UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/290,176	05/29/2014	Thomas Suwald	81541361US03	6508

65913 7590 01/21/2020
Intellectual Property and Licensing
NXP B.V.
411 East Plumeria Drive, MS41
SAN JOSE, CA 95134

EXAMINER	
CATTUNGAL, DEREENA T	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
01/21/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte THOMAS SUWALD

Appeal 2018-008976
Application 14/290,176[1]
Technology Center 2400

Before DAVID M. KOHUT, HUNG H. BUI, and PHILLP A. BENNETT, *Administrative Patent Judges*.

BUI, *Administrative Patent Judge.*

DECISION ON APPEAL

Appellant seeks our review under 35 U.S.C. § 134(a) from the Examiner's Final Rejection of claims 1–20, which are all the claims pending in the application. App. Br. 14–18 (Claims App.). We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.[2]

[1] We use the word "Appellant" to refer to "applicant(s)" as defined in 37 C.F.R. § 1.42. According to Appellant, the real party in interest is NXP B.V. App. Br. 1.

[2] Our Decision refers to Appellant's Appeal Brief filed May 25, 2018 ("App. Br."); Reply Brief filed September 18, 2018 ("Reply Br."); Examiner's Answer mailed August 27, 2018 ("Ans."); Final Office Action mailed February 13, 2018 ("Final Act."); and original Specification filed May 29, 2014 ("Spec.").

STATEMENT OF THE CASE[3]

Appellant's Invention

Appellant's invention relates to a security token and transaction authorization system for multi-factor user authentication. Spec. 1:3–4, 1:22–23, 4:1–6; Title. According to Appellant, the multi-factor user authentication authenticates based on multiple factors including [1] "something a user knows (e.g.[,] a personal identification number), [2] something a user has (the smart card) and [3] something that characterizes a user (a handwriting characteristic)." Spec. 4:3–6. A user-specific credential used to authenticate may be a challenge key or a one-time password, in addition to a personal identification number. Spec. 7:9–11.

Representative Claim

Claims 1 and 14 are independent. Representative claim 1 is reproduced below with disputed limitations in *italics*:

> 1. A security token configured to support multi-factor user authentication, said security token comprising:
>
> a tactile sensing user interface configured to capture a stream of input data corresponding to a sequence of positions of a finger engaging with said tactile sensing user interface and representing a user-specific credential for authorizing a transaction;
>
> a conversion unit configured to convert said stream of input data into a machine-readable credential;
>
> a computation unit configured to compute a machine-readable authentication code based on the machine-readable credential;
>
> *a comparison unit configured to compare the computed machine-readable authentication code with a machine-readable*

[3] See our Decision dated March 23, 2017 for additional context, where we affirmed an earlier obviousness rejection of claims 1–20 based on the same set of cited prior art.

> *reference code stored in the security token and to generate a corresponding authentication result [1]* ***without user interaction****, wherein the comparison is performed on the security token [2]* ***after capturing the stream of input data****;*
>
> a contact-bound interface configured to transmit said machine-readable authentication code to a first transaction device; and
>
> a contactless interface configured to transmit said machine-readable authentication code to a second transaction device, wherein the multi-factor user authentication requires both the user-specific credential and a handwriting characteristic.

App. Br. 14 (Claims App'x) (bracketing added).

Evidence Considered

Name	**Reference**	**Date**
Wendt	US 2008/0148393 A1	Jun. 19, 2008
Adams et al. "Adams"	US 2010/0275259 A1	Oct. 28, 2010
Black	US 6,539,101 B1	Mar. 25, 2003
Rhoads et al. "Rhoads"	US 2008/0112596 A1	May 15, 2008
Hammad et al. "Hammad"	US 2013/0218765 A1	Aug. 22, 2013
Armington et al. "Armington"	US 2003/0163739 A1	Aug. 28, 2003

Examiner's Rejections[4] & References

(1) Claims 1–6, 8, 14–18, and 20 [sic, claims 1–6, 8, and 14–18] stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wendt, Adams, and Black. Final Act. 5–12.

(2) Claim 7 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Wendt, Adams, Black, and Rhoads. Final Act. 12–13.

(3) Claims 9–13 and 20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wendt, Adams, Black, and Hammad. Final Act. 13–16.

(4) Claim 19 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Wendt, Adams, Black, and Armington. Final Act. 16–17.

Issue on Appeal

Based on Appellant's arguments, the dispositive issue on appeal is whether the cited prior art (Wendt) teaches or suggests "a comparison unit configured to compare the computed machine-readable authentication code with a machine-readable reference code stored in the security token and to generate a corresponding authentication result [1] <u>without user interaction</u>, wherein the comparison is performed on the security token [2] <u>after capturing the stream of input data</u>," as recited in Appellant's independent claims 1 and 14. App. Br. 6–7 (emphasis added); Reply Br. 2–3.

[4] Claims 1 and 14 were rejected under 35 U.S.C. § 112(a) as failing to comply with the written description requirement. Final Act. 4. However, the Examiner has withdrawn this rejection in Advisory Action dated May 15, 2018. As such, this rejection is no longer on appeal.

ANALYSIS

With respect to independent claims 1 and 14, the Examiner finds Wendt teaches Appellant's claimed "security token configured to support multi-factor user authentication" including "a tactile sensing user interface," "a conversion unit," "a computation unit," and "a comparison unit." Final Act. 5–6 (citing Wendt ¶¶ 15–17, 49–50, 53–55, 62–63, Figs. 1–4). The Examiner acknowledges Wendt does not expressly disclose "a contact-bound interface," "a contactless interface," and "multi-factor user authentication requiring both a user-specific credential and a handwriting characteristic, but relies on (1) Adams for teaching the claimed "contact-bound interface," and "contactless interface," and (2) Black for teaching such "multi-factor user authentication" to support the conclusion of obviousness. Final Act. 6–7 (citing Adams ¶¶ 179, 281; Black 10:45–51, 18:6–14, and 27–33).

Appellant does not dispute the Examiner's factual findings regarding Adams and Black. Nor does Appellant challenge the Examiner's rationale to combine those references. Appellant even acknowledges Wendt teaches the claimed "comparison unit configured to compare the computed machine-readable authentication code with a machine-readable reference code stored in the security token and to generate a corresponding authentication result," but argues Wendt's "comparison unit" does not make such comparison and authentication "[1] without user interaction, wherein the comparison is performed on the security token [2] after capturing the stream of input data [representing a user-specific credential for authorizing a transaction]" as recited in Appellant's independent claims 1 and 14. App. Br. 6–7 (citing

Wendt ¶¶ 47–48) (emphasis added); Reply Br. 2–3. In particular, Appellant argues "Wendt teaches away from the claimed subject matter by requiring user interactions" because "Wendt clearly requires a plurality of user interactions for authentication." Reply Br. 2–3. According to Appellant, "Wendt discloses two different time windows with user interaction," including "an initial password comparison in paragraph [0047] and additional user interaction during the second time window of paragraph [0048]." Reply Br. 3 (citing Wendt ¶¶ 47–48).

> As depicted in Fig. 4, Wendt requires input1 in step 205, defined by the user "applying pressure several times to the input1 sensor 170" in paragraph [0060], and entry of the neural biometric password in step 220. The user may be "once again prompted to enter" in paragraph [0061].

Reply Br. 3

We do not find Appellant's arguments persuasive. Rather, we find the Examiner has provided a comprehensive response to Appellant's arguments supported by a preponderance of evidence. Ans. 4. Therefore, we adopt the Examiner's findings and explanations provided therein. *Id.* For additional emphasis, we note Wendt teaches user biometric enabled universal smart card 100, shown in Figures 1 and 3, that utilizes (1) biometrics authentication, i.e., "measuring and analyzing human body characteristics such as fingerprints, eye retina and irises, voice and facial patterns and hand geometry for the purpose of validating an individual identity" (Wendt ¶¶ 5, 9); (2) embedded piezo transducers sensors 160–170, shown in Figures 1–2, to deliver tactile inputs based on user neural biometric password (Wendt ¶¶ 47–50); and (3) embedded firmware, i.e., CPU EEPROM 120, shown in Figure 3, to match the tactile inputs based on user neural biometric password (user-specific credential) with a stored reference for "comparison, verification and authentication" (Wendt ¶¶ 63). As correctly recognized by the Examiner:

> Wendt in para: 0047–0048 teaches "a comparison unit . . . to generate a corresponding authentication result without user interaction, wherein the comparison is performed on the security token after capturing the stream of input data.
>
> Figs. 1 and 3 shows the user biometric enabled universal smart card (smart token). In Fig. 3, element 120 is CPU EEPROM, which is the smart card processor performing the authentication verification. Therefore, the authentication result is done by a processor without user interaction, and the comparison is performed on the security token (smart card) after capturing the stream of input data.

Ans. 4 (citing Wendt ¶¶ 47–48). In other words, once the tactile inputs based on user neural biometric password (user-specific credential) are received, Wendt's CPU EEPROM 120, shown in Figure 3, is configured to make such a comparison and generate an authentication result in the manner recited in Appellant's claims 1 and 14, i.e., "without user interaction" and such a comparison is performed "after capturing the stream of input data [representing a user-specific credential for authorizing a transaction]." *See* Advisory Action, p. 2.

For the reasons set forth above, Appellant has not persuaded us of Examiner error. Accordingly, we sustain the Examiner's obviousness rejection of independent claims 1 and 14, and dependent claims 2–13, and 15–20, which Appellant does not argue separately. App. Br. 7–11.

CONCLUSION

On the record before us, we conclude Appellant has not demonstrated the Examiner erred in rejecting claims 1–20 under 35 U.S.C. § 103(a). As such, we AFFIRM the Examiner's Final Rejection of claims 1–20.

DECISION SUMMARY

In summary:

Claims Rejected	**35 U.S.C. §**	**Reference(s)/Basis**	**Affirmed**	**Reversed**
1–6, 8, 14–18	103	Wendt, Adams, Black	1–6, 8, 14–18	
7	103	Wendt, Adams, Black, Rhoades	7	
9–13, 20	103	Wendt, Adams, Black, Hammad	9–13, 20	
19	103	Wendt, Adams, Black, Armington	19	
Overall Outcome			1–20	

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED