Trials@uspto.gov
571-272-7822

Paper 10
Date: August 31, 2021

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TCL INDUSTRIES HOLDINGS CO., LTD.,
Petitioner,

v.

KONINKLIJKE PHILIPS N.V.,
Patent Owner.

IPR2021-00547
Patent 9,590,977 B2

Before KEVIN F. TURNER, STACEY G. WHITE, and RUSSELL E. CASS, *Administrative Patent Judges.*

CASS, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background

TCL Industries Holdings Co., Ltd. ("Petitioner") filed a Petition requesting an *inter partes* review of claims 22–31 (the "challenged claims") of U.S. Patent No. 9,590,977 B2 (Ex. 1001, "the '977 patent"). Paper 1 ("Pet."). Koninklijke Philips N.V. ("Patent Owner") filed a Preliminary Response. Paper 7 ("Prelim. Resp.").

We have authority to determine whether to institute an *inter partes* review under 35 U.S.C. § 314 and 37 C.F.R. § 42.4. An *inter partes* review may not be instituted unless it is determined that "the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314 (2018); *see also* 37 C.F.R § 42.4(a) (2020) ("The Board institutes the trial on behalf of the Director."). The reasonable likelihood standard is "a higher standard than mere notice pleading," but "lower than the 'preponderance' standard to prevail in a final written decision." *Hulu, LLC v. Sound View Innovations, LLC*, IPR2018-01039, Paper 29 at 13 (PTAB Dec. 20, 2019) (precedential) (footnote omitted).

For the reasons provided below and based on the record before us, we determine Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing the unpatentability of at least one of the challenged claims. Accordingly, we do not institute an *inter partes* review.

B. Real Parties in Interest

Petitioner states that the "real parties in interest for this IPR are TCL Industries Holdings Co., Ltd., TCL Electronics Holdings Ltd., TCL King

Electrical Appliances (Huizhou) Co. Ltd., TTE Technology, Inc., TCL Moka International Ltd., TCL Moka Manufacturing S.A. de C.V., TCL Smart Device (Vietnam) Company Ltd., TCL Industries Holdings (Hong Kong) Co. Ltd., TTE Corporation, TCL Holdings (BVI) Limited, Shenzhen TCL New Technology Co., Ltd., and TCL Technology Group Corporation." Pet. 2. Patent Owner states that "[t]he real parties-in-interest are Koninklijke Philips N.V. and Philips North America LLC." Paper 5 (Patent Owner's Mandatory Notices), 2.

C. Related Proceedings

Petitioner states that Patent Owner has asserted the '977 patent and two other patents assigned to Patent Owner (U.S. Patent Nos. 10,298,564 (the "'564 patent") and 7,052,152 (the "'152 patent")) against TTE Technology in the United States District Court for the Central District of California in Case No. 2:20-cv-01406. Pet. 2. Petitioner further states that this district court case has been stayed due to a later filed ITC action, *In the Matter of Certain Digital Video-Capable Devices and Components Thereof*, Investigation No. 337-TA-1224. *Id.* at 2–3, 4. Petitioner also identifies other district court litigation proceedings in which Philips has filed complaints alleging infringement of the '977 patent. *Id.* at 3–4.

Petitioner has also challenged the '977 patent in two additional *inter partes* review proceedings: IPR2021-00495 and IPR2021-00496. IPR2021-00495, Paper 3; IPR2021-00496, Paper 1. Petitioner also has challenged the '564 patent in IPR2021-00497. IPR2021-00497, Paper 1.

D. The '977 Patent (Ex. 1001)

The '977 patent relates to a system for communicating secure content from a first communication device to a second communication device by

using a commonly-shared secret to perform a distance measurement between the first and second communication devices. Ex. 1001, code (57). The '977 patent explains that this system allows a user to watch a movie the user owns on a neighbor's television screen if the user (or a device that the user owns) is near the neighbor's television screen, but prevents the movie from being played from a transmitting device at a remote location (for example over the Internet). *Id.* at 2:12–25.

An overview of the steps performed by the first communication device and second communication device is shown in Figure 2, reproduced below.

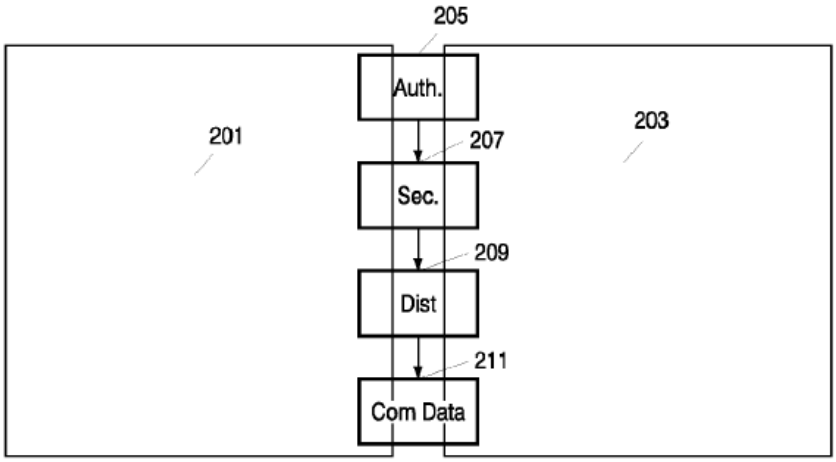


FIG. 2

As shown in Figure 2, first device 201 has content that second device 203 has requested. Ex. 1001, 5:20–25. In step 205, first device 201 authenticates second device 203, for example, by checking whether device 203 is a compliant device and really is the device identified to the first device. *Id.* at 5:26–31. Then, in step 207, first device 201 exchanges a secret with second device 203, such as a randomly generated bit word, which may be carried out using a key management protocol. *Id.* at 5:31–36.

Then, in step 209, first device 201 transmits a signal for distance measurement to second device 203. Ex. 1001, 5:38–39. The second device modifies the received signal according to the secret, and retransmits the modified signal back to the first device. *Id.* at 5:39–41. First device 201 measures the round trip time between the transmission and receipt of the signal and checks to see if the returned signal was modified according to the exchanged secret. *Id.* at 5:41–45. If the round trip time is less than a predetermined interval, first device 201 is allowed to send protected content to second device 203. *Id.* at 6:24–27.

The step of performing an authenticated distance measurement is shown in Figure 3, illustrated below.

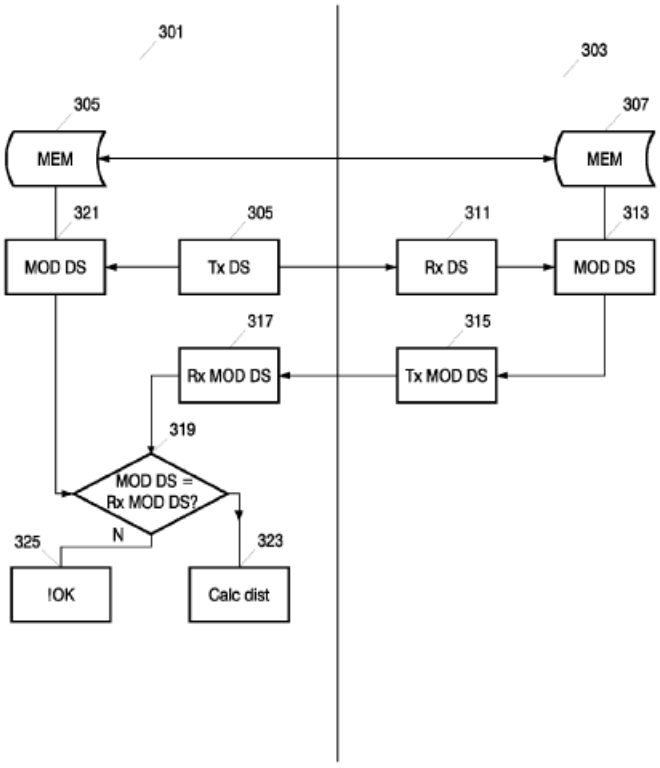


FIG. 3

In Figure 3, first device 301 and second device 303 have exchanged a secret, which is stored in memory 305 of the first device and memory 307 of

the second device. Ex. 1001, 6:28–32. In order to perform the distance measurement, transmitter 305[1] transmits a signal to second device 302, which receives the signal using receiver 311. *Id.* at 6:34–35. Second device 303 modifies the signal (313) using the locally stored secret according to rules known by first device 301, and transmits the modified signal back to the first device. *Id.* at 6:35–39. First device 301 receives the modified signal using receiver 317 and compares it to a locally modified signal, which is created by taking the original signal transmitted by the first device to the second device and modifying it using the first device's locally stored secret (319). *Id.* at 6:39–45. If the received modified signal and the locally modified signal are identical, the received signal is authenticated. *Id.* at 6:45–49. In 323, first device 301 calculates the distance between the first and second devices, such as by measuring the time from the transmission of the signal from the first device to the receipt of the signal by the second device. *Id.* at 6:52–57.

E. Illustrative Claims

Of the challenged claims, claim 22 is independent. Claim 22 is illustrative and is reproduced below.

> 22. [Pre] A method for a second device controlling of receiving a protected content, the method comprising:
>
> [a] sending a certificate to a first device, the certificate providing information regarding the second device;
>
> [b] receiving a first signal from the first device after the first device determines, based on the certificate, whether the second device is compliant with a set of compliance rules;

[1] The '977 patent appears to erroneously refer to the transmitter using reference number 309. Ex. 1001, 6:34.

> [c] sending a second signal to the first device after receiving the first signal;
>
> [d] generating a secure authenticated channel using the secret;
>
> [e] receiving over the secure authenticated channel the protected content after the first device determines that the second signal is derived using the secret and a time between a transmission of the first signal and receipt of the second signal by the first device is less than a predetermined time.

Ex. 1001, 8:39–57 (bracketed paragraph identifiers added).

F. Evidence of Record

Petitioner relies upon the following references found in the record:

> Maillard et al., EP 1045585 A1, pub. Oct. 18, 2000 (Ex. 1004, "Maillard");
>
> Davis et al., WO 97/39553 A1, pub. Oct. 23, 1997 (Ex. 1005, "Davis");
>
> Lundkvist, WO 02/35036 A1, publ. May 2, 2002 (Ex. 1006, "Lundkvist"); and
>
> Alfred Menezes et al., *Handbook of Applied Cryptography* (1997) (Ex. 1009, "HAC").

Pet. iii, 1.

Petitioner submits the Declaration of Dr. Seth James Nielson ("Dr. Nielson," Ex. 1003).

G. Challenges to Unpatentability

Petitioner challenges the patentability of claims 22–31 of the '977 patent based on the following grounds:

Claims Challenged	35 U.S.C. §	Reference(s)/Basis
22–25, 29–31	103(a)[2]	Maillard, Davis, Lundkvist
26–28	103(a)	Maillard, Davis, Lundkvist, HAC

II. DISCUSSION

A. Claim Construction

A claim "shall be construed using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. § 282(b)." 37 C.F.R. § 42.100(b). Petitioner states that, "for the purposes of this Petition, the claim terms are to be understood according to their plain and ordinary meaning." Pet. 15. Patent Owner does not provide any proposed claim constructions at this stage of the proceeding. *See generally* Prelim. Resp. Based on our review of the Petition and Preliminary Response, we do not believe that any claim terms require express construction at this stage of the proceeding. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Ltd.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017); *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803

[2] The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) ("AIA"), included revisions to 35 U.S.C. § 103 that became effective as of March 16, 2013. The application for the '977 patent was filed after March 16, 2013, but includes a priority claim to an application filed before this date. Ex. 1001, code (22), (63). Petitioner asserts that the '977 patent has an effective filing date of June 27, 2003, and Patent Owner asserts that the '977 patent has a priority date of July 26, 2002. Pet. 7; Prelim. Resp. 4. For purposes of institution, we apply the pre-AIA versions of 35 U.S.C. § 103.

(Fed. Cir. 1999) ("[O]nly those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy.").[3]

B. Principles of Law

A claim is unpatentable under 35 U.S.C. § 103 if "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) where in evidence, objective evidence of non-obviousness.[4] *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). When evaluating a combination of teachings, we must also "determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)). Whether a combination of prior art elements would have produced a predictable result weighs in the ultimate determination of obviousness. *Id.* at 416–417.

In an *inter partes* review, the petitioner must show with particularity why each challenged claim is unpatentable. *Harmonic Inc. v. Avid Tech.,*

---

[3] On March 16, 2021, the ITC issued an order construing certain claims of the '977 patent. *In the Matter of Certain Digital Video-Capable Devices and Components Thereof*, Investigation No. 337-TA-1224, Order No. 16 (Mar. 16, 2021). We have reviewed the ITC's claim construction order and find it to be consistent with our Decision.

[4] At this stage of the proceeding, Patent Owner has not presented objective evidence of non-obviousness.

Inc., 815 F.3d 1356, 1363 (Fed. Cir. 2016); 37 C.F.R. § 42.104(b). The burden of persuasion never shifts to Patent Owner. *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

We analyze the challenges presented in the Petition in accordance with the above-stated principles.

C. Level of Ordinary Skill in the Art

Petitioner contends that a person of ordinary skill in the art at the time of the alleged invention "would have had at least a bachelor's degree in Computer Science, Computer Engineering, or Electrical Engineering and 1–2 years of industry or research experience in the area of secure cryptographic communications." Pet. 14. Petitioner further asserts that "[t]his description is approximate and additional education could make up for less work experience and vice versa." *Id.* (citing Ex. 1003 ¶¶ 105–108). At this stage of the proceeding, Patent Owner does not set forth a definition of the level of ordinary skill. *See generally* Prelim. Resp. For the purposes of this Decision, we adopt Petitioner's assessment of the level of skill in the art, which is consistent with the '977 patent and the asserted prior art of record.

D. Ground 1: Alleged Obviousness of Claims 22–25 and 29–31 Over Maillard, Davis, and Lundkvist

Petitioner contends that claims 22–25 and 29–31 are obvious in view of Maillard, Davis, and Lundkvist. Pet. 19–72. Patent Owner disagrees, arguing, *inter alia*, that the Petition does not sufficiently establish that it would have been obvious to combine the distance measurement security techniques disclosed by Davis and Lundkvist into Maillard. Prelim. Resp. 45–46, 48–50. For the reasons discussed below, we find that Petitioner has

not demonstrated a reasonable likelihood that the claims challenged in this ground are unpatentable.

1. Overview of Maillard (Ex. 1004)

Maillard discloses a system for securely communicating digitally recorded data between devices to prevent illegal copying and redistribution. Ex. 1004 ¶ 1. For example, a DVD player may provide content to a TV and a video recorder. *Id.* at ¶¶ 75–76. Before communication, a security module may be used to validate one or more of the devices, such as by using an exchange of certificates. *Id.* ¶¶ 78–79. The security module may be a smartcard that can be inserted into a socket of one of the devices, or may be a separate module connected to one or more of the devices. *Id.* ¶¶ 9, 11. If validation is successful, the security module transmits a randomly-generated session key (SK) to the device(s) in encrypted form, which is decrypted by the device(s). *Id.* at ¶¶ 104–106. The session key is thereafter used to encrypt protected content that is transferred to the device(s). *Id.* at ¶ 106.

Maillard explains that use of the security module to validate device(s) provides an extra level of security to the system. Ex. 1004 ¶ 8. The security module can also be used to create a personalized digital audio-visual system by allowing a DVD player to send data to a digital television only if both the player and the television are validated by the security module, thus restricting a user's viewing of the digital data to their own personal television. *Id.* at ¶ 9. Additionally, the security module receives device identifiers and validates devices (such as a DVD and television) separate from the communication link between the devices themselves, so that the device identifiers cannot be obtained if the communication link between the devices is intercepted by a third party. *Id.* at ¶ 10.

The security module may contain a "revocation list" for blacklisting non-compliant devices and an "authorization list" for allowing transfer of data between pre-registered devices only. Ex. 1004 ¶ 15. Device identifiers intentionally published by third parties, for example on the Internet, can be added to the revocation list when periodically updating the security module in order to prevent data from being transferred to or from these devices. *Id.* The use of an authorization list can also block use of device identifiers intentionally published on the Internet because those identifiers will not be valid anywhere except in, for example, a home network. *Id.*

2. Overview of Davis (Ex. 1005)

Davis discloses a system that prevents unauthorized use of a device (such as a computer) by a user. Ex. 1005, code (57). Davis explains that existing systems allow a user to insert a smartcard to gain access to a computer, but these systems can be vulnerable when the user leaves the computer unattended without removing the card or disabling the computer during the user's absence. *Id.* at 2:28–3:19. Davis's system addresses this problem by providing a wireless device carried by the user that: (1) communicates with the PC to establish authorization using a challenge-response protocol, and (2) ensures proximity of the user to the PC by requiring the response to be received within a prescribed period of time. *Id.* at 4:1–19, 11:8–13:16, Fig. 5.

An overview of Davis's system is shown in Figure 1, reproduced below.

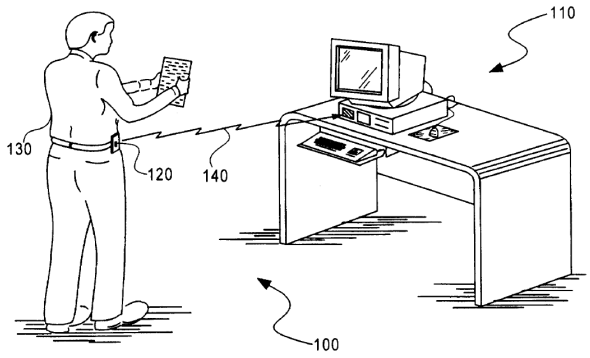


FIG. 1

Ex. 1005, Fig. 1. As shown in Figure 1, wireless authentication system 100 includes a personal computer 110, a security device (not shown) implemented within computer 110, and user authorization token 120 worn by authorized user 130. *Id.* at 6:28–7:1. Personal computer 110 periodically attempts to establish a wireless communication link 140 with token 120, which can be established and maintained only when token 120 is within a predetermined distance from personal computer 110. *Id.* at 7:6–13. Upon establishing communication link 140, the computer 110 and token 120 exchange information in an encrypted format. *Id.* at 7:20–22. When the security device determines that token 120 responded correctly, user 130 is granted access to personal computer 110. *Id.* at 7:22–26.

Davis's wireless authentication process uses a challenge-response protocol shown in Figure 5, reproduced below.

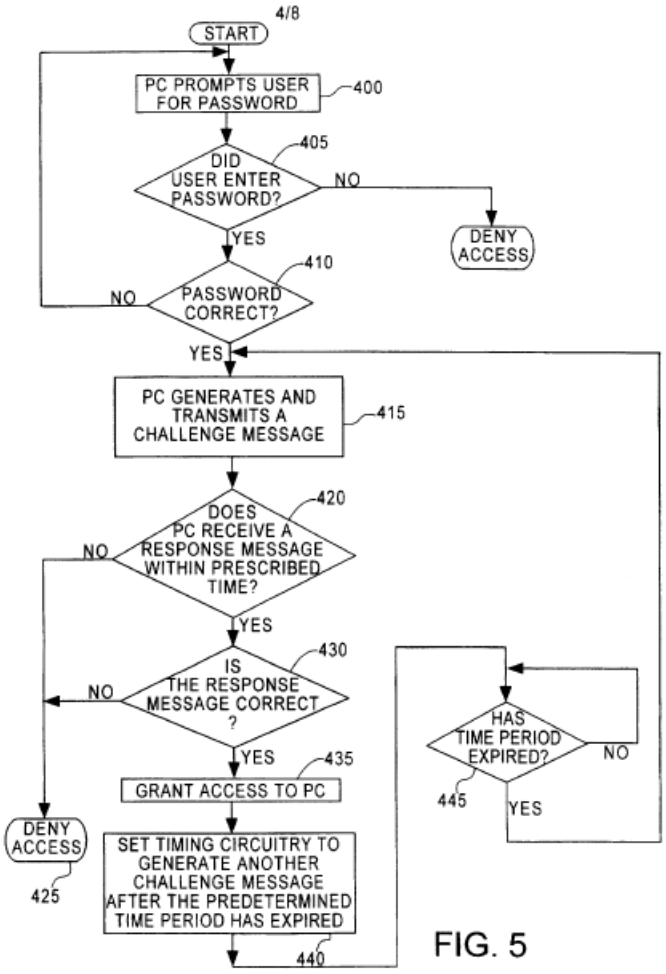


FIG. 5

Ex. 1005, Fig. 5; *see id.* at 11:8–13:16. As shown in Figure 5, the computer prompts the user for a password (step 400). Ex. 1005, 11:12–14. If the password is correct, the security device within the computer generates a challenge message and transmits it over a predetermined distance range from the computer (step 415). *Id.* at 11:21–24. Thereafter, the security device awaits a response message from the token. *Id.* at 11:24–26. If no response message is received after a prescribed period of time, access is denied (step 425). If a response message is received, the node verifies whether the response message is correct (step 430). *Id.* at 11:28–30. If the response message is not correct, access is denied (step 425). *Id.* at 11:30–12:3. If the response message is correct, the user is granted access to the computer and

the computer sets a timing circuit to signal when the computer will generate another challenge message and undergo another challenge/response session (steps 435–445). *Id.* at 12:3–6. This ensures that the computer will periodically require authentication and determine that the user is in proximity to the computer while the computer is operational. *Id.* at 12:6–9.

3. Overview of Lundkvist (Ex. 1006)

Lundkvist discloses a method for authorizing access to an object, in which communication "is established between the object and a wireless portable unit when a tripping device on the object is actuated." Ex. 1006, 1:5–8. The invention is described for controlling access to a vehicle, such as a car or truck, and in that case, "the tripping device normally consists of a door handle on the vehicle." *Id.* at 1:23–25. The signal communication verifies the identity of the wireless portable unit and determines whether the distance between the vehicle and the portable unit is less than a maximum permitted distance. *Id.* at 1:8–17.

The signaling method between the vehicle and the portable unit when the door handle is actuated is illustrated in Figure 2, reproduced below:

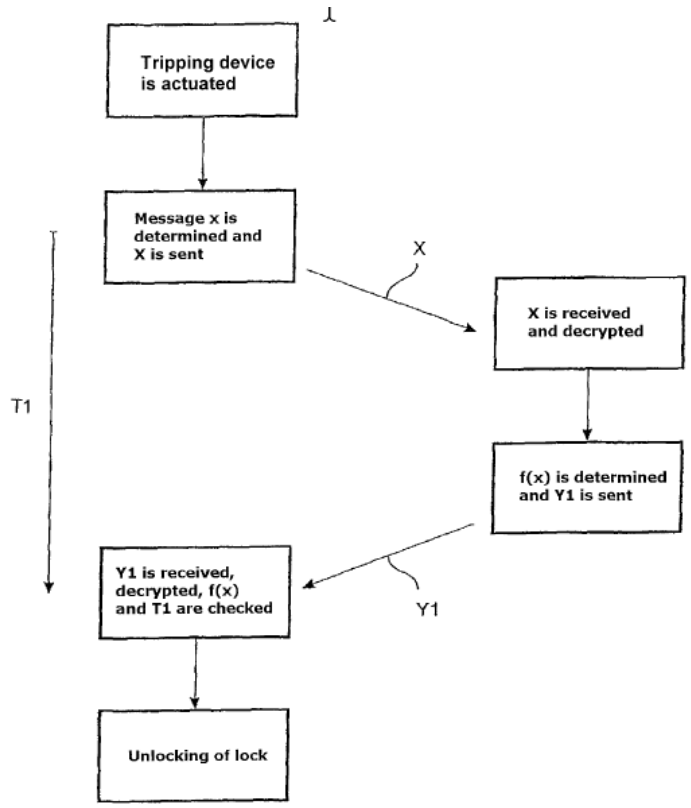


Fig.2

Ex. 1006, Fig. 2. As shown in Figure 2, when the tripping device (door handle) is actuated, the vehicle 1 creates a message that includes first information x that is intended to be used to verify the identity of the portable unit. *Id.* at 8:11–14. First information x consists of identity information unique to the vehicle and a random number generated by the vehicle. *Id.* at 8:14–16. The message is encrypted and sent to the portable unit in first signal X. *Id.* at 8:16–17. The portable unit receives first signal X, and decrypts the message to obtain first information x. *Id.* at 8:19. The portable unit processes first information x to generate second signal Y1, which is a function f(x) of first information x, and sends second signal Y1 to the vehicle. *Id.* at 8:19–23. The vehicle receives and decrypts second signal Y1, and measures time T1 from the transmission of first signal X until the

receipt of second signal Y1. *Id.* at 8:23–26. The vehicle is unlocked if the decrypted information matches first information x and measured time T1 is less than a predetermined value. *Id.* at 8:26–28.

4. Analysis of Independent Claim 22

Petitioner asserts that Maillard's security module is the claimed "first device," and that Maillard's digital TV or recorder corresponds to the claimed "second device." Pet. 34–35. Petitioner further asserts that Maillard's security module can be a smart card inserted into a DVD player that may send content to the digital TV or recorder. *Id.* at 35. Petitioner does not rely on Maillard for claim limitation 22(e) requiring that protected content is received after the first device determines that "a time between a transmission of the first signal and receipt of the second signal by the first device is less than a predetermined time," but instead relies on Davis and Lundkvist for this limitation. Pet. 56–61.

> Petitioner argues that a person of ordinary skill
>
> would have found it obvious to combine the complementary teachings of these references to authorize the transfer of protected content to the (second) device over the channel upon: (A) first validating the identity of the device (as explained in Elements 22[a] and 22[b-1] per Maillard), and if the validation is successful, (B) determining that a time between a transmission of the first signal and receipt of the second signal by the first device is less than a predetermined time (per combination of Davis and Lundkvist), and (C) determining that the second signal is derived using the secret (per combination of Davis and Lundkvist).

Pet. 58 (citing Ex. 1003 ¶¶ 188–197).

More specifically, Petitioner argues that Maillard, Davis, and Lundkvist "all relate to providing secure access that is conditioned on successful completion of exchanges between two devices." Pet. 31 (citing

Ex. 1004, code (57), ¶¶ 79, 104–108; Ex. 1005, 1:18–21, 2:28–3:30, 4:2–19, 11:8–12:9; Ex. 1006, code (57), 3:14–4:5). According to Petitioner, a person of ordinary skill would have been motivated to combine Maillard with Davis because Davis recognizes that smartcard systems can be vulnerable when "the user accesses his or her personal computer and leaves the personal computer unattended for some duration without removing the card or disabling the personal computer during his or her absence." Pet. 31 (quoting Ex. 1005, 3:15–19).

Petitioner further argues that one of ordinary skill would have "recognized that Maillard's technique, which was described using an example home network using [an] IEEE 1394 communication link . . . could be susceptible to attacks that would allow devices outside of the home network to infiltrate the home network." Pet. 31 (citing Ex. 1003 ¶¶ 131–135). Thus, according to Petitioner, one of ordinary skill would have "been motivated to look for additional security procedures such as those in Davis, and would have found it obvious[] to utilize Davis'[s] additional and complementary authentication steps that ensured proximity of the user device to the node by requiring the response to be received within a predetermined time." *Id.* (citing Ex. 1005, code (57), 4:2–19, 11:8–12:9, Fig. 5; Ex. 1003 ¶¶ 132–137). Petitioner also argues that it would have been obvious to combine Davis and Lundkvist because Davis stated that other challenge-response protocols can be used, and Lundkvist's challenge-response protocol is one of a limited number of alternatives. *Id.* at 32 (citing Ex. 1003 ¶¶ 138–140).

Patent Owner argues that the Petition "fails to identify a legitimate reason that it was obvious to combine [Davis and Lundkvist] with Maillard."

Prelim. Resp. 48. According to Patent Owner, Maillard does not address the problem of ensuring that the first and second devices are within a predetermined distance "because there is no need to do so—in Maillard, the purported first device (security module 64) and purported second device (television or recorder) preferably **are physically connected to one another**, such as by a cable or by inserting the security module smart card in a port in the television or recorder." *Id.* at 48 (emphasis omitted). Thus, Patent Owner asserts, "[t]here is no need to determine the proximity of devices that are already physically connected to one another." *Id.* at 48–49.

As for Petitioner's argument that one of ordinary skill would have recognized that Maillard's implementation using IEEE 1394 is susceptible to attacks allowing devices outside of a home network to infiltrate the network (Pet. 31), Patent Owner argues that Maillard only mentions IEEE 1394 in the form of "a physical cable that connects two devices together." Prelim. Resp. 50 (emphasis omitted). According to Patent Owner, Petitioner is "essentially arguing that a bad actor could enter a user's home and physically plug an IEEE 1394 bus link into a DVD player to transmit to another unauthorized TV." *Id.* at 50. Thus, Patent Owner argues, the distance between Maillard's transmitting and receiving devices is irrelevant, and adding a distance measurement would add no additional protection. *Id*.

We do not find that Petitioner has articulated sufficient reasoning for combining Maillard with Davis and Lundkvist based on the present record. First, Petitioner's assertion that the references "all relate to providing secure access that is conditioned on successful completion of exchanges between two devices" (Pet. 31), fails to sufficiently explain *why* one would have used a distance measurement in Maillard's system. Second, Petitioner's argument

that Davis recognizes the vulnerability of smartcard systems when a user leaves a computer unattended (Pet. 31), fails to sufficiently explain why this problem would apply to Maillard's system, i.e., why it would be a problem for the user to leave the security module unattended while connected to the DVD player.

Finally, Petitioner's argument that one would have been motivated to add a distance measurement to prevent an unauthorized person from breaking into Maillard's home network from a remote location lacks sufficient evidentiary support. *See* Pet. 31–32; Ex. 1003 ¶¶ 131–135. Petitioner does not point to any statements in Maillard or other prior art references suggesting that this could be a problem. Instead, Petitioner relies on the following testimony from Dr. Nielson:

> 135. A POSITA, however, would recognize that while Maillard's white-list would provide the necessary step of identifying authorized devices, it does not provide a mechanism for enforcing that those devices are on the "home network," i.e., physically within the bounds of the home network. ***It was known to a POSITA that data signals of one communication type, such as IEEE 1394 as mentioned in Maillard, can be vulnerable to attacks, where signals could be adapted and retransmitted over more traditionally long distance mechanisms, such as Ethernet.*** US patent 6,496,862, with a priority date of 1998, describes a "gateway" that interconnects ethernet and IEEE 1394 specifically for media and television. ***A POSITA would readily comprehend that Maillard's security module for device authorization and authentication in a home network could be exfiltrated to a remote location.*** Thus, instead of a DVD player transmitting data to a local TV on a home network, Maillard's security module would enable the DVD player to transmit to another unauthorized TV anywhere in the world so long as the security module is connected in this way. Maillard 0055.

> 136. Thus, the POSITA would have been motivated to find mechanisms for enforcing the security module and associated devices were on the "home network." Maillard in view of Davis provides an obvious solution.

Ex. 1003 ¶¶ 135–136 (emphases added), *cited in* Pet. 31–32.

Neither Petitioner nor Dr. Nielson, however, point to any statements in Maillard, Davis, Lundkvist, or any other reference in the record supporting Dr. Nielson's assertions that: (1) "[i]t was known to a POSITA that data signals of one communication type, such as IEEE 1394 as mentioned in Maillard, can be vulnerable to attacks, where signals could be adapted and retransmitted over more traditionally long distance mechanisms, such as Ethernet," or (2) "[a] POSITA would readily comprehend that Maillard's security module for device authorization and authentication in a home network could be exfiltrated to a remote location." *See* Pet. 30–33, 56–61; Ex. 1003 ¶¶ 131–141. Dr. Nielson cites U.S. Patent No. 6,496,862, but that patent is not part of the record and, in any event, is only cited for its disclosure of "a 'gateway' that interconnects Ethernet and IEEE 1394 specifically for media and television," not to show that the problem of exfiltrating a device like Maillard's security module would have been well understood by a person of ordinary skill in the art. Ex. 1003 ¶ 135.

Moreover, as Patent Owner explains, Maillard discloses IEEE 1394 in the form of "a[n] IEEE 1394 bus link" connecting the first and second devices. Ex. 1004 ¶ 53. Patent Owner introduces evidence that an IEEE 1394 bus link is a physical cable that connects two devices together. *See* Ex. 2001, 94 ("First introduced as Firewire by Apple Computer in the late 1980s, the now-approved IEEE 1394 standard was designed to support high bandwidth requirements of devices such as digital video equipment and high performance mass storage. . . . The 1394 spec calls for six wires—two

differential pairs plus power and ground."). We agree with Patent Owner that, in Maillard's system, where the devices are physically connected, Petitioner does not sufficiently explain, based on the present record, why adding a distance measurement between the security module and one of the other devices would enhance security.

For the foregoing reasons, Petitioner has not demonstrated a reasonable likelihood of prevailing in showing that claim 22 would have been obvious over Maillard, Davis, and Lundkvist.

5. Analysis of Dependent Claims 23–25 and 29–31

Claims 23–25 and 29–31 depend from claim 22. Petitioner's arguments and evidence regarding these dependent claims do not compensate for the deficiencies discussed above for claim 22. *See* Pet. 62–72. Thus, for the same reasons discussed above for claim 22, Petitioner does not demonstrate a reasonable likelihood of prevailing in showing that claims 23–25 and 29–31 would have been obvious over Maillard, Davis, and Lundkvist.

E. Ground 2: Alleged Obviousness of Claims 26–28 Over Maillard, Davis, Lundkvist, and HAC

Petitioner contends that claims 26–28 would have been obvious in view of Maillard, Davis, Lundkvist, and HAC. Pet. 72–78. Claim 26 depends from claim 25, which depends from claim 22, and claims 27–28 depend from claim 26. Petitioner's arguments and evidence regarding these dependent claims do not compensate for the deficiencies discussed above for claim 22. *See* Pet. 72–78. Thus, for the same reasons discussed above for Ground 1, Petitioner does not demonstrate a reasonable likelihood of

prevailing in showing that claims 26–28 would have been obvious in view of Maillard, Davis, Lundkvist, and HAC.

III. CONCLUSION

After considering the evidence and arguments presented in the current record, we determine Petitioner has not demonstrated a reasonable likelihood of prevailing with respect to at least one claim challenged in the Petition. Therefore, we do not institute an *inter partes* review in this proceeding.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that the Petition is denied and no *inter partes* review is instituted in this proceeding.

For PETITIONER:

Babak Tehranchi
John Schnurer
Bing Ai
Kevin Patariu
Yun Lu
PERKINS COIE LLP
Tehranchi-ptab@perkinscoie.com
Schnurer-ptab@perkinscoie.com
Ai-ptab@perkinscoie.com
Patariu-ptab@perkinscoie.com
Lu-ptab@perkinscoie.com

For PATENT OWNER:

William Meunier
Michael Renaud
Derek Constantine
MINTZ, LEVIN, COHN, FERRIS, GLOVSKY AND POPEO, P.C.
wameunier@mintz.com
mtrenaud@mintz.com
deconstantine@mintz.com