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.
13/787,510	03/06/2013	Philip HAWKES	122551 (1059592)	2367

15093 7590 09/23/2019

Kilpatrick Townsend & Stockton/Qualcomm
Mailstop: IP Docketing - 22
1100 Peachtree Street
Suite 2800
Atlanta, GA 30309

EXAMINER	
TENG, LOUIS C	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
09/23/2019	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):

ipefiling@kilpatricktownsend.com
ocpat_uspto@qualcomm.com
qcominst@kilpatricktownsend.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte PHILIP HAWKES, OLIVIER JEAN BENOIT, and ANAND PALANIGOUNDER

Appeal 2018-008873
Application 13/787,510
Technology Center 2400

Before JOHN A. EVANS, MATTHEW J. McNEILL, and JASON M. REPKO, *Administrative Patent Judges*.

EVANS, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant[1] seeks our review under 35 U.S.C. § 134(a) of the Examiner's Final Rejection of all pending claims, i.e., Claims 1–11, 13, 15–27, 29, 31–43, 45, 47–59, 61, and 63–72. App. Br. 2. We have jurisdiction under 35 U.S.C. § 6(b).

[1] We refer collectively to the inventors as "Appellant." The Appeal Brief identifies Qualcomm Incorporated, as the real party in interest. App. Br. 2.

We REVERSE.[2]

STATEMENT OF THE CASE

The claims relate to a method for configuring an internal entity of a WiFi-enabled remote station with a certificate. *See* Abstract.

INVENTION

Claims 1, 17, 33, and 49 are independent. An understanding of the invention can be derived from a reading of illustrative Claim 1, which is reproduced below with some formatting added:

> 1. A method for configuring an application-layer internal entity of a WiFi-enabled remote station with an internal-entity certificate, comprising:
>
> receiving, by the remote station, the internal-entity certificate and a registrar certificate in at least one WiFi message from a registrar smartphone acting as a root-of-trust certificate authority for the application-layer internal entity, wherein the registrar certificate is self-signed by the registrar smartphone;
>
> providing, by the remote station, the internal-entity certificate and the registrar certificate to the application-layer internal entity; and

[2] Rather than reiterate the arguments of Appellant and the Examiner, we refer to the Appeal Brief (filed April 16, 2018, "App. Br."), the Reply Brief (filed September 14, 2018, "Reply Br."), the Examiner's Answer (mailed July 25, 2018, "Ans."), the Final Action (mailed October 18, 2017, "Final Act."), and the Specification (filed October 15, 2014, "Spec.") for their respective details.

securely communicating, by the application-layer internal entity, with an external entity based on the internal-entity certificate and the registrar certificate.

References and Rejections

Yeager	US 2005/0086300 A1	Apr. 21, 2005
Aull	US 7,475,250 B2	Jan. 6, 2009
Averbuch	US 8,724,515 B2	Filed Sep. 16, 2011

Wi-Fi Alliance, Wi-Fi Protected Setup Specification ["WPS"], Version 1.0h, Dec. 2006, https://www.wi-fi.org/.

Ken Holbrook, ed., Smart Energy Profile version 2.0 Technical Requirements Document, ZigBee Alliance and HomePlug Powerline Alliance, Feb. 3, 2012.

The Claims stand rejected as follows:

1. Claims 1, 5–11, 13, 16, 17, 21–27, 29, 32, 33, 37–43, 45, 48, 49, 53–59, 61, and 64–72 stand rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over WPS, Holbrook, and Averbuch. Final Act. 5–12.
2. Claims 2–4, 18–20, 34–36, and 50–52 stand rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over WPS, Holbrook, Averbuch, and Aull. Final Act. 12–14.
3. Claims 15, 31, 47, and 63 stand rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over WPS, Holbrook, Averbuch, and Yeager. Final Act. 14–15.

ANALYSIS

We have reviewed the rejections of Claims 1–11, 13, 15–27, 29, 31–43, 45, 47–59, 61, and 63–72 in light of Appellant's arguments that the Examiner erred. We consider Appellant's arguments as they are presented in the Appeal Brief, pages 7–23.

INDEPENDENT CLAIMS 1, 17, 33, AND 49: OBVIOUSNESS OVER WPS, HOLBROOK, AND AVERBUCH

Appellant argues the independent claims as a group and designates Claim 1 as representative. *See* App. Br. 5–6. Moreover, the Examiner's Answer applies the findings regarding Claim 1 to all pending claims. Ans. 4, 6. Therefore, we decide the appeal on the basis of representative Claim 1, and refer to the rejected claims collectively herein as "the claims." *See* 37 C.F.R. § 41.37(c)(1)(iv); *In re King*, 801 F.2d 1324, 1325 (Fed. Cir. 1986).

Independent Claim 1 recites, *inter alia*, "receiving, by the remote station, the internal-entity certificate and a registrar certificate in at least one WiFi message from a registrar smartphone acting as a root-of-trust certificate authority for the application-layer internal entity." Appellant argues, and we agree, that independent Claims 17, 33, and 49 contain commensurate recitations.

The Examiner finds the WPS reference teaches the basic system architecture, as claimed, including a method for configuring an internal entity of a WiFi-enabled remote station with an internal-entity certificate. Final Act. 5. But the Examiner finds WPS does not teach:

- the registrar smartphone acting as a root-of-trust certificate authority for the application-layer internal entity;
- the remote station receiving the internal-entity certificate and a registrar certificate in at least one message, wherein the registrar certificate is self-signed by the registrar smartphone;
- the remote station providing the internal-entity certificate and the registrar certificate to the internal entity; and
- the internal entity securely communicating with an external entity based on the internal-entity certificate and the registrar certificate. *Id.* 6.

The Examiner finds Holbrook teaches an application-layer X.509 certificate being used for SEP2 servers and client entities which are examples of application-layer internal entities. *Id.* The Examiner then finds it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of WPS to incorporate the teachings of Holbrook by using the WPS specifications for implementing certificate provisioning of SEP2 entities. Final Act. 7.

Appellant contends Holbrook fails to teach providing certificates to the application-layer internal entity. App. Br. 7. Appellant quotes Holbrook as disclosing: "[t]he single credential mechanism for SE[P] 2.0 Device Authentication SHALL be comprised of signed X.509 Certificates as stated in the requirement below. *We are limiting our credentials to* ***Devices*** *defined by this standard*, and are not defining credentials for other actors to the system, like users at user-interfaces." *Id.* (quoting Holbrook, 87, ll.

3042–3044). According to Appellant, Holbrook defines "Device" as "[a] single **physical unit** with one or more network interfaces capable of performing one or multiple functions as part of an SEP 2.0 Network application (e.g., Meter, In-Premises Display)." *Id.* (quoting Holbrook, 26, ll. 780–783). Appellant argues Holbrook defines three types of entities: Physical Unit, Network Node, and Application Device. *Id.* (quoting Holbrook, 91, ll. 3155–3159) ("An Application Device resides on a Physical Unit and performs an application level function.") *Id.* (quoting Holbrook, 91, ll. 3166–3167). Based on this disclosure, Appellant argues Holbrook expressly limits the use of X.509 certificates to "Devices" i.e., physical units, rather than "Application Devices." *Id.*

The Examiner finds because an Application Device is defined as part of a Device, limiting the credentials to Devices, as opposed to other actors to the system, in the context of Holbrook does not necessarily preclude Application Devices. Ans. 4. The Examiner finds Holbrook teaches Application Devices use credentials of section 12.9 for a Transport Layer Security (TLS) protocol to establish secure connections with other Application Devices. *Id.* (citing App. Br. 8). The Examiner finds Holbrook teaches each Application Device must have a unique identity, interoperate in a wide inter-network, and be governed by authentication and authorization rules. *Id.* (citing App. Br. 7). The Examiner finds one of ordinary skill in the art would recognize, the credentials that Holbrook refers to are in fact

TLS X.509 certificates. *Id.* (citing TLS Protocol Version 1.2, RFC 5246, 56).[3]

Appellant contends the Examiner finds the use of X.509 certificates are inherent to the TLS protocol. Reply Br. 2. But contrary to the Examiner, Appellant contends the TLS RFC does not require using certificates, but makes their use entirely optional because the server does not have to request a certificate from the client. *Id.* (citing RFC, 36) ("* Indicates optional or situation-dependent messages that are not always sent."). Moreover, Appellant argues whether certificates are requested depends on the selected cipher suite. *Id.* (citing RFC, 53) ("A non-anonymous server can optionally request a certificate from the client, if appropriate for the selected cipher suite"). Additionally Appellant argues, even when a certificate is requested, it is possible to negotiate for a certificate other than a type X.509. *Id.* (citing RFC, 56) ("[t]he certificate MUST be appropriate for the negotiated cipher suite's key exchange algorithm, and any negotiated extensions. In particular . . . The certificate type MUST be X.509v3, unless explicitly negotiated otherwise (e.g., [TLSPGP])").

In addition to arguing the use of X.509 certificates is not inherent, Appellant argues Holbrook teaches away from using X.509 certificates in connection with TLS because they "tend to be verbose and large in size." Reply Br. 3 (citing Holbrook, 107, ll. 3648–3650). Appellant argues

[3] We follow Appellant's convention in referring to the document as "RFC."

Holbrook contemplates alternative certificates that are not supported by X.509. *Id.* (citing Holbrook, 107, ll. 3650–3652).

We find, in agreement with Appellant, that Holbrook's discussion of certificates was limited to a Physical Unit (not an Application Device), and even in the context of Application Devices, Holbrook teaches away from the use of X.509 certificates.

Because we find the cited art fails to teach at least one claimed limitation, we decline to sustain the rejections of Claims 1–11, 13, 15–27, 29, 31–43, 45, 47–59, 61, and 63–72 under 35 U.S.C. § 103.

DECISION

The rejections of Claims 1–11, 13, 15–27, 29, 31–43, 45, 47–59, 61, and 63–72 under 35 U.S.C. § 103 are REVERSED.

Claims Rejected	Basis	Affirmed	Reversed
1, 5–11, 13, 16, 17, 21–27, 29, 32, 33, 37–43, 45, 48, 49, 53–59, 61, and 64–72	§ 103(a) as being unpatentable over WPS, Holbrook, and Averbuch		1, 5–11, 13, 16, 17, 21–27, 29, 32, 33, 37–43, 45, 48, 49, 53–59, 61, and 64–72
2–4, 18–20, 34–36, and 50–52	§ 103(a) as being unpatentable over WPS, Holbrook, Averbuch, and Aull		2–4, 18–20, 34–36, and 50–52
15, 31, 47, and 63	§ 103(a) as being unpatentable over WPS, Holbrook,		15, 31, 47, and 63

Claims Rejected	Basis	Affirmed	Reversed
	Averbuch, and Yeager		
Overall Outcome			1–11, 13, 15–27, 29, 31–43, 45, 47–59, 61, and 63–72

REVERSED