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.
14/596,165	01/13/2015	Thomas E. F. Wille	81587305US03	2990

65913 7590 09/21/2020

Intellectual Property and Licensing
NXP B.V.
411 East Plumeria Drive, MS41
SAN JOSE, CA 95134

EXAMINER
HAILU, TESHOME

ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
09/21/2020	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 E.F. WILLE

Appeal 2019-002754
Application 14/596,165
Technology Center 2400

Before ROBERT E. NAPPI, BETH Z. SHAW, and
JAMES W. DEJMEK, *Administrative Patent Judges*.

DEJMEK, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant[1] appeals under 35 U.S.C. § 134(a) from a Final Rejection of claims 1, 2, 5–7, 9–11, and 13–20. Appellant has canceled claims 3, 4, 8, and 12. *See* Appeal Br. 14–19. We have jurisdiction over the remaining pending claims under 35 U.S.C. § 6(b).

We affirm in part.

[1] Throughout this Decision, we use the word "Appellant" to refer to "applicant" as defined in 37 C.F.R. § 1.42 (2018). Appellant does not identify by name the real party in interest in the Appeal Brief. Accordingly, we assume that the real party in interest is the named inventor, Thomas E.F. Wille. *See* 37 C.F.R. § 41.37(c)(1)(i).

STATEMENT OF THE CASE

Introduction

Appellant's disclosed and claimed invention generally relates to a data processing device executing an application in a secure mode. Spec. 1:6–7, 4:16–23, 6:21–24. In a disclosed embodiment, when the data processing device is executing an application in a secure mode, access to the user input interface and the user output interface are restricted. Spec. 6:30–7:1. More particularly, while operating in a secure mode, access to the user input interface and user output interface is permitted only to the secure application. Spec. 7:14–17.

Claim 1 is exemplary of the subject matter on appeal and is reproduced below with the disputed limitations emphasized in *italics*:

> 1. A data processing device configured to execute an application, the data processing device comprising:
>
> a processing unit comprising a user interface access controller that is configured to *control access to both a user input interface and a user output interface, wherein the access to the user input interface is restricted by setting at least one control register in the processing unit to a value indicative of a secure access mode*;
>
> a secure element configured to control the user interface access controller in the secure access mode, *wherein the secure element is further configured to load a user interface access control program into the processing unit before switching the user interface application controller to the secure access mode* and cause the user interface access controller in the processing unit to restrict access to the user input interface and the user output interface during execution of the application in the secure access mode, wherein a security driver function resides in the secure element.

The Examiner's Rejection

Claims 1, 2, 5–7, 9–11, and 13–20 stand rejected under 35 U.S.C. § 103 as being unpatentable over Delfs et al. (US 2006/0195907 A1; Aug. 31, 2006) ("Delfs"); Levin et al. (US 5,432,934; July 11, 1995) ("Levin"); and Holm et al. (US 2009/0055637 A1; Feb. 26, 2009) ("Holm").[2] Final Act. 4–9.

ANALYSIS[3]

A. Claims 1, 5–7, 9, 10, and 13–19

Appellant argues the Examiner erred in finding Delfs teaches a user interface access controller that is configured to control access to both a user input interface and a user output interface. Appeal Br. 7–8; Reply Br. 2–3. More particularly, Appellant asserts that Delfs is limited to controlling access to only a user input interface rather than controlling access to both a user input interface and a user output interface. Appeal Br. 7–8; Reply Br. 2–3 (citing Delfs ¶¶ 31–32).

As an initial matter, we note the Examiner relies on the combined teachings of Delfs and Levin to teach the claimed user interface access

[2] We note that in the statement of rejection, the Examiner identifies Kim (US 2008/0280636 A1; Nov. 13, 2008) instead of Holm. However, in the body of the rejection, the Examiner relies on Holm, rather than Kim. *See* Final Act. 6. Appellant notes that Holm was omitted from the list of references, but does not otherwise assert being prejudiced by the omission. Appeal Br. 6. Accordingly, we treat the Examiner's typographical error as harmless.

[3] Throughout this Decision, we have considered the Appeal Brief, filed October 23, 2018 ("Appeal Br."); the Reply Brief, filed February 19, 2019 ("Reply Br."); the Examiner's Answer, mailed January 23, 2019 ("Ans."); and the Final Office Action, mailed July 19, 2018 ("Final Act."), from which this Appeal is taken.

controller that controls access to both a user input interface and a user output interface. *See* Final Act. 4–5. In particular, the Examiner explains Delfs does not "clearly disclose" controlling access to both a user input interface and user output interface and relies on Levin for a more express teaching. *See* Final Act. 5 (citing Levin, Abstract). As relied on by the Examiner, Levin teaches an access restriction system that restricts (i.e., controls) "user input through the user interface apparatus [(i.e., the user input interface)] and computer output through the user interface apparatus [(i.e., the user output interface)]." Levin, Abstract. Thus, Appellant's arguments do not apprise us of Examiner error because, at least, they are not responsive to the Examiner's rejection, which relies on both Delfs and Levin to teach a user interface access controller that controls access to both a user input interface and a user output interface.

Moreover, the Examiner responds to Appellant's arguments with respect to Delfs and finds that Delfs describes the data input unit as being "a keyboard, a data communication interface or an input/output interface to a communication network or to another peripheral device of the data processing device, a touchpad, a touch screen, a computer mouse or a microphone." Ans. 9 (quoting Delfs ¶ 115) (emphases omitted). The Examiner explains that it is known that an input and output interface may be included in a single interface such as a touch screen of a device. Ans. 9. Accordingly, the Examiner finds Delfs teaches a processor controlling access to both a user input interface and a user output interface. Ans. 9.

Appellant does not persuasively rebut the Examiner's findings or technical reasoning that a touch screen is known to be used to an input interface and as an output interface to the user. *See* Reply Br. 2.

Accordingly, we are unpersuaded of Examiner error. Further, contrary to Appellant's assertion, the Examiner's explanation does not amount to a new ground of rejection as the thrust of the rejection has not changed. Rather, the Examiner is merely responding to Appellant's arguments.[4] *Cf. In re Leithem*, 661 F.3d 1316, 1319 (Fed. Cir. 2011).

Appellant also argues that Levin's access restriction system teaches away from restricting access by setting at least one control register in a process unit to a value indicative of a secure mode "because Levin places user restrictions on workspaces." Appeal Br. 7–8 (citing Levin, col. 6, ll. 13–14); Reply Br. 3.

"A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant." *Ricoh Co., Ltd. v. Quanta Computer, Inc.*, 550 F.3d 1325, 1332 (Fed. Cir. 2008) (citations omitted). "[T]he 'mere disclosure of more than one alternative' does not amount to teaching away from one of the alternatives where the reference does not 'criticize, discredit, or otherwise discourage the solution claimed.'"

[4] To the extent that Appellant believes the Examiner set forth an undesignated new ground of rejection in the Answer (*see* Reply Br. 2), that is a petitionable matter not properly before the Board. *See* 37 C.F.R. § 41.40(a) ("Any request to seek review of the primary examiner's failure to designate a rejection as a new ground of rejection in an examiner's answer must be by way of a petition to the Director"); *see also* Manual of Patent Examining Procedure ("MPEP") § 706.01 (9th ed., Rev. 10.2019, June 2020) ("[T]he Board will not hear or decide issues pertaining to objections and formal matters which are not properly before the Board."); *see also* MPEP § 1201 ("The Board will not ordinarily hear a question that should be decided by the Director on petition . . . .").

SightSound Techs., LLC v. Apple Inc., 809 F.3d 1307, 1320 (Fed. Cir. 2015) (*quoting In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004)).

We disagree with Appellant that Levin teaches away from the claimed solution. We note that the Examiner does not rely on Levin, but rather Delfs, to teach a user access controller configured to control access to the user input (and output, *see* above) by setting at least one control register to a value indicative of a secure access mode. *See* Final Act. 4 (citing Delfs ¶ 170, Fig. 8). As relied upon by the Examiner, Delfs teaches data stored in a control register generates a switch state control signal to drive a switch unit that places the device (e.g., keyboard peripheral block) into a secure mode. *See* Delfs ¶¶ 170–173, Figs. 1, 8.

Regarding Appellant's arguments that Levin teaches away from the claimed solution "because Levin places user restrictions on workspaces" (*see* Appeal Br. 7–8 (citing Levin, col. 6, ll. 13–14)), we disagree. Rather, Levin generally describes access restrictions as a means of configuring a user interface. *See* Levin, Title. Levin describes the access restrictions may be filtered by a particular user mode. *See* Levin, col. 19, ll. 46–47. Levin describes a "new proprietary mode construct" in which restrictions (e.g., user restrictions or class restrictions) may be specified in a table. *See, e.g.*, Levin, col. 25, l. 16–col. 26, l. 46, Fig. 13D. We disagree that Levin's approach criticizes, discredits, or discourages one of ordinary skill in the art from setting a value in a control register indicative of a secure mode as a means of setting a particular user access restriction setting. Accordingly, Levin does not teach away from the claimed solution.

Appellant also argues that Holm, as relied on by the Examiner, fails to teach a secure element configured to load a user interface access control

program into the processing unit before switching into a secure access mode. Appeal Br. 8–9; Reply Br. 3–4. In particular, Appellant argues Holm's teaching of placing a chip in a secure mode of operation fails to teach loading a user interface access control program into the processing unit. Appeal Br. 8–9; Reply Br. 3–4. Appellant argues "Holm's chip cannot be reasonably interpreted as equivalent to the recited user interface application controller." Appeal Br. 8. Moreover, Appellant asserts the language of claim 1 requires that a user interface access control program be loaded into the claimed processing unit rather than the user interface application controller. Reply Br. 4.

As an initial matter, we note that claim 1 recites the processing unit comprises a user interface access controller. Thus, even if (without deciding) Holms teaches loading a user interface access control program into a user interface access controller, Holms would still teach that the user interface access control program has been loaded into the processing unit.

In addition, Holm describes a secure power-on reset engine for a processor chip, "which guarantees a secure initialization of the chip to enable secure code execution." Holm, Abstract. As relied on by the Examiner, Holm teaches that on power-on, security and configuration information are read from security and configuration information storage devices to place the chip in a secure mode of operation. Holm ¶¶ 74–76, Fig. 7. Accordingly, the Examiner's finding that Holm teaches a secure element is configured to load a user interface access control program into the processing unit, as claimed, is supported by a preponderance of the evidence.

For the reasons discussed *supra*, we are unpersuaded of Examiner error. Accordingly, we sustain the Examiner's rejection of independent claim 1. For similar reasons, we also sustain the Examiner's rejection of independent claims 10 and 15, which recite similar limitations and were argued collectively with independent claim 1. *See* Appeal Br. 7–9; *see also* 37 C.F.R. § 41.37(c)(1)(iv). Additionally, we sustain the Examiner's rejection of claims 5–7, 9, 13, 14 and 16–19, which depend directly or indirectly therefrom and were not argued separately. *See* Appeal Br. 12; *see also* 37 C.F.R. § 41.37(c)(1)(iv).

B. Claims 2 and 11

Claim 2 depends from claim 1 and recites "restricting the access to the user input interface and the user output interface to instructions comprised in said application." Claim 11 recites a commensurate limitation.

Appellant argues "Delfs cannot restrict access to both user input and output interfaces to instructions comprised in said application because Delfs only places a restriction on a data input mode." Appeal Br. 10 (emphases omitted); Reply Br. 4.

For similar reasons to those discussed with respect to claim 1, we disagree that the combined teachings of Delfs, Levin, and Holm are limited only to restricting access on a data input mode (i.e., the user input interface). Further, as explained by the Examiner Delfs teaches a second processor operating as a secure-mode processor that has control over the data input unit (which, as discussed above, may include a touch screen and, therefore data input and output interfaces). Thus, Delfs teaches the instructions

comprised in an application running on the second (secure) processor restrict access to the user input and output interfaces.

Additionally, as the Examiner finds (*see* Ans. 11), Holm teaches that once the chip in the secure mode, no external access to the resources of the chip is permitted. Thus, access to the user input and user output interfaces are restricted to the instructions comprised in the application running on the chip.

For the reasons discussed *supra*, we are unpersuaded of Examiner error. Accordingly, we sustain the Examiner's rejection of claims 2 and 11.

C. Claim 20

Claim 20 depends indirectly from claim 1 and recites the processing unit further comprises "a plurality of TrustZone control registers, each TrustZone control register configured to control a respective TrustZone function."

In rejecting claim 20, the Examiner relies on the same teaching of a control register of Delfs as was relied on in rejecting claim 1. *See* Final Act. 8–9. Further, in response to Appellant's arguments that the rejection fails to show a plurality of registers wherein each register is associated with a respective TrustZone function (*see* Appeal Br. 11), the Examiner explains that having a plurality of control registers "does not have any patentable weight unless a new and unexpected result is produced." Ans. 12 (citing MPEP § 2144).

Appellant replies that each of the plurality of TrustZone control registers are different rather than duplicative because each is configured to control a respective TrustZone function. Reply Br. 5.

At the outset, we note that "apparatus claims cover what a device *is*, not what a device *does*." *Hewlett-Packard Co. v. Bausch & Lomb Inc.*, 909 F.2d 1464, 1468 (Fed. Cir. 1990). Our reviewing court guides that the patentability of an apparatus claim "depends on the claimed structure, not on the use or purpose of that structure." *Catalina Mktg. Int'l Inc. v. Coolsavings.com, Inc.*, 289 F.3d 801, 809 (Fed. Cir. 2002); *but cf. In re Giannelli*, 739 F.3d 1375, 1379 (Fed. Cir. 2014) (explaining that when supported by the specification, recited elements of an apparatus "adapted to" or "configured to" perform a function have a narrower meaning than merely an intended use of the elements themselves).

Although we note that, as drafted, the claim does not define or use the respective TrustZone functions or even preclude duplicative TrustZone functions, when read in light of the Specification (*see, e.g.*, Spec. 8:29–9:5), we construe claim 20 to recite a plurality of TrustZone control registers wherein each TrustZone control register is configured to a TrustZone function distinct from the other TrustZone functions controlled by the other TrustZone control registers.

Accordingly, we disagree with the Examiner that claim 20 merely recites a duplication of parts (i.e., control registers). Constrained by the record before us, we do not sustain the Examiner's rejection of claim 20.

CONCLUSION

We affirm the Examiner's decision rejecting claims 1, 2, 5–7, 9–11, and 13–19 under 35 U.S.C. § 103.

We reverse the Examiner's decision rejecting claim 20 under 35 U.S.C. § 103.

DECISION SUMMARY

Claims Rejected	35 U.S.C. §	Reference(s)/Basis	Affirmed	Reversed
1, 2, 5–7, 9–11, 13–20	103	Delfs, Levin, Holm	1, 2, 5–7, 9–11, 13–19	20

TIME PERIOD FOR RESPONSE

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). *See* 37 C.F.R. § 41.50(f).

AFFIRMED IN PART