule 111(2) EPC, and based on grounds on which the appellant had not had the opportunity to comment, Article 113(1) EPC 1973.

III. In an annex to the summons to oral proceedings, the board informed the appellant of its preliminary opinion that the claimed invention lacked inventive step over D3. An objection under Article 123(2) EPC was also raised. Moreover, the board was not convinced that a substantial procedural violation had occurred. Beyond that, however, it stated that the alleged procedural deficiencies did not warrant a direct remittal of the case to the department of first instance und Article 11 RPBA.

IV. Oral proceedings were held on 4 October 2016, during which the appellant filed claims 1-15 according to a new and sole auxiliary request.

V. Claim 1 of the main request reads as follows:

"A method of providing access to a service comprising:
receiving an RF signal (108, 330) from a proximate wireless token (104, 316) by a wireless proximity reader (106, 306) comprised in an integrated circuit (312);
obtaining (410) information from the RF signal (108, 330) indicating proximity of the wireless token to the integrated circuit (312);
encrypting or signing the information by a cryptographic processor (114, 308) comprised in the integrated circuit (312), and
sending the encrypted or signed information by a service access processor (310) to a service provider (110,304); and
providing (420), by the service provider (110, 304), access to a service."

Claim 1 of the auxiliary request differs from claim 1 of the main request only in that the "sending" step reads as follows (emphasis by the board):

"... sending the encrypted or signed information by a service access processor (310) via a network to a service provider (110,304); ..."

Both requests comprise another independent claim directed to an integrated circuit with features corresponding to those of the respective independent method claim 1.

VI. At the end of the oral proceedings, the chairman announced the decision of the board.

Reasons for the Decision

Article 11 RPBA

1. The appellant argues that the decision of the examining division was insufficiently reasoned (Rule 111(2) EPC) because it was based on unproven assertions of and allusions to what had been known to the skilled person (see grounds of appeal, section B). It further suggests (point B.1.3) that the examining division may not have raised these points during the oral proceedings (Article 113(1) EPC 1973).

1.1 The board does not consider that the decision is insufficiently reasoned in this respect, because it sets out what the examining division considered to be common knowledge in the art and why, in its view, this rendered the claimed invention obvious over D3.

1.2 The board is unable to deduce from the file - and in particular from the minutes - whether these statements were made explicitly during the oral proceedings or appeared only in the written decision. However, the board notes that the examining division had already expressed in the summons to oral proceedings its general understanding of the pertinent common knowledge in the art (see point 6.5). On this basis, the board disagrees with the appellant's suggestion that the decision might be based on grounds on which it did not have the opportunity to comment.

1.3 The board also takes the view that the statements in question are neither unreasonable or speculative, nor central to the decision under appeal. Thus, even if it were assumed, for the sake of argument, that they were made without proof and were hence objectionable, no purpose would have been served by the board remitting the case for further prosecution to the department of first instance without having assessed its merits.

1.4 The board considered this to constitute a special reason within the meaning of Article 11 RPBA for not remitting the case.

The invention

2. The invention relates to controlling user access to a computing service.

2.1 The proposed security architecture comprises

i) a wireless proximity (e.g. RFID) token with which the user produces his credentials (see figures 1 and 3, nos. 104 and 316; page 23, lines 7-10);
ii) the service provider (nos. 110 and 304), and
iii) a mediating "access device" (nos. 102 and 302).

2.2 The service provider may be accessible over a network and thus separate from the access device, or both may be integrated in one device (see esp. figure 8 and page 34, lines 3-9 and 22-23).

2.3 The access device comprises the wireless proximity reader which will request and receive credentials from the token (such as the token identity and a user's password). This information is encrypted or signed by a cryptographic processor (see figures 1 and 3, nos. 114

and 308) before being forwarded to the service provider (see page 18, lines 22-33; page 22, lines 16-20), where it will be used to verify that the user is authorized to access the requested service (page 18, line 34, to page 19, line 5; page 26, lines 20-23). It is disclosed that components may be placed with a single integrated circuit for security reasons (page 21, lines 25-27). For example, this applies to the wireless proximity reader which may be integrated with the cryptographic processor (page 21, lines 27-30; see also figure 3, nos. 306, 312, and 320).

2.4 A typical application scenario is depicted in figure 6 and explained on page 29 *et seq.*. A user may try to access a service from a mobile device (a laptop, PDA or smartphone) containing the access device (figure 6, nos. 602, 604 and 606), and access may only be authorized if the user places a suitable wireless token (618) close to the mobile device.

The prior art

3. D3 discloses a wireless authentication system based on an RFID token communicating with a "security device" implemented within a computer "node" in a network (nos. 110, 120, 213 in figures 1, 3 and 4; column 3, line 52, to column 4, line 11).

3.1 Communication between token and security device is encrypted (in at least one direction; see column 4, lines 12-19) and successful authentication of the token gives the user carrying it access to the computer and its possibly networked resources (see also column 4, lines 12-19, and column 5, lines 24-33). The security device is disclosed to contain one or more processors

and a memory and to have the relevant cryptographic capabilities; optionally, processor and memory may be combined in one integrated circuit to mitigate the risk o f tampering (column 5, lines 34-49). The same optional integration is disclosed for the token (column 5, lines 56-59, figure 3).

3.2 D3 contemplates that, in addition to the token authentication, another, further authentication step may be required (column 4, lines 20-27; column 7, lines 35-62), based e.g. on a PIN or a fingerprint entered on the token (*loc. cit.* in column 7). D3 discloses that normally the security device validates the credentials received from the token (see column 4, lines 12-19, and column 7, 28-34), but also that the "authentication operations could be performed by the host processor", provided that the bus communication was safe (column 4, lines 44-49 and figure 2).

Article 56 EPC 1973, Main request

4. The board agrees with the decision under appeal that D3 is a suitable starting point for the assessment of inventive step. As regards the main request, the appellant has not challenged this.

5. The board agrees with the analysis of the examining division, which was also not challenged by the appellant, according to which the features of the independent claims which are not known from D3 are that

(a) the wireless proximity reader is not integrated with the cryptographic processor in an integrated circuit; and that

(b) the "information from the RF signal" is encrypted or signed by the "integrated circuit" in the "service access processor" before it is sent to the service provider.

5.1 Regarding difference (b), the board notes that the host processor must be considered to constitute a "service provider" within the meaning of the claims, as it controls the access to the relevant contents, resources or functionality (see column 4, lines 12-19, and column 5, lines 24-33). In this regard it is noted that claim 1 does not define either the service or the service provider in any detail, so that both must be construed broadly.

5.2 Using encryption according to difference (b) makes communication between the service access processor and the service provider more secure. Circuit integration according to difference (a) may have several effects. On the one hand, as an integrated circuit can be less easily tampered with, the communication between the wireless proximity reader and the cryptographic processor is better protected against eavesdropping. Integrated circuits, however, may also have other advantages, such as being smaller, faster and more reliable.

5.3 The board accepts the appellant's argument that both differences have some impact on security and also notes that differences (a) and (b) are interdependent to some extent because it is the cryptographic processor of (a) which is referred to in (b). On the other hand, the board notes that security of communication between the service access processor and the service provider can be addressed separately from the integration of the

wireless reader and with the service access processor, be this to ensure secure communication between these two components, or for other reasons such as miniaturization.

5.4 At any rate, due to the mentioned interdependence, the board considers that the inventive step of providing a cryptographic processor must be assessed first.

6. The independent claims do not specify what kind of information is obtained "from the RF signal", encrypted or signed and sent on to the service provider, or what the service provider does with it. It must therefore be assumed that the transmission of the information is a given, i.e. part of the problem rather than the solution. On that assumption, the board considers it to be obvious to use encryption to protect that transmission against eavesdropping and an electronic signature to establish the authenticity of the transmitted data.

7. According to the description, the information received and sent on comprises credentials which are provided by the token but evaluated and validated only by the service provider (see e.g. page 26, lines 11-26).

7.1 The appellant argues that in D3 it is the "security device" which verifies whether the token has responded correctly to the challenge and to whether or not to grant access to the required contents and resources (see column 4, lines 12-19) and that, therefore, there is no need to transmit any information from the token via the security device to the host, let alone any encrypted information (see grounds of appeal, points III.3 to III.3.6).

7.2 The board does not accept this argument.

7.2.1 D3 discloses that "the wireless authentication system may be utilized with another authentication system" based on passwords, smartcards or biometrics (see column 4, lines 20-27). As one specific example, it is disclosed that "a thumbprint or fingerprint reader could be integrated into the token" (see column 7, lines 35-62, esp. lines 51-53).

7.2.2 Furthermore, it is disclosed that "authentication operations" may not be carried out by the security device but on the host processor, on the condition that the bus is secure against eavesdropping (column 4, lines 44-49). This implies that, in order to enable the host processor to perform the authentication operation, security relevant information has to be transmitted from the security device.

7.2.3 If, moreover, the authentication operation requires user input on the token, it is at least suggested that security-relevant information is indeed transmitted from the token to the host processor. For instance, if the second authentication is based on a biometric measurement, the skilled person would be prompted by the cited passage to consider transmitting the fingerprint data to the host processor so that the computationally costly fingerprint validation could be carried out there.

7.2.4 If, now, the chassis of the personal computer in question were insufficient to guarantee safe communication over the bus, the skilled person would, in the board's view, consider making the bus communication safe by other means, for instance by using encryption.

7.3 The appellant also appears to argue that no further encryption would be obvious because the data received by the security device from the token is already encrypted (see grounds of appeal, III.6.1).

7.4 The board disagrees again.

7.4.1 The encryption sufficient to protect the communication between the security device and the token need not be sufficient to protect the bus communication between the security device and the host processor as well. Furthermore, even if it were, it might be undesirable to make available to the host processor the key used by the security device for its communication with the token. Indeed, the fact that D3 makes security of the bus communication an issue at all is, in the board's judgement, a suggestion that for some reason the data cannot simply be passed on to the host processor in the available form (see again column 4, lines 44-53).

7.5 The board thus concludes that, starting from D3, it would have been obvious to the skilled person to use encryption to secure the transmission to the host processor of information which the security device has received from the token.

8. Coming back to difference (a), the board recalls that D3 discloses the integration of processor and memory as a means to mitigate the risk of tampering (see column 5, lines 43-47 and 56-59).

8.1 The skilled person would understand this as a suggestion that circuit integration is a means to reduce security risks - apart from the fact that the

board considers this insight also to be part of the common knowledge in the art.

8.2 Given that, if the bus communication between the wireless interface and the security device was too insecure (as suggested in D3), it would be obvious to the skilled person to integrate the two into one integrated circuit.

8.3 During the oral proceedings, the appellant argued that the integration of processor and memory was significantly different from the claimed integration of a cryptographic processor with a wireless proximity reader. However, apart from mentioning that the reader would have to have an antenna, the appellant did not explain why its integration with a processor would cause any particular problem for the skilled person or how that problem was overcome by the invention. The description also lacks any disclosure in this respect.

8.4 Therefore, the board takes the position that the invention in this regard lies in the idea of integrating the two components rather than in the way in which this is done. However, the board judges that the skilled person in the field of electronic circuitry would always have integration in mind as an obvious solution to problems such as miniaturization, increasing speed, or improving reliability.

9. In summary, the board concludes that neither of the two differences (a) or (b), individually or in combination, establishes an inventive step over D3, Article 56 EPC 1973.

Article 56 EPC 1973, Auxiliary request

10. Claim 1 of the auxiliary request adds the feature that the communication between the service access processor and the service provider is "via a network".

10.1 If the host processor 220 in figure 2 is identified with the claimed service provider, that communication is disclosed to be over a bus "within a node". Thus the new feature adds the limitation that the service provider is remote from the service access processor, i.e. at a different node in the network.

10.2 During the oral proceedings, the appellant suggested that, due to this change, D3 might no longer be a suitable starting point for the assessment of inventive step of the auxiliary request, the subject-matter of amended claim 1 and D3 belonging to different fields. However, the appellant did not develop this argument further. In particular it did not define the different fields to which the invention and D3 might belong. The board furthermore disagrees with the appellant's suggestion in substance: The board does consider D3 to be a suitable starting point for assessing inventive step of the auxiliary request as well. Apart from this, there are no inherent restrictions on the choice of starting point for the inventive-step assessment according to the problem-solution approach in any case (see T 1742/12, reasons 9).

10.3 Returning to D3, the board recalls that the authenticated user is also given access to the "networked resources" of the local personal computer (column 4, lines 15-19). This means that access to the "service" in question requires the transmission of data "via a network". It will depend on the particular service what

data is to be transmitted, and in particular whether this includes data received from the token. If, however, the circumstances so require, it is, in the board's judgment, obvious to do transmit such data.

10.4 This is the case in particular because the local security architecture according to D3, for instance as depicted in figure 3, will not have to be changed significantly if the service provider is connected to it via a network.

10.5 The board therefore concludes that claim 1 of the auxiliary request, too, lacks an inventive step over D3, Article 56 EPC 1973.

Summary

11. There being no allowable request, the appeal has to be dismissed.

Rule 103(1)(a) EPC

12. Since the appeal is not allowable, the requested reimbursement of the appeal fee under Rule 103(1)(a) EPC is not possible.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated