Internal distribution code:

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

Datasheet for the decision of 26 March 2014

Case Number: T 1121/10 - 3.5.06

Application Number: 03256912.1

Publication Number: 1418485

IPC: G06F1/00

Language of the proceedings: EN

Title of invention:
Security and authentication of information processing apparatus

Applicant:
FUJITSU LIMITED

Headword:
Secure transactions/FUJITSU

Relevant legal provisions:
EPC 1973 Art. 56

Keyword:
Inventive step - (no)

Decisions cited:
T 0641/00

Catchword:

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 1121/10 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 26 March 2014

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 2 March 2010 refusing European patent application No. 03256912.1 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman: D. Rees
Members: M. Müller
M.-B. Tardo-Dino

Summary of Facts and Submissions

I. The appeals lies against the decision of the examining division, with reasons dispatched on 2 March 2010, to refuse the European patent application no. 03256912.1. The decision made reference in particular to document

D4: WO 02/03178

and came to the conclusion that claim 1 of the then main and auxiliary requests lacked an inventive step over D4 in view of common general knowledge Article 56 EPC 1973.

II. A notice of appeal against this decision was filed on 30 April 2010, the appeal fee having been paid on 28 April 2010. A statement of grounds of appeal was received on 8 May 2010. The appellant requested that the decision under appeal be set aside and that the application be remitted for further examination based on claims 1-12 according to a main or an auxiliary request as filed with the grounds of appeal, the other application documents being description pages 3-5 as filed on 4 June 2007, pages 1, 2, and 26-86 as originally filed (original pages 6-25 having been deleted), and drawing sheets 1-37 as originally filed.

III. With a summons to oral proceedings the board informed the appellant of its preliminary opinion according to which the claimed invention lacked an inventive step over D4 and common general knowledge in the art, Article 56 EPC 1973. Clarity objections were also raised, Article 84 EPC 1973.

IV. In response to the summons, with letter of 24 February 2014, the appellant filed new claims 1-11 according

to a new main request and claims 1-10 according to a new auxiliary request. The appellant indicated that these were, if admitted, to replace the previous main and auxiliary requests, implying that the previous requests were maintained should the board not admit the new ones.

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

"A safety judgment method for judging safety of an information processing apparatus for processing a transaction, the method performed among the information processing apparatus, a first authentication apparatus, a second authentication apparatus and a shop computer which are connected through a communication network, comprising the steps of:

receiving an input of transaction information at said information processing apparatus (1) and in response to the receipt of the transaction information, starting a process for transmission of the transaction information from said information processing apparatus (1);

receiving biometric information by said information processing apparatus (1);

authenticating the biometric information by judging whether the received biometric information is proper or not by said information processing apparatus (1), said first authentication apparatus (2), or said second authentication apparatus (3);

collecting environment information including information about the information processing apparatus (1), about peripheral equipment connected to said information processing apparatus (1) and about software installed in said information processing apparatus (1);

transmitting the collected environment information from said information processing apparatus (1) to said first authentication apparatus (2);

transmitting an electronic certificate issued in advance by said second authentication apparatus (3) and the transaction information encrypted with a secret key issued by said second authentication apparatus (3) from said information processing apparatus (1) to said first authentication apparatus (2);

authenticating the electronic certificate by said first authentication apparatus (2) by decrypting the encrypted transaction information with a public key 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 information is proper;

authenticating the environment information by said first authentication apparatus (2) by judging whether or not the transmitted environment information is proper with reference to an environment information database (251);

judging said information processing apparatus (1) to be safe by said first authentication apparatus (2) when all the authentications performed in the step of authenticating the biometric information, the step of authenticating the environment information, and the step of authenticating an electronic certificate are successful, and

transmitting said transaction information from the first authentication apparatus (2) to the shop computer (4);

wherein:

said step of collecting environment information includes collecting a device name, version of the information processing apparatus, and version of software comprising an operating system of the

information processing apparatus, an equipment name and version of said peripheral equipment connected to the information processing apparatus, and the name and version of said software installed in the information processing apparatus,

said environment information database (251) stores environment conditions classified according to a degree of security of the transaction information to be transmitted and received and including multiple combinations of the device name, version of the information processing apparatus, and version of software comprising an operating system of the information processing apparatus,

said step of authenticating the environment information is based on the classification according to the degree of security of the transaction information and the multiple combinations of the device name, version of the information processing apparatus, and version of software comprising an operating system of the information processing apparatus, and

the authentication performed in the step of authenticating the environment information is judged to be successful when said transmitted environment information matches the environment condition according to the classification based on the degree of security of the transaction information."

Claim 1 of the new auxiliary request differs from that of the main request in that the step of "receiving input" is further specified to read as follows:

"... receiving an input of transaction information including product information or price information ...",

and that its last paragraph has been replaced by the following text:

"[said step of authenticating] includes reading an environment condition related to a class corresponding to the transmitted product information or price information from said environment information database (251) and judging whether or not the environment condition is proper, based on whether or not the transmitted environment information matches the read environment condition."

Both requests also comprise an independent system claim 4 which closely corresponds to respective independent method claim 1, in particular comprising the information processing apparatus, the first and second authentication apparatus, and the shop computer, and a further independent claim 11 or 10, respectively, which is limited to the first authentication apparatus.

Since the board admitted the new requests (see below), the wording of the independent claims of the previous requests are irrelevant for this decision.

VI. Oral proceedings were held as scheduled on 26 March 2014, at the end of which the chairman announced the board's decision.

Reasons for the Decision

1. Article 13 (1) RPBA provides that any amendment to a party's case after it has filed its grounds of appeal may be admitted and considered at the board's discretion, which will 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. The new main and auxiliary requests were amended in response to the board's clarity objections set out in the annex to the summons to oral proceedings. The board is satisfied that the amendments do not introduce matter going beyond the contents of the application documents as originally filed, do not introduce any complex new issue nor, in fact, change substantially the issues to be addressed under inventive step. The board therefore exercises its discretion accorded to it under Article 13 (1) RPBA and admits both requests.

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, p. 1, lines 16-21).

2.1 When the "information processing apparatus" has initiated the "transaction" (*e.g.* by a customer pressing a BUY button on the web page of an online shop, see fig. 6 and p. 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 fig. 1) and a "second authentication server" (or "certificate authority", see fig. 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 a public key, and the "safety posture" of the 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 fig. 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 p. 37, lines 6- 19). This data is verified (for being "proper") by the information processing apparatus or either of the authentication apparatus (compare claim 1). Then, also at the information processing apparatus, "environment information" is "collected". This information relates to the information processing apparatus (device name and version), 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 first 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 certification authority, which in turn is validated via the certification authority's public key.

The prior art

3. D4 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, D4 discusses "Web sites" which "attempt to verify the security of the client host before allowing transactions from that host" and, more specifically, "banking applications" (p. 3, lines 7-10). The network server makes the decision whether to process the request by 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 p. 4, lines 25-29; p. 6, 1st par.).

3.1 When a workstation requests some service at a server, a "workstation assessment service" examines the workstation so as to determine "actual or potential vulnerabilites" or "security risks" of the workstation (see p. 11, lines 33-35; p. 12, lines 33-35; p. 15, lines 6-12). D4 does not disclose in details the "workstation credentials" on which this assessment are based, but generally refers to "workstation integrity information" and "workstation security posture" (p. 9, line 1; p. 20, line 1). Based on this assessment, a "score" is computed. In the system of D4, different "levels of service" are defined, each requiring a minimal such score. That is, in view of the security score, a

requested level of service may not be granted. Proposals may be made how to repair a detected vulnerability and sometimes a suitable tool may be able do this automatically (p. 15, lines 33-35; p. 8, lines 2-3).

3.2 After the workstation credentials the system assesses user credentials - as examples of which D4 discloses passwords, biometrics and smart cards (p. 2, lines 9-11 and last par.; p. 3, lines 1-2). D4 teaches that checking user credentials after successful checking workstation credentials has the benefit of reducing the risk that user credentials are stolen (p. 13, lines 27-30).

3.3 This process is referred to as an "extend[ed] ... log-in process" (abstract and p. 7, lines 25-31). According to 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 p. 4, 1st and penult. par.; p. 6, 1st par.; p. 19, line 33 - p. 20, line 2).

Security posture

4. The disclosure of D4 crucially relies on the term "workstation security posture" which is assessed on the basis of "workstation credentials" obtained, for instance, by "remotely examining" (or "scan[ning]") "the workstation", and evaluated against a "workstation security policy" (see *e.g.* p. 9, 1st par., p. 11, last par., p. 12, last four lines). D4 does not however define any of these terms in detail. For the assessment of inventive step it is thus central how the skilled reader of D4 would have understood the term "security

posture" at the priority date of the present application.

4.1 The appellant argued in the grounds of appeal that the "security posture" according to D4 is confined to "software capabilities" of the workstation and that the scan of the workstation for "vulnerability risks" which are "present at the workstation" (p. 15, line 11) has to be likened to a conventional virus scan. In support of this argument, the appellant refers to the fact that, according to D4, the "security risk assessment may be performed using a remote examination by a server" and that "it is envisaged that the remote server by itself may be able to repair the vulnerability of the workstation" (grounds of appeal, par. bridging pp. 3-4).

4.2 The board does not find the appellant's interpretation of D4 convincing. On the one hand, D4 discloses the possibility of automatic repair only as an option; elsewhere D4 discloses that the user is informed about actions he could take "to bring the host into compliance" (see p. 14, lines 19-26). In the board's judgment, this language does not exclude actions that relate to peripheral devices. On the other hand, the board cannot see why the "remote examination" of a workstation could not produce information relating to peripheral devices either. Also the reference in D4 to a possible "misconfigur[ation]" (see p. 2, lines 27-28) does not appear to be limited to software.

4.3 The board thus concedes that D4 does not explicitly disclose that "security posture" of a workstation subsumes aspects of hardware and peripheral devices but at the same time does not accept the argument that this

option is specifically excluded by the disclosure of D4.

4.4 The board further considers that the term "security posture" itself was an established one in the art well before the priority date of the application. Security posture in the computing context was and is meant to subsume the totality of measures taken by a company to secure their computing systems and networks, including non-technical ones relating to policies, procedures and controls, and technical ones relating to software and hardware. In the annex to the summons, this argument was put to the appellant who did not challenge it.

Inventive Step, Main request

5. The appellant argued during oral proceedings that D4 disclosed a negotiation to determine whether or not a user at a workstation was allowed to access a network service (see D4 p. 3, lines 16-18), whereas the invention presupposed the network service to be available and was concerned with allowing or prohibiting a transaction over the network. The board disagrees, considering that the extended login procedure according to D4 - starting with a service request and ending, possibly, with the provision of some service - constitutes a transaction in the sense of the claims and that the information defining the service request qualifies as "transaction information". The board accepts however that the workstation assessment service according to D4 is provided by the network server which also provides the requested network service, and, hence, that D4 does not disclose the claimed separation between the first authentication apparatus and the shop computer.

6. The decision under appeal considered claim 1 to differ from D4 in requiring biometric information to be part of the user credentials. The board does not concede this difference, because biometric information is disclosed in D4 as an example of user credentials (p. 2, lines 11-14 and p. 3, lines 1-2). The appellant argues that, according to D4, user credentials are authenticated only after the vulnerability analysis of the workstation (p. 13, lines 27-30) whereas, according to the application, biometric information is authenticated before the environment information (see e.g. figs. 34 and 37, nos. S343 and S372). Even though it seems questionable whether the claim language implies this order of steps, the board is satisfied that the description provides basis for a potential clarifying amendment and thus, to the appellant's benefit, adopts the interpretation that it does.

7. Therefore, in the board's present view, claim 1 of the main request differs from D4 by the following features.

i) D4 discloses that user credentials are authenticated before the workstation credentials while the invention, in view of the description, implies the inverse order.

ii) D4 does not disclose a first authentication apparatus transmitting the transaction information to a separate "shop computer" after authentication.

iii) D4 does not disclose that transmitted information is digitally signed (via encryption and decryption) nor the claimed transmission and use of certificates providing the relevant keys.

iv) D4 does not disclose the environment information to include the specifically claimed items, that is device name and version of the information processing apparatus, name and version of (operating system) software installed on the information processing apparatus, and name and version of peripheral equipment connected to it.

v) D4 discloses that the individual results of the "workstation assessment result set" are combined into an overall security score by means of some kind of calculation (see p. 6, lines 1-7) but does not disclose the use of an "environment information database storing environment conditions" mapping "multiple combinations of" environment conditions to a "degree of security of the transaction information".

Differences iii) and iv) broadly correspond to the differences 2) and 3) as determined in the decision under appeal (see p. 4, last par. - p. 5, 1st par.).

Re. difference i)

8. The appellant argued that collecting the "environment information" after authenticating the biometrics implied that the environment information had a better chance of being up-to-date.

8.1 In principle, the board concedes a safety judgment made on some environment information may become invalid if the environment information changes after it has been collected: For example, if an SD card was inserted into the requesting apparatus only after a transaction was cleared on the basis that it did not have any detachable storage device. However, the application does

not discuss this advantage, neither in general nor by way of example, nor do the claims imply how up-to-date the "environment information" actually is when "collected" because they leave open details and frequency of this collection.

8.2 Moreover, checking the user credentials early also means that workstation credentials need not be determined, let alone checked, if the user credentials cannot be authenticated, which may be computationally advantageous and reduces the risk that workstation credentials are tampered with by an intruder.

8.3 The board considers that the skilled person would be aware of these respective advantages and disadvantages of the different orders of steps and would balance them routinely and without exercising an inventive step.

Re. difference ii)

9. D4 discloses - or at least directly suggests - online banking as a possible application domain for the disclosed network service negotiation. In this context it would appear commonly known to use a Web server as the frontend to some legacy service running on a separate backend server. More generally, too, the board deems it to be obvious that a requested network service - or a part of it - may be provided on two separate computers.

Re. differences iii) and iv)

10. The board considers that the three kinds of credentials according to the invention serve different and rather independent purposes. The user authentication serves to protect the user against impersonation and is used to

eventually confirm the user's wish to perform the transaction (*e.g.* buy the selected product). Digitally signing the transaction information protects the integrity of the transmitted data. And assessing the environment information protects the security of the transaction. Each of these security measures may be dispensed with, if technical circumstances and the required level of trust permit, without any impact on the other ones. In general terms, the board considers that the skilled person would, as a matter of course, consider the combination of several different security measures if this appears to be promising under the circumstances.

10.1 *Re. difference iii)* The board considers that the use of digital signatures was a commonly known way of certifying the origin of transmitted information which the skilled person would not hesitate to incorporate into the system of D4 as an additional security measure depending to circumstances. The use of certificates as claimed to provide and authenticate the relevant keys appears to be a standard feature of commonly known public key infrastructures. Hence, once the decision to use digital signatures has been made the specifically claimed features relating to this certificate would have been obvious for the skilled person, too.

10.2 *Re. difference iv)* In the board's view it will also depend on the circumstances which bits of "environment information" are relevant for assessing security of a given system. Depending, *inter alia*, on the kind of computer system being protected - its components, architecture, configuration, etc. - and the threat against which the system is meant to be protected, it would be apparent for the skilled person which aspects of the "environment" are responsible for a vulnerabili-

ty and which are therefore relevant to counteract a threat. From this perspective, the board considers that each of the listed bits of "environment information" would, in general, have been obvious for the skilled person. In particular, the board considers it obvious for the skilled person that security of a given system may depend on the software installed on it (*e.g.* is the operating system still supported?" or "has the latest patch been installed?"), the peripherals connected to it (*e.g.* "does the device have detachable storage?"), or the device type (*e.g.* "does this device have a cryptographic processor"?).

Re. difference v)

11. The "metric" according to D4 is used to map the set of workstation parameters to a scalar score representing the workstation security. The board deems it to be obvious that such a mapping may also be expressed in terms of rules mapping certain sets of parameters directly to a score. Whether an evaluation based on a metric such as that of D4 or a rule-based system as claimed is preferable will typically depend on the kind of "mapping" to be evaluated. The choice between them would have been obvious for the skilled person according to circumstances.

It is a non-technical issue that different levels of security are required depending on the value of a transaction (see point 2.2 above) which follows, for instance, from the economic consideration that higher transaction values - and thus higher possible losses - warrant higher investments in security. Therefore the feature that the required level of security may vary with the "transaction information", *i.e.* may depend on the "degree of security of the transaction informa-

tion" (see point 2.2 above), does not, in the board's view, contribute to inventive step (see T 641/00, headnote 1). Incorporating such a dependency in either means for comparing the security level provided with the security level required would have been straightforward to the skilled person, too.

12. Therefore, the board comes to the conclusion that independent claim 1 of the main request lacks an inventive step over D4 and common knowledge in the art, Article 56 EPC 1973.

Inventive step, Auxiliary request

13. Claim 1 of the auxiliary request differs from that of the main request by requiring that "transaction information includ[e] product and price information", that an environment condition be read from the environment information database "related to a class corresponding to the transmitted product information or price information". This "class" apparently refers to the classification "according to a degree of security" mentioned earlier in the claim in the context of the environment information database and is therefore construed as "security class". The board considers that the arguments made above (point 11) with respect to difference v) are sufficient to address these amendments and thus do not change the board's conclusion as to inventive step. Rather, the board finds that also claim 1 of the auxiliary request lacks an inventive step, Article 56 EPC 1973.

14. There being no allowable request, the appeal must be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

A. Vottner D. Rees

Decision electronically authenticated