Petitioner's Trial Hearing Demonstratives

APPLE INC.,
Petitioner,

v.

PROXENSE, LLC,

Patent Owner.

IPR2024-00232, IPR2024-00233[1]

Trial Hearing
April 22, 2025

[1] Apple Inc. is joined as Petitioner to these proceedings via joinders granted in IPR2024-01333 and IPR2024-01334.

Table of Contents

- Introduction
  - ’730 Patent Claims
  - ’954 Patent Claims
- Overview of Issues
- Overview of ’730 / ’954 Patents
- Claim Construction
- Overview of Prior Art Ludtke
- Issues

’730 Claims Are Unpatentable

- Proxense **concedes** that the ’730 claims are unpatentable.
  - Proxense filed a Request for Adverse Judgment
  - “has conceded” that the ’730 claims are unpatentable over the prior art

> at any time during a proceeding.” Pursuant to 42.73(b)(3) a party may request adverse judgment by a “concession of unpatentability.” Patent Owner has conceded the unpatentability of the claims at issue in this proceeding by authorizing entry of the Examiner’s amendment in EPR 90/015,052. As such, Patent Owner requests adverse judgment pursuant to 42.73(b)(3).

- “Concession of unpatentability…of the contested subject matter” 37 C.F.R. § 42.73(b)
- Proxense **admits** the ’730 claims are unpatentable over Ludtke

IPR2024-00232, Paper 29 at 1

’954 Claims Are Unpatentable

- For same reasons Proxense concedes the ’730 claims are unpatentable, the ’954 claims are unpatentable
- ’954 claims and ’730 claims are nearly identical
- Main difference is certain limitations in ’730 claim 1 are deleted in ’954 claim 1:
  - “verifying a user during authentication…” in preamble
  - “wherein the biometric data…”
  - “possessing a list of device ID codes…”
  - “wherein the application is selected from a group consisting of…”
- Some limitations are added in ’954 claim 1:
  - “and other codes”
  - “to a third party that operates a”
  - “at an application”
  - “a trusted authority indicating…”
- Proxense did not challenge or argue any differences in its IPR papers

IPR2024-0232, -0233, Ex. 1001; POR; POSR

’954 Claims Are Unpatentable

The ’954 claims are unpatentable for the same reasons as the ’730 claims.

’954 Claim 1

1. A method comprising:

persistently storing biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is not capable of being subsequently altered;

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 and other values from the plurality of codes and other data values for authentication to a third party that operates a trusted authority, wherein the one or more codes and other data values includes the device ID code; and

receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party and allowing the user access to the application.

’730 Claim 1

1. 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 from the agent allowing the user access to an 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.

’954 Claims Are Unpatentable

’954 Claim 1 - marked up versus ’730 Claim 1

1. A method ~~for verifying a user during authentication of an integrated device,~~ comprising ~~the steps of~~:

persistently storing biometric data of ~~the~~ a user and a plurality of codes and other data values comprising a device ID code uniquely identifying ~~the~~ an 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~~ not capable of being 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 and other values from the plurality of codes and ~~the~~ other data values for authentication ~~by an agent that is a third-party~~ to a third party that operates a 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, at an application, an access message from the ~~agent~~ trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party and allowing the user access to ~~an~~ 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~~.

Red – indicates claim language deleted

Blue – indicates claim language added

’954 Claims Are Unpatentable

’954 Claim 16 - marked up versus ’730 Claim 12

~~12~~ 16. A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

wirelessly receiving one or more codes and other data values from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and other data values comprises the device ID code uniquely identifying ~~the~~ an 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~~ for authentication, the trusted authority operated by a third party;

requesting authentication of the integrated device using 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~~ trusted authority;

receiving, at an application, an access message from the ~~agent~~ trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party; and

in response to ~~a positive~~ receiving the access message, allowing the biometrically verified user access to an application~~, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door open~~.

Red – indicates claim language deleted

Blue – indicates claim language added

’954 Claims Are Unpatentable

- Proxense relied on the same arguments for the ’954 claims and ’730 claims:
  - Patent Owner Responses in the ’954 and ’730 IPRs are nearly **identical**

TABLE OF CONTENTS

I. Introduction 1
II. Related Matters 2
III. The ‘954 Patent 3
IV. Claim Construciton 4
A. Applicable Law 4
B. Claim Construction issued by W.D. Texas 4
1. 37 C.F.R. § 42.100(b) Statement 4
2. Previously Construed Terms 6
C. Third Party Trusted Authority 6
D. Receiving an Access Message Allowing Access to an Application 7
E. Grounds 1 and 2: Obviousness over Ludtke and Obviousness over Ludtke and Kon 8
1. Third Party Trusted Authority 10
2. Receiving an Access Message Allowing Access to an Application 17
V. Conclusion 25

POR in ’954 IPR

TABLE OF CONTENTS

I. Introduction 1
II. Related Matters 2
III. The ‘730 Patent 3
IV. Claim Construciton 4
A. Applicable Law 4
B. Claim Construction issued by W.D. Texas 4
1. 37 C.F.R. § 42.100(b) Statement 4
2. Previously Construed Terms 6
C. Third Party Trusted Authority 6
D. Receiving an Access Message Allowing Access to an Application 7
E. Grounds 1 and 2: Obviousness over Ludtke and Obviousness over Ludtke and Kon 8
1. Third Party Trusted Authority 10
2. Receiving an Access Message Allowing Access to an Application 17
V. Conclusion 25

POR in ’730 IPR

’954 Claims Are Unpatentable

- Proxense relied on the same arguments for the ’954 claims and ’730 claims:
  - Patent Owner Sur-Replies in the ’954 and ’730 IPRs are nearly **identical**

TABLE OF CONTENTS

I. INTRODUCTION 1
II. THE TESTIMONY OF MR. CARROTHERS WITH RESPECT TO THE PROCESSING OF WEB TRANSACTIONS IS CORROBORATED. 1
III. CLAIM CONSTRUCTION 6
IV. THE RATIONALES PRESENTED IN THE PETITION WERE REJECTED BY THE CRU IN THE 730 REEXAM 10
A. THE RATIONALES PRESENTED IN THE PETITION 10
1. Rationale 1: TPCH Is a Third-Party Trusted Authority Due to Processing a Financial Transaction *10*
2. Rationale 2: The Access Message Permits Additional Services to be Downloaded to the Device *13*
3. Rationale 3: The Access Message Permits Access to Webpages *14*
B. THE RATIONALES PRESENTED IN THE PETITION WERE ADDRESSED AND REJECTED BY THE CRU IN THE 730 REEXAM 14
1. The CRU Determined That the TPCH Is Not a Third-Party Trusted Authority Due to Processing a Financial Transaction *14*
2. The CRU Determined That Ludtke Does Not Disclose an Access Message Permitting Additional Services to Be Downloaded *15*
3. The CRU Determined That Ludtke Does Not Disclose an Access Message Permitting Access to a Webpage *16*
V. NEW RATIONALE ASSERTED IN THE REPLY 17
VI. CONCLUSION 18

PO Sur-Reply in ’954 IPR

TABLE OF CONTENTS

I. INTRODUCTION 1
II. THE TESTIMONY OF MR. CARROTHERS WITH RESPECT TO THE PROCESSING OF WEB TRANSACTIONS IS CORROBORATED 1
III. CLAIM CONSTRUCTION 6
IV. THE RATIONALES PRESENTED IN THE PETITION WERE REJECTED BY THE CRU IN THE 730 REEXAM 10
A. THE RATIONALES PRESENTED IN THE PETITION 10
1. Rationale 1: TPCH Is a Third-Party Trusted Authority Due to Processing a Financial Transaction 10
2. Rationale 2: The Access Message Permits Additional Services to be Downloaded to the Device 14
3. Rationale 3: The Access Message Permits Access to Stored Messages 15
4. Rationale 4: The Access Message Permits Access to a Computer 15
B. THE RATIONALES PRESENTED IN THE PETITION WERE ADDRESSED AND REJECTED BY THE CRU IN THE 730 REEXAM 16
1. The CRU Determined That the TPCH Is Not a Third-Party Trusted Authority Due to Processing a Financial Transaction 16
2. The CRU Determined That Ludtke Does Not Disclose an Access Message Permitting Additional Services to Be Downloaded 18
3. The CRU Determined That Ludtke Does Not Disclose an Access Message Permitting Access to Stored Messages 19
V. CONCLUSION 20

PO Sur-Reply in ’730 IPR

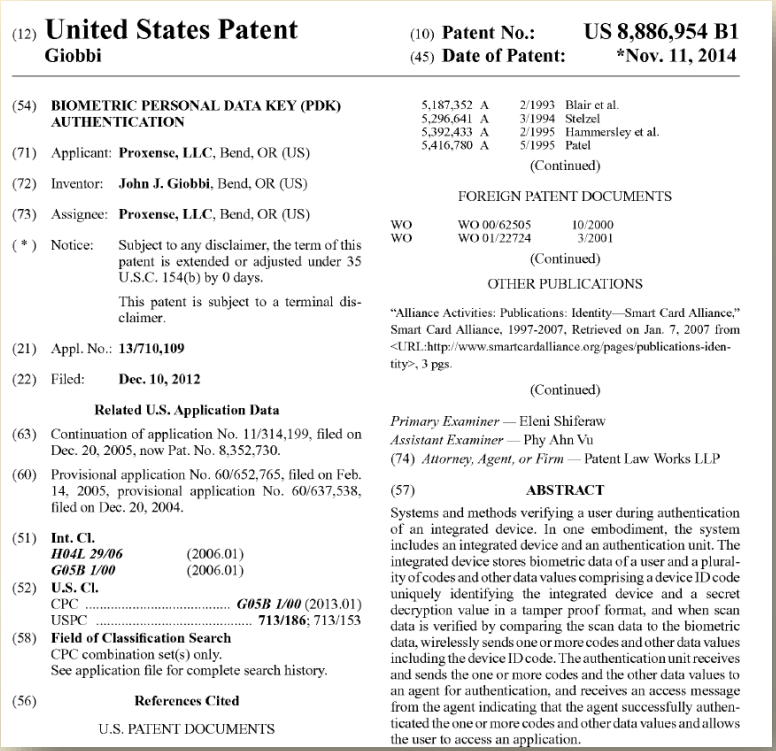
Overview of Issues

Issue	Basis	Slides
1	Whether Ludtke alone or in combination with the knowledge of a POSITA discloses or renders obvious "a third party that operates a trusted authority" / "the trusted authority" / "a third party trusted authority."	**28-33**
2	Whether Ludtke alone or in combination with the knowledge of a POSITA discloses or renders obvious "receiving, at an application, an access message from the trusted authority…allowing the user access to the/an application."	**34-41**

Overview of Issues (Cont.)

Issue	Basis	Slides
3	Whether Mr. Carrothers qualifies as a POSITA.	**42-44**
4	Whether Patent Owner's Untimely Arguments and Exhibits Regarding the '730 Reexam in the Sur-Reply Should Be Allowed.	**45-46**

Overview of ’954 Patent



(12) **United States Patent**
Giobbi

(10) **Patent No.: US 8,886,954 B1**
(45) **Date of Patent: *Nov. 11, 2014**

(54) **BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION**

(71) Applicant: **Proxense, LLC**, Bend, OR (US)

(72) Inventor: **John J. Giobbi**, Bend, OR (US)

(73) Assignee: **Proxense, LLC**, Bend, OR (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/710,109**

(22) Filed: **Dec. 10, 2012**

Related U.S. Application Data

(63) Continuation of application No. 11/314,199, filed on Dec. 20, 2005, now Pat. No. 8,352,730.

(60) Provisional application No. 60/652,765, filed on Feb. 14, 2005, provisional application No. 60/637,538, filed on Dec. 20, 2004.

(51) **Int. Cl.**
H04L 29/06 (2006.01)
G05B 1/00 (2006.01)

(52) **U.S. Cl.**
CPC ***G05B 1/00*** (2013.01)
USPC **713/186**; 713/153

(58) **Field of Classification Search**
CPC combination set(s) only.
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,187,352	A	2/1993	Blair et al.
5,296,641	A	3/1994	Stelzel
5,392,433	A	2/1995	Hammersley et al.
5,416,780	A	5/1995	Patel

(Continued)

FOREIGN PATENT DOCUMENTS

WO	WO 00/62505	10/2000
WO	WO 01/22724	3/2001

(Continued)

OTHER PUBLICATIONS

"Alliance Activities: Publications: Identity—Smart Card Alliance," Smart Card Alliance, 1997-2007, Retrieved on Jan. 7, 2007 from <URL:http://www.smartcardalliance.org/pages/publications-identity>, 3 pgs.

(Continued)

Primary Examiner — Eleni Shiferaw
Assistant Examiner — Phy Ahn Vu
(74) *Attorney, Agent, or Firm* — Patent Law Works LLP

(57) **ABSTRACT**

Systems and methods verifying a user during authentication of an integrated device. In one embodiment, the system includes an integrated device and an authentication unit. The integrated device 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, and when scan data is verified by comparing the scan data to the biometric data, wirelessly sends one or more codes and other data values including the device ID code. The authentication unit receives and sends the one or more codes and the other data values to an agent for authentication, and receives an access message from the agent indicating that the agent successfully authenticated the one or more codes and other data values and allows the user to access an application.

- Title: Biometric Personal Data Key (PDK) Authentication
- Earliest Claimed Priority: Dec. 20, 2004
- 29 Claims
  - Independent: 1 (method), 12 (device), 16 (method), 22 (system)
  - Dependent: 2-11, 13-15, 17-21, 23-29
  - Same specification as ’730 Patent

Overview of ’954 Patent

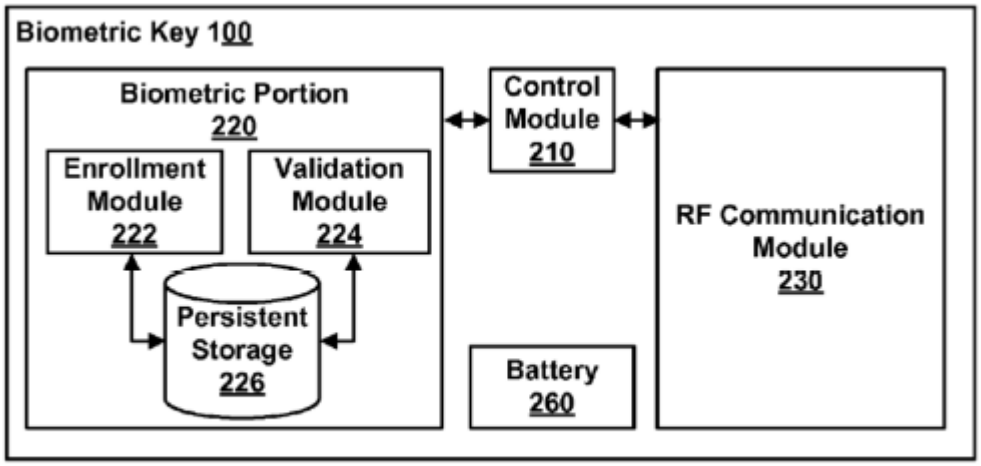


FIG. 2

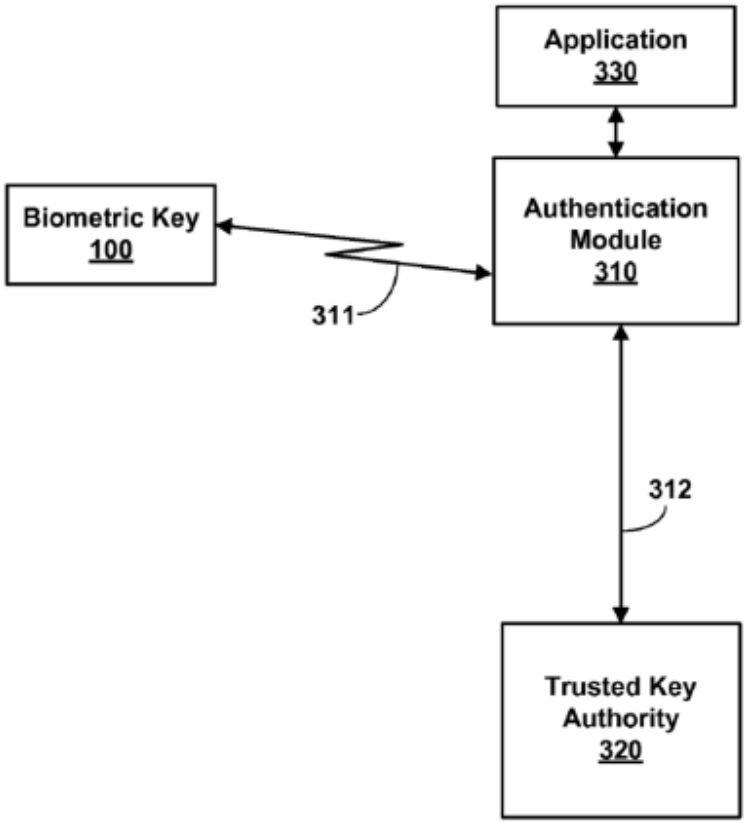


FIG. 3

D.I. 3-7; POR 3-4; Ex. 1001, FIGs. 2, 3

Overview of ’954 Patent

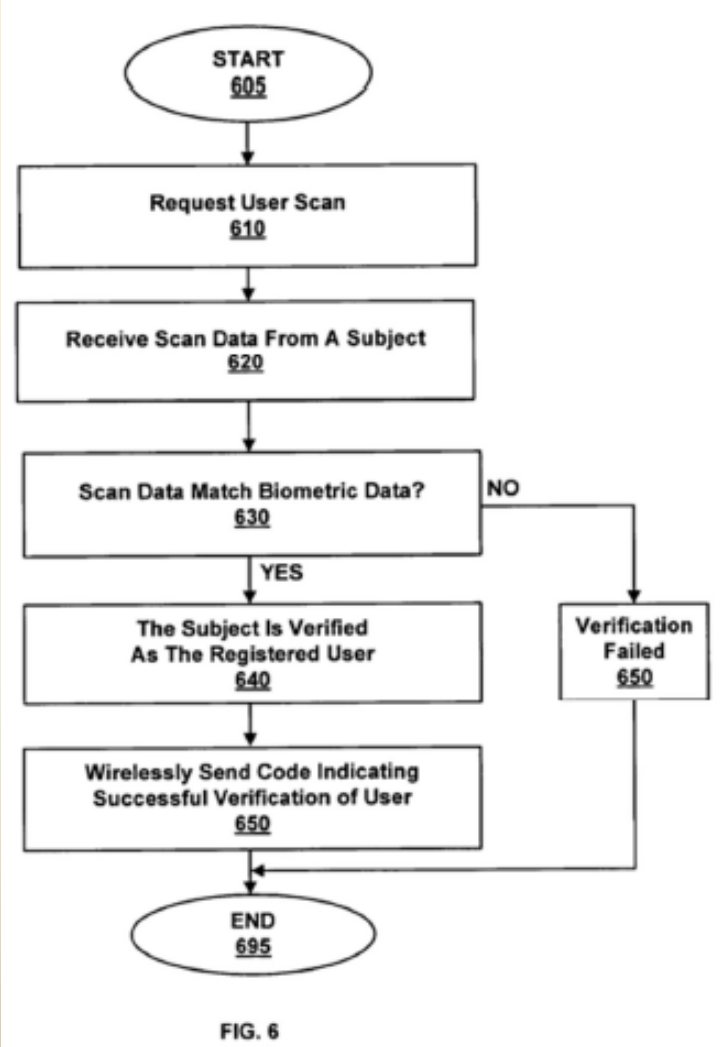


FIG. 6

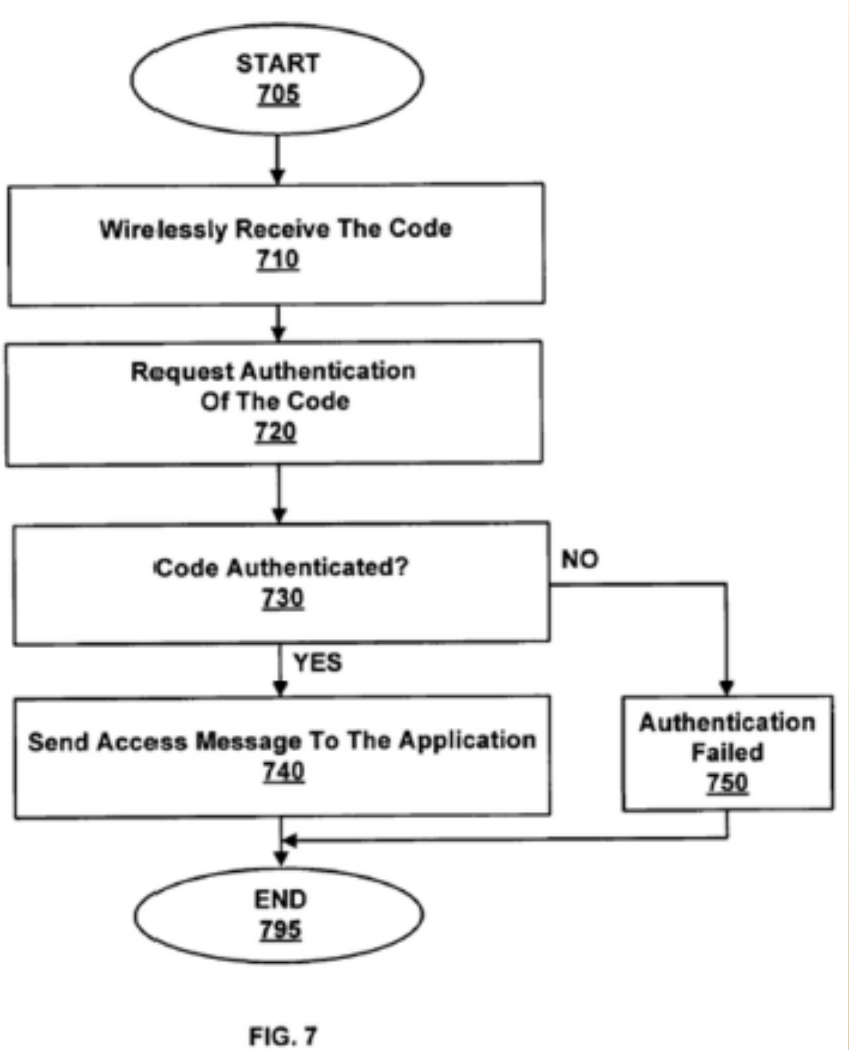


FIG. 7

IPR2024-00233, Pet. 1-3; Ex. 1001, FIGs. 6, 7

’954 Patent - Claim 1

1. A method comprising:

persistently storing biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is not capable of being subsequently altered;

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 and other values from the plurality of codes and other data values for authentication to **a third party that operates a trusted authority**, wherein the one or more codes and other data values includes the device ID code; and

receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party **and allowing the user access to the application.**

Overview of ’954 Grounds

Patent Owner’s Arguments Are All Based on Ground 1

Ground	Basis	Cited Art	’954 Claims
1	103	Ludtke (Ex. 1005)	1-2, 4-7, 10, 12-13, 15-16, 18-19, 22-27
2	103	Ludtke and Kon (Ex. 1006)	3, 14, 17

Claim Construction

Claim Construction

No Terms Need to Be Construed Now to Resolve Issues

Term	Construction	'954 Claims
"device ID code"	"a unique code identifying a device"	1, 3, 12, 14, 16, 22
"access message"	"a signal or notification enabling or announcing access"	1, 12, 16
"a third party that operates a trusted authority" / "the trusted authority"	"an entity separate from the parties to a transaction"	1, 12, 22, 16

Pet. 4; D.I. 8, 12; POR 5-7; RPOR 4; Ex. 2017

Claim Construction

No Terms Need to Be Construed Now to Resolve Issues

In the above identified related matter before the Western District Texas, the Hon. Alan Albright provided the following constructions:

Term	Court's Construction
"persistently storing biometric data of [a/the] user and a plurality of codes and other data values comprising a device ID code uniquely identifying [an/the] integrated device and a secret decryption value"	Plain and ordinary meaning wherein the meaning is: " persistently storing biometric data of [a/the] user and a plurality of codes and other data values are stored; within this storage is also (1) a device ID code uniquely identifying an integrated device and (2) a secret decryption value."
"an access message … [allowing / allows] The user [access to an application / to access an application]"	No Construction necessary. Plain and ordinary meaning.

In addition, Patent Owner and Petitioner agreed to the following constructions:

Term	Court's Construction
"device ID code"	"a unique code identifying a device"
"access message"	"a signal or notification enabling or announcing access"

Pet. 4; D.I. 8, 12; POR 5; Ex. 2017

Claim Construction

- PO argues an alternative construction for "third party trusted authority":
  - "at least one of the parties to the claimed transaction must be the application" POR 7
  - The Board rejected this construction in the Institution Decision (D.I. 11).
- PO's alternative construction ***excludes at least one embodiment***:
  - '954 Patent: "application" includes a "financial account" such as a "savings account" and a "file" Ex. 1001, 6:18-26; Gray Reply Decl., ¶14; RPOR 5-6
  - A "file" is not a principal party to a transaction. Gray Reply Decl., ¶13; RPOR 5.
- "[A] claim construction exclud[ing] a preferred embodiment is rarely, if ever correct." *Sequoia Tech., LLC v. Dell, Inc.*, 66 F.4th 1317, 1327 (Fed. Cir. 2023); D.I. 11; RPOR 5; Gray Reply Decl. ¶11 (*citing* Ex. 1001, 6:37-51, Figs. 3-4)

Ground 1

Overview of Ludtke

(12) **United States Patent**
Ludtke et al.

(10) **Patent No.: US 7,188,110 B1**
(45) **Date of Patent: Mar. 6, 2007**

(54) **SECURE AND CONVENIENT METHOD AND APPARATUS FOR STORING AND TRANSMITTING TELEPHONY-BASED DATA**

(75) Inventors: **Harold Aaron Ludtke**, San Jose, CA (US); **Brant L. Candelore**, Escondido, CA (US)

(73) Assignees: **Sony Corporation**, Tokyo (JP); **Sony Electronics Inc.**, Park Ridge, NJ (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 66 days.

(21) Appl. No.: **09/734,839**

(22) Filed: **Dec. 11, 2000**

(51) **Int. Cl.**
G06F 17/30 (2006.01)

(52) **U.S. Cl.** **707/10**

(58) **Field of Classification Search** 707/6, 707/10, 104.1; 704/273, 247; 705/51; 455/563, 455/411; 713/182, 178; 709/217, 219; 715/746
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,329,589	A	7/1994	Fraser et al.	
5,561,709	A	10/1996	Remillard	
5,654,746	A	8/1997	McMullan, Jr. et al.	
5,748,890	A	5/1998	Goldberg et al.	
5,815,665	A	9/1998	Teper et al.	
5,878,139	A	3/1999	Rosen	
5,933,811	A	8/1999	Angles et al.	
6,000,832	A	12/1999	Franklin et al.	
6,029,141	A	2/2000	Bezos et al.	
6,076,075	A	6/2000	Teicher	
6,119,101	A	9/2000	Peckover	
6,128,602	A	10/2000	Northington et al.	
6,144,848	A	11/2000	Walsh et al.	
6,148,241	A	11/2000	Ludtke et al.	
6,163,771	A	12/2000	Walker et al.	
6,166,730	A	12/2000	Goode et al.	
6,237,096	B1 *	5/2001	Bisbee et al.	713/178
6,263,311	B1 *	7/2001	Dildy	704/273
6,264,560	B1	7/2001	Goldberg et al.	
6,282,552	B1	8/2001	Thompson et al.	
6,311,214	B1	10/2001	Rhoads	
6,356,905	B1	3/2002	Gershman et al.	
6,393,305	B1 *	5/2002	Ulvinen et al.	455/563
6,434,403	B1	8/2002	Ausems et al.	
6,434,747	B1	8/2002	Khoo et al.	
6,609,113	B1	8/2003	O'Leary et al.	
6,668,322	B1 *	12/2003	Wood et al.	713/182
6,675,203	B1 *	1/2004	Herrod et al.	709/217
6,778,998	B2 *	8/2004	Kondo et al.	707/104.1
6,804,705	B2 *	10/2004	Greco et al.	709/219
6,895,558	B1 *	5/2005	Loveland	715/746

FOREIGN PATENT DOCUMENTS

TW	351799	2/1999

OTHER PUBLICATIONS

Tryllian Mobile Agents: Going Beyond the Web, A Commercial White Paper, Version 1.0- May 18, 2000, p. 1-21.

Alan Neibauer, "Running Microsoft Outlook 98", Microsoft Press, p. 44-55 (Copyright 1998).

About Gossip, http://www.Tryllian.com including Quickstart Guide, Products and Downloads (6 pgs.) (Copyright 1999-2000).

Alan Freedman, The Computer Desktop Encyclopedia (2nd Ed.), pp. 16, 86, 1029, The Computer Language Company Inc., Point Pleasant, PA (Copyright 1999).

* cited by examiner

Primary Examiner—Diane Mizrahi
(74) *Attorney, Agent, or Firm*—Blakely, Sokoloff, Taylor & Zafman LLP

(57) **ABSTRACT**

A method of identifying an authorized user with a biometric device and enabling the authorized user to access private information over a voice network is disclosed.

23 Claims, 31 Drawing Sheets

Pet. 5-8; Ex. 1005, Cover

Overview of Ludtke

A method of identifying an authorized user with a biometric device and enabling the authorized user to access private information over a voice network is disclosed.

this data for use outside the eCommerce system. The user connects to and performs transactions with the eCommerce system through a transaction device which has a unique identifier (ID). In one embodiment, a privacy card is used. In an alternate embodiment a digital wallet is used. In an

One embodiment of a system is illustrated in FIG. **1**. In this embodiment, a transaction privacy clearing house (TPCH) **110** interfaces a user **120** and a vendor **125**. In this particular embodiment, a transaction device, e.g., a privacy card **130**, is used to maintain the privacy of the user while enabling the user to perform transactions. The transaction

Pet. 5-8; Ex. 1005, Abstract, 3:32-36, 6:36-44; D.I. 13-16

Overview of Ludtke

A method of identifying an authorized user with a biometric device and enabling the authorized user to access private information over a voice network is disclosed.

this data for use outside the eCommerce system. The user connects to and performs transactions with the eCommerce system through a transaction device which has a unique identifier (ID). In one embodiment, a privacy card is used. In an alternate embodiment a digital wallet is used. In an

One embodiment of a system is illustrated in FIG. **1**. In this embodiment, a transaction privacy clearing house (TPCH) **110** interfaces a user **120** and a vendor **125**. In this particular embodiment, a transaction device, e.g., a privacy card **130**, is used to maintain the privacy of the user while enabling the user to perform transactions. The transaction

Pet. 5-8; Ex. 1005, Abstract, 3:32-36, 6:36-44; D.I. 13-16

Overview of Ludtke (Cont.)

sized for easy carrying and use. Thus, in one embodiment, the card **705** is configured to be the size of a credit card. The privacy card includes a processor **710**, memory **715** and

input/output logic **720**. The processor **710** is configured to execute instructions to perform the functionality herein. The instructions may be stored in the memory **715**. The memory is also configured to store data, such as transaction data and the like. In one embodiment, the memory **715** stores the

The user identity info block **760**, which was described previously in FIG. 7*b* PrivacyCard, may contain the authorized fingerprint recognition samples. In one embodiment,

FIG. **27** is a flow diagram illustrating one embodiment of securely sharing information. In this example embodiment, the back-end system may be in possession of several PKI key pairs, one for each password to be assigned. The back-end distributes one public key with each password and the biometric device stores and associates these back-end public keys with the associated password and data as illustrated in FIG. **26** at **2609**.

 Pet. 5; Ex. 1005 11:66-12:7, 14:19-21, 38:26-29

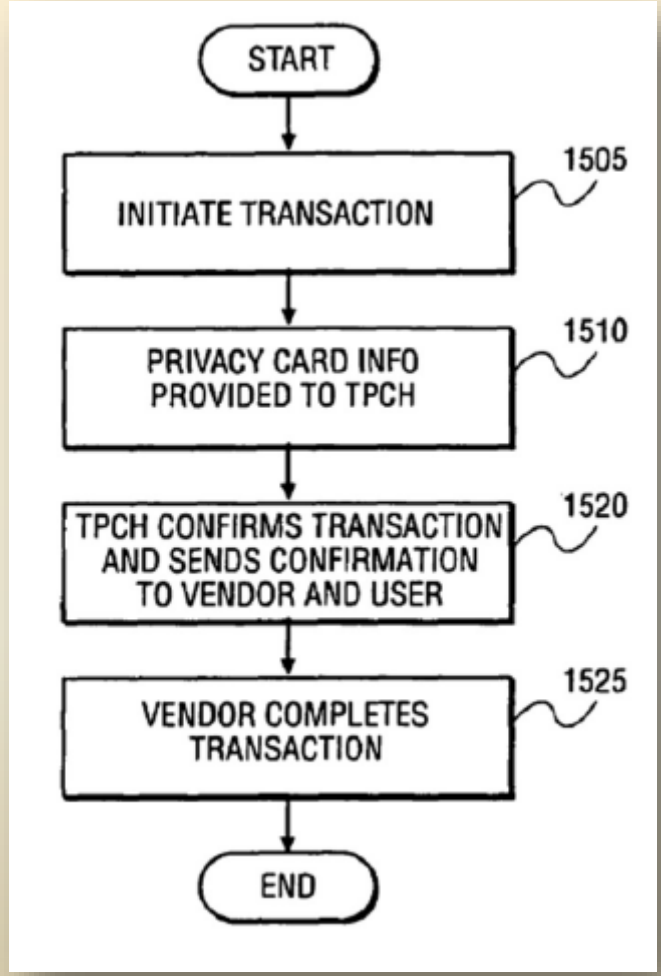
Overview of Ludtke (Cont.)

*The **Transaction Privacy Clearing House ("TPCH") is a trusted third-party agent**, separate from the transaction device, personal POS terminal and the back-end transacting entity (e.g., vendor).*

The transaction device receives confirmation of the transaction and validates that the user is authorized. When information on the user's side of the transaction has been set up to perform a transaction, the personal POS terminal opens a secure communications session to the TPCH, requesting a transaction. The personal POS terminal provides the transaction record that it received from the web browser and the unique ID of the transaction device. The TPCH uses the unique ID of the transaction device to process the transaction.

Pet. 6, 25; Ex. 1005 28:41-45, 29:5-12, 7:42-48, 9:26-34, FIG. 6

Overview of Ludtke (Cont.)



Pet. 5-8; Ex. 1005, FIG. 15; D.I. 13-16

Issue 1: Ludtke discloses or renders obvious "a third party that operates a trusted authority" / "the trusted authority" / "a third party trusted authority"

’954 Patent Claim 1

1. A method comprising:

persistently storing biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is not capable of being subsequently altered;

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 and other values from the plurality of codes and other data values for authentication to **a third party that operates a trusted authority**, wherein the one or more codes and other data values includes the device ID code; and

receiving, at an application, an access message from **the trusted authority** indicating that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party and allowing the user access to the application.

Ludtke discloses a "third party trusted authority" / "a third party that operates a trusted authority" / "the trusted authority

- Ludtke's TPCH 440 v. consumer 430 and vendors 450. D.I. 14; Ex. 1005, FIG. 4; 6:36-44
- Acts as third party trusted authority. RPOR 7; Pet. 28-29; Ex. 1005, 9:35-39, Fig. 6; D.I. 20-24.
- Meets Board's Construction. Pet. 6-7, 25-28; RPOR 4; D.I. 12.
- PO's repeated arguments rejected. POR 4-6; D.I. 20-24

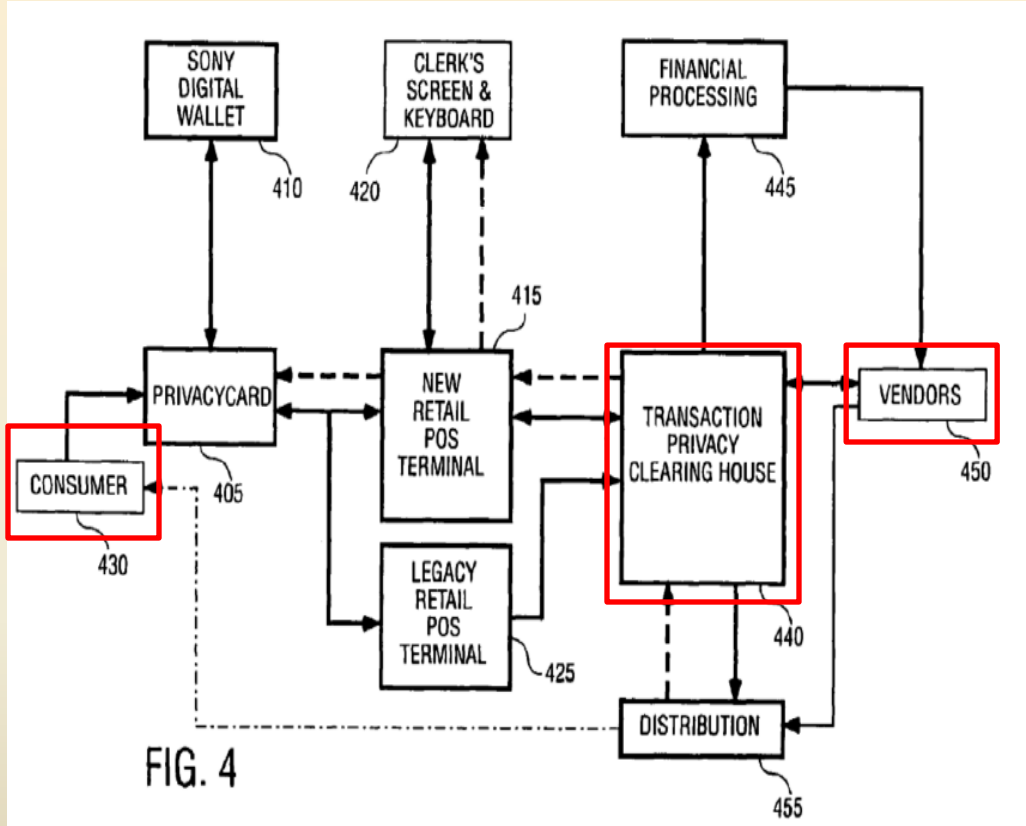


FIG. 4

Pet. 6-7, 25-28; D.I. 14; POR 4-6; RPOR 4, 7

Ludtke discloses a "third party trusted authority" / "a third party that operates a trusted authority" / "the trusted authority

- Ludtke's TPCH is "*an entity separate from the parties to a transaction*" D.I. 8, 11-12, 23.
- TPCH is not the user nor the vendor in the transaction.
  - TPCH is not the user or transaction device RPOR 7
  - TPCH is not the external retailer or the vendor RPOR 7
  - TPCH "***functions as the middleman***" Pet. 26-28; Ex.1005, 7:44-48; D.I. 20; Ex. 1003 ¶ 106

etc.) electronic distribution may be used. In one embodiment of electronic distribution, the TPCH **110** functions as the 45 middleman of the distribution channel. This allows the TPCH **110** to retain user privacy by not exposing addressing information and possibly email addresses to third parties. In

 Pet. 6-7, 25-28; Ex. 1003, ¶ 106; D.I. 20; RPOR 4, 7

Ludtke discloses a "third party trusted authority" / "a third party that operates a trusted authority" / "the trusted authority

- Ludtke's TPCH is not "an application" as defined by the patent. RPOR 7
  - "application" is defined as "a resource that can be accessed by a verified and authenticated user." EX1001, 6:19-24. RPOR 7.

> Application **330** is a resource that can be accessed by a verified and authenticated user. Application **330** can be, for example, a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file, a financial account (e.g. a savings account, checking account, brokerage account, credit card account, credit line, etc.) and the like. In one embodiment, a file

  - TPCH is not an "application" because it is **not accessed by a verified and authenticated user** of the transaction device
    - Rather, it "functions as the middleman of the distribution channel." Pet. at 31 (quoting Ludtke, 7:44-48). RPOR 7-8.

Pet. 6-7, 25-28, 31; D.I. 20; RPOR 4, 7

Ludtke discloses a "third party trusted authority" / "a third party that operates a trusted authority" / "the trusted authority

- PO repeats the same arguments the Board considered and rejected at institution. D.I. 2,11-12, 20-24; RPOR 9.
  - PO argues "the ability to pay the vendor with the user's account (the private information) is the application" POR at 14; RPOR 9.
  - This argument suggests that anything enabling the user to pay a vendor is an application (and therefore cannot be a third party). RPOR 9.
  - Such a reading is unsupported by evidence. RPOR 9.
  - Relies solely on Mr. Carrothers' conclusory testimony. RPOR 9
- PO's argument implies that the '954 Patent's "trusted key authority" is also an application—and by PO's logic—not a third party. RPOR 9.

D.I. 2, 11-12, 20-24; RPOR 9

Issue 2: Ludtke discloses or renders obvious "receiving, at an application, an access message from the trusted authority…allowing the user access to the/an application"

’954 Patent Claim 1

1. A method comprising:

persistently storing biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is not capable of being subsequently altered;

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 and other values from the plurality of codes and other data values for authentication to a third party that operates a trusted authority, wherein the one or more codes and other data values includes the device ID code; and

receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party and **allowing the user access to the application**.

LUDTKE DISCLOSES OR RENDERS OBVIOUS "RECEIVING, AT AN APPLICATION, AN ACCESS MESSAGE FROM THE TRUSTED AUTHORITY…ALLOWING THE USER ACCESS TO THE/AN APPLICATION."

- Ludtke discloses "receiving, at an application, an access message from the trusted authority…allowing the user access to the application":
  - TPCH "issues a transaction confirmation back to the personal POS terminal" (an access message from the trusted authority) after "validating that the transaction device is in good standing and…has sufficient funds for the transaction" Ex. 1005, 29:12-22; Pet. 30; EX1003, ¶107

unique ID of the transaction device. The TPCH uses the unique ID of the transaction device to process the transaction.

After validating that the transaction device is in good standing and that the selected account has sufficient funds for the transaction, the TPCH issues a transaction confirmation back to the personal POS terminal. The personal POS terminal reflects the transaction confirmation back to the web browser and the transaction device. The transaction device may display a transaction confirmation to the user and may additionally record the transaction in its local storage. The personal POS terminal may also record the

LUDTKE'S TPCH ISSUES A TRANSACTION CONFIRMATION THAT ALLOWS ACCESS

- *No dispute*: Ludtke's transaction confirmation is sent from the TPCH and received at an application. RPOR 10

- Ludtke: TPCH validates the transaction device → sends a "transaction confirmation" → a "content provider" has content "delivered to the transaction device" → allows user access. RPOR 10-11 (citing Pet. 31-32; Ludtke, 29-15-20, 31:41-50; Ex.1003, ¶114).

LUDTKE DISCLOSES OR RENDERS OBVIOUS "RECEIVING, AT AN APPLICATION, AN ACCESS MESSAGE FROM THE TRUSTED AUTHORITY…ALLOWING THE USER ACCESS TO THE/AN APPLICATION."

- Ludtke discloses "receiving, at an application, an access message from the trusted authority…allowing the user access to the application":
  - TPCH's "transaction confirmation" (an access message from the trusted authority) is "reflect[ed] back to the web browser [(application)] and transaction device" and "[s]ecure distribution of physical (or electronic) content to the user is performed" based on the confirmation. Ex. 1005, 29:15-22, 29:29-30; Pet. 30; Ex. 1003, ¶110

unique ID of the transaction device. The TPCH uses the unique ID of the transaction device to process the transaction.

After validating that the transaction device is in good standing and that the selected account has sufficient funds for the transaction, the TPCH issues a transaction confirmation back to the personal POS terminal. The personal POS terminal reflects the transaction confirmation back to the web browser and the transaction device. The transaction device may display a transaction confirmation to the user and may additionally record the transaction in its local storage. The personal POS terminal may also record the

LUDTKE DISCLOSES OR RENDERS OBVIOUS "RECEIVING, AT AN APPLICATION, AN ACCESS MESSAGE FROM THE TRUSTED AUTHORITY…ALLOWING THE USER ACCESS TO THE/AN APPLICATION."

- Ludtke discloses "receiving, at an application, an access message from the trusted authority…allowing the user access to the application":
  - TPCH's transaction confirmation (an access message) allows the user to access "content or a reference to the content" Ex. 1005, 29:15-20, 29:29-30, 31:41-52; Ex. 1003, ¶¶ 107-114; Pet. 29.
  - "[s]ecure distribution of physical (or electronic) content to the user is performed" based on the confirmation. Ludtke, 29:29-30; Pet. 30; Ex. 1003, ¶110

> Secure distribution of physical (or electronic) content to the user is performed once the transaction is authorized. 30

  - The distributed content includes the content itself or a reference to that content, such as a "web-URL." Ex. 1003, ¶ 110; Pet. 30.

LUDTKE DISCLOSES OR RENDERS OBVIOUS "RECEIVING, AT AN APPLICATION, AN ACCESS MESSAGE FROM THE TRUSTED AUTHORITY…ALLOWING THE USER ACCESS TO THE/AN APPLICATION."

- '954 Patent describes that "an application" can be "computer software," "**a web site**," or "a file" Ex. 1001, 6:19-24.

> Application **330** is a resource that can be accessed by a verified and authenticated user. Application **330** can be, for example, a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file, a financial account (e.g. a savings account, checking account, brokerage account, credit card account, credit line, etc.) and the like. In one embodiment, a file

- Thus, Ludtke discloses receiving, at **a web browser webpage** (an application), **a transaction confirmation** (an access message from the trusted authority) that **allows the user to access electronic content on the web browser** (allowing the user access to application). Ex. 1003, ¶110; Pet. 30.

LUDTKE DISCLOSES OR RENDERS OBVIOUS "RECEIVING, AT AN APPLICATION, AN ACCESS MESSAGE FROM THE TRUSTED AUTHORITY…ALLOWING THE USER ACCESS TO THE/AN APPLICATION."

- Ludtke also discloses **downloading "new functionality," software, and services** (an application) on the transaction device, and **accessing the service** (allowing the user access to the application) after **receiving the transaction confirmation** (an access message from the trusted authority) at the transaction device. Ex. 1003, ¶111-112; Pet. 30-31.
- The downloaded functionality and software/service is an "an application" Ex. 1005, 19:45-50, 31:11-52; Ex. 1001, 6:18-24; Ex. 1003, ¶ 113; Pet. 31.
  - after the TPCH issues a "transaction confirmation" (an access message)—a "content provider" has the content "delivered to the transaction device" thereby allowing the user to access the service(s) offered by the downloaded functionality/software. Ex. 1005, 29:15-20, 31:41-50; Ex. 1003, ¶ 114; Pet. 31-32.

Issue 3: Mr. Carrothers does not qualify as a POSITA

POSITA Definition

POSITA: "at the time of the purported invention would have had at least a bachelor's degree in Computer or Electrical Engineering or an equivalent engineering discipline, and at least three years of experience in the field of encryption and security, or the equivalent … .Additional education could substitute for professional experience, and significant work experience could substitute for formal education" Pet. 4-5; Ex. 1003 ¶¶ 31-32, 53-55.

- POSITA definition adopted by Board. RPOR 3; D.I. 13
- No challenge to POSITA definition after institution. RPOR 2-3

Mr. Carrothers is NOT a POSITA

- Mr. Carrothers doesn't meet POSITA definition. RPOR 3; Ex. 2018
- PO does not claim Mr. Carrothers testifies as a POSITA. RPOR 3 (citing POR; EX2018).
- Mr. Carrothers' declaration should be given no weight RPOR 3
  - *Kyocera Senco Indus. Tools Inc. v. Int'l Trade Comm'n*, 22 F.4th 1369, 1376–77 (Fed. Cir. 2022)
  - *Nespresso USA, Inc. v. K-fee System GmbH*, IPR2023-00485, Paper 26 at 9-14 (Sep. 10, 2024)
- PO's Sur-Reply arguments are too late. RPOR 4
  - *Nespresso*, IPR2023-00485, Paper 26 at 12 ("Patent Owner's attempt to establish Dr. Howle's qualifications in the Sur-reply … is too little too late.")
  - *In re NuVasive*, 842 F.3d 1376, 1380-81 (Fed. Cir. 2016)

Issue 4: Patent Owner's Untimely Arguments and Exhibits Regarding the '730 Reexam in the Sur-Reply Should Not be Allowed.

Patent Owner's Untimely Arguments and Exhibits Regarding the '730 Reexam in the Sur-Reply Should Not Be Allowed

- Patent Owner's arguments and exhibits were not raised in the POR.
  - They violate the Board's Rule on Sur-Replies and should not be allowed.

> **IV. THE RATIONALES PRESENTED IN THE PETITION WERE REJECTED BY THE CRU IN THE 730 REEXAM**

  - Patent Owner's Sur-Reply arguments at pp. 10-17 should not be allowed.
  - Patent Owner's Sur-Reply Exhibits 2020-2025 should not be allowed.

POSR 10-17

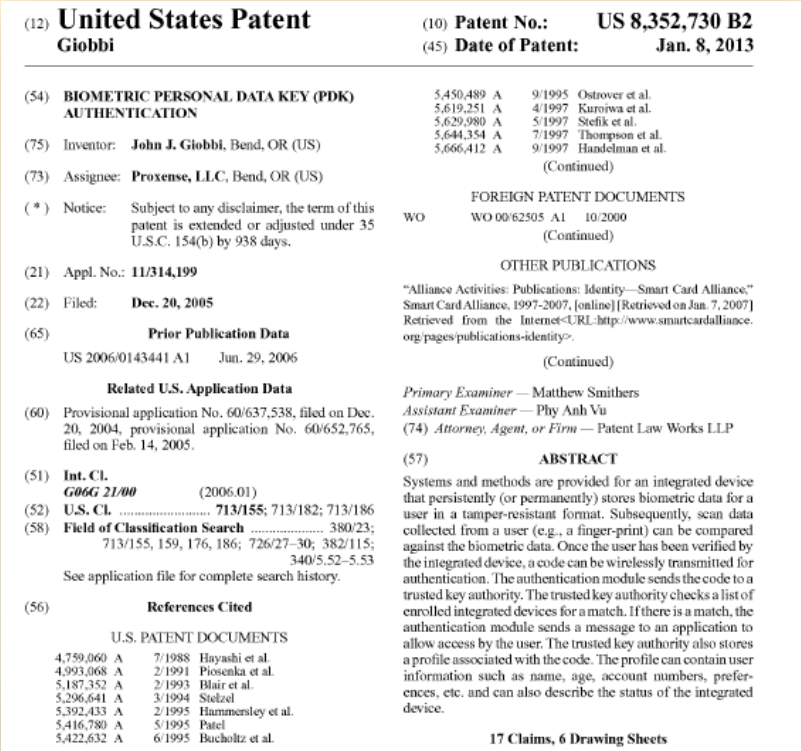
Mere Interaction With an Application is Not Access to the Application

- Patent Owner's argument that mere interaction with an application equates to access to the application should be rejected. RPOR 12.
  - Patent Owner's argument that "a user must have been allowed access to the website [application] prior to receipt of the confirmation from the TPCH"—conflates mere *interaction with* an application with access to the content of the application following user authentication. RPOR 11 (citing POR 20)
    - *See* POR 19 ("the user gains access to these resources at the beginning of the transaction").
    - Wrongly suggests that the user cannot have any interaction whatsoever with the application prior to authentication—narrow reading of "access" would exclude disclosed embodiments of the '954 Patent RPOR 11
    - '954 Patent discloses that a "slot machine" is a type of application, and that the user interacts with the slot machine prior to authorization (e.g., the user can input user data and attempt to play). RPOR 11-12
    - Such simple interaction is not "access" —the user cannot access the content (the actual game) of that slot machine until the user is authenticated. RPOR 12 (citing Ex. 1001, 4:34-36, 6:63-7:3, 7:21-26)
  - '954 Patent also describes an "open system, where unknown users can attempt authentication (e.g., in a public grocery store)." RPOR 12 (citing Ex. 1001, 6:48-51)
    - Such an "attempt" would require *interaction* with the resource to be accessed, but as the '954 Patent explains, access happens after authentication. RPOR 12 (citing EX1001, 6:48-51)
  - Constructions that exclude embodiments are "presumptively incorrect." RPOR 12 (citing D.I. at 11)
    - *See Sequoia Tech., LLC v. Dell, Inc.*, 66 F.4th 1317, 1327 (Fed. Cir. 2023)

Patent Owner's Arguments Fail to Address the Mapping in Petition

- Patent Owner presumes that the vendor is the application—this is not the mapping in the Petition. RPOR 12-13 (citing Pet. 28-30, 30-32)
  - Pet. 28-30 (explaining that Ludtke's content or a reference to content on a webpage corresponds to the claimed application to be accessed)
  - Pet. 30-32 (explaining that Ludtke's services prescribed by the downloaded software/functionality also correspond to the claimed application to be accessed).
- Patent Owner ignores Ludtke's disclosure that "[s]ecure distribution of physical (or electronic) content to the user is performed" once the transaction is authorized RPOR 13
  - after the TPCH authenticates the transaction device ID, and the TPCH sends an indication of an approval of the transaction to be performed. RPOR 13 (citing Pet. 31-32; Ex. 1005, 29:15-20, 31:41-50; Ex. 1003, ¶114).

Overview of ’730 Patent



(12) **United States Patent**
Giobbi

(10) **Patent No.: US 8,352,730 B2**
(45) **Date of Patent: Jan. 8, 2013**

(54) **BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION**

(75) Inventor: **John J. Giobbi**, Bend, OR (US)

(73) Assignee: **Proxense, LLC**, Bend, OR (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 938 days.

(21) Appl. No.: **11/314,199**

(22) Filed: **Dec. 20, 2005**

(65) **Prior Publication Data**

US 2006/0143441 A1 Jun. 29, 2006

Related U.S. Application Data

(60) Provisional application No. 60/637,538, filed on Dec. 20, 2004, provisional application No. 60/652,765, filed on Feb. 14, 2005.

(51) **Int. Cl.**
G06G 21/00 (2006.01)

(52) **U.S. Cl.** **713/155**; 713/182; 713/186

(58) **Field of Classification Search** 380/23; 713/155, 159, 176, 186; 726/27–30; 382/115; 340/5.52–5.53
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,759,060	A	7/1988	Hayashi et al.
4,993,068	A	2/1991	Piosenka et al.
5,187,352	A	2/1993	Blair et al.
5,296,641	A	3/1994	Stelzel
5,392,433	A	2/1995	Hammersley et al.
5,416,780	A	5/1995	Patel
5,422,632	A	6/1995	Bucholtz et al.
5,450,489	A	9/1995	Ostrover et al.
5,619,251	A	4/1997	Kuroiwa et al.
5,629,980	A	5/1997	Stefik et al.
5,644,354	A	7/1997	Thompson et al.
5,666,412	A	9/1997	Handelman et al.

(Continued)

FOREIGN PATENT DOCUMENTS

WO WO 00/62505 A1 10/2000

(Continued)

OTHER PUBLICATIONS

"Alliance Activities: Publications: Identity—Smart Card Alliance," Smart Card Alliance, 1997-2007, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet<URL:http://www.smartcardalliance.org/pages/publications-identity>.

(Continued)

Primary Examiner — Matthew Smithers
Assistant Examiner — Phy Anh Vu
(74) *Attorney, Agent, or Firm* — Patent Law Works LLP

(57) **ABSTRACT**

Systems and methods are provided for an integrated device that persistently (or permanently) stores biometric data for a user in a tamper-resistant format. Subsequently, scan data collected from a user (e.g., a finger-print) can be compared against the biometric data. Once the user has been verified by the integrated device, a code can be wirelessly transmitted for authentication. The authentication module sends the code to a trusted key authority. The trusted key authority checks a list of enrolled integrated devices for a match. If there is a match, the authentication module sends a message to an application to allow access by the user. The trusted key authority also stores a profile associated with the code. The profile can contain user information such as name, age, account numbers, preferences, etc. and can also describe the status of the integrated device.

17 Claims, 6 Drawing Sheets

- Title: Biometric Personal Data Key (PDK) Authentication
- Earliest Claimed Priority: Dec. 20, 2004
- 17 Claims
  - Independent: 1 (method), 8 (device), 12 (method), 15 (system)
  - Dependent: 2-7, 9-11, 13-14, 16-17
  - Same specification as ’954 Patent

’730 Patent - Claim 1

1. 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 from the agent allowing the user access to an 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.

Overview of ’730 Grounds

Patent Owner’s Arguments Are All Based on Ground 1

Ground	Basis	Cited Art	’730 Claims
1	103	Ludtke (Ex. 1005)	1-6, 8, 9, 11, 12, 14-17
2	103	Ludtke and Kon (Ex. 1006)	3, 10, 13