Exhibit 9

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Application No.:	10/531,259	Confirm. No.:	4669
Filing Date:	April 24, 2006	Examiner:	Doan, Trang T
First Inventor:	Gisela Meister	Art Unit:	2431
Attorney No.:	MEIS3002/JJC/BEL	Customer No.:	23364

For: METHOD FOR CARRYING OUT A SECURE ELECTRONIC TRANSACTION USING A PORTABLE DATA SUPPORT

REPLY TO FINAL OFFICE ACTION OF FEBRUARY 1, 2011

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

INTRODUCTORY COMMENTS

This is responsive to the final Office action dated February 1, 2011 in the above-identified application.

In view of the following remarks, reconsideration of the application is respectfully requested.

REMARKS

Reconsideration of the pending application is respectfully requested in view of the following observations.

1. Rejection of claims 1-6 and 8-14 under 35 USC 102(e) as being anticipated by US publication 2002/0016913 (*Wheeler*)

Reconsideration of the rejection is respectfully requested in view of the amendment to the claims and the following observations.

This rejection is respectfully traversed on the basis that *Wheeler* fails to disclose each and every element of claims 1 and 10.

By way of review, claim 1 recites a method for effecting a secure electronic transaction on a terminal using a portable data carrier arranged to perform different quality user authentication methods. The portable data carrier performs user authentication using one of the different user authentication methods, confirms the proof of authentication to the terminal, and performs a security-establishing operation within the electronic transaction. The method comprises creating authentication quality information by the portable data carrier about the user authentication method used and attaching the authentication quality information to the result of the security-establishing operation.

It is asserted that critical technical differences exist between claim 1 and *Wheeler*.

First, the Office Action on page 3 states that *Wheeler* discloses authentication quality information about the user authentication method used in paragraphs [0378]-[0379]. Paragraph [0378] discloses using a combination of values for Rs (PIN) and Rb(002) (thumbprint) in determining whether the suspect user (46) is an authorized user. An example is given that

> a correct PIN by itself, a correct PIN plus at least a 60% match of thumbprint, an incorrect PIN if the thumbprint exceeds 96%, and an incorrect PIN but two thumbprints exceeding 90% (but not identical) are all different types of verification statuses that may be sufficient for the banking authority 3320 to accept Factors B and C Entity Authentication of the suspect user 46 by card 95 (see par. [0378]).

The example describes different combinations of quantitative data between the PIN and thumbprint which a banking authority would find acceptable for authentication of a user. The quantitative data reflects on the closeness of the match for each actual application of an authentication method by representing the percentage matched. In other words, the quantitative data collected in *Wheeler* represents the quality of the match for different executions of a particular authentication method.

In contrast, the authentication quality information of claim 1, however, relates to the quality of the user authentication method, itself. The portable carrier attaches the quality information to the result of the security-establishing operation, where "the quality of the user authentication methods varies between an inherently relatively lower quality and an inherently relatively higher quality from a security perspective" (Claim 1, emphasis added). Thus, there is clear support in claim 1 that the quality of the user authentication method indicates the quality level of the authentication method used.

Different authentication methods provide different levels of protection. For example, a PIN check as a knowledge-based method is an inherently low-quality method while a fingerprint check as a biometric check method is an inherently higher-quality method (see page 5, lines 25-30 of the originally filed specification and the amended specification filed on May 18, 2009). The PIN check is a lower quality authentication method since a user merely needs to gain knowledge of the PIN to be successfully authenticated. A biometric check method is a higher-quality method since it would be more difficult for a user to duplicate a fingerprint in order to be authenticated and thus, the check "presupposes the personal presence of the user" (see specification, page 5, lines 3-5).

Since the quality information of *Wheeler* is based on the concrete input data, namely the PIN entered or the thumbprint scanned, the quality information is necessarily dependent on the concrete input data. In the instant application, the quality information of claim 1 is independent of the concrete input data since the quality information exclusively depends on the authentication method used.

Thus, *Wheeler* does not disclose "the difference in quality of the user authentication methods varies between an inherently relatively lower quality and an inherently relatively higher quality from a security perspective."

Next, *Wheeler* does not disclose attaching authentication quality information to the result of the security-establishing operation. The Office Action interprets the authentication quality information being attached to the result of the security-establishing operation of claim 1 as the indicator (460), in paragraph [0145] of *Wheeler*, being attached to a digital signature created by a device (see Office Action, page 3).

The indicator (460) does not represent authentication quality information as required by claim 1. In *Wheeler*, the indicator (460) output from device (440) is based on the last comparison of the verification data (450) with the prestored data (470). When the verification data (450) and the prestored data (470) comprise a Secret, four verification statuses may be present: whether verification data (450) is present, a match between the verification data (450) and the prestored data (470), a failed match between verification data (450) and prestored data (470), and a match between the verification data (450) and the prestored data (470) (see par. [0150]). When the verification method used is biometric, the verification data (450) and prestored data (470) comprise biometric values and "the set of predefined verification statuses comprises the possible percentages of match – or degrees of difference – between the verification data (450) and prestored data (470)" (see par. [0151]).

As discussed above, the verification statuses in either method represent the quality of the match and not the authentication quality of the method. Therefore, *Wheeler* does not disclose attaching the quality information to the result of the security-establishing operation, wherein the difference in quality of the user authentication methods varies between an inherently relatively lower quality and an inherently relatively higher quality from a security perspective.

Accordingly, *Wheeler* does not disclose each and every feature of claim 1. Moreover, claim 10 includes features similar to those of claim 1 and is likewise allowable for the reasons above.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

fastcase®
Smarter legal research.