

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO. LTD., and
SAMSUNG ELECTRONICS AMERICA, INC.,
Petitioners,

v.

FOUR BATONS WIRELESS, LLC,
Patent Owner.

Case IPR2025-00495
Patent 8,239,671

**PATENT OWNER'S PRELIMINARY RESPONSE
TO PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 8,239,671**

Mail Stop "PATENT BOARD"
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

EXHIBIT LIST

Exhibit	Description
EX2001	Declaration of Eric J. Enger in Support of Patent Owner’s Notice of Intent to Designate Provisionally Recognized Attorney Eric J. Enger as Back-Up Counsel Under 37 C.F.R. § 42.10(c)
EX2002	<i>Four Batons Wireless, LLC v. Samsung Electronics Co., Ltd. et al.</i> , Complaint for Patent Infringement, Case No. 2:24-cv-284, Dkt. No. 1 (E.D. Tex. Filed April 26, 2024)
EX2003	<i>Four Batons Wireless, LLC v. Samsung Electronics Co., Ltd. et al.</i> , Defendants Samsung Electronics Co., Ltd.’s and Samsung Electronics America, Inc.’s Motion To Stay Proceedings Pending <i>Inter Partes</i> Review, Case No. 2:24-cv-284, Dkt. No. 62 (E.D. Tex. Filed Feb. 7, 2025)
EX2004	<i>Four Batons Wireless, LLC v. Samsung Electronics Co., Ltd. et al.</i> , Plaintiff’s Opposition to Samsung’s Motion To Stay Proceedings Pending <i>Inter Partes</i> Review, Case No. 2:24-cv-284, Dkt. No. 63 (E.D. Tex. Filed Feb. 21, 2025)
EX2005	<i>Four Batons Wireless, LLC v. Samsung Electronics Co., Ltd. et al.</i> , First Amended Docket Control Order, Case No. 2:24-cv-284, Dkt. No. 69 (E.D. Tex. Filed April 30, 2025)
EX2006	United States District Courts — National Judicial Caseload Profile, available from https://www.uscourts.gov/sites/default/files/2025-02/fcms_na_distprofile1231.2024.pdf (accessed May 12, 2025)
EX2007	<i>Four Batons Wireless, LLC v. Samsung Electronics Co., Ltd. et al.</i> , Plaintiff’s Infringement Contentions, Case No. 2:24-cv-284 (E.D. Tex. served July 25, 2024)
EX2008	<i>Four Batons Wireless, LLC v. Samsung Electronics Co., Ltd. et al.</i> , Defendants’ Invalidity Contentions, Case No. 2:24-cv-284 (E.D. Tex. served Nov. 18, 2024)
EX2009	<i>Four Batons Wireless, LLC v. Samsung Electronics Co., Ltd. et al.</i> , Samsung’s Preliminary Claim Constructions And Extrinsic Evidence Pursuant To Patent Local Rule 4-2, Case No. 2:24-cv-284 (E.D. Tex. served May 5, 2025)
EX2010	<i>Four Batons Wireless, LLC v. Samsung Electronics Co., Ltd. et al.</i> , Plaintiff Four Batons Wireless, LLC’s Initial Proposed Constructions, Case No. 2:24-cv-284 (E.D. Tex. served May 5, 2025)
EX2011	Correspondence between Samsung and Four Batons

Exhibit	Description
EX2012	Comparison of Abobav3 vs. Abobav5, available at https://author-tools.ietf.org/iddiff?url1=draft-ietf-eap-keying-03&url2=draft-ietf-eap-keying-05&difftype=--hwdiff (accessed May 7, 2025)
EX2013	<i>iRhythm Technologies, Inc. v. Welch Allyn, Inc.</i> , IPR2025-00363, Paper 10 (P.T.A.B. June 6, 2025) (highlighting added)
EX2014	Office Action from Samsung’s Patent Application No. 12/152,354 (dated September 10, 2012) (highlighting added)
EX2015	Google Patents listing for U.S. Patent No. 8,239,671, available at https://patents.google.com/patent/US8239671B2/en?q=8%2c239%2c671 (accessed June 16, 2025) (highlighting added)
EX2016	Google Translate for “삼성전자주식회사,” available at https://translate.google.com/?sl=auto&tl=en&text=삼성전자주식회사&op=translate (accessed June 16, 2025)
EX2017	Extensible Authentication Protocol (EAP) Key Management Framework, IETF Internet-Draft, draft-ietf-eap-keying-09, January 8, 2006
EX2018	Extensible Authentication Protocol (EAP) Key Management Framework, IETF Internet-Draft, draft-ietf-eap-keying-12 (April 13, 2006)
EX2019	<i>Four Batons Wireless, LLC v. Samsung Electronics Co., Ltd. et al.</i> , The Parties’ P.R. 4-3 Joint Claim Construction and Pre-Hearing Statement, Case No. 2:24-cv-284, Dkt. No. 77 (E.D. Tex. Filed May 30, 2025)
EX2020	Excerpts from ANSI/IEEE Standard 802.11-1999, Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks—Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (1999)
EX2021	Expert Declaration of Dr. Aviel D. Rubin on Petition for Inter Partes Review of U.S. Patent No. 8,239,671
EX2022	Excerpts from IEEE Standard 802.11r-2008, Amendment 2: Fast Basic Service Set (BSS) Transition (2008)

TABLE OF CONTENTS

II.	Introduction.....	1
III.	Background.....	2
	A. The '671 Patent [EX1001].....	2
	B. The '671 Prosecution History [EX1004].....	8
	C. Petitioners' References	12
	1. Sood [EX1005].....	13
	2. Aboba [EX1006]	17
	3. Lee [EX1007]	18
IV.	Legal Standards	19
V.	Level of Ordinary Skill in the Art	20
VI.	Claim Construction.....	21
VII.	Arguments.....	23
	A. Grounds 1, 3-4: Petitioners' Art Fails To Present A Reasonable Likelihood Of Prevailing Against Independent Claims 1 and 6	23
	1. Sood, whether alone or in combination with Aboba and/or Lee, does not teach or suggest "cryptographically bind[ing] access network parameters to a [] key [] without [] needing to carry [the] parameters in [] authentication methods" (claims 1[a], 6[a(i), (iii)])	24
	2. Sood, whether alone or in combination with Aboba and/or Lee, does not teach or suggest "deriv[ing a] channel binding key from a channel binding master key bound to a key binding blob using a key derivation function" (claims 1[b], 6[b])	28
	3. Sood, whether alone or in combination with Aboba and/or Lee, does not teach or suggest "wherein said key binding blob is a string that is constructed from static parameters advertised from [an] authenticator" (claims 1[c], 6[c]).....	36
	B. Grounds 1-4: Petitioners' Art Fails To Present A Reasonable Likelihood Of Prevailing Against The Dependent Claims	40

VIII. Conclusion40

TABLE OF AUTHORITIES

Cases

Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.,
800 F.3d 1375 (Fed. Cir. 2015).....20

Harmonic Inc. v. Avid Tech., Inc.,
815 F.3d 1356 (Fed. Cir. 2016).....19

In re Magnum Oil Tools Int’l, Ltd.,
829 F.3d 1364 (Fed. Cir. 2016)..... 19, 20, 39

In re NuVasive, Inc.,
842 F.3d 1376 (Fed. Cir. 2016).....20

In re Warsaw Orthopedic, Inc.,
832 F.3d 1327 (Fed. Cir. 2016).....20

Microsoft Corp. v. FG SRC, LLC,
860 F. App’x 708 (Fed. Cir. 2021)39

Phillips v. AWH Corp.,
415 F.3d 1303 (Fed. Cir. 2005).....21

Statutes

35 U.S.C. § 312(a)(3).....20

37 C.F.R. § 42.100(b)21

I. Introduction

Petitioners Samsung Electronics Co. Ltd. and Samsung Electronics America, Inc. (“Samsung” or “Petitioners”) filed a Petition challenging Claims 1-8 and 10-19 of U.S. Patent No. 8,239,671 (“the ‘671 Patent”) on four separate grounds. Paper 2 (“Pet.”) at 2. Patent Owner Four Batons Wireless, LLC (“Four Batons” or “Patent Owner”) respectfully requests the Board deny institution of that Petition because Samsung has not shown a reasonable likelihood of prevailing on any of its grounds as to any challenged claim of the ‘671 Patent.

Petitioners’ primary Sood reference fails to disclose at least three elements of the ‘671 independent claims. First, rather than “cryptographically binding access network parameters to a key without needing to carry the parameters in authentication methods” as claimed, Sood does the opposite; Sood carries unencrypted access network parameters as part of the traditional 802.11i four-way handshake authentication method. Second, Sood does not perform the claimed “deriving a channel binding key from a channel binding master key bound to a key binding blob using a key derivation function;” Petitioners use three alternative mappings in an attempt to make Sood fit the claim language, but none quite work. Third, Petitioners have not shown that Sood’s alleged key binding blob is “a string that is constructed from static parameters advertised from authenticator” as claimed; Petitioners do not even address half of the parameters. And Petitioners’ secondary

references—Aboba and Lee—cannot plug the holes in Sood. Because these deficiencies infect all four grounds, Petitioners have not met their burden to prove they are reasonably likely to prevail at trial. The Board should decline to institute IPR.

Patent Owner has also filed its bifurcated discretionary denial briefing pursuant to the Director’s March 26, 2025 Memorandum. Paper 10 (Initial Brief); Paper 11 (Supplemental Brief). The PTAB should exercise its discretion to deny institution for the reasons presented in those briefs, as well.

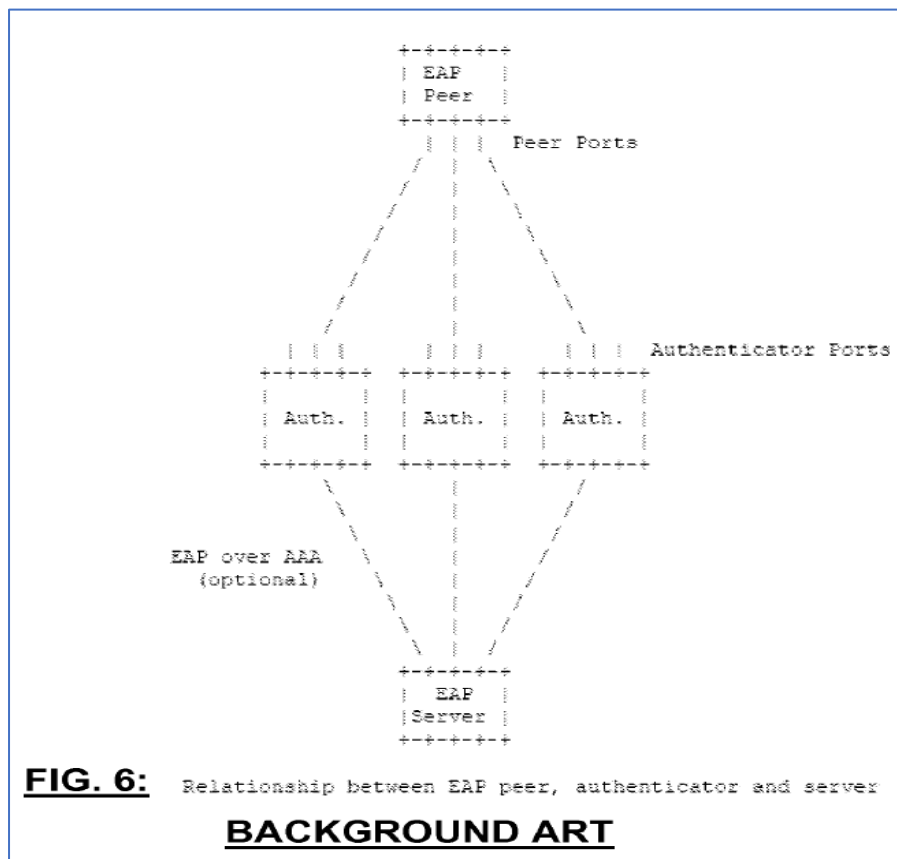
II. Background

A. The ‘671 Patent [EX1001]

The ‘671 Patent is titled “Channel Binding Mechanism Based on Parameter Binding in Key Derivation.” EX1001 (hereinafter, “‘671”). It was invented by Yoshihiro Oba while working at Toshiba. *Id.* The ‘671 Patent was filed on April 20, 2006, and issued on August 7, 2012. *Id.*

The ‘671 generally relates to securing wireless communications by authenticating the entities that communicate wirelessly. EX2021 (Rubin Dec.) at ¶73. Authentication is the process of verifying the identity of an entity before granting it access to a system or resource; the entity should only gain access if it is properly authenticated. *See id.* at ¶¶62-71. Authentication is a crucial security measure that protects wireless networks from unauthorized access and attacks. *Id.*

The '671 Patent references an authentication framework called the Extensible Authentication Protocol or "EAP" that supports multiple authentication algorithms. '671 at 12:40-43. EAP was defined in RFC 3748 on June 2004 and incorporated by reference into the '671 Patent. *Id.* at 9:57-61, 9:5-67. In EAP, there are three entities: (1) the server; (2) the authenticator; and (3) the peer (sometimes also referred to as a client or supplicant). EX2021 (Rubin Dec.) at ¶69. In general, the authenticator determines if the peer is who it claims to be and whether it should be granted access to the server. *Id.* To make this determination, the authenticator may verify that the peer has a valid key and knows the proper access parameters of the wireless network, for example. *Id.*

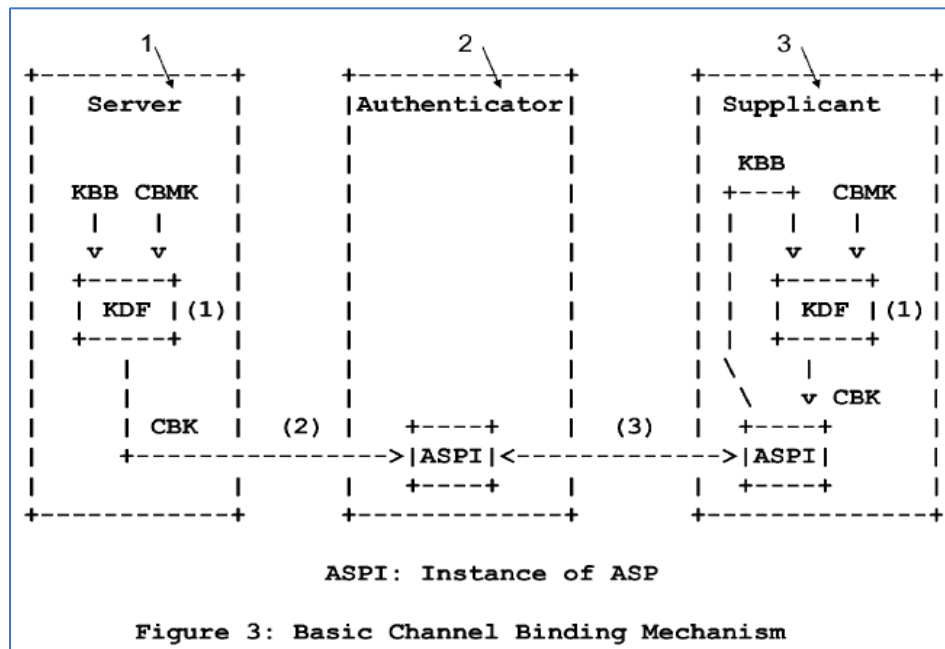


The '671 Patent teaches that prior authentication methods communicated the access network parameters used for verification from the server to the authenticator over a "protected channel." '671 at 12:65-67. However, despite the nature of the protected channel, those access network parameters could nonetheless be intercepted by a malicious adversarial user and then used to impersonate an authorized peer. EX2021 (Rubin Dec.) at ¶75.

The '671 Patent provides a secure alternative for communicating the access network parameters between the server and the authenticator in a way that cannot be easily intercepted and maliciously used. EX2021 (Rubin Dec.) at ¶¶73-75. In the preferred embodiment, rather than communicating the access network parameters themselves, the '671 Patent teaches to first cryptographically bind the access network parameters to a channel binding master key and then transmit the cryptographically bound combination from the server to the authenticator. '671 at 13:5-8. The '671 Patent refers to binding the access network parameters to a key for "channel binding." *See id.*; *see also id.* at 4:67-5:17. In this way, even if the cryptographically bound combination is intercepted, the access network parameters cannot be deciphered without a master key. *Id.*; EX2021 (Rubin Dec.) at ¶¶74-75.

Figure 3 illustrates a preferred embodiment of the '671 Patent's channel binding procedure. '671 at 13:54-58. Figure 3 shows three entities: server 1, authenticator 2, and supplicant 3. *Id.* at 13:58-60. Both the server and supplicant are

pre-configured with the same master key. Further, the server is also pre-configured with access network parameters, while the supplicant receives its access network parameters from the authenticator via an advertisement. *Id.* at 14:2-3, 10:17-19. The ‘671 Patent discloses a three-step procedure for using this architecture to securely authenticate the supplicant. *Id.* at 13:64-14:12.



First, the server and the supplicant use a Key Derivation Function or “KDF” to cryptographically bind (i) their respective access network parameters (referred to as a Key Binding Blob or “KBB”) to (ii) the common master key (referred to as a Channel Binding Master Key or “CBMK”). ‘671 at 13:64-14:2. The ‘671 Patent refers to the cryptographically bound combination of the “KBB” access network parameters and the “CBMK” key as the Channel Binding Key or “CBK.” *See id.*; *see also id.* at 10:21-23 (“deriving a channel binding key from a channel binding

master key bound to a key binding blob using a key derivation function”). This first step is called “CBK Creation.” *Id.* at 13:64.

Second, the server transfers its CBK—but not the access network parameters or KBB themselves—to the authenticator. ‘671 at 14:4-6. In this manner, even if the CBK is intercepted, it is impossible to decipher the access network parameters or KBB without also having the CBMK key. This second step is called “CBK Transfer.” *Id.* at 14:4.

Third, the supplicant and the authenticator verify proof of possession of the same CBK using an Authenticator-Supplicant Protocol (“ASP”). ‘671 at 14:7-10. If both the supplicant and the authenticator have the same CBK (and thus the same KBB access network parameters), then the supplicant and the authenticator are able to use that CBK to authenticate the supplicant. *Id.* at 14:10-12. This third step is called “CBK Verification.” *Id.* at 14:7.

The challenged ‘671 independent claims 1 and 6 recite the concepts discussed above. These claims are reproduced below using the Petitioners’ same numbering nomenclature:

1. [pre] A channel binding method based on parameter binding in a key derivation procedure for authentication of a mobile supplicant to an access network, comprising:
 - [a] cryptographically binding access network parameters to a key without needing to carry the parameters in authentication methods;

- [b] further including deriving a channel binding key from a channel binding master key bound to a key binding blob using a key derivation function; and
- [c] wherein said key binding blob is a string that is constructed from static parameters advertised from an authenticator.

‘671 at 17:13-23.

6. [pre] A channel binding method based on parameter binding in a key derivation procedure for authentication of a mobile supplicant to an access network, comprising:

- [a] [i] using an extensible authentication protocol server to cryptographically bind access network parameters to a channel binding key and to transmit said channel binding key to an extensible authentication protocol authenticator [ii] for use by the extensible authentication protocol authenticator as an extensible authentication protocol master session key [iii] without said extensible authentication protocol authenticator needing to carry said access network parameters in extensible authentication protocol authentication methods;
- [b] including using said extensible authentication protocol server to derive said channel binding key from a channel binding master key bound to a key binding blob using a key derivation function;
- [c] wherein said key binding blob is a string that is constructed from static parameters advertised from said extensible authentication protocol authenticator.

‘671 at 17:32-51.

B. The '671 Prosecution History [EX1004]

The Applicant filed for the '671 Patent on April 20, 2006. EX1004 (hereinafter, "'671 FH'") at 258-297.

On December 9, 2010, the Examiner rejected many pending claims in view of RFC3748,¹ which the Examiner referred to as "Adoba." *Id.* at 123-128. Specifically, the Examiner alleged that RFC3748/Adoba taught the claimed "cryptographically binding access network parameters to a key without needing to carry the parameters in authentication methods." *Id.* at 124.

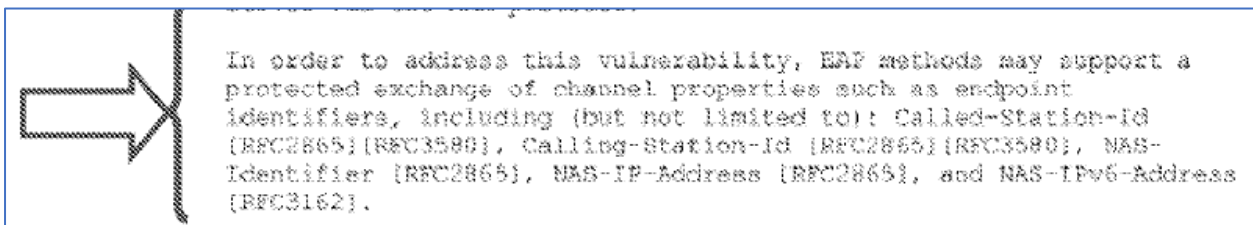
The Applicant traversed the rejection on April 11, 2011, noting the '671 Patent explicitly distinguished RFC3748/Adoba. *Id.* at 107. The Applicant explained that, rather than "cryptographically binding access network parameters to a key without needing to carry the parameters in authentication methods" as claimed, RFC3748/Adoba needed to carry the access network parameters in authentication methods via a protected channel of an EAP method:

¹ RFC 3748/Adoba is provided as EX1015.

First, it is respectfully noted that the Adoba reference does **not** teach that which the Patent Office asserts. In particular, the Adoba reference reflects the background art described in the present application, of which the present invention is a substantial improvement upon. See, e.g., page 20 of the present application which recites:

“A mechanism that is described in [RFC3748] to create such a binding is based on **communicating the access network parameters over a protected channel of an EAP method** to help the EAP peer and the EAP server detect a mismatch between the parameters exchanged over the protected channel and the ones advertised by the EAP authenticator to the EAP peer and the EAP server.” Emphasis added.

Id. Further, the Applicant copy-pasted section 7.15 of RFC3748/Adoba into the response and used an arrow to emphasize the portion showing that access network parameters were communicated over a protected channel of an EAP method:



Id. at 109 (citing RFC3748/Adoba at 55-56); *see also* EX1015 (RFC3748) at 55-56.

The Applicant also amended the independent claims to require “deriving a channel binding key from a channel binding master key bound to a key binding blob using a key derivation function” and that the key binding blob “is a string that is constructed from static parameters advertised from an authenticator” because neither of those limitations were taught by RFC3748/Adoba. ‘671 FH at 100-101, 110-111.

On August 12, 2011, the Examiner noted that, while he found the Applicant's prior arguments concerning RFC3748/Adoba persuasive, he nonetheless rejected the pending independent claims as obvious in view of RFC3748/Adoba in combination with U.S. Published Patent Application Nos. 2003/0226017 to Palekar and 2009/0019284 to Cho. *Id.* at 71-72. The Examiner first acknowledged that RFC3748/Adoba did not teach any of these three claim elements:

1. "cryptographically binding access network parameters to a key without needing to carry the parameters in authentication methods;"
2. "deriving a channel binding key from a channel binding master key bound to a key binding blob using a key derivation function;" or
3. "wherein said key binding blob is a string that is constructed from static parameters advertised from an authenticator."

Id. at 72-75. But the Examiner asserted that Palekar taught claim elements 1-2 and Cho taught claim element 3. *Id.*

On January 12, 2012, the Applicant traversed the rejection for several reasons. *Id.* at 47-63. First, the Applicant argued the Examiner's proffered combination of three references was erroneous and based on improper hindsight. *Id.* at 55. Second, the Applicant noted that RFC3748/Adoba "merely pertains to the background art" because its channel bindings are "based on communicating the access network parameters over a protected channel of an EAP method," rather than the claimed

invention that “creates a binding between the key exported and the parameters in a manner to specifically avoid the need for such a communication of the access network parameters over a protected channel of an EAP network.” *Id.* at 55-57. Third, the Applicant argued there was no basis to modify the structure in RFC3748/Adoba based on Palekar, as suggested by the Patent Office. *Id.* at 57-58. Fourth, the Applicant argued that combining RFC3748/Adoba and Palekar with Cho did not make sense because the technologies do not comport to one another. *Id.* at 58. Finally, the Applicant argued that Cho did not teach or suggest modifying a server and/or supplicant to generate a key binding blob based on an advertisement from an authenticator. *Id.*

The Examiner allowed the claims on April 16, 2012. *Id.* at 32. The Examiner acknowledged the Applicant’s arguments in the prior response were persuasive. *Id.* at 33. And the Examiner provided these reasons for allowance:

The following is a statement of reasons for the indication of allowable subject matter:

In interpreting the claims in light of the specification and applicant’s arguments examiner finds the claimed invention is patentable distinct from the prior art of record.

The prior art of record does not teach the following limitations in combination with other limitations in the claim: **“cryptographically binding access network parameters to a key without needing to carry the parameters in authentication methods” “wherein said key binding blob is a string that is constructed from static parameters advertised from an authenticator”**

Id.

The '671 Patent issued on August 7, 2012. *Id.* at 17. The Patent Office issued a certificate of correction addressing certain typos on October 28, 2014. *Id.* at 7.

C. Petitioners' References

Petitioners assert four grounds of invalidity based on combinations of three references:

Ground	Claims	Statute	References
1	1-4, 7, 8, 12, 14, 16	§103	Sood
2	5, 18	§103	Sood + Aboba
3	6, 10, 11, 13, 15, 17, 19	§103	Sood + Lee
4	1-8, 10-19	§103	Sood + Aboba + Lee

Pet., 2. None of those references, either alone or in combination, teach or suggest all the elements of challenged '671 independent claims 1 and 6.² EX2021 (Rubin Dec.) at ¶¶28-33, 106-176.

² For the purposes of this preliminary response, Four Batons has only addressed independent Claims 1 and 6. As shown herein, Petitioners have failed to demonstrate a reasonable likelihood of success of proving those independent claims are unpatentable. Consequently, Petitioners have also necessarily failed to show unpatentability of dependent claims 2-5, 7-8, and 10-19. If the Petition is instituted,

1. Sood [EX1005]

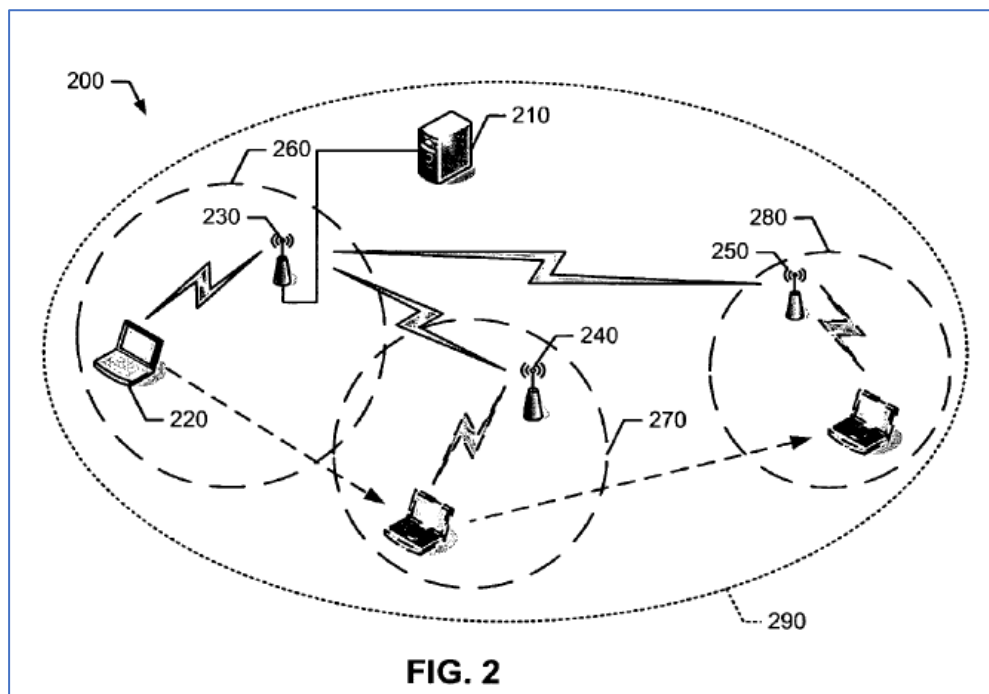
Petitioners' primary reference is U.S. Patent No. 7,787,627 to Sood et al. EX1005 (hereinafter, "Sood"). Sood is titled "Methods and Apparatus for Providing a Key Management System for Wireless Communication Networks." *Id.* It was filed on November 30, 2005, and issued on August 31, 2010. *Id.*

Sood generally relates to "methods and apparatus for providing a key management system for wireless communication networks." Sood at 1:8-11. More specifically, Sood discloses a key management system that operates in an 802.11 wireless environment with several different access points and coverage areas. EX2021 (Rubin Dec.) at ¶¶85-90, 109. When a mobile device moves between different coverage areas, Sood's key management system supports "fast roaming" handoff from one access point to another and does not require re-authenticating the mobile device with the Authentication Server using newly-generated authentication keys. *Id.*; Sood at 5:14-20, 6:36-50.

Sood Figure 2 illustrates the key management system 200. Sood at 4:14. It includes an authentication server 210 and three different access points 230, 240, and 250, each having its own coverage area 260, 270, and 280. *Id.* at 4:15-17, 19-22.

then Four Batons reserves the right to further address the deficiencies in Petitioners' theories, including deficiencies regarding the dependent claims.

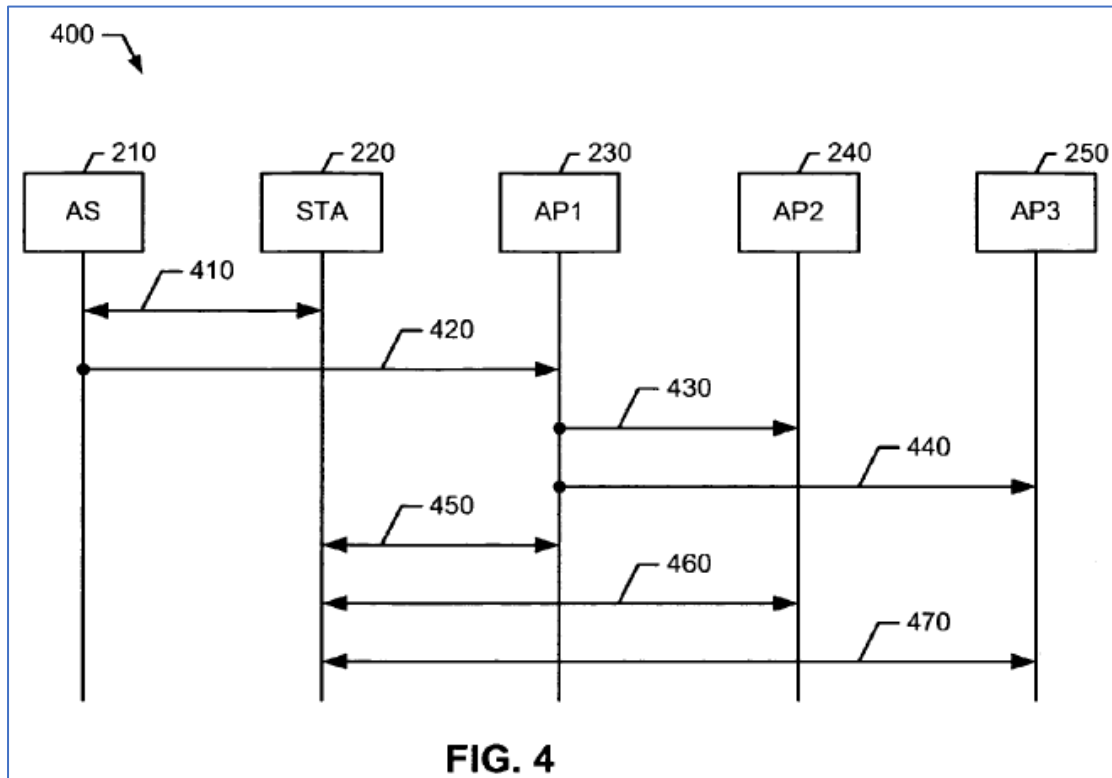
Each access point wirelessly communicates with the mobile stations in its coverage area, as well as the other access points in the other wireless networks, as depicted via the lightning bolts in the figure. *Id.* at 4:51-65. Notably, the mobile stations may roam between the different coverage areas, as depicted via the dashed arrows in the figure showing station 220 moving from coverage area 260 to coverage area 270 and then to coverage area 280. *Id.* at 4:20-22, 4:55-57.



Sood's invention is that "the key management system 200 may provide a key hierarchy so that the subscriber station 220 may avoid performing a full authentication process with the authentication server 210 when the subscriber station 220 roams from one coverage area to another within the mobility domain 290. In particular, the key management system 200 may optimize network resources and/or

reduce latency by providing a shared authentication key [] between the APs 230, 240, and 250 within the mobility domain 290.” *Id.* at 6:40-50.

Sood Figure 4 illustrates the operation of the key management system. Sood at 1:37-38.



In step 410, the authentication server 210 and the station 220 “communicate with each other to generate the [master authentication key] MSK.” *Id.* at 6:53-55. The authentication server then “generate[s] a first-level derived authentication key (e.g., PMK-R0) [that is] based on the MSK, a key derivation function (KDF), and concatenations of information elements[.]” *Id.* at 6:63-7:4. In step 420, the authentication server sends the first-level derived authentication key to access point 230, AP1. *Id.* at 7:64-67. AP1 then “generate[s] one or more second-level derived

authentication keys (e.g., PMK-R1-1, PMK-R1-2, PMK-R1-3, etc.)” that are “based on the first-level derived authentication key.” *Id.* at 8:3-6. “Each of the second-level derived authentication key[s] may be associated with an access point that may provide communication services to the subscriber station 220 when the subscriber station 220 may roam[.]” *Id.* at 8:6-9. For example, PMK-R1-1 is associated with AP1 230 and used when subscriber station 220 is in its network, PMK-R1-2 is associated with AP2 240 and used when subscriber station 220 is in its network, and PMK-R1-3 is associated with AP3 250 and used when subscriber station is in its network. *Id.* at 8:10-13. AP1 keeps its associated second-level derived authentication key, but forwards other second-level derived authentication keys to the respective AP2 and AP3 in steps 430-440. *Id.* at 8:17-20.

When subscriber station 220 wants to receive communication services in a wireless network, it initiates a session with the access point in that wireless network, e.g., AP1. *Sood* at 8:5-67. This includes using the second-level derived authentication key associated with AP1, PMK-R1-1, to establish full authentication between the two entities. *Id.* at 8:14-15. Then, the subscriber station 220 and AP1 each use the second-level derived authentication key PMK-R1-1 to generate a session key, PTK1, which may be a pairwise temporal key. *Id.* at 8:67-9:7. This session key PTK1 permits the subscriber station 220 to communicate with AP1, as shown in step 450. *Id.* at 9:7-9.

But if subscriber station 220 roams to another network, then that subscriber station and new AP will generate another session key using the second-level derived authentication key associated with that new AP. Sood at 9:10-35. For example, if the subscriber station roams to AP2's network, then the two entities will generate another session key (PTK2) using the second-level derived authentication key associated with AP2 (PMK-R1-2), as shown in step 460. *Id.* at 9:10-22. And if the subscriber station further roams to AP3's network, then those two entities will generate another session key (PTK3) using the second-level derived authentication key associated with AP3 (PMK-R1-3), as shown in step 470. *Id.* at 9:23-35.

Sood Figures 5-7 illustrate the contents of the first-level, second-level, and session keys, respectively. Sood at 1:39-46, 6:63-10:22.

2. Aboba [EX1006]

Petitioners' secondary reference is draft version 3 of the paper titled "Extensible Authentication Protocol (EAP) Key Management Framework" written by Aboba et al. EX1006 (hereinafter, "Aboba"); *see also* EX2021 (Rubin Dec.) at ¶¶91-98. Aboba is dated July 2004. *Id.* The '671 Patent incorporates by reference a later draft version 9 of Aboba, dated January 2006. '671 at 9:59-61, 10:3-5; EX2017 (Aboba v9). And the '671 Patent quotes extensively from an even later draft version 12 of Aboba, dated April 2006. '671 at 4:7-9:55; EX2018 (Aboba v12). Thus, the

Patent Office has largely considered the relevant aspects from Aboba while prosecuting the '671 Patent, and allowed the claims, nonetheless.

Petitioners rely on just one minor aspect of Aboba to challenge the '671 independent claims. Specifically, Petitioners rely on Aboba's general cite to the IEEE 802.11i standard and later statement that the authenticator "advertise[s] its name [] using a lower-layer mechanism like the 802.11 Beacon/Probe Response." Pet., 67 (citing Aboba at 11, 25). From this, Petitioners somehow infer that Aboba (unlike its primary Sood reference) teaches advertising parameters from an authenticator using an authenticator-suppliant protocol. *Id.* This is only relevant under a construction of the claimed "key binding blob" that requires "static parameters [to be] advertised from an authenticator **using an Authenticator-Suppliant Protocol (ASP)**." See '671 at 13:27-30 (emphasis added).

In this Preliminary Response, Patent Owner does not contend that the prior art fails to teach or suggest an authenticator that advertises parameters using an ASP; thus, Aboba is irrelevant at this stage.

3. Lee [EX1007]

Petitioners' tertiary reference is U.S. Published Patent Application No. 2004/0242228 to Lee et al. EX1007 (hereinafter, "Lee"); EX2021 (Rubin Dec.) at ¶¶99-105. Lee is titled "Method for Fast Roaming in a Wireless Network." *Id.* It was filed on January 8, 2004, and published on December 2, 2004. *Id.*

Petitioners cite just one small aspect of Lee to challenge one part of the ‘671 independent claims. Specifically, Petitioners cite Lee’s teaching that a “server” (as opposed to an authenticator, such as an access point) may centrally derive keys. Pet., 50. In this respect, Lee teaches “the servers generate PMKs for APs neighboring to a particular AP and transmits them to the neighbor APs.” Lee at ¶[0102]. This is only relevant to ‘671 claim 6, which requires “using an extensible authentication protocol server to cryptographically bind access network parameters to a channel binding key.” ‘671 at 17:35-37 (emphasis added).

In this Preliminary Response, Patent Owner does not contend that the prior art fails to teach or suggest using a server (as opposed to an authenticator) to cryptographically bind various elements; thus, Lee is irrelevant at this stage.

III. Legal Standards

An IPR should not be instituted unless Petitioners have shown a likelihood of success on the invalidity grounds presented in the petition. *See In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1381 (Fed. Cir. 2016) (“[T]he Board must base its decision on arguments that were advanced by a party, and to which the opposing party was given a chance to respond.”).

“In an IPR, the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (petitions must identify “with

particularity... the evidence that supports the grounds for the challenge to each claim”); 35 U.S.C. § 312(a)(3). This burden of persuasion never shifts to the patent owner. *See Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

“To satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.” *In re Magnum Oil Tools*, 829 F.3d at 1380. The obviousness inquiry requires considering whether one of skill in the art “would have been motivated to combine the prior art to achieve the claimed invention.” *In re NuVasive, Inc.*, 842 F.3d 1376, 1381 (Fed. Cir. 2016) (quoting *In re Warsaw Orthopedic, Inc.*, 832 F.3d 1327, 1333 (Fed. Cir. 2016)). “[T]he factual inquiry whether to combine references must be thorough and searching...” *Id.*

IV. Level of Ordinary Skill in the Art

For purposes of this Preliminary Response, Patent Owner has applied Petitioners’ recitation of the level of skill in the art, because even under Petitioners’ proposed level of skill, Petitioners have failed to demonstrate a reasonable likelihood of success. *See* Pet. at 11. Patent Owner reserves the right to propose its own definition of a person of ordinary skill in the art (“POSITA”) in the future, if necessary.

V. Claim Construction

Claims are construed according to *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). *See* 37 C.F.R. § 42.100(b). “Any prior claim construction determination concerning a term of the claim in a civil action...will be considered.”

Id.

In the parallel district court proceeding, the same parties agreed to the following constructions for the ‘671 Patent:

Claim Language	Agreed Construction
“channel binding key” (’671 Patent, claims 1, 6, 10, 11, 18, 19)	“a key that is derived from a Channel Binding Master Key and cryptographically bound to a Key Binding Blob using a Key Derivation Function”
“channel binding master key” (’671 Patent, claims 1, 6, 8, 11, 18)	“a key from which a Channel Binding Key is derived using a Key Derivation Function”
“key binding blob” (’671 Patent, claims 1, 6, 8, 11, 18)	“an octet-string that is constructed from static parameters advertised from an authenticator using an Authenticator-Supplicant Protocol”
“authenticator” (’671 Patent, claims 1, 3, 4, 7, 10, 11, 19)	“a network-side entity that uses a Channel Binding Key for an Authenticator-Supplicant Protocol”
“supplicant” / “mobile supplicant” (’671 Patent, claims 1, 3, 8, 10)	“a user-side entity that uses a Channel Binding Key for an Authenticator-Supplicant Protocol”

“authenticator-suppliant protocol” (’671 Patent, claims 7, 8, 10)	“a protocol that is executed between a supplicant and an authenticator and uses a Channel Binding Key for protecting the protocol”
“[deriving a / derive said] channel binding key from a channel binding master key bound to a key binding blob using a key derivation function” (’671 Patent, claims 1, 6)	“[deriving a / derive said] channel binding key from a channel binding master key and binding the channel binding key to a key binding blob using a key derivation function”
“said parameters” (’671 Patent, claims 3, 4)	“said access network parameters”
“said supplicant using the channel binding master key for protecting an authenticator-suppliant protocol” (’671 Patent, claim 8)	Plain and ordinary meaning

EX2019 (P.R. 4-3) at 2. For purposes of this Preliminary Response, Patent Owner submits that the Board should adopt the agreed constructions.³

In the parallel district court litigation, the parties dispute the constructions of the following terms from the ‘671 Patent:

Claim Language	Patent Owner Construction	Petitioners Construction
“server” (’671 Patent, claim 10)	Plain and ordinary meaning	“An entity that creates a CBK and transfers it to the authenticator. A server is a

³ Patent Owner reserves the right to propose additional constructions in the event the Petition is instituted.

		creator as well as a sender of the CBK.”
“EAP methods” (’671 Patent, claim 2)	Plain and ordinary meaning	“the authentication algorithms described in RFC 3748”

EX2019 (P.R. 4-3) at 7-8, 16. The constructions of these disputed terms do not matter for purposes of this Preliminary Response, however, since Patent Owner is not distinguishing the prior art on the basis of these disputed terms.

VI. Arguments

The Petition should be denied for multiple independent reasons, as described below.

A. Grounds 1, 3-4: Petitioners’ Art Fails To Present A Reasonable Likelihood Of Prevailing Against Independent Claims 1 and 6

Grounds 1 and 3-4 challenge independent Claims 1 and 6 of the ‘671 Patent. Pet. at 2. Yet for each of those Grounds, which are all the same with respect to the arguments presented below, Petitioners have failed to demonstrate a reasonable likelihood of success of proving that any of Claims 1 and 6 are unpatentable. None of those Grounds show the prior art teaches or suggests three “missing” elements of the challenged independent claims:

- “cryptographically bind[ing] access network parameters to a [] key [] without [] needing to carry [the] parameters in [] authentication methods” (claims 1[a], 6[a(i), (iii)]);

- “deriv[ing a] channel binding key from a channel binding master key bound to a key binding blob using a key derivation function” (claims 1[b], 6[b]); and
- “wherein said key binding blob is a string that is constructed from static parameters advertised from [an] authenticator” (claims 1[c], 6[c]).

Accordingly, the Board should decline to institute the IPR.

1. Sood, whether alone or in combination with Aboba and/or Lee, does not teach or suggest “cryptographically bind[ing] access network parameters to a [] key [] without [] needing to carry [the] parameters in [] authentication methods” (claims 1[a], 6[a(i), (iii)])

Independent claims 1[a] and 6[a] each require “cryptographically bind[ing] access network parameters to a [] key [] without [] needing to carry [the] parameters in [] authentication methods.” ‘671 at 17:16-18, 17:35-44. The ‘671 Patent teaches that, in a preferred embodiment, this is done by “creat[ing] a binding between a key exported by, e.g., [an] EAP method and access network parameters.” *Id.* at 13:5-8. The ‘671 Patent distinguishes this aspect of the claims from prior systems, such as those disclosed in RFC3748, that “create[d] such a binding based on communicating the access network parameters over a protected channel of an EAP method.” *Id.* at 12:65-13:4.

The Petition relies solely on Sood to teach this claim element. Pet. at 21-23 (Ground 1), 55-58 (Ground 3), 68-71 (Ground 4). Specifically, the Petition alleges that “Sood’s method does not need to carry the access network parameters in

authentication methods” because Sood’s access network parameters “are advertised by the access point to the subscriber station in a ‘beacon.’” *Id.* at 22 (citing Sood at 7:10-20, 8:27-36). And according to Petitioners, advertising parameters in a beacon is not the prohibited by the claim because “advertising [] occurs pre-authentication.” *Id.* at 23.

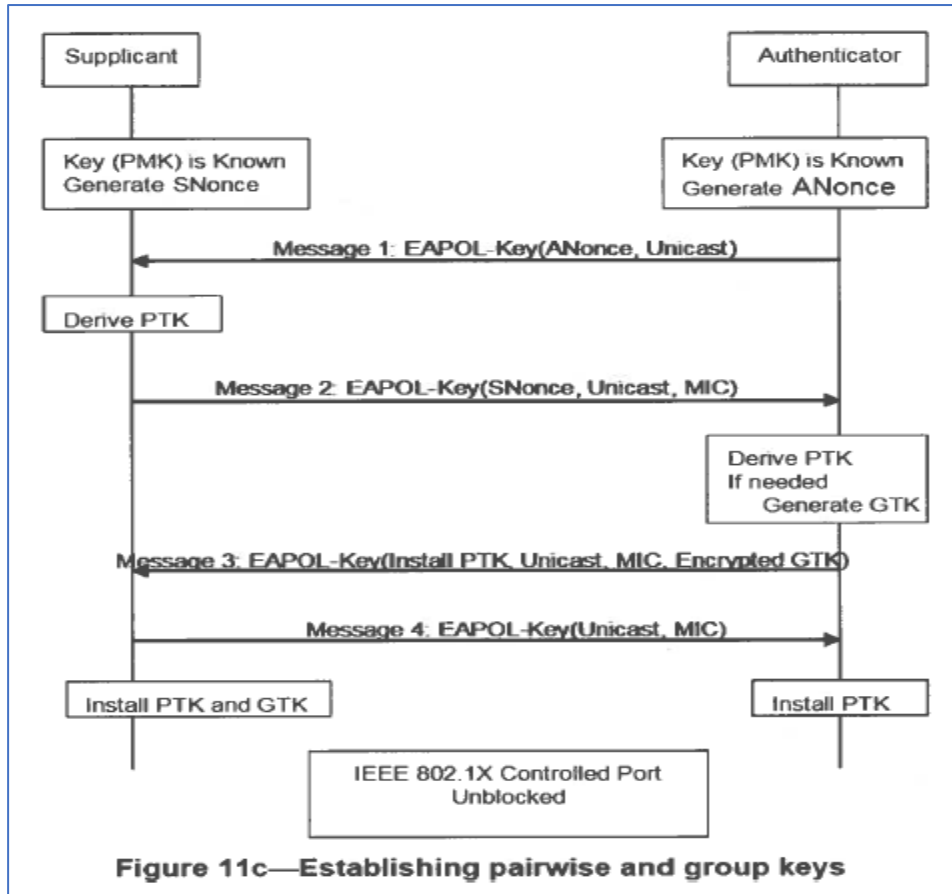
But although Sood advertises certain parameters via a pre-authentication beacon, Sood carries other access network parameters that are not cryptographically bound to any key—namely, the “AA” MAC Address of the Authenticator—during the 802.11 “four-way handshake” authentication method. EX2021 (Rubin Dec.) at ¶¶107-108. This is improper. As such, Sood does not disclose the portion of the claim that states “without [] needing to carry [the] parameters in [] authentication methods.” ‘671 at 17:17-18, 17:41-44.

Sood’s described embodiments use the 802.11 WLAN standard. EX2021 (Rubin Dec.) at ¶¶85-90, 109. Sood mentions “802.11” or “WLAN” at least twenty-one times. *See generally* Sood. Sood Figures 2 and 4 illustrate traditional 802.11 WLAN networks with AP access points and STA stations. *Id.* at Figs. 2, 4. And the particular network parameters in Sood that Petitioners rely on—NAS-ID and BSS-ID—are specific to the 802.11 WLAN standard. EX2021 (Rubin Dec.) at ¶109; EX2020 (802.11-1999) at 21 (“The BSSID field is a 48-bit field of the same format as an IEEE 802 MAC address”); EX2022 (802.11r) at 21 (defining the NAS-ID

parameters, R0KH-ID and R1KH-ID, as “an identifier that names the holder of the [derived key] in the Authenticator”); *see also id.* at 24-25. Accordingly, Sood is steeped in the 802.11 WLAN standard.⁴

The 802.11 WLAN standard, specifically 802.11i, teaches that access network parameters are exchanged during the authentication method colloquially known as the “four-way handshake.” EX2021 (Rubin Dec.) at ¶¶114. 802.11i Figure 11(c) illustrates the four-way handshake, which includes four messages labeled “Message 1” to “Message 4”:

⁴ Sood pays lip service to other wireless standards. Sood at 2:65-3:7. But Sood’s disclosures are technically incompatible with these other wireless standards. As explained in more detail in the accompanying expert declaration, Sood relies on the EAP protocol framework for key derivation and establishing a secure communication channel, specifically what can be referred to as the “traditional EAP” defined in RFC 3748. EX2021 (Rubin Dec.) at ¶¶111, 66-71. While the EAP framework is used in cellular communications (3G, 4G, 5G), there are fundamental differences. *Id.* at ¶¶112-113. Because of such, Sood is limited in its application to 802.11 networks. *Id.*



EX1009 (IEEE802.11i) at 31. “Upon successful completion of the 4-Way Handshake, the Authenticator and Supplicant have authenticated each other.” *Id.* Thus, the 802.11i Four-Way handshake is part of an authentication method. EX2021 (Rubin Dec.) at ¶¶114-115.

Importantly, Message 1 of the four-way handshake “identifies AA as the peer STA to the Supplicant’s STA.” EX1009 (IEEE802.11i) at 107 (emphasis added). And “AA” is defined as “the IEEE 802.11X Authenticator [] MAC address.” *Id.* at 18. When sent as part of Message 1, that “AA” authenticator address is not

cryptographically bound to a key. Instead, the “AA” is later used to derive the PTK Pairwise Transient Key according to this formula:

The PTK derivation step

$$\text{PTK} \leftarrow \text{PRF-X}(\text{PMK}, \text{“Pairwise key expansion”} \parallel \text{Min}(\text{AA}, \text{SPA}) \parallel \text{Max}(\text{AA}, \text{SPA}) \parallel \text{Min}(\text{ANonce}, \text{SNonce}) \parallel \text{Max}(\text{ANonce}, \text{SNonce}))$$

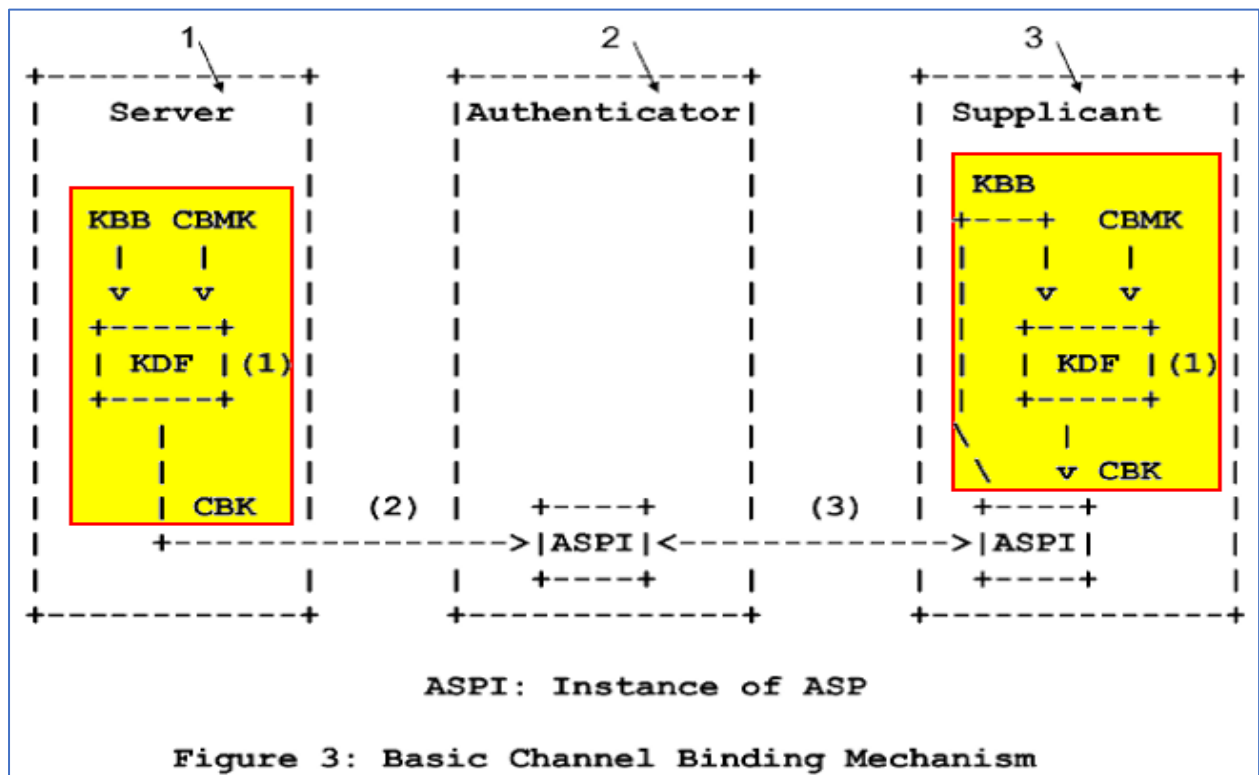
Id. at 106 (highlighting added). This is further explained by Four Baton’s expert, Dr. Aviel Rubin. EX2021 (Rubin Dec.) at ¶¶116-122.

Thus, “AA” is an access network parameter that is carried, unbound to any key, as part of the four-way handshake authentication method. This violates the ‘671 independent claims, which recite “cryptographically bind[ing] access network parameters to a [] key [] without [] needing to carry [the] parameters in [] authentication methods.” ‘671 at 17:16-18, 17:35-44.

2. Sood, whether alone or in combination with Aboba and/or Lee, does not teach or suggest “deriv[ing a] channel binding key from a channel binding master key bound to a key binding blob using a key derivation function” (claims 1[b], 6[b])

Independent claims 1[b] and 6[b] each require “deriv[ing a] channel binding key from a channel binding master key bound to a key binding blob using a key derivation function.” ‘671 at 17:19-21, 17:45-48. The parties agree that this claim language means: “[deriving a / derive said] channel binding key from a channel binding master key and binding the channel binding key to a key binding blob using a key derivation function.” EX2019 (P.R. 4-3) at 2.

The '671 Patent teaches that, in a preferred embodiment, “the [channel binding key] CBK is derived from a [channel binding master key] CBMK and bound to a [key binding blob] KBB associated with the authenticator using a [key derivation function] KDF.” ‘671 at 13:66-14:2. The ‘671 Patent further explains that, in a preferred embodiment, a [channel binding key] CBK can be computed using [a] pseudo random function (prf+) defined in IKEv2 [RFC4306] in the following way: $CBK = kdf+(CBMK, KBB)$; wherein KDF = Key Derivation Function.” *Id.* at 14:59-64. And the highlighted portions of Figure 3 illustrate a preferred embodiment where both the KBB and the CBM are input into a single KDF, and the CBK is the output of the KDF:



Id. at Fig. 3 (highlighting added).

The Petition relies solely on Sood to teach this claim element. Pet. at 23-32 (Ground 1), 58-59 (Ground 3), 66 (Ground 4). Specifically, the Petition maps Sood to the claim language in three alternative ways—none of which pass muster. EX2021 (Rubin Dec.) at ¶¶124-140. As explained below, none of those three mappings show one instance of Sood’s KDF-256 “key derivation function” binding Sood’s MSK “channel binding master key” to Sood’s “channel binding key.” *Id.*

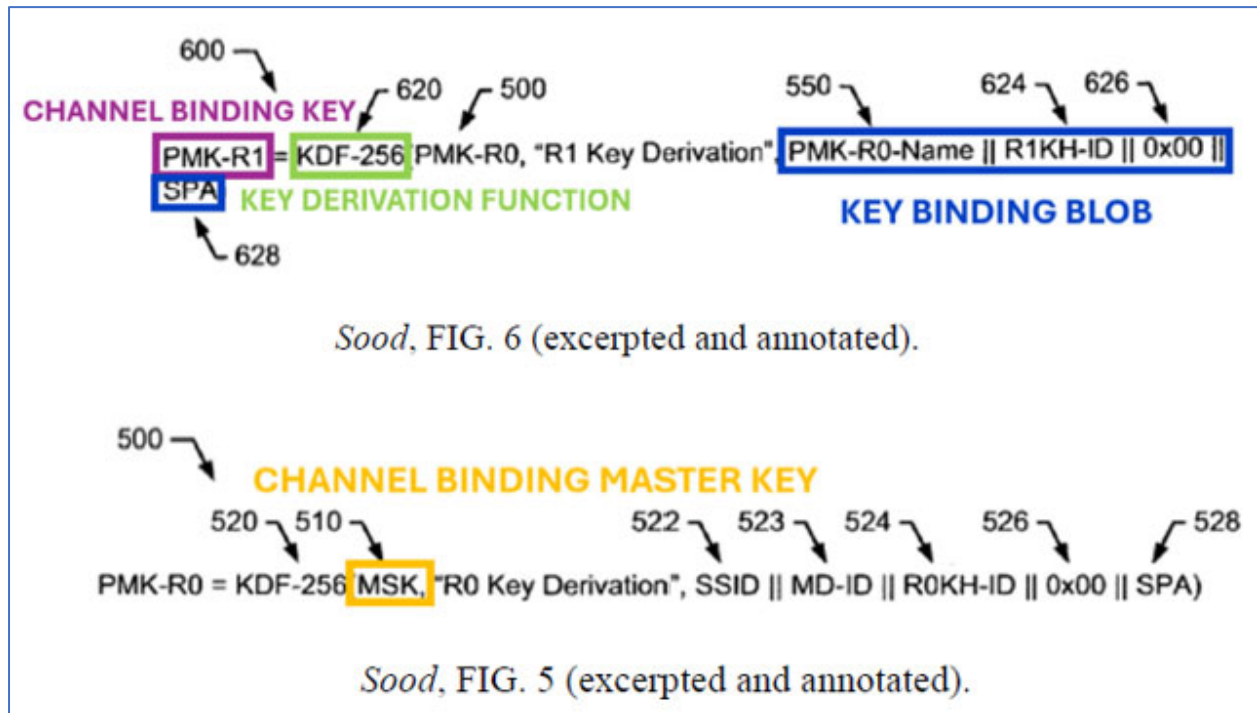
a) Petitioners’ First Claim Mapping Fails

In this first mapping (based on Sood Figures 5 and 6):

- the claimed “channel binding key” is Sood’s second-level derived authentication key 600 (PMK-R1), shown in Figure 6;
- the claimed “channel binding master key” is Sood’s master secret key 510 (MSK), shown in Figure 5;
- the claimed “key binding blob” is Sood’s concatenation of (i) the name of the first-level derived authentication key 550 (PMK-R0-Name) with (ii) the NAS identifier field 624 containing the IP address of the network entity holding the second-level derived authentication key (R1KH-ID), (iii) the separator field 626 used to prevent sliding window or perimeter attacks (0x00), and (iv) the sender protocol address 628 containing the MAC address of the subscriber station (SPA), shown in Figure 6; and

- the claimed “key derivation function” is a particular instance of the 256-bit key derivation function 620 (KDF-256), shown in Figure 6.

Pet. at 24. The following annotated figures from the Petition illustrate this first mapping:



Id. (annotations in Petition).

This first mapping does not satisfy the claim language. The alleged key derivation function (in green) is not used to derive the alleged channel binding key (in purple) from the alleged channel binding master key (in yellow), as claimed. EX2021 (Rubin Dec.) at ¶130. Rather, Sood Figure 6 shows, at most, the alleged key derivation function (in green) being used to derive the alleged channel binding key (in purple) from a first-level derived authentication key 550, PMK-R0. *Id.* But

Sood does not teach that first-level derived authentication key 550 is the claimed “channel binding master key.” *Id.* Rather, Sood teaches that its “channel binding master key” is master secret key/master authentication key MSK 510. *Id.*; Sood at 6:51-56; *c.f.* ‘671 at 13:25 (“an MSK [] is a CBMK”). Sood’s MSK 510 is generated when the authentication server 210 and the subscriber station communicate with each other as part of the authentication step 410. Sood at 6:51-56. And this MSK 510 may be used to generate a first-level derived authentication key (e.g., PMK-R0), as shown in Figure 5. *Id.* at 6:56-66. But Sood Figure 6 does not teach or suggest using the alleged key derivation function (in green) to derive the alleged channel binding key (in purple) from MSK 510 (what Sood teaches is its channel binding “master” key); MSK 510 is not part of the Figure 6 equation. EX2021 (Rubin Dec.) at ¶130.

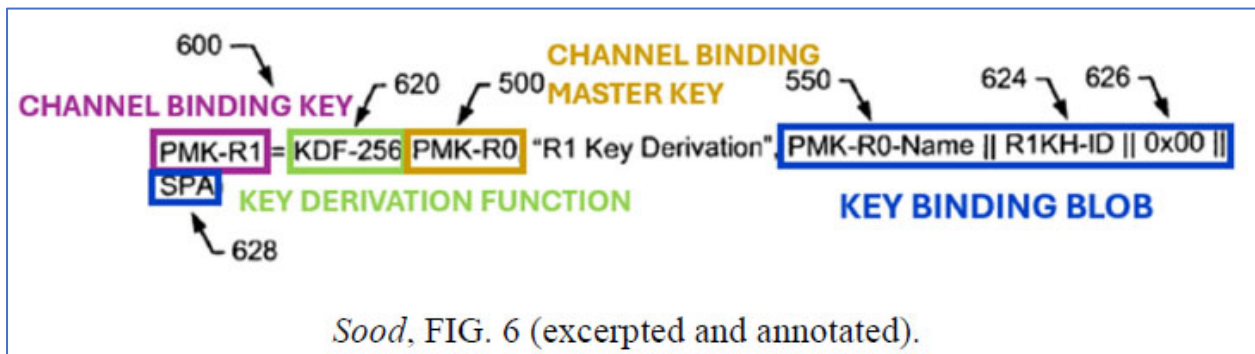
b) Petitioners’ Second Claim Mapping Fails

In this second mapping (based on Sood Figure 6 alone):

- the claimed “channel binding key” is Sood’s second-level derived authentication key 600 (PMK-R1), shown in Figure 6;
- the claimed “channel binding master key” is Sood’s first-level derived authentication key 500 (PMK-R0), shown in Figure 6;
- the claimed “key binding blob” is Sood’s concatenation of (i) the name of the first-level derived authentication key 550 (PMK-R0-Name) with (ii)

- the NAS identifier field 624 containing the IP address of the network entity holding the second-level derived authentication key (R1KH-ID), (iii) the separator field 626 used to prevent sliding window or perimeter attacks (0x00), and (iv) the sender protocol address 628 containing the MAC address of the subscriber station (SPA), shown in Figure 6; and
- the claimed “key derivation function” is a particular instance of the 256-bit key derivation function 620 (KDF-256), shown in Figure 6.

Pet. at 24-25. The following annotated figures from the Petition illustrate this second mapping:



Id. (annotations in Petition).

This second mapping does not satisfy the claim language, either. As discussed above, Sood does not teach that the first-level derived authentication key 500 (PMK-R0) is the claimed “channel binding master key.” EX2021 (Rubin Dec.) at ¶134. Rather, Sood teaches that its “channel binding master key” is the master secret key/master authentication key MSK 510. *Id.*; Sood at 6:51-56; *c.f.* ‘671 at 13:25 (“an

MSK [] is a CBMK”). Sood’s MSK 510 is generated when the authentication server 210 and the subscriber station communicate with each other as part of the authentication step 410. Sood at 6:51-56. And this MSK 510 may be used to generate a first-level derived authentication key (e.g., PMK-R0), as shown in Figure 5. *Id.* at 6:56-66. But MSK 510 is not part of the Figure 6 equation that is central to Petitioners’ second mapping. Accordingly, Petitioners’ second mapping from Fig. 6 does not show deriving a channel binding key from a “channel binding master key,” as required by the claims. EX2021 (Rubin Dec.) at ¶134.

c) Petitioners’ Third Claim Mapping Fails

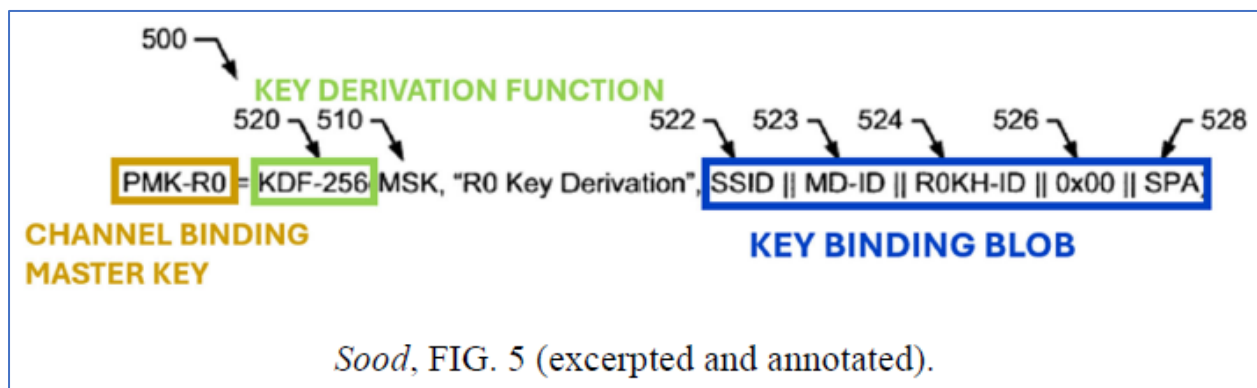
In this third mapping (based on Sood Figure 5 alone):

- there is no claimed “channel binding key”;
- the claimed “channel binding master key” is Sood’s first-level derived authentication key 500 (PMK-R0), shown in Figure 5;
- the claimed “key binding blob” is Sood’s concatenation of (i) the service set identifier field 522 (SSID) with (ii) the mobility domain identifier field 523 (MD-ID), (iii) the NAS identifier field 524 containing the IP address of the network entity holding the first-level derived authentication key (R0KH-ID), (iv) the separator field 526 used to prevent sliding window or perimeter attacks (0x00), and (iv) the sender protocol address 528

containing the MAC address of the subscriber station (SPA), shown in Figure 5; and

- the claimed “key derivation function” is a particular instance of the 256-bit key derivation function 520 (KDF-256), shown in Figure 5.

Pet. at 31-32. The following annotated figures from the Petition illustrate this third mapping:



Id. (annotations in Petition).

This third mapping also does not satisfy the claim language for at least two reasons. First, it is based on an erroneous claim construction. For this third mapping, the Petitioners assume that “this claim element requires that the key binding blob be bound to the channel binding master key.” Pet. at 30 (emphasis added). But the Parties agree this claim language requires the key binding blob to be bound to the channel binding key (and not the channel binding master key). EX2019 (P.R. 4-3) at 2 (construing this term as “[deriving a / derive said] channel binding key from a channel binding master key and binding the channel binding key to a key binding

blob using a key derivation function”). Accordingly, this third mapping fails because it does not apply the agreed claim construction.

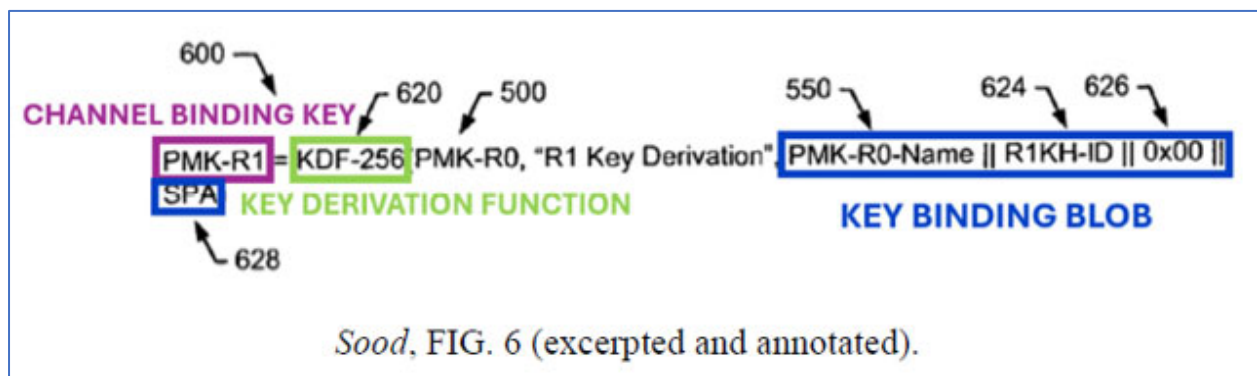
Second, this mapping does not include a “channel binding key.” Pet. at 30-32. Yet the claim language clearly requires “deriv[ing a] channel binding key.” ‘671 at 17:19, 17:46. So this third mapping fails because it does not satisfy all the claim elements, including explaining how Sood derives a channel binding key. EX2021 (Rubin Dec.) at ¶¶138-140.

3. Sood, whether alone or in combination with Aboba and/or Lee, does not teach or suggest “wherein said key binding blob is a string that is constructed from static parameters advertised from [an] authenticator” (claims 1[c], 6[c])

Independent claims 1[c] and 6[c] each require “wherein said key binding blob is a string that is constructed from static parameters advertised from [an] authenticator.” ‘671 at 17:22-23, 17:49-51. The ‘671 Patent teaches that, in a preferred embodiment, the access network parameters are “advertised by an authenticator to the supplicant.” *Id.* at 10:17-19. Those access network parameters include static parameters, such as “the identity of the authenticator.” *Id.* at 10:19-20. Further, the authenticator-supplicant protocol ASP (*e.g.*, 802.11i) “define[s] how a KBB is constructed.” *Id.* at 15:53-56.

The Petition relies solely on Sood to teach this claim element. Pet. at 32 (Ground 1), 59 (Ground 3), 66 (Ground 4). Specifically, the Petition cursorily alleges this element “is taught by Sood for the same reasons discussed [for] Element 1[b].”

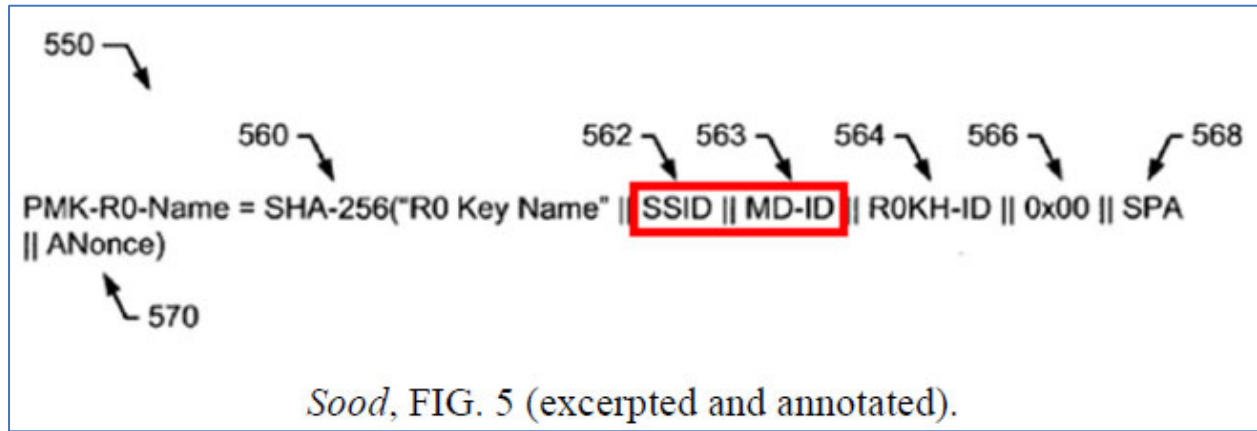
Id. at 32. And for Element 1[b], the Petition maps the claimed “key binding blob” to Sood’s concatenation of four parameters: (1) the name of the first-level derived authentication key 550 (PMK-R0-Name) with (2) the NAS identifier field 624 containing the IP address of the network entity holding the second-level derived authentication key (R1KH-ID), (3) the separator field 626 used to prevent sliding window or perimeter attacks (0x00), and (4) the sender protocol address 628 containing the MAC address of the subscriber station (SPA), as shown in blue in this annotated Figure 6:



Pet. at 24; *see also id.* at 25 (“the concatenation of PMK-R0-Name, R1KH-ID, 0x00, and SPA [is] together the ‘key binding blob’ as shown in figure 6”).

Yet the Petition only explains why two of those four parameters are “static parameters advertised from [an] authenticator,” as required by the ‘671 claims. With respect to the first parameter—“PMK-R0-Name” 550, the name of the first-level derived authentication key—Petitioners allege that it satisfies the claim language because PMK-R0-Name is constructed using SSID and MD-ID, each of which is

itself allegedly a static parameter advertised from an authenticator, as shown in annotated Figure 5:



Pet. at 26-29.

And with respect to the second parameter—“R1KH-ID” 624, the NAS identifier field containing the IP address of the network entity holding the second-level derived authentication key—Petitioner alleges that it satisfies the claim language because the access point advertises R1KH-ID as a beacon and R1KH-ID is the unchanging name of a network entity. *Id.* at 28.

However, Petitioners never address why the third and fourth parameters in Sood’s alleged “key binding blob”—namely, (3) “0x00” 626, the separator field used to prevent sliding window or perimeter attacks and (4) “SPA” 628, the sender protocol address containing the MAC address of the subscriber station—are “static parameters advertised from [an] authenticator,” as per the ‘671 claims. *See* Pet. at 23-32, 59, 66-68; EX2021 (Rubin Dec.) at ¶¶144-147. This failure dooms the Petition because “the Board must base its decision on arguments that were advanced

by a party, and to which the opposing party was given a chance to respond.” *In re Magnum Oil Tools*, 829 F.3d at 1381. The Board is not “free to adopt arguments on behalf of petitioners that could have been, but were not, raised by the petitioner.” *Id.* at 1380-81. Arguments that are not “particularly” asserted in a petition are not to be given any weight. *See Microsoft Corp. v. FG SRC, LLC*, 860 F. App’x 708, 713 (Fed. Cir. 2021).

There is good reason why Petitioners do not address the third and fourth parameters in Sood’s alleged “key binding blob.” EX2021 (Rubin Dec.) at ¶¶145-146. Sood teaches that the third parameter, separator field 626, includes “a value added after variable length fields to prevent sliding window or parameter attacks on the KDF 620.” Sood at 8:37-39. For example, “the separator field 626 may include a value within a range from 0x00 to 0x7F.” *Id.* at 8:39-41. But Sood never says where this separator value comes from. Accordingly, Petitioners have not met their burden to prove that the third parameter is a “static parameter[] advertised from [an] authenticator,” as claimed.

Similarly, Petitioners have not shown that the fourth parameter, sender protocol address field 628, satisfies the claim language. Sood merely teaches that the sender protocol address field 628 “may include the MAC address or other suitable address of the subscriber station 220.” Sood at 8:41-42. Neither Sood nor the Petition

explain why SPA 628 is the claimed “static parameter[] advertised from an authenticator.”

B. Grounds 1-4: Petitioners’ Art Fails To Present A Reasonable Likelihood Of Prevailing Against The Dependent Claims

Grounds 1-4 challenge the dependent claims of the ‘671 Patent. Pet. at 2. However, because Petitioners failed to present a reasonable likelihood of success of invalidating any independent claims (*see supra*), their challenges to the dependent claims necessarily fail as well.

VII. Conclusion

Four Batons respectfully requests that the Board refuse to institute *inter partes* review for the reasons stated herein.

Dated: June 23, 2025

Respectfully submitted,

By: /Michael F. Heim/
Michael F. Heim (Reg. No. 32,702)
Attorney for Patent Owner
Four Batons Wireless, LLC

CERTIFICATE OF SERVICE

The undersigned certifies that pursuant to 37 C.F.R. § 42.6(e), a copy of the foregoing Patent Owner’s Preliminary Response was served via email to lead and backup counsel of record for Petitioners as follows:

Lead Counsel	Back-Up Counsel
Ali R. Sharifahmadian (No. 48,202) Arnold & Porter Kaye Scholer LLP 601 Massachusetts Ave., NW Washington, DC 20001-3743 Phone: (202) 942-5000 Fax: (202) 942-5999 ali.sharifahmadian@arnoldporter.com	Jeffrey Miller (No. 35,287) David Caine (No. 52,683) Arnold & Porter Kaye Scholer LLP 3000 El Camino Real Five Palo Alto Square, Suite 500 Palo Alto, CA 94306-3807 Phone: (650) 319-4500 Fax: (650) 319-4700 jeffrey.miller@arnoldporter.com david.caine@arnoldporter.com
Service Email: xSamsungFourBatonsAP@arnoldporter.com	

Dated: June 23, 2025

Respectfully submitted,
By: /Michael F. Heim/
Michael F. Heim (Reg. No. 32,702)
Attorney for Patent Owner
Four Batons Wireless, LLC

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24(d), the undersigned hereby certifies that this brief complies with the type-volume limitation of 37 C.F.R. § 42.24 because this brief contains 7,449 words as calculated by Microsoft Word, excluding the items exempted under 37 C.F.R. § 42.24.

Dated: June 23, 2025

Respectfully submitted,
By: /Michael F. Heim/
Michael F. Heim (Reg. No. 32,702)
Attorney for Patent Owner
Four Batons Wireless, LLC