Internal distribution code:

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

Datasheet for the decision of 30 January 2018

Case Number: T 1948/15 - 3.5.06

Application Number: 07109695.2

Publication Number: 1826700

IPC: G06F21/00

Language of the proceedings: EN

Title of invention:
Security and authentication of information processing apparatus

Applicant:
FUJITSU LIMITED

Headword:
Mutual device authentication/FUJITSU

Relevant legal provisions:
EPC 1973 Art. 56

Keyword:
Inventive step (no)

Decisions cited:
T 1121/10

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 1948/15 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 30 January 2018

Appellant: (Applicant)	FUJITSU LIMITED 1-1, Kamikodanaka 4-chome, Nakahara-ku Kawasaki-shi, Kanagawa 211-8588 (JP)
Representative:	Stebbing, Timothy Charles Haseltine Lake LLP Lincoln House, 5th Floor 300 High Holborn London WC1V 7JH (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 21 April 2015 refusing European patent application No. 07109695.2 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 is against the decision of the examining division, with reasons dated 21 April 2015, to refuse European patent application No. 07109695.2 for lack of inventive step in view of

D1: WO 02/03178 A.

II. Notice of appeal was filed on 15 June 2015, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 20 August 2015. The appellant requested that the decision be set aside and that a patent be granted on the basis of amended claims 1-4 according to a main or an auxiliary request as filed with the grounds of appeal, in combination with the description and the drawings as originally filed.

III. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that the claimed invention lacked inventive step over D1, Article 56 EPC 1973.

IV. In response to the summons, by letter dated 29 December 2017, the appellant filed amendments to claims 1-4 of the main and the first auxiliary request, and new claims 1-4 of a second and a third auxiliary request.

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

"A safety judgment system for judging safety of an information processing apparatus, the system comprising the information processing apparatus, a first authentication apparatus and a second authentication

apparatus which are connected through a communication network, wherein

said information processing apparatus (1) comprises:

biometric information receiving means (112) for receiving biometric information of a user of the information processing apparatus;

environment information collecting means (51) for collecting environment information of the information processing apparatus wherein the environment information includes information about name or version of installed software, equipment name or version of connected peripheral equipment, or device name or version of said information processing apparatus (1);

encrypting means (51) for encrypting the biometric information received by said biometric information receiving means (112) and the environment information collected by said environment information collecting means (51), with a secret key issued by said second authentication apparatus (3);

encrypted information transmitting means (51) for transmitting, when communicating with the first authentication apparatus (2), an electronic certificate issued by said second authentication apparatus (3) and the encrypted biometric information and environment information to said first authentication apparatus (2);

sub-electronic certificate authenticating means (51) for decrypting encrypted environment information about the first authentication apparatus (2) with a public key which is acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus (3), and judging whether or not the decrypted environment information is proper, wherein the encrypted environment information about the first authentication apparatus (2) is sent from the first authentication apparatus (2) after the first authentication apparatus

(2) judges the information processing apparatus (1) to be safe;

sub-environment information authenticating means (51) for judging whether or not the transmitted environment information about the first authentication apparatus is proper with reference to a sub-environment information database (151), which stores environment conditions classified according to information to be transmitted and received, and the decrypted environment information; and

sub-safety judging means (51) for judging said first authentication apparatus (2) to be safe when all the authentications performed by said sub-biometric information authenticating means (51), said sub-environment information authenticating means (51) and said sub-electronic certificate authenticating means (51) are successful and said safety judging means (51) judges that said information processing apparatus (1) is safe; and

said first authentication apparatus (2) comprises:

electronic certificate authenticating means (21) for decrypting the encrypted biometric information and environment information with a public key, which is acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus (3), and judging whether or not the decrypted biometric information and environment information are proper;

environment information authenticating means (21) for judging whether or not the transmitted environment information is proper with reference to an environment information database (251), which stores environment conditions classified according to information to be transmitted and received, and the decrypted environment information;

biometric information authenticating means (21) for judging whether or not the biometric information is proper by comparing the decrypted biometric information with pre-stored biometric information;

safety judging means (21) for judging said information processing apparatus (1) to be safe when all the authentications performed by said biometric information authenticating means (21), said environment information authenticating means (21) and said electronic certificate authenticating means (21) are successful;

sub-biometric information receiving means (212) for receiving biometric information acquired at the first authentication apparatus after the safety judging means (21) judges the information processing apparatus (1) to be safe;

sub-biometric information authenticating means (21) for judging whether or not the biometric information received by said sub-biometric information receiving means (212) is proper;

sub-environment information collecting means (21) for collecting environment information about the first authentication apparatus including information about name or version of installed software, equipment name or version of connected peripheral equipment, or device name or version of the first authentication apparatus (2) after the safety judging means (21) judges the information processing apparatus (1) to be safe;

sub-encrypting means (21) for encrypting the environment information collected by said sub-environment information collecting means (21), with a secret key issued by said second authentication apparatus (3); and

sub-encrypted information transmitting means (21) for transmitting an electronic certificate issued by said second authentication apparatus (3) and the

encrypted environment information to said information processing apparatus (1);

whereby when all of the biometric information authentication, environment information authentication and electronic certificate authentication are judged to be successful in both the information processing apparatus (1) and the first authentication apparatus (2), the information processing apparatus (1) and the first authentication apparatus (2) are judged to be safe, and subsequent transmission and reception of information are permitted."

VI. Claim 1 of the *first auxiliary request* reads as follows. The differences over claim 1 of the main request have been highlighted by the board.

"A safety judgment system for judging safety of an information processing apparatus, the system comprising the information processing apparatus, a first authentication apparatus and a second authentication apparatus which are connected through a communication network, wherein

said information processing apparatus (1) comprises:

biometric information receiving means (112) for receiving biometric information of a user of the information processing apparatus;

biometric information authenticating means (51) for judging whether the biometric information received by said biometric information receving means (112) is proper or not by comparing the decrypted biometric information with pre-stored biometric information;

environment information collecting means (51) for collecting environment information of the information processing apparatus wherein the environment information includes information about name or version of installed software, equipment name or version of

connected peripheral equipment, or device name or version of said information processing apparatus (1);

encrypting means (51) for encrypting the biometric information indicating the biometric information received by said biometric information receiving means (112) is proper or not and the environment information collected by said environment information collecting means (51), with a secret key issued by said second authentication apparatus (3);

encrypted information transmitting means (51) for transmitting, when communicating with the first authentication apparatus (2), an electronic certificate issued by said second authentication apparatus (3) and the encrypted biometric information and environment information to said first authentication apparatus (2);

sub-electronic certificate authenticating means (51) for decrypting encrypted biometric information and encrypted environment information about the first authentication apparatus (2) with a public key which is acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus (3), and judging whether or not the decrypted biometric information and the decrypted environment information are ~~is~~ proper, wherein the encrypted environment information about the first authentication apparatus (2) is sent from the first authentication apparatus (2) after the first authentication apparatus (2) judges the information processing apparatus (1) to be safe;

sub-environment information authenticating means (51) for judging whether or not the transmitted environment information about the first authentication apparatus is proper with reference to a sub-environment information database (151), which stores environment conditions classified according to information to be

transmitted and received, and the decrypted environment information;

sub-biometric information authenticating means (51) for judging whether or not the biometric information decrypted by the sub-electronic certificate authenticating means (51) is proper; and

sub-safety judging means (51) for judging said first authentication apparatus (2) to be safe when all the authentications performed by said sub-biometric information authenticating means (51), said sub-environment information authenticating means (51) and said sub-electronic certificate authenticating means (51) are successful and said safety judging means (51) judges that said information processing apparatus (1) is safe; and

said first authentication apparatus (2) comprises:

electronic certificate authenticating means (21) for decrypting the encrypted biometric information ~~and the encrypted~~ environment information with a public key, which is acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus (3), and judging whether or not the decrypted biometric information and the environment information are proper;

environment information authenticating means (21) for judging whether or not the transmitted environment information is proper with reference to an environment information database (251), which stores environment conditions classified according to information to be transmitted and received, and the decrypted environment information;

biometric information authenticating means (21) for judging whether or not the transmitted biometric information is proper ~~by comparing the decrypted biometric information with pre-stored biometric information~~;

safety judging means (21) for judging said information processing apparatus (1) to be safe when all the authentications performed by said biometric information authenticating means (21), said environment information authenticating means (21) and said electronic certificate authenticating means (21) are successful;

sub-biometric information receiving means (212) for receiving biometric information acquired at the first authentication apparatus after the safety judging means (21) judges the information processing apparatus (1) to be safe;

sub-biometric information authenticating means (21) for judging whether or not the biometric information received by said sub-biometric information receiving means (212) is proper;

sub-environment information collecting means (21) for collecting environment information about the first authentication apparatus including information about name or version of installed software, equipment name or version of connected peripheral equipment, or device name or version of the first authentication apparatus (2) after the safety judging means (21) judges the information processing apparatus (1) to be safe;

sub-encrypting means (21) for encrypting the environment information collected by said sub-environment information collecting means (21) and the biometric information indicating the biometric information received by the sub-biometric information receiving means (212) is proper or not, with a secret key issued by said second authentication apparatus (3); and

sub-encrypted information transmitting means (21) for transmitting an electronic certificate issued by said second authentication apparatus (3) and the encrypted environment information and encrypted

biometric information to said information processing apparatus (1);

whereby when all of the biometric information authentication, environment information authentication and electronic certificate authentication are judged to be successful in both the information processing apparatus (1) and the first authentication apparatus (2), the information processing apparatus (1) and the first authentication apparatus (2) are judged to be safe, and subsequent transmission and reception of information are permitted."

Claim 1 of the *second and third auxiliary requests* differs from claim 1 of the main and first auxiliary requests, respectively, in that the various means are renamed. For example, the "sub-safety judging means" is now referred to as "safety judging sub-means", and the other "sub-means" are renamed accordingly. This follows an observation on this matter in the decision under appeal and the board's preliminary opinion (see point 5).

All requests also contain an independent method claim 4 which corresponds to independent system claim 1.

VII. By letter dated 18 January 2018 the appellant indicated its intention not to attend the oral proceedings, and by further letter dated 25 January 2018 it withdrew its request for oral proceedings. The oral proceedings were then cancelled.

Reasons for the Decision

Decision in the appellant's absence

1. According to Article 15(3) RPBA, the board is not obliged to delay any step in the proceedings, including its decision, by reason only of the absence at the oral proceedings of any party duly summoned. Therefore, and likewise in accordance with Article 15(3) RPBA, the board here treats the appellant as relying only on its written case. The reasons given below are based on the board's preliminary opinion, while taking account of the appellant's submission dated 29 December 2017.

The invention

2. The application generally concerns the safety of computing transactions, in particular of electronic commerce transactions initiated from a mobile telephone. The claims refer more generally to an "information processing apparatus" which, as the description states, could also be any PC, fax machine, refrigerator or microwave oven (see original application, page 1, lines 16-21).

2.1 When the information processing apparatus has initiated a "transaction" (e.g. after a customer presses a BUY button on the web page of an online shop, see figure 6 and page 45, lines 8-23), a "safety judgment subroutine" is entered, which checks a number of "credentials" before the transaction is cleared. This safety judgment subroutine involves three devices: an "information processing apparatus for processing a transaction" (e.g. the mobile telephone), a "first authentication apparatus" (or "safety judgment center",

see figure 1) and a "second authentication server" (or "certificate authority", see figure 1).

2.2 The safety judgment subroutine validates three different credentials relating to the information processing apparatus or its user: biometric information of the user, a certificate authenticating the public key of the information processing apparatus, and the "safety posture" of the information processing apparatus. When the biometrics and the certificate are validated and the safety posture is verified to be high enough in view of "the degree of security of the transaction information" (e.g. the higher the value of a transaction, the higher the required security level), the safety test is determined to be successful and the transaction is cleared. "Transaction information", typically comprising "order information" such as price and product information, will then be transmitted to the shop computer (see figure 12, No. 122).

2.3 The biometric measurement of the user is made at the information processing apparatus: typically, a fingerprint is taken, but alternatives are also disclosed (see page 37, lines 6-19). This data is verified (as being "proper") by the information processing apparatus or one of the authentication apparatuses (see page 47, paragraph 2). Then, also at the information processing apparatus, "environment information" is "collected". This information relates to the information processing apparatus itself (device name and version), to peripheral equipment connected to it and to software installed on it. The environment information is used to assess, at the "first authentication apparatus", the security level of the information processing apparatus.

2.4 The transaction information (e.g. the order and payment information) is digitally signed (encrypted) using the secret key issued to the information processing apparatus. The first authentication apparatus validates the transaction information by decrypting the signature with a public key issued to the information processing apparatus. This public key is obtained from a certificate signed by the second authentication apparatus, i.e. the certificate authority, which in turn is validated via the certificate authority's public key.

2.5 The application also discloses that, once the first authentication apparatus has successfully authenticated the information processing apparatus, the information processing apparatus may, in turn, have to authenticate the first authentication apparatus in essentially the same way (see figure 11 and 24 to 27, as well as page 3, lines 14-15, and page 76, especially lines 6-7).

The prior art

3. D1 discloses a network server establishing whether a workstation requesting a network service is a sufficiently "trusted" platform or not. Online shopping is not specifically mentioned, but in its background section D1 discusses "Web sites" which "attempt to verify the security of the client host [...] before allowing transactions from that host" and, more specifically, "banking applications" (page 3, lines 7-10). The network server decides whether to process the request from the workstation "based on the user credentials and/or the workstation credentials" in view of a given "security policy" or which "level of network

service" may alternatively "be supplied to the workstation" (see page 4, lines 25-29; page 6, paragraph 1).

3.1 When a workstation requests some service at a server, a "workstation assessment service" examines it so as to determine its "actual or potential vulnerabilities" or "security risks" (see page 11, lines 33-35; page 12, lines 33-35; page 15, lines 6-12). D1 does not detail the "workstation credentials" on which this assessment is based, but refers in general to "workstation integrity information" and "workstation security posture" (page 9, line 1; page 20, line 1). Based on the assessment, a "score" is computed. In the system of D1, different "levels of service" are defined, each requiring the workstation to have at least a minimal score. That is, in view of the security score, a requested level of service may not be granted. Proposals may be made as to how to repair a detected vulnerability, and sometimes a suitable tool may be able do this automatically (page 15, lines 33-35; page 8, lines 2-3).

3.2 After the workstation credentials, the system assesses user credentials, such as passwords, biometrics and smart cards (page 2, lines 9-11 and last paragraph; page 3, lines 1-2). D1 teaches that checking user credentials only after successfully checking workstation credentials has the benefit of reducing the risk that user credentials are stolen (page 13, lines 27-30).

3.3 This process is referred to as an "extend[ed] log-in process" (abstract and page 7, lines 25-31). On the basis of the security assessment, the network service decides whether to process the service request.

Optionally, it may decide to provide a "degraded level of service" which is consistent with the perceived security vulnerability of the workstation (see page 4, first and penultimate paragraphs; page 6, paragraph 1; page 19, line 33, to page 20, line 2).

The decision and the appeal

4. Apart from a few clarity objections made in a section entitled "Further Remarks" regarding the claim language, the decision under appeal turns on inventive step over D1.

5. The examining division summarised the differences between claim 1 of the then requests in the following three groups (reasons 1.2). In the claimed invention, but not in D1,

1. secure transmission was based on asymmetric encryption and a trusted third party,
2. the assessment of whether environment information is "proper" was made with reference to a database, and
3. not only was the information processing apparatus (mobile phone) authenticated by the first authentication apparatus (center server) but also *vice versa* and both in the equivalent ways.

The use of biometric authentication was not accepted as a further difference (reasons 2), following the decision in appeal case T 1121/10 relating to the earlier application of which this is a divisional application.

5.1 These differences were said to improve security, one way or another, but not to interact synergistically so

that their inventive merit could be considered separately (reasons 1.3 and 1.4). It was then argued:

1. that the use of asymmetric encryption and PKI infrastructures according to difference 1 was "notorious" (reasons 1.5, paragraph 1),
2. that the use of a database according to difference 2 was an obvious choice (reasons 1.5, paragraph 2), and
3. that the decision "which entities to trust and which not to trust" and so which "requir[ed] authentication" was a non-technical requirement; that therefore the objective technical problem solved by this feature could legitimately be formulated as: "also [authenticating] the first authentication apparatus" (see reasons 1.3, item 3); and that it was "the most straightforward choice" to implement this requirement by re-using the existing authentication mechanism (reasons 1.5, paragraphs 3 and 4).

5.2 The appellant did not challenge this grouping of differences or the assertion that differences 1 and 2 were obvious to the skilled person. Moreover, as regards difference 3, the appellant primarily challenged the assumption that the authentication of the center server was a given requirement but not that, *if* it was a given, the symmetric implementation itself was obvious (see the grounds of appeal, in particular page 4, last two paragraphs, and page 5, paragraphs 4 to 6). The appellant did, however, explain why two particular features of that implementation solved technical problems in a non-obvious manner (see the grounds of appeal, page 5, paragraph 9 *et seq.*, page 7, penultimate paragraph *et seq.*, and the discussion below).

Article 56 EPC 1973

Main request

6. In view of the above, the central contentious point in this appeal is whether mutual authentication of the two apparatuses would have been obvious to the skilled person in view of D2 and, if so, why.

7. The examining division referred to "the entity responsible for the security policy of the system in general" as the skilled person in question.

7.1 The appellant challenged this notion by saying that there was "no entity responsible for the security policy on the internet" (see grounds of appeal, page 5, paragraph 1).

7.2 However, the above-mentioned "system in general" does not refer to the Internet as a whole. Rather, both D1 and the invention disclose transaction systems which use a network such as the Internet as a platform. Obviously, in the board's view, a person or a team of persons is responsible for setting up such a transaction system, for instance an individual service provider such as a bank, possibly in co-operation with the providers of client software and hardware. The board agrees with the examining division that it is the task of these persons to identify and define security requirements of the system, and to design it so as to satisfy those requirements.

8. The examining division took the view that "stipulating which entities to trust" did "not require any technical knowledge but rather knowledge which is non-technical in nature, such as who has access to the entity

resources and how trustworthy these people are, as well as how easy it would be for a malicious entity to gain access to the entity's resources (e.g. how secure is the building in which this entity is located)".

8.1 The board agrees with the appellant that there are reasons to be sceptical about these statements in their generality. While non-technical considerations may play a role - even a major one - in determining which parties to trust, the board is unable to see why an assessment of how well a system's resources are protected against a malicious entity is *not* a technical issue. The invention proposes that a transaction should be permitted only if, *inter alia*, "environment information" about the software or hardware constituting the first authentication apparatus is found to be "proper". Again, even acknowledging that the claims do not specify how that decision is made in an individual case, the board is unable to see why the fact that the software and hardware equipment of the center server is security-relevant is not a technical issue.

8.2 The board therefore agrees with the appellant that the claimed mutual authentication is a technical feature rather than a non-technical requirement of the claimed invention, and it accepts that the claimed invention solves the objective technical problem proposed by the appellant (see the decision under appeal, page 12, paragraph 3): how to improve the security of the system of D1.

8.3 The appellant correctly observes that D1 does not disclose or suggest the need to address possible vulnerabilities of the server. It takes this line to argue that D1 too does not motivate the skilled person to consider authenticating the server (see grounds of

appeal, page 5, paragraph 6). The board takes this argument to mean that the skilled person, setting out to solve the above-mentioned problem, could, but would not, consider improving security in the claimed manner.

8.4 However, the board considers that security architects do not blindly try to "improve system security", but consider what potential vulnerabilities there are and address those.

8.5 If there were no actual or potential security problem with the servers, mutual authentication would be pointless. In fact, though, such security problems were known before the priority date of the present application. The board considers that this statement needs no documentary proof and made a statement to that effect in its preliminary opinion (see point 9.6), which the appellant did not challenge.

8.6 D1 discloses that sensitive data may be stolen when a workstation (i.e. a client computer) has been compromised (see page 3, paragraph 1). In principle, this risk is symmetric: for instance, malware running on a server might steal a client user's biometric data. While in many cases "servers" might be less prone to attacks than clients, the skilled person would be aware that this is not always the case. More specifically, the skilled person would have known at the priority date that any Internet node could be set up to run a "server program" so that the existence of a "network service" on the Internet did not allow any conclusion about the security of that service.

8.7 In that light the board takes the following view: The skilled person setting out to increase the security of

the system of D1 would first assess the risks of that system. He would then realise, without exercising inventive skill, that servers might also be compromised and that therefore their security might have to be assessed, too. The board agrees with the examining division that, with this insight, it would have been obvious for the skilled person to task the "information processing apparatus" with authenticating the server in the same manner as it was known for the latter to authenticate the former.

9. The appellant explained that it was technically advantageous - in terms of security and time efficiency - if the "terminal" was authenticated *before* the "server", because "the terminal tend[ed] to have lower safety than the server" and because it was computationally more demanding to "confirm[] the safety of the server" (see grounds of appeal, e.g. paragraphs 1 and 11). The appellant also argued (see its letter of 29 December 2017, page 1, last paragraph) that "it would be clear to the skilled person in the art [...] that the first authentication apparatus has a larger hardware and software resources (and provides more functions) than the information processing apparatus", such that there would be "a clear distinction between the 'information processing apparatus' and the 'first authentication apparatus' as regards their relative security or the relative cost of establishing their security".

9.1 The board disagrees.

9.1.1 Firstly, the board doubts that, in general, terminals are less safe than servers and that it is computationally more demanding to confirm server safety. If, for example, the "information processing

apparatus" is a preconfigured hardware token and the server runs on a private PC, it may well be argued that the former is less vulnerable than the latter.

9.1.2 And secondly, the board notes that the claims give no hint as to the "hardware and software resources" or the "functions" provided by the two apparatuses. Also, the amendment (to all present requests) whereby the transmission from the "second authentication apparatus [...] to [the] first authenticat[ion] apparatus" took place "when communicating with the first authentication apparatus" (see the appellant's letter of 29 December 2017, page 2, paragraph 2) does not add information in this regard.

9.1.3 The board thus concludes that the claims, even in the light of the description, do not allow any conclusion regarding the relative security, or the relative cost of establishing the security, of the two apparatuses.

9.2 Moreover, the board takes the view that the order of steps cannot be inventive. Firstly, since there are only three possibilities for the order of two authentication steps (A before B, B before A, or both in parallel), the skilled person would, without exercising inventive skill, select any of these alternatives after weighing up their relative advantages and disadvantages. Secondly, none of the advantages of the claimed order are discussed in the application, and, as just explained, no potential advantage of the claimed order can be derived from the relative security of the two apparatuses (see the appellant's letter of 29 December 2017, page 1, paragraph 2). And thirdly, the claimed efficiency advantage is relevant only if authentication fails, and

it is thus immaterial for the typical and more frequent case where a transaction is eventually allowed.

9.3 Hence, the board does not accept that the claimed order of the authentication procedures establishes an inventive step over D1.

10. Thus, the appellant's submission of 29 December 2017 has not swayed the board's preliminary opinion that the independent claims of the main request do not comply with Article 56 EPC 1973.

Auxiliary request 1

11. The independent claims of the first auxiliary request specify that the information processing apparatus validates the biometric information and sends only a success flag to the first authentication apparatus (see the grounds of appeal, in particular page 3, paragraph 5, and page 7, penultimate paragraph; description page 46, lines 18-22, and figure 7, S73-S75 and S77).

11.1 Firstly, the board takes the view that sending a "success flag" is essentially redundant in this situation. In an equivalent manner, the information processing apparatus could terminate the entire process if (and only if) the biometric data could not be validated, and could dispense with the success flag altogether.

11.2 Secondly, it is considered obvious to store the biometric information at the device at which the user has provided it, and to validate it locally as well. *Inter alia*, there are known login procedures which rely

on locally obtained biometric information and validate it locally, too (see also D2, page 2, lines 4-7).

11.3 The board thus considers that the features added to claim 1 of the auxiliary request do not change the inventive step assessment of the main request.

Auxiliary requests 2 and 3

12. The small clarifications made in the claims of the second and third auxiliary requests leave the substance of the claims unchanged. The inventive step assessment of the main and first auxiliary requests thus applies to these requests as well.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

L. Malécot-Grob W. Sekretaruk

Decision electronically authenticated