

REMARKS

Amendments to the Claims

By way of this Supplemental Amendment, Patent Owner has renumbered claims 1-17 as new claims 18-34. No other amendments have been made to the claims. Accordingly, the amendments to the claims do not present any new matter.

Claim Rejections – 35 U.S.C. § 102

Claims 1, 2, 4-9, 11, 12, and 14-17 were rejected under pre-AIA 35 U.S.C. § 102(e) for allegedly being anticipated by Burger (U.S. Publication No. 2005/0050367). Claims 18, 19, 21-26, 28, 29, and 31-34 correspond directly to claims 1, 2, 4-9, 11, 12, and 14-17. Accordingly, Patent Owner's remarks presented in the Response filed June 2, 2025, are directly applicable to claims 18, 19, 21-26, 28, 29, and 31-34.

Claim Rejections – 35 U.S.C. § 103

Claim 11 was rejected under pre-AIA 35 U.S.C. § 103 for allegedly being obvious over Burger.

Claims 3, 10, and 13 were rejected under pre-AIA 35 U.S.C. § 103 for allegedly being obvious over Burger in view of Robinson (U.S. Publication No. 2003/01777102)

Claims 20, 27, 28, and 30 correspond directly to claims 3, 10, 11, and 13. Accordingly, Patent Owner's remarks presented in the Response filed June 2, 2025, are directly applicable to claims 20, 27, 28, and 30.

Control No. 90/015052
Supplemental Amendment
June 30, 2025

CONCLUSION

In view of the foregoing remarks, the withdrawal of all rejections and termination of these proceedings is respectfully requested.

June 30, 2025

Respectfully submitted by:

/Peter J. Park/

Attorney for Patent Owner
Proxense, LLC
Reg. No. 71,267

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

AMENDMENTS TO THE CLAIMS

Patent Owner respectfully requests the claims be amended as indicated below. No new matter is added by way of the following amendments. Rather, the amendments merely repeat cancelled claims 1-17 as new claims 18-34; essentially renumbering the current claims.

1. (Cancelled)
2. (Cancelled)
3. (Cancelled)
4. (Cancelled)
5. (Cancelled)
6. (Cancelled)
7. (Cancelled)
8. (Cancelled)
9. (Cancelled)
10. (Cancelled)
11. (Cancelled)
12. (Cancelled)
13. (Cancelled)
14. (Cancelled)
15. (Cancelled)
16. (Cancelled)
17. (Cancelled)

18. (New) A method for verifying a user during authentication of an integrated device, comprising the steps of:

persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered; wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

responsive to a determination that the scan data matches the biometric data, 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 by an application from the agent allowing the user access to the application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

19. (New) The method of claim 1, wherein the one or more codes and the other data values are transmitted to the agent over a network.
20. (New) The method of claim 1, further comprising:
 - registering an age verification for the user in the association with the device ID code.
21. (New) The method of claim 1, wherein the one or more codes and the other data values indicate that the biometric verification was successful.
22. (New) The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.
23. (New) The method of claim 1, further comprising:
 - establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication.
24. (New) The method of claim 1, further comprising:
 - receiving a request for the one or more codes and the other data values without a request for biometric verification; and
 - responsive to receiving the request for the one or more codes and the other data values without a request for biometric verification, sending the one or more codes and the other data values without requesting the scan data.
25. (New) An integrated device for verifying a user during authentication of the integrated device, comprising:
 - a memory stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the memory that is unable to be

subsequently altered; wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

a verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, 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 by an application from the agent allowing the user access to the application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

26. (New) The integrated device of claim 8, wherein the one or more codes and the other data values are transmitted to the agent over a network.
27. (New) The integrated device of claim 9, wherein an age verification is registered in association with the device ID code.
28. (New) The integrated device of claim 8, wherein the verifier comprises: an LED to be activated for requesting the biometric scan.
29. (New) A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

receiving one or more codes from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and the other data values comprises the device ID code uniquely identifying the integrated device and a secret decryption value associated with a biometrically verified user, 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;

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 by an application from the agent; and

in response to a positive access message, allowing the biometrically verified user access to the application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file

30. (New) The method of claim 12, further comprising:

Registering a date of birth or age with the agent.

31. (New) The method of claim 12, further comprising:

establishing a secure communications channel with a biometric key, wherein the one or more codes and the other data values associated with the biometrically verified user is received from the biometric key.

32. (New) A system comprising:

a biometric key stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the biometric key and a secret decryption value in a tamper proof format written to a storage element on the biometric key that is unable to be subsequently altered, and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending, one or more codes from the plurality of codes and other data values wherein the one or more codes and the other data values include the device ID code, and the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition; and

an authentication unit receives the plurality of codes and the other data values and 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 by an application from the agent allowing the user to access the application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

33. (New) The system of claim 15, wherein the biometric key receives an authentication request from the authentication unit, and in response, requests a biometric scan from the user to generate the scan data.

34. (New) The system of claim 15, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the one or more codes and the other data values.

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

SUPPLEMENTAL AMENDMENT UNDER 37 C.F.R. § 1.111

Dear Commissioner:

This Supplemental Amendment is being filed to supplement the response to the Office Action mailed May 20, 2025, filed on June 2, 2025, regarding the above-identified proceedings.

This Supplemental Amendment contains the following sections:

Amendments to the Claims, beginning on page 2; and

Remarks, beginning on page 9.