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.
15/085,869	03/30/2016	Josh Powers	15-063	6243

63023 7590 09/22/2020

Schweitzer Engineering Laboratories, Inc.
Law Department
2350 NE HOPKINS COURT
PULLMAN, WA 99163-5603

EXAMINER
LE, THANH T

ART UNIT	PAPER NUMBER
2495	

NOTIFICATION DATE	DELIVERY MODE
09/22/2020	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):

IPMail@selinc.com
Rick_Edge@selinc.com
rosemary_fitzgerald@selinc.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte JOSH POWERS, TRISTAN LLOYD MULLIS, JASON A. DEARIEN, MICHAEL DYLAN CONE, COBY SOSS, and BARRY JAKOB GRUSSLING[1]

Appeal 2019-003106
Application 15/085,869
Technology Center 2400

Before JASON V. MORGAN, DEBORAH KATZ, and JOHN A. EVANS, *Administrative Patent Judges*.

EVANS, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

This is a decision on appeal under 35 U.S.C. § 134(a) from the Examiner's Final Rejection of Claims 1–6, 10–17, and 21–26. Appeal Br. 2. We have jurisdiction over the pending claims under 35 U.S.C. § 6(b).

We REVERSE.

---

[1] We use the word "Appellant" to refer to "applicants" as defined in 37 C.F.R. § 1.42(a). The Appeal Brief identifies Schweitzer Engineering Laboratories, Inc., as the real party in interest. Appeal Br. 2.

INVENTION

The invention is directed to systems and methods for establishing trust relationships between a software defined network (SDN) controller and a SDN communication device. *See* Abstract. Claims 1 and 11 are independent. Illustrative claim 1 is reproduced below.

> 1. A software defined network (SDN) controller, the SDN controller comprising:
>
> a communications interface configured to communicate with a plurality of SDN network devices;
>
> a memory;
>
> a processor operatively coupled to the memory, wherein the processor is configured to execute instructions stored on the memory to cause the processor to:
>
> detect a new device associated with the SDN based on receipt of an initial certificate indicating that the new device is in a factory configured state;
>
> receive a user approval to commission the new device;
>
> establish a first SDN controller trusted credential;
>
> transmit a first device trusted credential based on the first SDN controller credential to the new device;
>
> issue programming instructions to the new device authenticated using the first SDN controller trusted credential; and
>
> remove the initial certificate from the new device upon receiving the user approval to commission the new device onto the SDN to require a factory

reset to recommission the new device to a different SDN controller.

PRIOR ART

Name[2]	Reference	Date
Krywaniuk	US 2007/0217344 A1	Sep. 20, 2007
Giniger	US 8,520,670 B1	Aug. 27, 2013
Ramatchandirane	US 2017/0026187 A1	Jan. 26, 2017[3]
Vidyapoornachary	US 9,760,504 B2	Sep. 12, 2017[4]

REJECTIONS[5] AT ISSUE[6]

1. Claims 1–5, 10–15, and 21–26 stand rejected under 35 U.S.C. 103 as obvious over Ramatchandirane, Krywaniuk, and Vidyapoornachary. Final Act. 3–8.
2. Claims 6, 16, and 17 stand rejected under 35 U.S.C. 103 as obvious over Ramatchandirane, Krywaniuk, Vidyapoornachary, and Giniger. Final Act. 8–10.

---

[2] All citations herein to the references are by reference to the first named inventor/author only.

[3] Filed September 11, 2015.

[4] Filed September 29, 2015.

[5] The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA. Final Act 2.

[6] Throughout this Decision, we refer to the Appeal Brief ("Appeal Br.") filed November 19, 2018, the Reply Brief ("Reply Br.") filed March 7, 2019, the Final Office Action ("Final Act.") mailed June 11, 2018, the Examiner's Answer mailed January 24, 2019, and the Specification ("Spec.") filed March 30, 2016.

ANALYSIS

We have reviewed the rejections of Claims 1–6, 10–17, and 21–26 in light of Appellant's arguments that the Examiner erred. Appellant's arguments have persuaded us the Examiner erred.

CLAIMS 1–5, 10–15, AND 21–26: OBVIOUSNESS OVER RAMATCHANDIRANE, KRYWANIUK, AND VIDYAPOORNACHARY.

User approval to commission the new device onto the SDN to require a factory reset.

Claim 1 recites, *inter alia*, "remove the initial certificate from the new device upon receiving the user approval to commission the new device onto the SDN to require a factory reset to recommission the new device to a different SDN controller." Independent Claim 11 contains commensurate recitations.

The Examiner finds: "Ramatchandirane and Krywaniuk do not explicitly disclose the initial certificate indicating that the new device is in a factory configured state and removing the initial certificate from the new device to require a factory reset to commission the new device to a different SDN controller." Final Act. 5. The Examiner finds, however, this teaching is known in the art and cites Vidyapoornachary's teaching as an example:

> The key stored on the memory device may initially be set to a factory reset state such as, for example, all zero. The memory controller may be configured to use the factory reset state key until new key generation is initiated. In some embodiments, the memory controller may be configured to reset the key to its

> factory reset state. This may allow the memory device to be transferred to another system.

Id. (quoting Vidyapoornachary, col. 2, ll. 48–54).

Appellant contends "Ramatchandirane is directed to authenticating a device without user intervention using a unique client identifier, a server security certificate, and a manufacturer security certificate." Appeal Br. 6 (citing Ramatchandirane, FIG. 7, ¶ 2). Appellant further acknowledges the Examiner relies on Vidyapoornachary to teach removing the initial certificate from the new device upon such user approval to require a factory reset to recommission the new device to a different SDN controller. Appeal Br. 7.

Appellant contends "[t]here does not appear to be any further explanation of resetting the key to the factory reset state other than that it *may occur*." *Id.* Appellant argues that to generate a new key, Vidyapoornachary discloses:

> A timer may be configured to trigger the periodic generation of a new key. The timer may be initiated in several ways. In some embodiments, the memory device may be configured to automatically start the timer after access to the nonvolatile memory is unlocked. In some embodiments, the memory controller is configured to send a key update enable command to the memory device to initiate the timer after unlocking access to the memory.

Appeal Br. 7 (quoting Vidyapoornachary, col. 3, ll. 4–16). Appellant argues none of these references appear to teach removing the initial certificate from the new device upon receiving the user approval to commission the new device onto the SDN to require a factory reset to recommission the new device to a different SDN controller, as claimed. *Id.*

The Examiner's Answer repeats the Final Action findings. *See* Ans. 4–5.

We agree with Appellant that Vidyapoornachary fails to teach removing the initial certificate from the new device upon receiving the user approval to commission the new device onto the SDN to require a factory reset to recommission the new device to a different SDN controller, as claimed. Vidyapoornachary teaches removing the certificate in response to a timer, but not in response to a user approval. The Examiner finds Krywaniuk user approval to provision a device. Ans. 4 (quoting Krywaniuk, ¶ 58) ("after the connection has been established, the administrator can verify, either manually or automatically, the unique identifier of the managed device."). We disagree, the cited portion of Krywaniuk discloses an administrator may verify the device identifier, but is silent regarding he administrator approving the removal of the certificate.

CLAIMS 6, 16, AND 17: OBVIOUSNESS OVER RAMATCHANDIRANE, KRYWANIUK, VIDYAPOORNACHARY, AND GINIGER.

Appellant does not separately argue Claims 6, 16, or 17, but asserts their patentability as dependent from either independent Claim 1 or 11. Appeal Br. 16.

The Examiner stands by the findings for independent Claims 1 and 11. Ans. 9.

In view of the foregoing, we decline to sustain the rejection of Claims 6, 16, or 17 under 35 U.S.C. 103 over Ramatchandirane, Krywaniuk, Vidyapoornachary, and Giniger.

CONCLUSION

In summary:

Claims Rejected	35 U.S.C. §	References	Affirmed	Reversed
1–5, 10–15, 21–26	103	Ramatchandirane, Krywaniuk, Vidyapoornachary		1–5, 10–15, 21–26
6, 16, 17		Ramatchandirane Krywaniuk, Vidyapoornachary Giniger		6, 16, 17
Overall				**1–6, 10–17, 21–26**

REVERSED