BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS	BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE	CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS

Internal distribution code:

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

Datasheet for the decision of 15 March 2012

Case Number:	T 1672/06 - 3.5.01
Application Number:	01309186.3
Publication Number:	1223524
IPC:	G06F 17/60, G07F 19/00
Language of the proceedings:	EN

Title of invention:
System and method for private and secure financial transactions

Applicant:
Authernative, Inc.

Opponent:
-

Headword:
Secure transaction/AUTHERNATIVE

Relevant legal provisions (EPC 1973):
EPC Art. 56

Keyword:
"Inventive step - no (administrative/business contribution)"

Decisions cited:
T 0641/00, T 0258/03

Catchword:
-

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

Case Number: T 1672/06 - 3.5.01

DECISION
of the Technical Board of Appeal 3.5.01
of 15 March 2012

Appellant: Authernative, Inc.
(Applicant) 1958 Stratton Circle
Walnut Creek, California 94598 (US)

Representative: Wright, Hugh Ronald
Brookes Batchellor
102-108 Clerkenwell Road
London EC1M 5SA (GB)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 16 May 2006 refusing European patent application No. 01309186.3 pursuant to Article 97(1) EPC 1973.**

Composition of the Board:

Chairman: S. Wibergh
Members: K. Bumes
D. Prietzel-Funk

Summary of Facts and Submissions

I. The appeal is against the decision of the examining division to refuse European patent application No. 01309186.3 entitled "*System and method for private and secure financial transactions*", published as

A2: EP-A2-1 223 524.

The refusal was based on Article 123(2) EPC in respect of inadmissible amendments in a claim set filed during the examination phase. *Obiter,* the examining division discussed lack of clarity (Article 84 EPC 1973) and obviousness (Article 56 EPC 1973) with respect to prior art according to

D1: US-A-5 485 510.

II. In a communication under Rule 100(2) EPC, the Board gave its preliminary analysis of the case. In particular, interpreting claim 1 broadly, the Board did not identify any inventive technical contribution in the claimed method.

III. In response to the communication, the appellant filed an amended set of claims 1 to 18 to deal with the Board's objections, and put forward arguments in particular in favour of inventiveness.

IV. At oral proceedings before the Board, held on 15 March 2012, the appellant further amended the independent claims in response to doubts voiced by the Board. It requested that the decision under appeal be set aside and that a patent be granted on the basis of claims 1 to 18 submitted at the oral proceedings.

V. Claim 1 reads:

"1. A method for managing financial transactions using a computer system arranged for communication with remote devices (401-405) using communication lines, comprising:

performing a plurality of authentication processes in response to initiations of respective sessions with the computer system by data communications from remote devices, for predicted transactions having predicted transaction amounts and predicted transaction time out intervals by particular account holders, the authentication processes respectively comprising the steps of:

generating in the computer system requests (504, 506, 508, 509) for input for the corresponding predicted transaction, and receiving in the computer responses to the requests for input from one of said remote devices, wherein said responses to the requests include an identifier of the account (ACC#) used for authenticating the account, one factor (ID_PIN) personal to the account holder for authenticating the account holder and further factors related to the predicted transaction including a predicted transaction amount (W/D)$, a predicted transaction time out interval (T_INT), and a transaction type identifier (T_PIN) personal to the account holder used for authenticating the predicted transaction;

storing (510) a first time-stamped record (510, 907) in memory including the identifier of the account (ACC#), the one factor (ID_PIN) personal to the account holder, the predicted transaction amount (W/D)$, the transaction type identifier (T_ PIN) and a time parameter (TX1) as a part of or as data associated with the first record in memory; and

producing a transaction signature ((W/D)# GEN, 511) as a function of the identifier of the account (ACC#), the one factor (ID_PIN) personal to the account holder, the predicted transaction amount (W/D)$, the transaction type identifier (T_PIN) and the time parameter (TX1), for presentation upon execution of the predicted transaction upon authenticating the account, the account holder and the predicted transaction using said responses, associating the transaction signature with the first time-stamped record and transmitting the transaction signature to one of said remote devices associated with the particular account holder;

performing, in the computer system, a plurality of authorization processes for particular transactions in response to authorization requests from parties to actual transactions, the authorization process for a particular transaction characterized by being independent of disclosure of personal information of said account holder to said parties and including the steps of:

receiving (704) an account identifier (ACC#), a presented transaction signature ((W/D)# GEN, 706), and an actual transaction amount (T-AM 709) at an actual transaction time (TX2) associated with the authorization request for the particular transaction having a transaction type from one of said remote devices;

storing a second time-stamped record (906) in memory for the authorization request for the particular transaction, the record including the received account identifier (ACC#), the presented transaction signature ((W/D)#GEN), the actual transaction amount (T-AM) and the actual transaction time (TX2);

processing the second time-stamped record (502), to verify that the presented transaction signature matches the transaction signature associated with one of said first time-stamped records (703), the actual transaction amount matches the predicted transaction amount associated with said one of said first time-stamped records (707), the actual transaction type matches the transaction type associated with said one of said first time-stamped records and the actual transaction time (TX2) is within the predicted transaction time out interval (901); and

transmitting authorization messages upon successful authorization (306) to one of said remote devices associated with said particular transaction; and performing, in the computer system, a plurality of accounting processes (307, 707) for respective transactions, subject of authorization processes, including reconciling the predicted transaction amounts and the actual transaction amounts for each transaction of the particular account holders."

VI. *Appellant's arguments*

(a) *Technical character*

The appellant asserts technical effects of the claimed transaction method. A first major aspect put forward is a gain in data security for all parties involved in a transaction:

- The account holder has complete control of his personal information (name, address) which does not have to be revealed to a vendor. A transaction signature can be used only once, for a limited period of time and for a limited amount of money chosen by the account holder so that the risk of fraud is minimised. As the transaction signature is a financial value, authentication barriers provided by the present application have a bearing on the security of transactions executed by machines.

- The financial institution (which manages the account) and the vendor benefit from the transaction scheme since the account holder cannot repudiate the transaction once he has provided the unique transaction signature.
- The vendor benefits from the authorisation scheme as he can be sure at the time of the actual transaction that his financial claim will be fulfilled although he does not have to check the account holder's personal information.

A second aspect emphasised by the appellant resides in a separation of the authentication and authorisation processes. During the authentication phase, an account holder requests a transaction signature using his own time and equipment (phone, computer) before the actual transaction takes place. At the point of sale (POS), only the authorisation process needs to be performed. Thus, the actual transaction, which is a time-critical process, is decoupled from the authentication process and can be performed quickly and reliably even at peak business times without overloading communication lines and servers; i.e. less bandwidth is required between the point of sale and the financial institution, and the server of the financial institution needs less computing power.

(b) *Novelty over D1*

The appellant argues that D1 is not concerned with privacy of personal information but explicitly mentions that its authorisation code should include a credit card holder's name and/or address (column 2, lines 56 to 58). While the method of the present application uses the account holder's account identifier (e.g. a credit card number) during the authorisation phase, the appellant does not consider such data to be personal information that needs to be protected.

D1 does not identify transactions as time-critical processes at the point of sale and, therefore, D1 is not concerned with separating the authentication and authorisation processes. Consequently, D1 does not contemplate that (a plurality of) authorisation codes might be generated *for later use* by account holders, vendors and the financial institution. The transaction method of D1 does not allow the authorisation process to be decoupled from the authentication process. The authorisation code of D1 is not a transaction signature within the meaning of present claim 1. D1 does not disclose that its dollar and time limits might be set by the credit card holder, and D1 does not disclose a transaction type identifier personal to the account holder.

(c) *Inventive step*

The appellant argues that the distinguishing features achieve considerable benefits as set out above. As D1 does not address the time-critical aspect of transactions, it cannot suggest a solution to that problem and in particular fails to suggest the fundamental solution proposed by the present application, namely a separation of the authentication and authorisation processes, let alone the specific implementation claimed.

Reasons for the Decision

1. *The application*

1.1 The application addresses privacy and security deficiencies in financial transactions (see in particular paragraph 0012 of A2). For example, when an account holder uses his credit card in a conventional purchasing transaction, the credit card data may be re-used by fraudulent third persons authenticating themselves only at the point of sale. Therefore, the application proposes a secure authentication procedure vis-à-vis the financial institution which then transmits a transaction-specific signature to the account holder before an actual transaction is performed. The transaction signature is generated by the computer system of the financial institution on the basis of predicted transaction parameters (type, amount and time of a transaction envisaged by the account holder) and can be used for one transaction only (see e.g. paragraph 0022 of A2). During the actual transaction at a point of sale, the account holder uses the transaction signature to authorise the transaction based on actual transaction data. Upon successful authorisation, an accounting process finally settles the account. (The application uses the acronym "AAA" to express the cycle of authentication, authorisation and accounting, see e.g. A2, column 1, lines 42 to 46.)

1.2 With respect to technical effects put forward by the appellant, the Board notes that the objects listed by the application (A2, paragraphs 0019 to 0039) are concerned with data security and privacy and do not address any bandwidth bottleneck.

In particular, the application as filed does not present separate authentication and authorisation processes as a solution to a time-critical process at the point of sale. According to the application, the authorisation process at the point of sale may be speeded up by specific technical means, such as "*specialized point-of-sale POS devices, which allow for high speed electronic data entry*" (A2, paragraph 0076, lines 32 to 38) or "*smart cards at the point of sale locations to speed up authorization session requests*" (A2, paragraph 0078, lines 14 to 23). The Board notes that amended claim 1 does not relate to such means.

2. *Admissibility of the amendments*

The Board is satisfied that amended claim 1 does not add any matter to the application as filed (Article 123(2) EPC).

3. *Construction of claim 1*

3.1 The authentication processes defined in paragraphs 1 to 5 of amended claim 1 establish the authenticity of initiators of predicted transactions and result in associated transaction signatures. The authorisation processes as defined in the remainder of the claim authorise actual transactions and, if successful, result in authorisation messages and accounting processes.

According to an amendment made at the oral proceedings, the authorisation processes are independent of disclosure of the account holders' "personal information" to transaction parties.

The Board notes that this amendment does not concern the authentication processes. In fact, the transaction signature is explicitly generated as a function of personal information (including two PINs and transaction parameters of the envisaged transaction).

3.2 The appellant interprets the term "personal information" as not encompassing the account identifier, explaining that the method as claimed is meant to allow an account holder to conceal his name and address from the vendor, whereas the account identifier (e.g. a credit card number) is transmitted with the transaction signature from a remote device (typically the vendor's device) to the computer system.

3.3 The Board accepts the appellant's interpretation of "personal information" because claim 1 implicitly distinguishes personal information from the account identifier. On the other hand, the appellant's interpretation allows the account identifier to be a (conventional) credit card number, which the Board considers as a vulnerable piece of information (vulnerable to fraudulent re-use) since the claim does not stipulate that the account identifier (e.g. credit card number) can only be used in conjunction with the transaction signatures generated according to claim 1.

3.4 The appellant argues that the authentication process uses the account holder's own time and equipment (phone, computer) before the actual transaction takes place at the vendor's point of sale.

According to claim 1, the authentication process is finalised by transmitting the transaction signature to a remote device (i.e. remote from the computer system of the financial institution) "associated" with the account holder.

In the Board's judgement, the word "associated" has a broad meaning and encompasses any dedicated remote access, even on a temporary basis, by the account holder to the computer system of the financial institution. Therefore, a remote device associated with the account holder is not necessarily a device owned by the account holder (even assuming that ownership can be given a technical meaning, which is doubtful) but may be owned by the vendor at the point of sale and used temporarily by the account holder to contact his financial institution and obtain a transaction signature (like in D1, column 3, lines 42 to 49).

3.5 A prominent argument of the appellant relates to a separation of the authentication and authorisation processes.

3.5.1 The Board notes that claim 1 sets out the authentication and authorisation processes in separate paragraphs without, however, specifying any explicit decoupling feature such as a minimum time span between said processes. The application discloses merely that a *maximum* life time of the transaction signature (time-out interval T_INT) is set to "*a reasonable time interval sufficient enough to perform the financial transaction*" (A2, paragraph 0044), which may be a matter of 15 minutes (A2, paragraph 0064, line 33). This makes practical sense as account holders (e.g. credit card holders) wish to keep the conventional ability to shop spontaneously.

3.5.2 Therefore, the question is whether the separation between the authentication and authorisation processes is only a logical concept in the reader's mind or expressed by any substantive feature of the transaction method.

When the transaction signature is presented for authorisation of an actual transaction, no authentication is necessary at that stage of the transaction since the authorisation process for a particular transaction is "*independent of disclosure of personal information of said account holder to said parties*".

In the Board's judgement, this is the only feature which seeks to define a functional separation between the authentication process and the authorisation process: the authorisation process at the point of sale need not include any authenticating step (cf. A2, paragraph 0030, lines 29 to 34).

In practice, even that functional separation gets blurred if a vendor nevertheless chooses to check the identity of an account holder who is presenting a transaction signature. The wording of claim 1 covers such an embodiment.

In summary, in its most general aspect, the alleged functional separation between the authentication and authorisation processes is ultimately defined by a policy of the financial institution not to oblige vendors to ask for authenticating data from account holders presenting transaction signatures.

3.5.3 Effects and objectives not disclosed by the application but introduced in the form of arguments after the filing date cannot serve as a basis for construing claim 1 in a specific desired way. Therefore, the Board does not base its interpretation of the alleged separation aspect on the alleged effect that the communication and server load is spread out over time so that load peaks can be avoided and bandwidth requirements lowered.

4. *Article 54(2) EPC - Prior art according to D1*

4.1 The Board concurs with the examining division in considering D1 to represent the closest available prior art. D1 is acknowledged in the introductory portion of the present application (A2, paragraphs 0007/0008).

4.2 D1 relates to a secure credit/debit card authorisation (title) which does not reveal the vulnerable card number to the vendor of services or goods (abstract). According to Figure 2, a card holder (CDCH) who wishes to perform a specific transaction with a vendor asks his card company to prepare an authorisation code which will allow that particular transaction to be performed (D1, column 2, line 63 to column 3, line 9). The card holder authenticates himself vis-à-vis the card company by entering a personal identification number (PIN) and/or a voice sample (D1, column 3, lines 1 to 6 and lines 29 to 31).

The card company transmits the authorisation code either directly to the vendor (D1, column 3, lines 7 to 9 or lines 29 to 34) or to a station/terminal used by the card holder/customer in the vendor's store (D1, column 3, lines 42 to 49). The authorisation code includes a "dollar limit" (maximum amount of credit authorised for the transaction), a time limit, the identity of the vendor, and the name and/or address of the credit card holder (D1, column 2, lines 51 to 62).

Finally, using the authorisation code, the vendor charges the actual transaction amount against the card (D1, column 3, lines 13 to 20; lines 37/38) without getting to know the credit card number (column 3, lines 39 to 41). The charge is valid only if the authorization code and the vendor identification correspond and the dollar and time limits are satisfied (column 2, lines 40 to 42).

The charging (i.e. accounting) step is performed either by a separate action of the vendor (filling out a credit ticket) or by the vendor providing information which is immediately sent back as a data message to the card company's database (D1, column 3, lines 13 to 20).

4.3 The authorisation code of D1 anticipates the following aspects of a transaction signature defined in present claim 1.

- The authorisation code is only generated upon a successful authentication of the account holder based on a PIN.

- The authorisation code limits the amount of credit and the period of time for which the credit is allowed.

- The authorisation code allows one particular transaction to be authorised. The purpose of D1 is to prevent re-use of a number which represents financial value (D1, column 1, lines 23 to 29).

4.4 The transaction cycle of D1 implies that the card company stores a copy of the authorisation code in its database when it prepares the code. Otherwise, the card company would not be able to verify the authorisation code when the code is returned by the vendor.

The transaction cycle of D1 further implies that the card company's computer system stores the time of the actual transaction at least in its working memory in order to check whether the transaction exceeds the time limit assigned to the transaction.

When the card company receives an authorisation code returned by the vendor, the computer system has to store the returned code at least in its working memory in order to compare the returned code with the prepared code.

4.5 D1 does not mention explicitly that the computer system of the financial institution informs the vendor about a successful authorisation of the actual transaction. However, such a confirmation is inherent to any payment system as vendors do not carry out transactions until such a confirmation is received.

4.6 D1 does not mention explicitly that a *plurality* of authentication, authorisation and accounting processes are performed (in parallel). However, any credit card system comprises a multiplicity of credit card holders and, thus, implies that the computer system of the financial institution must be designed to perform a plurality of related processes at any point in time.

5. *Article 54(1) EPC 1973 - Novelty over D1*

5.1 The authentication process according to claim 1 is novel over the authentication process of D1 in that it requires the account holder to input

- a predicted transaction amount,
- a predicted transaction time-out interval, and
- a transaction type identifier personal to the

account holder.

Accordingly, the step of producing the transaction signature is novel insofar as the signature is also a function of the above parameters.

5.2 According to the authorisation process defined in claim 1, the parties to a transaction may decide on their own whether the account holder's name and/or address is disclosed to the vendor. The financial institution does not insist on such a disclosure at the point of sale but is prepared to authorise a transaction upon presentation of a valid transaction signature, an account identifier and actual transaction parameters (amount, time, type).

6. *Article 56 EPC 1973 - Inventive step*

6.1 Allowing/requiring an account holder to set individual parameters (predicted amount, time-out and type) for an upcoming transaction increases the security of the resulting transaction signature as only he knows the details of the envisaged transaction. A third person who happens to obtain the transaction signature is less likely to perform a transaction which matches the individual parameters of the transaction signature. Hence, a fraudulent use of the transaction signature can be recognised more easily than in the conventional scheme (D1) where the financial institution sets the amount and time limits according to general rules.

However, that gain in security is a predictable effect of investing more and more confidential details in the transaction signature and in the process of generating it. The skilled person weighs up the beneficial effects and drawbacks of such a sophistication which obviously requires more system resources and customer education. The usual trade-off and choice that the skilled person finally has to make to find an optimum between effort and effect does not involve an inventive step.

6.2 Allowing the transaction parties to decide whether the account holder's name and/or address is disclosed to the vendor is a non-technical administrative or business contribution which has no bearing on the assessment of inventive step (see decision T 641/00-*Two identities/COMVIK*, Headnote I, OJ EPO 2003, 352).

Requiring no authentication (e.g. no name or address) at the point of sale has an obvious disadvantage (the transaction signature may be presented by a fraudulent third person) and an obvious advantage (it saves time and data traffic). However, the underlying technical problem, i.e. the bandwidth bottleneck of communication lines and the limited capacity of server computers, is not remedied but only circumvented by the administrative measure. Such a step does not contribute to the technical character of the claimed method (T 258/03-*Auction method/HITACHI*, Headnote II, OJ EPO 2004, 575).

The technical infrastructure used by the prior authentication and authorisation processes (D1) does not require any inventive modification when a policy decision is taken not to insist on the disclosure of an account holder's name or address at the point of sale.

6.3 The authorisation process according to claim 1 reveals the account identifier to the vendor's device for transmission to the financial institution. The use of account identifiers obviously facilitates the retrieval and matching of pairs of authentication and authorisation records. On the other hand, revealing an account identifier such as a credit card number creates a security problem if the number can be re-used without a transaction signature (a scenario not ruled out by claim 1).

In any event, it is obvious to collect, during the authorisation process at the point of sale, data items (such as actual transaction parameters) that were used as security features when the transaction signature was generated at the end of the authentication process.

6.4 In view of the appellant's emphasis on a separation between the authentication and authorisation processes, the Board reiterates that claim 1 seeks to express such a separation in broad terms which effectively present the separation as an optional feature left to the discretion of the transaction parties.

Even if claim 1 were to be construed as defining a functional or temporal separation between the authentication and authorisation processes, the claimed transaction method and its disclosed purposes would still be close to the conventional alternative embodiment described in D1, column 3 (lines 42 to 49) which allows an account holder to obtain an authorisation code when he is already at the vendor's premises. Claim 1 does not define a spatial separation between the authentication and authorisation processes.

A delay between the authentication and authorisation processes of claim 1 is technically possible as data records are stored so that they can be retrieved for later matching. However, the storage facility does not define or imply a minimum delay or structural separation.

It is true that a plurality of time-out intervals have to be managed by the computer system since a plurality of authentication processes and a plurality of authorisation processes are performed (in parallel). However, even that complexity does not imply a minimum delay between an authentication process and the related authorisation process.

Therefore, the relatively short delay according to the alternative embodiment of D1 constitutes a separation within the broad terms of claim 1.

6.5 The Board concludes that the method according to claim 1 does not involve an inventive step.

Order

For these reasons, it is decided that:

The appeal is dismissed.

The Registrar:	The Chairman:
T. Buschek	S. Wibergh