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.
15/075,577	03/21/2016	Matus Harvan	ABBCH-25	1459

129925 7590 08/21/2020

ABB Inc.
Taft, Stettinius & Hollister LLP
One Indiana Square
Suite 3500
Indianapolis, IN 46204-2023

EXAMINER	
GUNDRY, STEPHEN T	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
08/21/2020	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):

taft-ip-docket@taftlaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte MATUS HARVAN, ROMAN SCHLEGEL,
SEBASTIAN OBERMEIER, and THOMAS LOCHER

Appeal 2019-003238
Application 15/075,577
Technology Center 2400

Before ST. JOHN COURTENAY III, JUSTIN BUSCH, and
JAMES W. DEJMEK, *Administrative Patent Judges.*

BUSCH, *Administrative Patent Judge.*

DECISION ON APPEAL

Pursuant to 35 U.S.C. § 134(a), Appellant[1] appeals from the Examiner's decision to reject claims 1–7 and 10–20, which are all the claims pending. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm in part and enter a new ground of rejection. *See* 37 C.F.R. § 41.50(b) (2018).

[1] We use the word Appellant to refer to "applicant" as defined in 37 C.F.R. § 1.42(a). Appellant identifies the real party in interest as ABB Schweiz AG. Appeal Br. 2.

CLAIMED SUBJECT MATTER

The disclosed and claimed subject matter relates to methods and devices for providing secure vendor service access to the device for maintenance of the device by granting or denying access to an instruction set of the device. Spec. 1:2–20, Abstract. In particular, the claimed subject matter relates to a device that is only operable when access rights are set, allows only certain transitions between access states, stores a device configuration for operating the device (e.g., firmware), and includes a security module for granting or denying access to the device configuration. Spec. 1:2–20, 3:27–4:8. Claims 1, 11, and 15 are independent claims, and claim 1 is reproduced below:

> 1. A device providing secure vendor service access for its maintenance, comprising:
>
> a configuration storage providing a device configuration for operating the device; and
>
> a security module being arranged to set at least one access right for accessing the configuration storage;
>
> wherein the device is only operable if the at least one access right is set;
>
> wherein the device is arranged such that a transition from (1) a condition of access rights not being set, to (2) a condition of access enabled or access disabled, and vice versa, is shiftable; and
>
> wherein the device is arranged such that a direct transition from (1) the condition of access rights enabled, to (2) access rights disabled, and vice versa, is prohibited.

REJECTIONS

Claims 1–7, 10, and 16–20 stand rejected under 35 U.S.C. § 112(a) for failing to comply with the written description requirement. Final Act. 7.

Claims 1–7 and 10–20 stand rejected under 35 U.S.C. § 112(b) as indefinite for failing to particularly point out and distinctly claim the subject matter which Appellant regards as the invention. Final Act. 8–9.

Claims 1–7 and 10–20 stand rejected under 35 U.S.C. § 103 as obvious in view of Wood (US 2012/0210113 A1; Aug. 16, 2012), Onno (US 2007/0192851 A1; Aug. 16, 2007), and Dinker (US 2003/0131041 A1; July 10, 2003). Final Act. 9–16.

OPINION

CLAIM CONSTRUCTION ("SECURITY MODULE")

The Examiner concludes the "security module being arranged to set at least one access right for accessing the configuration storage," as recited in independent claim 1, invokes 35 U.S.C. § 112(f). Among other arguments, Appellant asserts the recited security module does not invoke 35 U.S.C. § 112(f) because it does not use the term "means" and the Examiner has not rebutted the presumption that § 112(f) does not apply. Appeal Br. 7–8.

We agree with the Examiner that the recited security module invokes 35 U.S.C. § 112(f) because it recites a means for performing a function without reciting the structure required to perform the function. As the Examiner explained, Ans. 4–5, the claim limitation in question is not the "security module" by itself; it includes the function the security module performs. *See Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1350 (Fed. Cir. 2015) (en banc).

Generic terms such as "mechanism," "element," "device," and other "nonce words" used in a claim can also be considered as a substitute for the "means-plus-function" limitation and, as such, may invoke the application of

35 U.S.C. § 112(f),[2] even without reciting the term "means," because these generic terms or nonce words "'typically do not connote sufficiently definite structure."' *Williamson*, 792 F.3d at 1350 (en banc). As in *Williamson*, the claims here do not recite the term "means," but "the [security module] limitation is drafted in the same format as a traditional means-plus-function limitation, and merely replaces the term 'means' with 'nonce' word 'module,' thereby connoting a generic 'black box' for performing the recited computer-implemented functions." *Williamson*, 792 F.3d at 1350. The term "module" in this context is used as a generic term tantamount to reciting a means because "module" provides no indication of the structure necessary to perform the recited function.

Similarly, the "security" modifier provides one of ordinary skill in the art no insight on the structure necessary to perform the recited function. Here, as in *Williamson*, even if one of ordinary skill in the art were capable of constructing or programming a "security module being arranged to"[3]

[2] The pre-AIA sections of the statute were applicable in *Williamson*, but pre-AIA 35 U.S.C. § 112, sixth paragraph, corresponds to the current § 112(f). We refer to 35 U.S.C. § 112(f) throughout this opinion, including when we reference determinations made in cases when 35 U.S.C. § 112, sixth paragraph, was in effect, except when directly quoting cases.

[3] Although means-plus-function limitations generally use a gerund rather than the infinitive form of a verb, we see no difference between reciting, for example, a nonce word *for performing* an action and a nonce word *being arranged to perform* an action. *See also IMS Tech., Inc. v. Haas Automation, Inc.*, 206 F.3d 1422, 1432 (Fed. Cir. 2000) (finding claim 1's "means to sequentially display data block inquiries" recited no structure for performing the display function and, therefore, invoked 35 U.S.C. § 112(f)); *Kemco Sales, Inc. v. Control Papers Co.*, 208 F.3d 1352, 1361 (Fed. Cir. 2000) (finding claim 27's "plastic envelope closing means . . . to close the opening and to form a closed pocket" invoked 35 U.S.C. § 112(f)).

perform the recited function, it is not sufficient to "create structure where none otherwise is disclosed." *Williamson*, 792 F.3d at 1351.

Thus, even to the extent a person of ordinary skill in the art would have understood the recited "security module" to be "an electronic component" or include generic computer components[4] (e.g., some combination of processing hardware, software, and firmware), such generic computer components without specific programming are not capable of setting at least one access right for accessing the configuration storage. *Williamson*, 792 F.3d at 1350–51 (finding the presumption against invoking 35 U.S.C. § 112(f) is overcome because the recitation of a "distributed learning control module" connotes insufficient structure for carrying out the recited functions).

Contrary to Appellant's argument, we further find that no other limitations recite structure for performing the recited function. Appellant first points to the recited function—"set[ting] at least one access right for accessing the configuration storage"—as reciting the necessary structure. However, as already explained, this is merely the function the recited security module performs. Because the "security module" is the means whose recited function is "to set at least one access right for accessing the configuration storage," *see* Appeal Br. 15, we look to the remaining claim limitations to determine whether the claim recites structure for performing the recited function. If not, the claim invokes 35 U.S.C. § 112(f).

[4] *See, e.g.*, Reply Br. 2 ("the claimed security module is best described as an electronic component"); Spec. 4:19–21 ("the security module may comprise further hardware or software components that allow the configuration of access rights"), Fig. 1 (depicting security module 20 as an empty box).

Appellant argues the "security module is best described as an electronic component that controls access for the configuration storage," Reply Br. 2. Appellant asserts the Examiner "ignores the detailed definition of the security module . . . recited in Applicant's claims." Appeal Br. 8; *see also id.* at 8 (reproducing the security module's recited function of "set[ting] at least one access right for the configuration storage" and the recited wherein clause that "the device is only operable if the at least one access right is set"); Reply Br. 2 (additionally reproducing two wherein clauses that recite limits on the device's permissible access right state transitions). Appellant contends "[t]hese limitations define the bounds of the security module, and additional mechanical definitions are not needed to circumscribe the invention." Reply Br. 2. Pointing to the same wherein clauses, Appellant further argues the claim recites the specific algorithm that the security module follows. Reply Br. 3.

Claims that recite performing particular functions and disclose only generic computers or processing elements as the structure amount to pure functional claiming. *Aristocrat Techs. Austl. Pty v. Int'l Game Tech.*, 521 F.3d 1328, 1333 (Fed. Cir. 2008). In such claims (i.e., claims that recite a generic computer or processor programmed to perform certain functions), "a particular algorithm may be the corresponding structure under § 112, sixth paragraph." *Ex Parte Rodriguez*, 92 U.S.P.Q.2d 1395, 1401–02 (BPAI Oct. 1, 2009) (precedential) (citing *Aristocrat*, 521 F.3d at 1333); *see also Harris Corp. v. Ericsson Inc.*, 417 F.3d 1241, 1249 (Fed. Cir. 2005) ("the corresponding structure for a § 112 ¶ 6 claim for a computer-implemented function is the algorithm disclosed in the specification").

As the expanded panel in *Rodriguez* noted, the presumption that 35 U.S.C. § 112(f) does not apply is overcome when the limitation in question is merely a nonce word or verbal construct used as a substitute for the term "means for"—i.e., when the limitation fails to convey the name of a particular structure capable of performing the recited function. *Rodriguez*, 92 U.S.P.Q.2d at 1404 (quoting *Lighting World, Inc. v. Birchwood Lighting, Inc.*, 382 F.3d 1354 (Fed. Cir. 2004)). We find no description of the term "security module" in any of Appellant's evidence or argument that would inform a person of ordinary skill in the art of a meaning of the term that includes particular structure for performing the recited function.

We also find the three wherein clauses fail to define structure for performing the *recited function*. The wherein clauses recite limitations on when the device is operable (i.e., "only . . . if the at least one access right is set") and access right state transitions that are allowed (i.e., between "a condition of access rights not being set" and "a condition of access enabled or access disabled) and not allowed (i.e., directly between "access rights enabled" and "access rights disabled"). *See* Appeal Br. 15.

As noted above, Appellant contends the three wherein clauses "define the bounds of the security module, and additional mechanical definitions are not needed to circumscribe the invention" and provide a specific algorithm that the security module follows. Reply Br. 2–3. We disagree. These limitations merely recite a characteristic of the device itself (that it "is only operable if the at least one access right is set") or controls on access right state transitions. For clarity, we emphasize that these limitations recite "*the device* is only operable if the at least one access right is set," "*the device* is arranged such that [certain] transition[s] . . . [are] shiftable," and "*the device* is arranged such that [certain other] direct transition[s] . . . [are] prohibited." Appeal Br. 15 (emphases added).

Appellant's argument implies that the security module controls these limitations on the device, but we disagree that the claim language requires the security module to enforce these requirements. Accordingly, the wherein clauses define how the device functions but do not provide structure (e.g., an algorithm) regarding the "security module." Moreover, we note Appellant asserts the wherein clauses "control[] access for the configuration storage." *See* Reply Br. 2. However, the function recited in the disputed means-plus-function limitation is "set[ting] at least one access right for accessing the configure storage." Thus, even to the extent we infer that the security module enforces these requirements, the wherein clauses do not provide an algorithm for the recited setting an access right function because they do not describe how the security module sets the rights.

Appellant also asserts that the Specification "describes in detail how the claimed elements work." Appeal Br. 9. To the extent the Specification provides support for the recited security module's structure, that relates to whether the means-plus-function limitations is definite and has sufficient written description support, not whether the claim recites a means-plus-function limitation.

The presumption against applying 35 U.S.C. § 112(f) is overcome because the claim merely "recites 'function without reciting sufficient structure for performing that function.'" *Williamson*, 792 F.3d at 1348 (quoting *Watts v. XL Sys., Inc.*, 232 F.3d 877, 880 (Fed. Cir. 2000)). Furthermore, the "security module" is properly construed as a means-plus-function limitation because neither the "security module" nor the rest of the claim recites limitations that would be "understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure" that is *capable of carrying out the recited function*. *Williamson*, 792 F.3d at 1348 (citing *Greenberg v. Ethicon Endo-Surgery, Inc.*, 91 F.3d 1580, 1583 (Fed. Cir. 1996)).

Because we agree with the Examiner that the system claims[5] invoke 35 U.S.C. § 112(f), we next address the Examiner's rejection of the claims as being indefinite and as lacking sufficient written description support.

REJECTION OF CLAIMS 1–7, 10, AND 16–20[6] UNDER 35 U.S.C § 112 ("SECURITY MODULE" MEANS)

The Examiner finds the Specification fails to describe sufficient structure to perform the recited function, such that a person of ordinary skill in the art would be unable to ascertain the proper scope of the means-plus-function limitation. Final Act. 7–8; Ans. 4–6. Therefore, the Examiner rejects claim 1 both as indefinite and as lacking sufficient written description support. Final Act. 4, 7–8; Ans. 4–6; *see* Manual of Patent Examining Procedure ("MPEP") § 2163(II)(A)(3)(a) (9th Ed., Rev. 10.2019, June 2020) ("when a means- (or step-) plus-function claim limitation is found to be

[5] The Examiner finds only the system claims invoke 35 U.S.C. § 112(f). However, we note independent claims 11 and 15 recite "*providing* a security module being arranged to assign at least one access right for accessing the configuration storage." Appeal Br. 17–18. Should this matter undergo further prosecution, we leave it to the Examiner to decide whether these claims also invoke 35 U.S.C. § 112(f).

[6] As explained in the previous footnote, the Examiner does not determine that the "security module" recited in claims 11–15 invokes 35 U.S.C. § 112(f) and, therefore, does not reject these claims for failing to provide written description support for the recited security module or as indefinite for failing to clearly define the scope of the recited security module.

indefinite based on failure of the specification to disclose sufficient corresponding structure, materials, or acts that perform the entire claimed function, then the claim limitation necessarily lacks an adequate written description").

As briefly mentioned above, Appellant asserts that the Specification "describes in detail how the claimed elements work." Appeal Br. 9. Appellant does not cite to any particular portion in the Specification that allegedly provides support for how the security module performs the recited function of setting or assigning "at least one access right for accessing the configuration storage." *See* Appeal Br. 9.

The Examiner notes that Appellant did not cite particular disclosures in the Specification and explains that the Specification's disclosure that "the security module may comprise further hardware or software components that allow the configuration of access rights" is broad enough to cover any possible hardware implementation and, therefore, is insufficient. Ans. 5 (quoting Spec. 4:19–21). We agree with the Examiner. Appellant has not identified anything in the Specification that sufficiently describes the security module's *structure* (e.g., an algorithm) capable of performing the *recited function.* Accordingly, we sustain the rejection of claims 1–7, 10, and 16–20, which recite the means-plus-function term "security module," under both 35 U.S.C. § 112(a) for failing to provide sufficient written description support and 35 U.S.C. § 112(b) as indefinite.

REJECTION OF CLAIMS 1–7 AND 10–20 UNDER 35 U.S.C § 112(B) (NUMBERED LABELS)

The Examiner rejects all claims as indefinite because the independent claims use numbered labels to describe permitted and prohibited access right state transitions and, moreover, reuses the same numbers in distinct limitations. Final Act. 8–9; Ans. 6–7. The Examiner finds the numbered states make the claims ambiguous and, "[b]ecause the claim fails to sufficiently relate the cited phrase to the other claim features, the claim is amenable [to] multiple plausible constructions." Final Act. 8; Ans. 6. We understand the Examiner's rejection to find that because the claims use the same numbered label to refer to different states, it would confuse a person of ordinary skill as to whether each state labeled "(1)" is in a single group and, therefore, renders the claim scope unclear. *See* Final Act. 8; Ans. 6–7.

Appellant argues the claims would be clear without the numbered labels, but the numbered labels were added to distinguish between states *within* each wherein clause. Appeal Br. 10. Appellant argues the numbered labels for the states therefore provide clarity rather than ambiguity because it is clear that the numbered states *between* wherein clauses are not related. Appeal Br. 10; Reply Br. 3.

We agree with Appellant. Although Appellant could just as easily have used different numbered states in each of the two wherein clauses, we disagree with the Examiner that a person of ordinary skill in the art would not have been able to ascertain the scope of the claim due to the numbered labels for the different states. As Appellant argues, we find the labels clearly indicate that: (1) in the first of the two wherein clauses including the numbered labels, there are two states or sets of states (i.e., a first state in which access rights have not been set and a second set of states in which either access is enabled or access is disabled) between which transitions are permitted and (2) in the second of the two wherein clauses including the numbered labels, there are two states (i.e., a first state in which access is enabled and a second state in which access is disabled) between which a direct transition is prohibited. Therefore, we do not sustain this rejection.

REJECTION OF CLAIMS 1–7, 10, AND 16–20 UNDER 35 U.S.C. § 103

The Examiner rejects claims 1–7, 10, and 16–20 as obvious in view of Wood, Onno, and Dinker. Final Act. 9–16. Of particular relevance, the Examiner finds Onno and Dinker teach or suggest the recited limitations on permissible and prohibited access right state transitions. Final Act. 10–11 (citing Onno, Figs. 5, 6; Dinker, Fig. 8); Ans. 7–8. With respect to claim 1's recited limitation that "the device is arranged such that a transition from (1) a condition of access rights not being set, to (2) a condition of access enabled or access disabled, and vice versa, is shiftable," the Examiner finds "the states presented in Fig[ures] 5 and 6 could easily be combined to arrive [at the] 3 states presented in the claims." Ans. 7.

Figure 5, which "illustrates a state diagram of the system according to a preferred embodiment of the invention," is reproduced below:

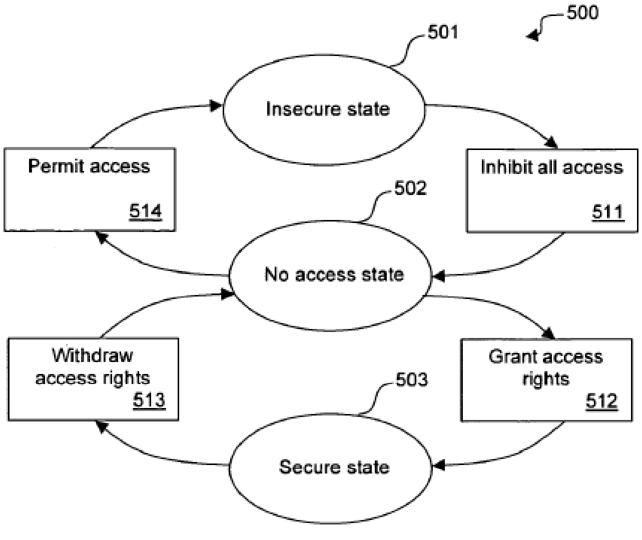

Figure 5

Onno, Fig. 5 (depicting a state diagram relating to an administrator setting access rights to device services); *see* Onno ¶ 82.

Figure 6, which "illustrates a service access state diagram according to a preferred embodiment of the invention," is reproduced below:

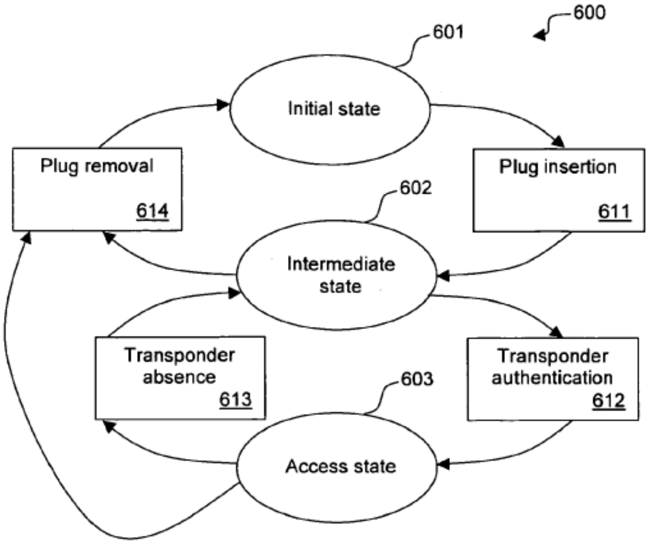

Figure 6

Onno, Fig. 6 (depicting a state diagram relating to users accessing device services); *see* Onno ¶ 85.

The Examiner finds a person of ordinary skill in the art could replace Figure 6's "Intermediate state" with Figure 5's "No access state." Ans. 8. The Examiner finds Dinker is relied on only to teach that direct state transitions between access enabled (i.e., Dinker's write-lock state that enables writing to storage) and access disabled (i.e., Dinker's state without a write lock that disables writing to storage) is not allowed. Ans. 8 (citing Dinker, Fig. 8). The Examiner makes similar findings and conclusions with respect to independent claims 11 and 15, which recite commensurate limitations.

Among other arguments, Appellant asserts Onno does not include the three claimed states (i.e., "access rights not being set," "access enabled," and "access disabled"). Appeal Br. 12. Appellant argues the rejection does not clearly indicate which particular state from Onno's Figures allegedly teaches each of the three claimed states. Appeal Br. 12; Reply Br. 5. Appellant also argues Onno's "Initial state" in Figure 6 is the same state as Onno's "Secure state" in Figure 5 and Onno's "Intermediate state" and "Access state" in Figure 6 "are merely states within the secure state of Figure 5." Appeal Br. 12 (citing Onno ¶ 85, Figs. 5, 6). Appellant further argues that, not only is the Examiner's proposed combination of the states from Figures 5 and 6 based on hindsight, Onno's disclosure that the Figure 6 "Initial state" is the same as the Figure 5 "Secure state" teaches that the states are not interchangeable because the states have a particular arrangement for specific purposes. Reply Br. 4 (citing Onno ¶¶ 82, 85).

Onno generally relates to controlling access to a portable device by requiring a plug to be inserted into a port and a transponder to remain close to the person. Onno, Abstract; *see* Onno ¶ 16. More specifically, Onno includes an access manager that provides access to device services (e.g., "use of the disk drive, use of a digital interface (such as for example a USB interface, a WIFI® card or a Bluetooth® adapter card), access to a certain programme, or combinations thereof") only when certain conditions are met—a plug is inserted into the device, a transponder is in the presence of the plug, and the plug and transponder are authorized to access the service. Onno ¶¶ 16, 82; *see* Onno ¶¶ 44–48 (describing embodiments of devices with plug interfaces, plugs, and transponders), 49–50 (describing what it means for a transponder to be "in the presence of a plug"), 69–72 (describing an embodiment of a security apparatus including a plug and transponder).

Different users may have access to different services on the same device and the same user may have access to different services on different devices. Onno ¶ 43. Onno's access manager identifies relationships between devices, device services, plugs, and transponders in order to assign access rights. Onno ¶ 51; *see* Onno ¶¶ 52–68 (describing how an access manager may identify relationships and how the various elements interact to grant or deny access to devices or device services). When a user attempts to access a device or device service, the system evaluates restrictions for the requested device or service and, depending on the restrictions, evaluates the presence of any necessary plug and transponder. Onno ¶¶ 77–81.

Onno enforces these access rights by restricting certain access right state transitions. Initially, the device is in an "insecure state" with no security, at which point an administrator can restrict access rights to the device or parts of the device or its services, which puts the device into a "no access state." Onno ¶ 82. From the "no access state," the administrator can either return the device to the "insecure state" or grant access rights to particular users (i.e., plugs and transponders associated with users) to put the device into a "secure state" in which only users who have been granted access to services can access those services. Onno ¶ 83. If the administrator withdraws all granted access, the device returns to the "no access state." Onno ¶ 84.

Once in the "secure state" (alternatively referred to as the "initial state"), a user accesses services for which they have been granted access rights by first inserting their plug into the device, placing the device into an "intermediate state." Onno ¶ 85. Once in the "intermediate state," if the transponder is present, the plug authenticates the transponder and grants access to the authorized services, which places the device into an "access state." Onno ¶ 85. When in either the "intermediate state" or the "access state," the device returns to the "initial state" if the plug is removed. Onno ¶ 85. If the transponder loses its connection to the plug while the device is in the "access state," the device returns to the "intermediate state." Onno ¶ 85.

Appellant is correct that Onno explicitly equates Figure 5's "secure state" to Figure 6's "initial state." *See* Onno ¶ 85. Thus, we agree with Appellant that substituting Figure 5's "no access state" in place of Figure 6's "intermediate state" is inconsistent with Onno's teachings. Furthermore, the Examiner fails to provide an explanation supported by the record that indicates Onno would have suggested to a person of ordinary skill in the art that *any* of the states in Figures 5 and 6 could be substituted for any other state. Onno teaches particular transitions from one state to another in Figures 5 and 6, and Figure 6's intermediate and access states may only be reached *after* the device is in the "initial state," which corresponds to Figure 5's "secure state." *See* Onno ¶¶ 82–85.

For the above reasons, we disagree with the Examiner's finding that Onno's various states are interchangeable. Accordingly, the rejection of independent claim 1 is based on faulty factual findings and, constrained by this record, we cannot sustain the rejection of claim 1. For the same reasons, we cannot sustain the rejection of independent claim 11 and 15, which recite commensurate limitations or claims 2–7, 10, 12–14, and 16–20, which depend ultimately from one of claims 1 and 11 and, therefore, incorporate the limitations of those independent claims.

NEW GROUND OF REJECTION UNDER 35 U.S.C. § 103

We enter a new ground of rejection pursuant to our authority under 37 C.F.R. § 41.50(b). In particular, we newly reject independent claims 1, 11, and 15 under 35 U.S.C. § 103 as obvious in view of Wood and Onno.

We agree with and adopt the Examiner's findings with respect to Wood's teaching. *See* Final Act. 9–10 (citing Wood ¶¶ 25–27, 32–36, 41–44, Figs. 3, 4). As discussed above, the findings with respect to the last two wherein clauses (i.e., the clauses that identify allowable and prohibited state transitions) are problematic. However, for the reasons explained below, we find Onno teaches these limitations.

As discussed above, Onno explicitly describes the state transitions that a device allows to grant a user access to device services. *See* Onno ¶¶ 82–85. In light of Onno's purpose of securing access to a device and its services, a person of ordinary skill in the art would have understood that Onno's explicitly disclosed allowable state transitions teaches, or at least suggests, prohibiting other transitions.

We discussed the state transitions above in detail. We find Onno's "No access state" teaches or suggests the recited "condition of access rights not being set" because Onno discloses that the "No access state" is a state in which no users have access to the device or its services because the administrator has not yet set access rights for any users (or has revoked previously granted user access). *See* Onno ¶¶ 82–83. We find Onno's "Insecure state" teaches or suggests the recited "access enabled state" because Onno discloses that in the "Insecure state" "there is no security," which allows access by anyone to the device and its services. Onno ¶ 82. Finally, we find Onno's "Secure state" teaches or suggests the recited "access disabled" state because Onno discloses that in the "Secure state" access is disabled for anyone other than user to whom the administrator explicitly granted access. Onno ¶ 83.

We also find Onno teaches the particularly recited permitted and prohibited state transitions. Here, we include Onno's Figure 5 annotated to indicate the states that we find correspond to Appellant's claimed states. Specifically, we find Onno's "Insecure state" teaches or suggests the recited "access enabled" state, Onno's "No access state" teaches or suggests the recited state or "condition of access rights not being set," and Onno's "Secure state" teaches or suggests the recited "access disabled state. *See* Onno ¶¶ 82–84, Fig. 5. An annotated version of Onno's Figure 5 depicts a state diagram of Onno's system (with our annotated text in brackets directly below Onno's corresponding state), and is reproduced below:

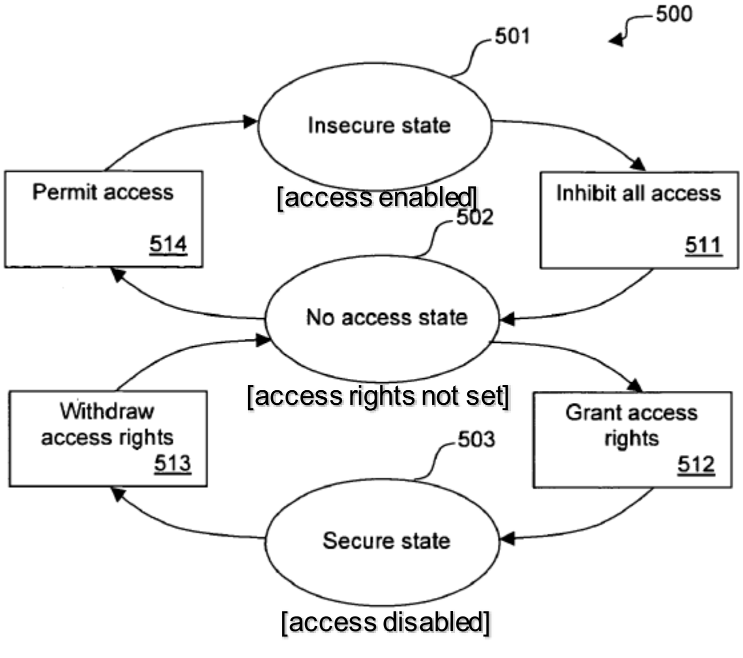

Figure 5

Figure 5 illustrates a state diagram including three states—"Insecure state" 501, "No access state" 502, and "Secure state" 503. Onno ¶ 39; *see* Onno ¶¶ 82–84.

As seen in our annotated version of Onno's Figure 5, "a transition from (1) a condition of access rights not being set [(mapped to Onno's 'No access state')], to (2) a condition of access enabled [(mapped to Onno's 'Insecure state')] or access disabled [(mapped to Onno's 'Secure state')], and vice versa, is shiftable," as recited in claim 1. Furthermore, "a direct transition from (1) the condition of access rights enabled [(mapped to Onno's 'Insecure state')], to (2) access rights disabled [(mapped to Onno's 'Secure state')], and vice versa, is prohibited." We adopt the Examiner's rationale that it would have been obvious to apply Onno's known system and states for granting access to a device or its services to Wood's known device and method for securing a portion of a device to yield predictable results. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007) ("The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.").

For the reasons discussed above, we reject independent claim 1 as obvious under 35 U.S.C. § 103 in view of Wood and Onno. For the same reasons, we reject independent claims 11 and 15, which recite limitations having similar scope, as obvious under 35 U.S.C. § 103 in view of Wood and Onno. The Patent Trial and Appeal Board is a review body rather than a place of initial examination. We have made a new rejection regarding independent claims 1, 11, and 15 under 35 U.S.C. § 103, pursuant to 37 C.F.R. § 41.50(b). However, we have not reviewed the remaining claims to the extent necessary to determine whether these claims are unpatentable over this combination or any other combination not before us. We leave it to the Examiner to ascertain the appropriateness of any further rejections based on these or other references. Our decision not to enter a new ground of rejection for all claims, however, should not be considered as an indication regarding the appropriateness of further rejection or allowance of the non-rejected claims. *See* MPEP § 1213.02.

DECISION SUMMARY

Claims Rejected	**35 U.S.C. §**	**Basis/References**	**Affirmed**	**Reversed**	**New Ground**
1–7, 10, 16–20	112(a)	Written Description	1–7, 10, 16–20		
1–7, 10–20	112(b)	Indefinite	1–7, 10, 16–20	11–15	
1–7, 10–20	103	Wood, Onno, Dinker		1–7, 10–20	
1, 11, 15	103	Wood, Onno			1, 11, 15
Overall Outcome			1–7, 10, 16–20	11–15	1, 11, 15

TIME PERIOD FOR RESPONSE

This decision contains a new ground of rejection pursuant to 37 C.F.R. § 41.50(b). Section 41.50(b) provides "[a] new ground of rejection pursuant to this paragraph shall not be considered final for judicial review." Section 41.50(b) also provides:

> When the Board enters such a non-final decision, the appellant, within two months from the date of the decision, must exercise one of the following two options with respect to the new ground of rejection to avoid termination of the appeal as to the rejected claims:
>
> (1) *Reopen prosecution.* Submit an appropriate amendment of the claims so rejected or new Evidence relating to the claims so rejected, or both, and have the matter reconsidered

> by the examiner, in which event the prosecution will be remanded to the examiner. The new ground of rejection is binding upon the examiner unless an amendment or new Evidence not previously of Record is made which, in the opinion of the examiner, overcomes the new ground of rejection designated in the decision. Should the examiner reject the claims, Appellant may again appeal to the Board pursuant to this subpart.
>
> (2) *Request rehearing*. Request that the proceeding be reheard under § 41.52 by the Board upon the same Record. The request for rehearing must address any new ground of rejection and state with particularity the points believed to have been misapprehended or overlooked in entering the new ground of rejection and also state all other grounds upon which rehearing is sought.

Further guidance on responding to a new ground of rejection can be found in the Manual of Patent Examining Procedure § 1214.01.

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

AFFIRMED IN PART; 37 C.F.R. § 41.50(b)