

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Ex Parte Reexamination of

U.S. Patent No. 8,352,730

Inventor: John J. Giobbi

Assignee: Proxense, LLC

Control No. 90/015,052

Issue Date: Jan. 8, 2013

Confirmation No. 9657

Art Unit: 3992

Examiner: Tarae, Catherine Michelle

Title: **BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION**

Mail Stop Ex Parte Reexam

Attn: Central Reexamination Unit

Commissioner for Patents

United States Patent and Trademark Office

P.O. Box 1450

Alexandria, VA 22313-1450

INTERVIEW AGENDA

During the Interview scheduled for Tuesday, December 6, 2024, at 10:00 AM, Patent Owner respectfully requests discussion of the topics presented in this Interview Agenda.

The Access Message Must Be Separate from the Application Being Accessed

The express language of the claims requires the access message to be something different than the application being accessed.

Claim 1 recites:

“receiving ***an access message*** from the agent allowing the user access to ***an application.***”

Likewise, Claim 8 recites:

“receives ***an access message*** from the agent allowing the user access to ***an application.***”

Similarly, Claim 12 recites:

“receiving ***an access message*** from the agent; and
in response to a positive access message, allowing the biometrically verified user access to ***an application.***”

Finally, Claim 15 recites:

“receiving ***an access message*** from the agent allowing the user to access ***an application.***”

Each of the independent claims expressly recites “***an access message***” and “***an application***”. As both terms are first used with the article “an”, neither term provides antecedent basis for the other. Furthermore, “an application” is not an inherent component of “an access message” such that an access message necessarily provides antecedent basis for an application. Accordingly, “an access message” and “an application” are recited in each of the independent claims as separate and distinct elements.

Additionally, the District Court has construed “access message” to mean “a signal or notification enabling or announcing access.” The Office Action proposes a similar construction

of access message – i.e., “a message/notification indicating the user is allowed access, or otherwise allowing access.” Thus, the District Court and Examiner agree an access message operates on an application by enabling, allowing, announcing or indicating access. An access message would not be able to operate on the application if they were one in the same. Accordingly, the access message must be something separate from the application being accessed.

The Access Message is Received Only After Authentication by a Third-Party Trusted Authority

The express language of the claims requires that an access message is received from a third-party trusted authority only after the third-party trusted authority has authenticated a device ID.

Claim 1 recites:

“wirelessly sending one or more codes from the plurality of codes and the other data values ***for authentication by an agent that is a third-party trusted authority*** possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values ***includes the device ID code***; and

responsive to authentication of the one or more codes and the other data values by the agent, ***receiving an access message from the agent.***”

Likewise, Claim 8 recites:

“wirelessly sends one or more codes from the plurality of codes and the other data values ***for authentication by an agent that is a third-party trusted authority*** possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and the other data values ***includes the device ID code***; and

responsive to the agent authenticating the one or more codes and the other data values, a radio frequency communicator, *receives an access message from the agent.*”

Similarly, Claim 12 recites:

“the device ID code being registered with *an agent that is a third-party trusted authority* possessing a list of *device ID codes* uniquely identifying legitimate integrated devices;

requesting authentication of the one or more codes and the other data values *by the agent*, wherein the authentication determines whether the one or more codes and the other data values are-legitimate;

receiving an access message from the agent.”

Finally, Claim 15 recites:

“send the plurality of codes and the other data values *to agent for authentication* to determine whether the one or more codes and the other data values are legitimate, wherein the *agent is a third-party trusted authority* possessing a list of device ID codes uniquely identifying legitimate integrated devices, and *responsive to the device ID code being authenticated*, the authentication unit *receiving an access message from the agent.*”

Each of the independent claims recites that receipt of the access message is responsive to and/or follows the third-party trusted authority authenticating a device ID. Furthermore, each of the independent claims recites the access message is received from the third-party trusted authority (i.e., agent). Thus, each of the independent claims recites that the access message is received from the third-party trusted authority only after the third-party trusted authority has authenticated a device ID.

***Access to the Application Occurs Only After Authentication
by the Third-Party Trusted Authority***

As detailed above, each of the independent claims requires that the access message operates on an application by enabling, allowing, announcing, or indicating access. As also detailed above, each of the independent claims also requires that the access message is received from the third-party trusted authority only after authentication of a device ID by the third-party trusted authority. Consequently, each of the independent claims requires that access to the application is only enabled after authentication by the third-party trusted authority.

Access to Ludtke's eCoupons Does Not Occur After Authentication by the TPCB

The Office Action mailed November 25, 2024, equates eCoupons stored within Ludtke's transaction device to an application. While eCoupons stored within Ludtke's transaction device certainly could be a file, they are not accessed after authentication by the TPCB. Rather, Ludtke teaches that access to the eCoupons stored on the transaction device occurs after authentication of the user by the transaction device itself.

Ludtke details the use of eCoupons during purchases in Col. 27, lines 25-43, with reference to Fig. 16 (reproduced below).

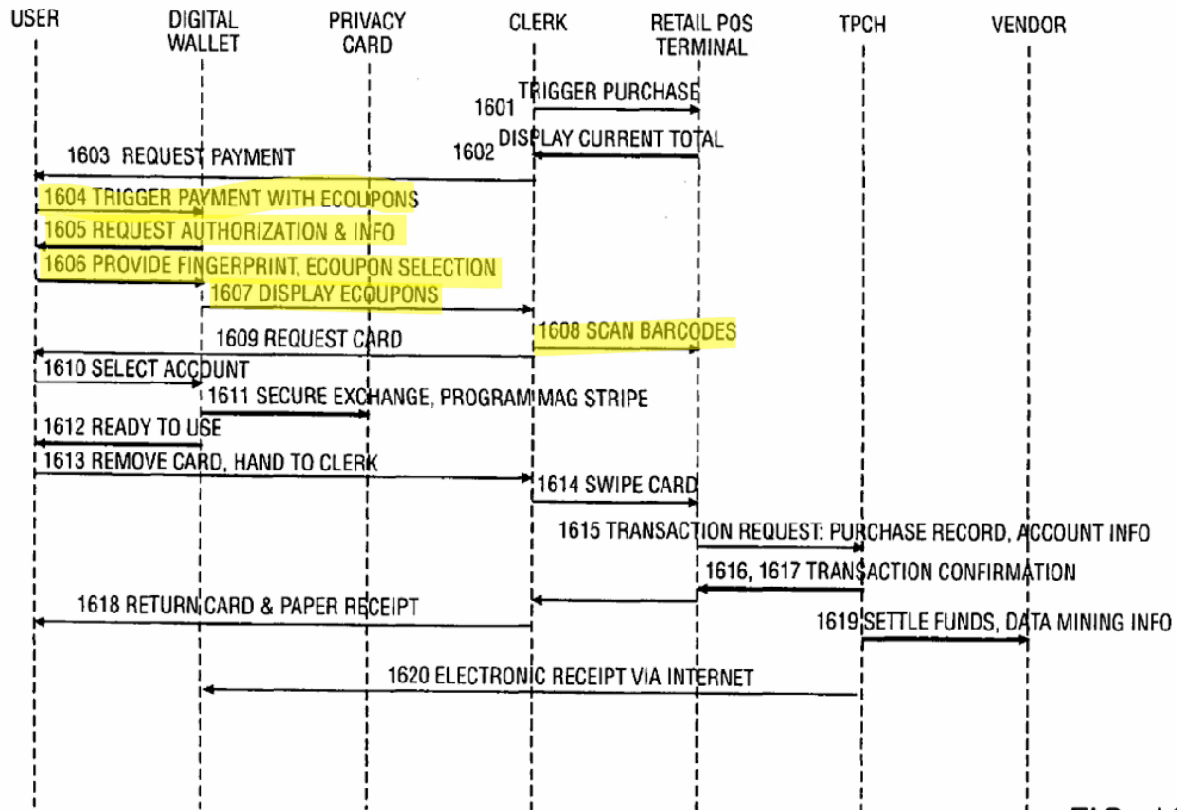


FIG. 16

RETAIL TRANSACTION

“At step 1604, the user activates the transaction device, requesting a payment transaction using any *eCoupons* that might have been *collected by the transaction device* prior to or during shopping. The *transaction device requests the user to authenticate himself*, for example, by fingerprint recognition, step 1605. The user presses on the fingerprint recognition pad to continue, step 1606. *After verifying the user, the transaction device displays the collection of eCoupons* that the user requested on its display screen, step 1607.

The user hands the transaction device to the clerk, who successively scans the eCoupons barcodes into the legacy POS terminal in a manner similar to how paper coupons are scanned into the terminal. After each barcode is scanned, the clerk presses a “next” button, which indicates to the transaction device that the eCoupon was successfully entered. The transaction device then displays a bar code of a next eCoupon, and this process continues until all eCoupons have been entered for the transaction, step 1608.” Ludtke, 27:25-43 (emphasis added).

As the above details, “[t]he transaction device requests the user to authenticate himself,” and “after verifying the user, the transaction device displays the collection of eCoupons that the user requested on its display screen, step 1607.” Thus, access to the eCoupons only requires verification of the user by the transaction device. This is further shown in Fig 16, which depicts access and use of the eCoupons prior to sending information to the TPOCH at step 1615. Accordingly, access to Ludtke’s eCoupons occurs after verification of the user by the device, and **not** after authentication by the TPOCH.

However, each of the independent claims requires that access to the application occurs only after authentication by a third-party trusted authority. The Office Action has equated Ludtke’s TPOCH with a third-party trusted authority. But even if the TPOCH is a third-party trusted authority it is not authenticating the transaction device prior to the user being allowed access to the eCoupons stored on the transaction device. Consequently, the eCoupons are not an application accessed after verification by the TPOCH. Thus, to the extent a TPOCH can be considered a third-party trusted authority (Patent Owner believes it cannot), the eCoupons are not an application accessed only after authentication by the TPOCH. Therefore, the eCoupons are not an application to which access is enabled only after authentication by a third-party trusted authority as required by each of the independent claims. As such, eCoupons are not applications as recited in each of the independent claims.

***Electronic Distribution of a Digital Product by the TPOCH Is Not
An Access Message Separate from the Application***

The Office Action contends that the electronic distribution of a purchased digital product by the TPOCH is an application to which access is enabled by receipt of an access message. Each

of the independent claims, however, requires that the access message be separate from the application being accessed.

The basic steps of a purchase using Ludtke's transaction device and TPOCH are outlined by Ludtke in Fig. 15 (reproduced below).

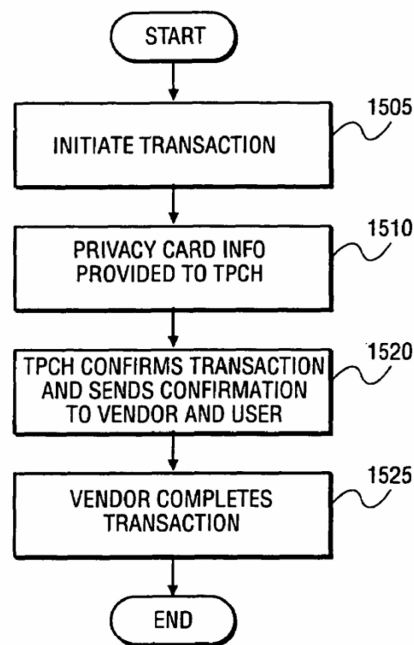


FIG. 15

The process is one in which “the user initiates the transaction” by attempting to use their privacy card (i.e., transaction device) to make a purchase. Ludtke, 27:9. When making a purchase, a “POS terminal may collect the necessary information from the transaction device, e.g., the digital wallet, combine it with the purchase data, and send it to the TPOCH.” Ludtke, 23:50-52. Accordingly, the transaction device is a credit card, or surrogate therefore, issued by the TPOCH. As such, “the TPOCH maintains secure information linking a user to a particular transaction card identification and interfaces among the transaction device, vendor and any financial systems to provide the user authorization to perform and complete a transaction.”

Ludtke, 11:8-12. Thus, as with any credit card purchase, “Privacy card information is provided to TPOCH, step 1510.” Ludtke, 27:12-13. Upon receipt of the card information, “[t]he TPOCH may then authorize the transaction, store data relevant to the transaction in its records and trigger a financial transfer to the vendor's account.” Ludtke, 23:52-55. Having processed and authorized the transaction, “[t]he TPOCH, at step 1520, confirms the transaction and provides the confirmation to the vendor and the user.” Ludtke, 27:13-14. At this point the user has successfully used his transaction device to provide to the vendor what the vendor has agreed to accept as payment – i.e., a confirmation message from the TPOCH. Thus, the transaction confirmation message delivered to the vendor by the TPOCH is payment for the product being purchased and not an access message.

Having been paid, “[a]t step 1525 the vendor completes the transaction without knowledge of the identity of the user.” Ludtke, 27:14-16. A vendor completes a transaction after receiving payment by delivering the purchased product to the user. “The system described herein also provides a distribution functionality 150 whereby *products purchased via the system* are distributed. In one embodiment, *the distribution function 150 is integrated with the TPOCH 110 functionality*.” Ludtke, 7:30-33 (emphasis added). Thus, the vendor may utilize Ludtke’s TPOCH to deliver the purchased product to the user. In other words, the TPOCH may become UPS.

When acting as a distribution system, “the TPOCH 110 functions as the middleman of the distribution channel.” Ludtke, 7:45-46. This implies the TPOCH receives the content and then passes it along to its intended destination. Alternatively, it could deliver it to a POS acting as the final mile carrier when “POS terminal is used for distribution”. Ludtke, 7:49-50. Accordingly, “the content may be encrypted at the source and distributed via the system to the POS terminal wherein the POS terminal subsequently decrypts the distributed material. The POS terminal may

then pass the data to an appropriate place desired by the user, for example, to a user controlled device such as PC storage, a digital wallet or a privacy card.” Ludtke, 7:50-56. Regardless of if a POS is used for the final mile or not, the TPCCH is merely a delivery service that delivers paid for content to the user.

Of course, receipt of the content at the user’s device would announce and enable access, just like receipt of a physical package from UPS announces and enables access to a purchased product. But what is announcing and enabling access is receipt of the product itself. Accordingly, the purchased software or file becomes one in the same with the access message. Each of the independent claims, however, requires that the access message and the application be separate and not one in the same. Consequently, Ludtke’s electronic distribution system does not provide the *separate* access message *and* application required by the claims.

December 6, 2024

Respectfully submitted by:

/James A. Zak, Esq./

Attorney for Patent Owner
Proxense, LLC
Reg. No. 60,190

Hecht Partners LLP
125 Park Ave. 25th Floor
New York, NY 10017
E: jzak@hechtpartners.com
P: (651) 357-8517