

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MEDIATEK INC.,
Petitioner,

v.

DAEDALUS PRIME LLC,
Patent Owner.

IPR2025-00100
Patent 9,887,838 B2

Before THOMAS L. GIANNETTI, GREGG I. ANDERSON, and
ARTHUR M. PESLAK, *Administrative Patent Judges*.

GIANNETTI, *Administrative Patent Judge*.

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

I. INTRODUCTION

MediaTek Inc. (Petitioner) filed a Petition (Paper 1, “Pet.”) requesting *inter partes* review of claims 1–24 (the “challenged claims”) of U.S. Patent No. 9,887,838 B2 (Ex. 1001, the “’838 patent”). Pet. 1. Daedalus Prime LLC (Patent Owner) filed a Preliminary Response (Paper 6, “Prelim. Resp.”).

We have authority to determine whether to institute an *inter partes* review. 35 U.S.C. § 314 (2018); 37 C.F.R. § 42.4(a) (2023). The standard for instituting *inter partes* review is set forth in 35 U.S.C. § 314(a), which provides that *inter partes* review may not be instituted unless “there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.”

However, institution of *inter partes* review is discretionary. *See Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1367 (Fed. Cir. 2016) (“[T]he PTO is permitted, but never compelled, to institute an IPR proceeding.”). Patent Owner requested the Board to exercise its discretion under 35 U.S.C. § 314(a) to deny the Petition in light of pending parallel district court litigation. Prelim. Resp. 1–10. Subsequently, with Board authorization, the parties filed additional briefing directed to this request. *See* Paper 7 (“Prelim. Reply”); Paper 9 (“Prelim. Sur-reply”).

For the reasons provided below, we determine, based on the record before us, there is a reasonable likelihood Petitioner would prevail in showing at least one of the challenged claims is unpatentable. Furthermore, we deny Patent Owner’s request that we exercise our discretion to deny institution in this proceeding under 35 U.S.C. § 314(a). We therefore institute *inter partes* review on all challenged claims and all grounds. *See*

SAS Inst. Inc. v. Iancu, 584 U.S. 357 (2018); 37 C.F.R. § 42.108(a) (“When instituting . . . review, the Board will authorize the review to proceed on all of the challenged claims and on all grounds of unpatentability asserted for each claim.”).

II. BACKGROUND

A. Related Proceedings

The parties identify the following current and past district court proceedings involving the ’838 patent: *Daedalus Prime LLC v. MediaTek Inc.*, No. 2:24-cv-00235 (E.D. Tex.) (pending); *Daedalus Prime LLC v. Samsung Electronics Co., Ltd. et al.*, No. 2:22-cv-00354 (E.D. Tex.) (terminated). Pet. 100; Paper 3, 2.

The parties also identify the following terminated USPTO proceeding involving the ’838 patent: *Samsung Electronics Co., Ltd. et al v. Daedalus Prime LLC*, IPR2023-00727 (PTAB). Pet. 100; Paper 3, 2.

B. Real Parties-in-Interest

Petitioner names itself as the real party-in-interest. Pet. 100. Patent Owner names itself as the real party-in-interest. Paper 3, 2.

C. The ’838 Patent

The ’838 patent is titled “Method and Device for Secure Communications over a Network Using a Hardware Security Engine.” Ex. 1001, code (54). The patent describes a method, device, and system for establishing a secure communication session with a server that “includes initiating a request for a secure communication session such as a Secure

Sockets Layer (SSL) communication session with a server.” *Id.* at code (57).

According to the ’838 patent, the SSL protocol and the related Transport Layer Security (TLS) protocol are “used for many different types of secure communication sessions including, for example, secure web-browsing, ecommerce, secure upgrades, and other secure communication sessions between two computing devices on an untrusted network such as the Internet.” *Id.* at 1:10–17. The ’838 patent also describes that some computing and electronic devices use system-on-a-chip (SOC) designs “due to their relatively small footprint,” where “SOC devices are integrated circuits that incorporate various components, in addition to the processing core, of electronic systems on a single die.” *Id.* at 1:25–29.

The ’838 patent discloses “a system for establishing a secure communication session between a client device having a system-on-a-chip (SOC) and a server over a network.” Ex. 1001, 1:45–48. This is illustrated by Figure 1 of the ’838 patent reproduced below.

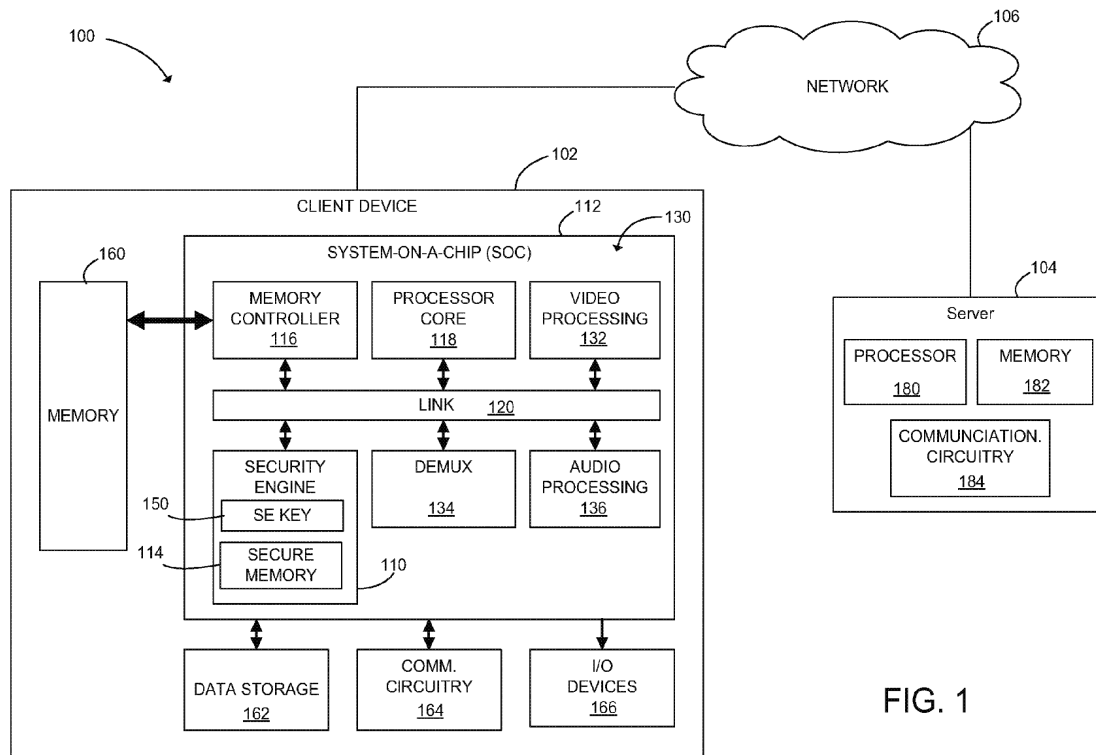


FIG. 1

In Figure 1, “client device 102 initiates a request for a secure communication session with the server 104 over the network 106.” *Id.* at 3:26–28. “To establish the secure communication session, the client device 102 and the server 104 perform a cryptographic key exchange, such as a Diffie-Hellman or a Rivest-Shamir-Adleman (RSA) key exchange, to generate a secret symmetric session key,” which “may then be used to encrypt and decrypt messages between the client device 102 and the server 104.” *Id.* at 3:28–35.

In Figure 1, “SOC 112 includes the security engine 110, a memory controller 116, a processor core 118, and a plurality of hardware peripherals 130, which are communicatively coupled to each other via a link 120.” *Ex.* 1001, 3:63–67. According to the ’838 patent, “[t]o ensure a secure communication session, the various keys and other cryptographic functions generated by the client device 102 are done so within a security engine 110

of a system-on-a chip (SOC) 112 of the client device 102.” *Id.* at 3:35–39. “The security engine 110 may be embodied as a security co-processor or processing circuitry separate from the processor core 118.” *Id.* at 4:17–19. According to the ’838 patent, the security engine 110 stores the security key 150, which may be “provisioned during the manufacturing of the SOC 112, but may be generated by the SOC 112 during operation in other embodiments.” *Id.* at 4:21–27.

D. Illustrative Claim

The Petition challenges claims 1–24 of the ’838 patent. Pet. 1. Claims 1, 9, and 17 are independent. Claim 1 is illustrative of the claimed subject matter and is reproduced below.¹

1. [1p] A system-on-a-chip apparatus comprising:
 - [1a-1] a system-on-a-chip comprising a security engine that is separate from a processor core of the system-on-a-chip and
 - [1a-2] has a secure memory accessible only by the security engine,
 - [1a-3] wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip,
- [1b] the security engine to:
 - generate a random nonce for initiating a request for a secure communication session with a remote server over a network using the nonce;

¹ For consistency, we rely on Petitioner’s bracketing annotations referencing particular claim 1 limitations. *See* Pet. viii.

[1c] perform a cryptographic key exchange with the remote server;

[1d] generate a symmetric session key, based on the cryptographic key exchange, to encrypt messages sent to the remote server and decrypt messages received from the remote server during the secure communication session;

[1e] encrypt the symmetric session key based on the security key; and

[1f] store the encrypted session key in the secure memory,

[1g] the system-on-a-chip to establish the secure communication session with the remote server over the network using the session key.

Ex. 1001, 11:57–12:13.

E. Prior Art and Other Evidence

The Petition relies on the following references:

Name	Reference	Publication/Issue Date	Exhibit(s)
Bugiel	“TruWalletM: Secure Web Authentication on Mobile Platforms,” Second Intl. Conf. on Trusted Systems (INTRUST 2010) (Dec. 13–15, 2010), 219–236	2011	Ex. 1002
Chou	US 2011/0191599 A1	Aug. 4, 2011	Ex. 1003
Tkacik	US 2010/0296651 A1	Nov. 25, 2010	Ex. 1005
TLS-1.2	The Transport Layer Security (TLS) Protocol Version 1.2, IETF Network Working Group RFC 5246	Aug. 2008	Ex. 1004

In addition, Petitioner submits a Declaration of Paul D. Martin, Ph.D. (Ex. 1013, “Martin Decl.”).

F. Asserted Grounds of Unpatentability

Petitioner asserts the challenged claims are unpatentable on the following grounds:

Claims Challenged	35 U.S.C. §²	References
1–24	103	Bugiel, Chou
1–24	103	Bugiel, Chou, Tkacik
1–24	103	Bugiel, Chou, TLS-1.2
1–24	103	Bugiel, Chou, TLS-1.2, Tkacik
1–24	103	Tkacik, TLS-1.2
1–24	103	Tkacik, TLS-1.2, Bugiel

See Pet. 1.

III. ANALYSIS OF THE CHALLENGED CLAIMS

A. Claim Construction

In an *inter partes* review proceeding, the Board applies the same claim construction standard as is applied in federal courts in a civil action

² Because the earliest application from which the ’838 patent claims priority was filed before March 16, 2013 (Ex. 1001, code (22)), the pre-AIA (“America Invents Act”) version of § 103 applies. Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 285–88 (2011).

under 35 U.S.C. § 282(b), which is generally referred to as the *Phillips* standard. *See* 37 C.F.R. § 42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). Under the *Phillips* standard, “words of a claim ‘are generally given their ordinary and customary meaning.’” *Phillips*, 415 F.3d at 1312.

We construe claim terms only as relevant to the parties’ contentions and only to the extent necessary to resolve the issues in dispute. *See Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999); *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

Neither party proposes claim constructions for our consideration. Petitioner asserts that “[g]iven the ’838 patent’s similarities to the prior art, no terms require construction here.” Pet. 4. Patent Owner does not dispute Petitioner’s position or discuss claim construction in the Preliminary Response.

B. Level of Ordinary Skill in the Art

Petitioner contends a person of ordinary skill in the art of the ’838 patent “would have had at least a bachelor’s degree in electrical engineering, computer science, computer engineer, or a similar field, and approximately two years of experience in a field related to cryptography and secure communications between network devices,” and that “[w]ork experience can substitute for formal education and additional formal education can substitute for work experience.” Pet. 3–4 (citing Martin Decl. ¶¶ 66–68). At this stage, Patent Owner does not respond to this contention.

For the purpose of this Decision, we adopt Petitioner’s definition of a person of ordinary skill in the art because it is consistent with the level of skill reflected by the ’838 patent specification and the asserted prior art.

C. Overview of the Principal Prior Art

1. Bugiel (Ex. 1002)

Bugiel is titled “TruWalletM: Secure Web Authentication on Mobile Platforms.” Ex. 1002, 11.³ According to Bugiel, TruWalletM is “a hardware-assisted wallet-based web authentication as a mechanism to protect user credentials from malware, phishing and physical attacks on mobile platforms.” Ex. 1002, 12. Bugiel’s design relies on “the availability of a Trusted Execution Environment (TrEE) to protect the execution of critical code from tampering.” *Id.* According to Bugiel, its “key design solution . . . is to split a single SSL/TLS connection between the user device and the server into two logically separated channels, where one is protected by TrEE and is used to transmit passwords, and another one is intended for conventional data.” *Id.*

Figure 1 of Bugiel, reproduced below, depicts TruWalletM’s architecture. Ex. 1002, 16.

³ Unless otherwise specified, page citations to exhibits use the page numbers assigned by the parties and not the original page numbers.

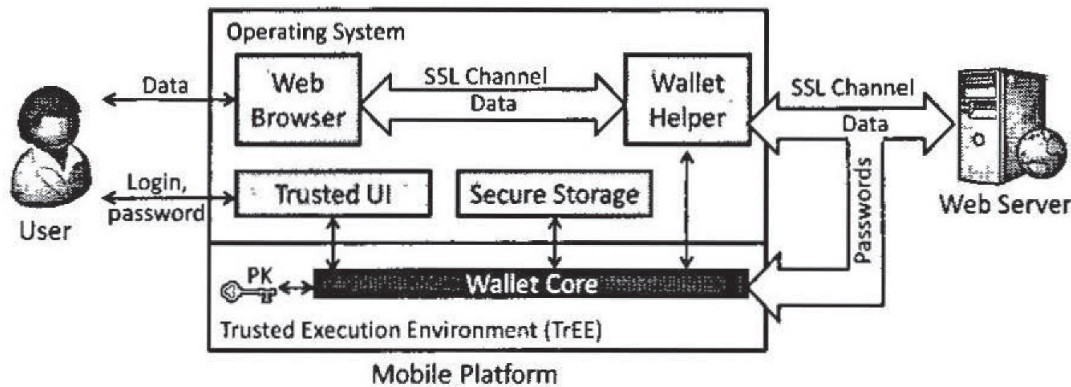


Fig. 1. TruWalletM Architecture

The architecture of TruWalletM is shown in Figure 1. Bugiel explains that “[t]he execution environment of a mobile platform is divided into two isolated parts: “open world” and the Tr EE. Ex. 1002, 15. According to Bugiel, “*TruWalletM* consists of two main components, WalletHelper (in open world) and WalletCore (in TrEE).” *Id.* Bugiel explains that “[t]he main work is done by WalletHelper (e.g., parsing pages), while WalletCore is only intermittently invoked to perform security-critical operations.” *Id.* “To prevent unauthorized credential usage by other users, the wallet requires user authentication (e.g., a user password) to login into the wallet.” *Id.* at 17. According to Bugiel, “[t]he authentication is done through TrustedUI.” *Id.* “In this way, passwords stored by the wallet are bound to the corresponding user.” *Id.*

2. Chou (Ex. 1003)

Chou is titled “Apparatus and Method for Providing Hardware Security.” Ex. 1003, code (54). Chou relates to “a hardware security module that provides a secure boundary for retention of a secure key within the secure boundary and prevention of unauthorized accesses from external

sources outside of the secure boundary to obtain the secure key.” *Id.* at code (57).

Figure 1 of Chou is reproduced below.

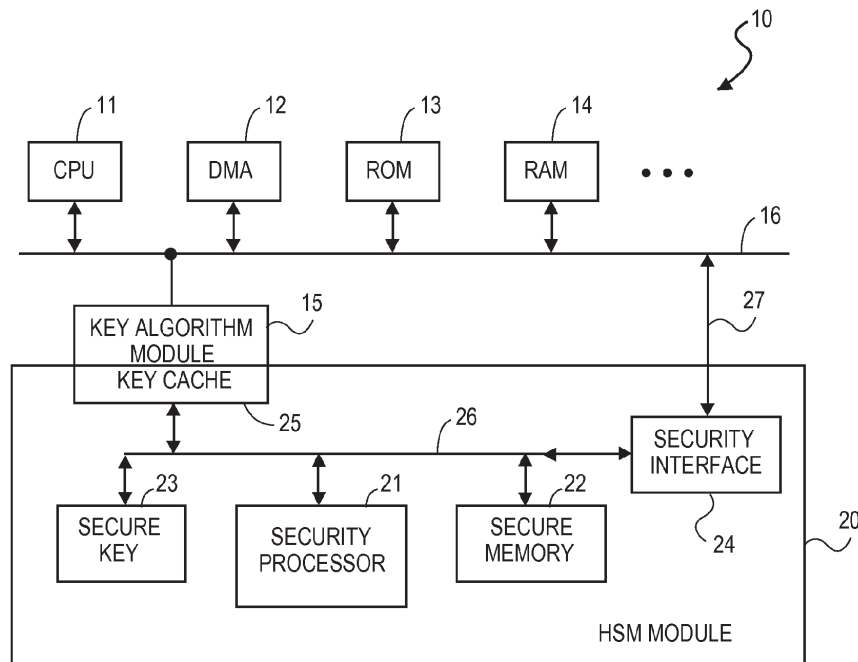


FIG. 1

Figure 1 depicts a device or system 10 incorporating a hardware security module (HSM) 20 to set a secure domain, zone, or boundary to protect a secure key. Ex. 1003 ¶¶ 12, 18. HSM 20 includes security processor 21, secure memory 22, secure key module 23, secure bus 26 and security interface 24. *Id.* ¶ 21. “Security processor 21 provides the various processing within HSM 20, including key authentication and the encrypting and/or decrypting operation to encrypt and/or decrypt data.” *Id.* Secure key module 23 is a storage medium for storing one or more key value(s) used by security processor 21 to encrypt and decrypt data. *Id.*

According to Chou, “all accesses to HSM 20 and data transfers into and out of HSM 20 are routed through security interface 24.” *Id.* ¶ 22. When encrypted data is received by device 10 and transferred to security interface 24, “a wrapped content key may be sent with the data and this wrapped content key, when unwrapped, is utilized to decrypt the data content.” *Id.* ¶ 23. “Security processor 21 may use a device unique key that is unique to the device to unwrap the content key.” *Id.* Chou explains that “since the unwrapping of secure keys is done solely within HSM and since the only route to internal hardware components of HSM 20 is through security interface 24, any unauthorized attempts from the non-secure domain to access an unwrapped key is prevented.” *Id.* ¶ 25.

3. *Tkacik (Ex. 1005)*

Tkacik is titled “Encryption Apparatus and Method Therefor.” Ex. 1005, code (54). According to Tkacik, “[d]evices concerned with data security may use a secure processing device, such as a secure microprocessor or the like, which includes physical and logical features to provide a secure execution environment (SEE).” *Id.* ¶ 4.

Figure 1 of Tkacik is reproduced below.

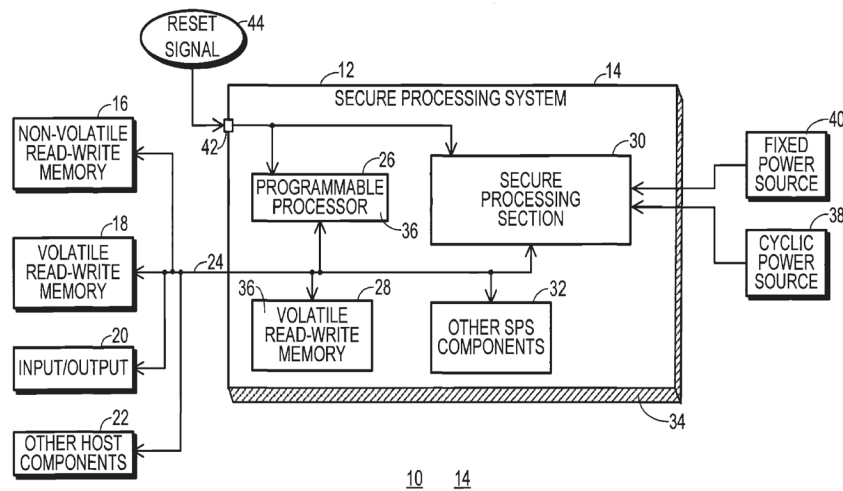


FIG. 1

Figure 1 depicts host device 10 using secure processing system 12 that performs data encryption and/or decryption operations. Ex. 1005 ¶ 20. Secure processing system 12 includes secure processing section 30 that provides a secure execution environment (SEE) for secure processing system 12 and host device 10. *Id.* ¶ 26.

According to Tkacik, secure processing section 30 includes “a long-lived, non-volatile key register 60,” which “desirably stores one or more plaintext master keys 160.” Ex. 1005 ¶ 44. Tkacik describes an embodiment in which “long-lived key register 60 is desirably programmed with plaintext master key 160 during the manufacturing process of secure processing system 12 and cannot thereafter be altered.” *Id.* ¶ 46.

4. TLS-1.2 (Ex. 1004)

TLS-1.2 “specifies Version 1.2 of the Transport Layer Security (TLS) protocol,” which “provides communications security over the Internet” and

“allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.” Ex. 1004, 1.

According to TLS-1.2, the TLS Handshake Protocol “allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data.” Ex. 1004, 4. According to the TLS Handshake Protocol, “[t]he peer’s identity can be authenticated using asymmetric, or public key, cryptography,” and “[t]he negotiation of a shared secret is secure” and “reliable.” *Id.*

D. Principles of Law

A claim is unpatentable under 35 U.S.C. § 103 if the differences between the claimed subject matter 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 the 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) if in evidence, so-called secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).⁴

⁴ At this stage, Patent Owner does not present evidence related to secondary considerations.

E. Bugiel Grounds

Petitioner contends that claims 1–24 would have been obvious over (1) Bugiel and Chou; (2) Bugiel, Chou, and Tkacik; (3) Bugiel, Chou, and TLS-1.2; and (4) Bugiel, Chou, TLS-1.2, and Tkacik (collectively, the “Bugiel Grounds”). *See* Pet. 1. Petitioner combines its analysis of these grounds in the Petition. *See id.* at 8–67. Petitioner supports its element-by-element analysis with testimony by Dr. Martin. Martin Decl. ¶¶ 73–277.

At this stage, Patent Owner does not directly address the merits of Petitioner’s element-by-element analysis. Patent Owner addresses the merits of the Petition more generally, and only in connection with its argument for discretionary denial under 35 U.S.C. § 314(a). *See* Prelim, Resp. 8–9. We discuss those arguments *infra*.

1. Motivation to Combine

Petitioner contends a person of ordinary skill would have combined Bugiel with Chou and with Chou and TLS-1.2. Pet. 8. Petitioner asserts that “[i]t would have been obvious to implement Bugiel’s system using Chou’s HSM 20.” *Id.* Petitioner explains, “[a person of ordinary skill] would have understood both Chou and Bugiel relate to secure communication using cryptographic keys for encryption and decryption.” *Id.* Dr. Martin testifies that “[g]iven the express teachings in Bugiel and the ubiquity of the SSL/TLS communication protocol, a [person of ordinary skill] would have been motivated to review the relevant SSL/TLS protocol for more details regarding how to implement the TLS Handshake Protocol

for generating cryptographic keys based on cryptographic key exchange.”
Martin Decl. ¶ 77.

He further testifies that a person of ordinary skill “would have understood that the SSL/TLS processes contemplated by Bugiel and TLS-1.2 require hardware components.” *Id.* ¶ 78. He testifies that “[b]ecause Chou teaches an apparatus with hardware components that satisfy the requirements specified by Bugiel and TLS-1.2, a [person of ordinary skill] would have found it obvious to implement the techniques described in Bugiel, including TLS-1.2 as required by Bugiel, using Chou’s SOC apparatus.” *Id.* ¶ 80. He testifies that a person of ordinary skill “would have understood that the combination of Bugiel and Chou, and Bugiel and TLS-1.2 with Chou, would have been nothing more than combining known prior art elements according to understood methods to perform the well-known TLS handshake process using a secure hardware environment. This would have yielded predictable results in establishing secure, encrypted communication between a client mobile device and a server. A [person of ordinary skill] would have had an expectation of success in the result, as Bugiel contemplates using TLS-1.2 communication protocols and secure hardware to store protected keys and to encrypt and decrypt data, as taught by Chou.” *Id.* ¶ 81. Dr. Martin provides additional reasons motivating the combination of Bugiel and Chou, and Bugiel, Chou, and TLS-1.2. *Id.* ¶¶ 82–83.

Petitioner also asserts that a person of ordinary skill “would have found it obvious to combine Bugiel and Chou with Tkacik . . . to implement Chou’s secure memory with a security key encoded during a manufacturing process of the SOC.” Pet. 11 (citing Martin Decl.

¶¶ 84–85). Dr. Martin testifies that “[c]ombining Bugiel-Chou with Tkacik would have been nothing more than combining known methods of programming one-time programmable memory using blown fuses and applying this process during manufacturing of the memory, as taught by the prior art.” *Id.* ¶ 88. He testifies that “[t]he result would have been predictable in an OTP memory that is encoded, either by laser burning or electronic burning, during the manufacturing of the OTP memory of Chou” and a person of ordinary skill “would have had an expectation of success.” *Id.* ¶ 90.

At this stage, Patent Owner does not respond to these arguments by Petitioner or refute the testimony by Dr. Martin. On this record, we find for the reasons given that Petitioner has sufficiently demonstrated a motivation to combine Bugiel and Chou and to further combine those references with Tkacik, TLS-1.2, or both, with a reasonable expectation of success. Pet. 8–13.

2. Independent Claim 1

Petitioner presents an element-by element analysis of claim 1 supported by testimony by Dr. Martin. Pet. 13–47; Martin Decl. ¶¶ 92–180. For the reasons given by Petitioner, which we summarize *infra*, we determine that Petitioner demonstrates a reasonable likelihood of prevailing on its challenges to this claim.

[1p]: “A system-on-a-chip apparatus comprising:”

Petitioner relies on Chou as disclosing the preamble of claim 1. Pet. 13–15.⁵ Petitioner asserts “Chou discloses implementing components of device 30 ‘within a single integrated circuit (IC) chip 91 that incorporates a complete system on the IC chip (System-On-Chip or SOC).’” *Id.* at 13 (citing Ex. 1003 ¶ 5) (internal quotation marks omitted).

[1a-1]: “a system-on-a-chip comprising a security engine that is separate from a processor core of the system-on-a-chip and”

Petitioner identifies Chou’s HSM as a “security engine” that is separate from CPU on SOC to meet this limitation. Pet. 15–20.

[1a-2]: “has a secure memory accessible only by the security engine”

Petitioner relies on Chou’s secure memory 22, secure key module 23, and key cache 25 in HSM module 20 to meet this limitation. Pet. 20–21. Petitioner explains that all accesses to HSM 20 are routed through security interface 24 and no other accesses are permitted other than for operating the key cache. *Id.* at 22.

Furthermore, Petitioner asserts that Bugiel discloses or suggests implementing a secure memory accessible only by its TrEE in the secure execution environment. Pet. 23. Dr. Martin testifies that a person of ordinary skill would have found it obvious to implement the secure storage disclosed by Bugiel using Chou’s flexible secure hardware. Martin Decl. ¶ 105.

⁵ We do not express an opinion on whether the preamble recitations of the challenged claims are limiting. We find that Petitioner establishes a reasonable likelihood that the cited art discloses the preambles.

[1a-3]: “wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip”

Petitioner relies on Chou to meet this limitation. Pet. 23–25. Petitioner explains that “Chou’s unique key/root key is ‘encoded in the secure memory during a manufacturing process of the system-on-a-chip.’” *Id.* at 24 (internal quotation marks omitted). Petitioner asserts also that encoding the key during manufacturing would have been obvious. *Id.* Petitioner argues that “[a person of ordinary skill] . . . would have programmed Chou’s OTP 54 during manufactur[ing], just as Chou teaches and suggests.” *Id.* (citing Martin Decl. ¶ 118)

Alternatively, Petitioner relies in addition on Tkacik. Pet. 25–26. Petitioner asserts “Tkacik discloses a plaintext master key 160 stored in a nonvolatile, read-only register, where ‘long-lived key register 60 is desirably programmed with plaintext master key 160 *during the manufacturing process* of secure processing system 12 and cannot thereafter be altered.’” *Id.* at 25 (quoting Ex. 1005 ¶¶ 44–46) (emphasis in original).

[1b]: “the security engine to: generate a random nonce for initiating a request for a secure communication session with a remote server over a network using the nonce”

Petitioner contends that Bugiel discloses a secure communication session with a remote server over a network and also discloses generating a random nonce for initiating a request for a secure communication session. Pet. 26–27. In the proposed combination with Chou, Bugiel’s ClientHello message would use a random number generated by, e.g., Chou’s random number generator 58 of HSM 20. *Id.* at 27–28 (citing Ex. 1003 ¶¶ 34, 42, claim 11, Fig. 3; Martin Decl. ¶ 136).

[1c]: “perform a cryptographic key exchange with the remote server”

Petitioner contends that “[m]essages between Bugiel’s device and Web Server are standard messages of SSL/TLS handshake.” Pet. 28 (quoting Ex. 1002, 225) (internal quotation marks omitted). Petitioner explains that “Bugiel discloses a cryptographic key exchange in which its server sends a certificate message according to the SSL/TSL handshake, where WalletHelper ‘acts as an SSL/TLS proxy’ when communicating with the web server.” *Id.* at 31 (quoting Ex. 1002, 225–226, Fig. 2).

As an alternative, Petitioner contends that it would have been obvious to modify Bugiel with TLS-1.2 to send a public key in a separate ServerKeyExchange message, as contemplated by the TLS-1.2 specification. Pet. 33 (citing Martin Decl. ¶¶ 145–146). Petitioner argues that “Bugiel incorporates the TLS-1.2 specification into its disclosure and contemplates using TLS-1,2 to perform ‘standard messages of [an] SSL/TLS handshake.’” *Id.* (citing Ex. 1002, 225) (alteration in original). As discussed, Petitioner asserts a person of ordinary skill would have combined Bugiel with Chou and thus would have implemented Bugiel’s WalletHelper and WalletCore using Chou’s hardware, including, for example, Chou’s security interface 24 and key algorithm module 15 in Figure 1. *Id.* at 34–35; *see* Martin Decl. ¶ 150.

[1d]: “generate a symmetric session key, based on the cryptographic key exchange, to encrypt messages sent to the remote server and decrypt messages received from the remote server during the secure communication session”

Petitioner contends the symmetric session key of Bugiel-Chou would have been implemented by the HSM 20 of Chou. Pet. 40. Petitioner asserts

that TLS-1.2 also discloses the claimed session key. *Id.* Dr. Martin testifies that a person of ordinary skill would have implemented Bugiel to generate the claimed symmetric session key via TLS-1.2's "master secret" or "keyblock" with an expectation of success. Martin Decl. ¶¶ 162–163.

[1e]: "encrypt the symmetric session key based on the security key; and"

Petitioner contends that "[i]n the Bugiel-Chou-TLS-1.2 combination, Chou's KEK [Key-Encryption Key] 55 would encrypt [Bugiel's] master key or key block (e.g., the symmetric session key) using Chou's device unique key/root key stored in OTP 54." Pet. 43 (citing Martin Decl. ¶¶ 168–170).

[1f]: "store the encrypted session key in the secure memory"

Petitioner contends "[a person of ordinary skill] would have stored Bugiel's session-token ST_C in one of Chou's secure memory locations." Pet. 44 (citing Martin Decl. ¶ 174).

[1g]: "the system-on-a-chip to establish the secure communication session with the remote server over the network using the session key."

Petitioner relies on Bugiel for this limitation. Pet. 46. Petitioner contends that Bugiel teaches establishing a secure communication session with a remote server over a network using a session key. *Id.* Dr. Martin testifies that "[a person of ordinary skill] would have found it obvious to implement Bugiel using Chou's hardware to achieve this." Martin Decl. ¶ 176. Alternatively, Petitioner relies on TLS-1.2. Pet. 46 (citing Martin Decl. ¶ 177 ("TLS-1.2 discloses that its TLS handshake protocol serves to establish secure communication between the client and server.")) (citing Ex. 1004, 1)).

3. *Summary – Claim 1*

For the reasons given by Petitioner, including those summarized above, we find that Petitioner has demonstrated a reasonable likelihood of prevailing on its challenges to claim 1 based on Bugiel in various combinations with Chou, Tkacik, and TLS-1.2. We have considered Patent Owner’s arguments and do not find them persuasive. Rather than addressing Petitioner’s element-by-element analysis or the motivation to combine the references, Patent Owner relies entirely on the argument that “all the references cited in the petition are cumulative to the art already considered during prosecution of the ’838 patent.” Prelim. Resp. 8. This argument is not persuasive. None of the references cited in the Petition were considered by the examiner, and on the record before us at this stage, Patent Owner’s argument that they are “cumulative” of the cited art is unconvincing.⁶ We discuss Patent Owner’s arguments further in Section IV.F, *infra*, in connection with Patent Owner’s request for discretionary denial under 35 U.S.C § 314(a).

4. *Independent Claims 9 and 17*

Petitioner’s analyses of these claims in relation to the Bugiel Grounds references are similar to its analysis of claim 1. *See* Pet. 62–63, 65; Martin Decl. ¶¶ 234–240, 258–265.

⁶ Patent Owner has not requested that we deny the Petition under 35 U.S.C § 325(d), and we therefore do not address the applicability of that statute to the facts before us.

For the reasons given, we determine that Petitioner has demonstrated a reasonable likelihood of proving that these claims would have been obvious over the cited references.

5. Dependent Claims 2–8, 10–16, and 18–24

Claims 2–8 and 24 depend directly or indirectly from claim 1. Claims 10–16 depend directly or indirectly from claim 9. Claims 18–23 depend directly or indirectly from claim 17. Petitioner provides a separate analysis for each of these dependent claims. Pet. 48–67. Patent Owner’s Preliminary Response does not address these claims.

For the reasons given for independent claims 1, 9, and 17, we determine that Petitioner has demonstrated a reasonable likelihood of prevailing on its challenge to claims 2–8, 10–16, and 18–24, based on the Bugiel Grounds references.

6. Conclusion on Claims 1–24

In sum, after considering the reasons summarized above and set forth in the Petition, we determine that Petitioner has demonstrated a reasonable likelihood of prevailing on its challenge to claims 1–24 based on Bugiel and Chou, and on those references further combined with Tkacik, TLS-1.2, or both.

F. Remaining Challenges to Patentability

Petitioner presents additional challenges to claims 1–24. Pet. 68–98. As set forth above, after considering the evidence and arguments presented in the Petition, we determine that there is a reasonable likelihood that Petitioner would prevail with respect to at least the challenges to claims 1–24 based on the Bugiel Grounds references. We, therefore, do not address

the other challenges at this stage and institute trial as to all challenged claims on all grounds stated in the Petition. *See SAS Inst. Inc.*, 584 U.S. at 365; 37 C.F.R. § 42.108(a) (“When instituting *inter partes* review, the Board will authorize the review to proceed on all of the challenged claims and on all grounds of unpatentability asserted for each claim.”).

G. Conclusion Regarding the Merits

For the reasons given, we determine that Petitioner has demonstrated a reasonable likelihood of prevailing in showing at least one of the challenged claims is unpatentable.

IV. REQUEST FOR DISCRETIONARY DENIAL

In exercising the Director’s discretion under 35 U.S.C. § 314(a), the Board may consider “events in other proceedings related to the same patent, either at the Office, in district courts, or the ITC.” Patent Trial and Appeal Board Consolidated Trial Practice Guide, 58 & n.2 (Nov. 2019).⁷ The Board’s precedential order in *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 at 5–6 (PTAB Mar. 20, 2020) (precedential) (“*Fintiv*”) identifies several factors (“*Fintiv* factors”) for analyzing issues related to the Director’s discretion to deny institution in view of related litigation, with the goal of balancing efficiency, fairness, and patent quality.

When determining whether to exercise discretion to deny institution in view of a parallel proceeding, we consider the following *Fintiv* factors:

1. whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted;

⁷ Available at <https://www.uspto.gov/TrialPracticeGuideConsolidated>.

2. proximity of the court’s trial date to the Board’s projected statutory deadline for a final written decision;
3. investment in the parallel proceeding by the court and the parties;
4. overlap between issues raised in the petition and in the parallel proceeding;
5. whether the petitioner and the defendant in the parallel proceeding are the same party; and
6. other circumstances that impact the Board’s exercise of discretion, including the merits.

Fintiv, Paper 11 at 5–6. “These factors relate to whether efficiency, fairness, and the merits support the exercise of authority to deny institution in view of an earlier trial date in the parallel proceeding.” *Id.* at 6. In evaluating the *Fintiv* factors, we take “a holistic view of whether efficiency and integrity of the system are best served by denying or instituting review,” recognizing that “there is some overlap among these factors” and that “[s]ome facts may be relevant to more than one factor.” *Id.*

In the analysis that follows, we consider whether the *Fintiv* factors weigh in favor of denying institution.

A. Evidence of a Stay (Factor 1)

A district court stay of parallel litigation pending resolution of an *inter partes* review “allays concerns about inefficiency and duplication of efforts,” and strongly weighs against exercising our authority to deny institution. *Fintiv*, Paper 11 at 6.

Petitioner and Patent Owner both note that the district court has not granted a stay in the parallel Eastern District of Texas litigation. Prelim. Reply 1; Prelim. Resp. 2. Petitioner asserts that neither party has requested

a stay, and Patent Owner asserts that the district court is unlikely to grant a stay should Petitioner decide to request one. Prelim. Reply 1; Prelim. Resp. 2. Petitioner argues that this factor is neutral, while Patent Owner argues that this factor favors discretionary denial. Prelim. Reply 1; Prelim. Resp. 4.

The Board’s decision in *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 15 at 12 (PTAB May 13, 2020) (informative), cautions against speculating whether the district court would grant a stay if one were requested. Therefore, this factor has a neutral effect on the overall balancing of the *Fintiv* factors.

B. Proximity of Trial Date to Projected Statutory Deadline (Factor 2)

Fintiv factor 2 looks to the “proximity of the court’s trial date to the Board’s projected statutory deadline.” *Fintiv*, Paper 11 at 9. “If the court’s trial date is at or around the same time as the projected statutory deadline . . . the decision whether to institute will likely implicate other factors.” *Id.* Conversely, “[i]f the court’s trial date is earlier than the projected statutory deadline,” this has generally weighed “in favor of exercising authority to deny institution.” *Id.*

Jury selection in the parallel litigation in the Eastern District of Texas is scheduled to begin on January 26, 2026, which is about four months prior to the expected date for the final written decision here (i.e., by early June 2026). See Ex. 1014 (Docket Control Order), 1. Patent Owner asserts that this factor favors discretionary denial. Prelim. Resp. 4–5.

Petitioner argues this trial date “is not determinative because the Eastern District of Texas often schedules multiple trials on the same date

and the trial schedule is subject to change.” Prelim. Reply 2. Further, Petitioner asserts that “[t]ime-to-trial statistics instead suggest trial will begin 23 to 25 months from the complaint, which places trial between March and May 2026.” *Id.* (citing Ex. 1027; Ex. 1028). Petitioner argues that this factor “is at worst neutral because the district court trial is likely to be near the statutory deadline for the Board’s final written decision.” *Id.* at 2.

From this evidence, we are persuaded that a trial court will likely reach the merits of the invalidity of the ’838 patent before we issue a final written decision by four months or less. Accordingly, this factor favors discretionary denial of the Petition.

C. Investment in the Parallel Proceeding (Factor 3)

This factor relates to the “amount and type of work already completed in the parallel litigation by the court and the parties at the time of the institution decision.” *Fintiv*, Paper 11 at 9.

Patent Owner asserts that, “by the time any institution decision in this case is likely to be issued, claim construction discovery will be complete, the parties may well have filed their opening claim construction briefs and technology tutorials, and discovery will be ongoing.” Prelim. Resp. 5 (citing Ex. 1014, 4).

Petitioner responds that “[t]he parties’ *Markman* hearing is not scheduled until July 31, 2025, fact discovery does not close until August 28, 2025, and the deadlines for expert discovery and dispositive motions fall well after institution (October 2025).” Prelim. Reply 4 (citing Ex. 1014, 3–4). Petitioner also points out that “Patent Owner’s opening claim construction brief is not due until after institution (on June 18, 2025), and

there is no indication there will be any claim construction discovery in the case.” *Id.* Petitioner asserts that it “diligently filed the Petition just two months after receiving Patent Owner’s infringement contentions on September 4, 2024, and before serving invalidity contentions on November 20, 2024.” Prelim. Reply 5 (citing Ex. 1016, 29–36; Ex. 1014, 4).

Considering the evidence before us, we are persuaded that the extent of the activity by the district court and the parties in the parallel litigation has little to no impact on our analysis of the third *Fintiv* factor. While the parties appear to have invested some effort in the parallel litigation, the bulk of the investment from the court and the parties lies ahead. Petitioner’s diligence in filing its Petition weighs neither for nor against exercising our discretion. Accordingly, this factor is neutral.

D. Overlap of Issues (Factor 4)

Under the fourth *Fintiv* factor, we consider “overlap between issues raised in the petition and in the parallel proceeding.” *Fintiv*, Paper 11 at 12 (citing *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020) (precedential)).

Petitioner has stipulated in its Preliminary Reply that “it will not pursue the grounds raised in the Petition or any other ground that Petitioner could have reasonably raised in this proceeding in the parties’ district court litigation.” Prelim. Reply 1 (citing *Sotera*, Paper 12 at 18–19). Patent Owner contends that “the Board should disregard this late-filed [*Sotera*] stipulation because it should have been part of the original petition.” Prelim. Sur-reply 1. We disagree that the stipulation is untimely, or that Patent Owner has been prejudiced. Patent Owner requested discretionary denial in

its Preliminary Response. The *Sotera* stipulation followed in Petitioner's next filing. We do not expect Petitioner to anticipate such a request by Patent Owner before it is made.

While *Sotera* is binding precedent and “may mitigate some concern of duplication between the parallel proceeding and this proceeding,” the stipulation does not “outweigh” the other *Fintiv* factors. *Motorola Solutions, Inc. v. Stellar, LLC*, IPR2024-01205, Paper 19 at 4 (PTAB Mar. 28, 2025) (Coke Morgan Stewart, Acting Director). On the present record, therefore, we find that Petitioner's stipulation mitigates some concerns of duplicative efforts between the district court and the Board. *Sotera*, Paper 12 at 19. Accordingly, factor 4 favors not exercising our discretion to deny institution, but is not dispositive of the issue.

E. Identity of Parties (Factor 5)

Under the fifth *Fintiv* factor, we consider “whether the petitioner and the defendant in the parallel proceeding are the same party.” *Fintiv*, Paper 11 at 13. If the parties are the same in the *inter partes* proceeding and in the parallel proceeding this factor supports denying institution. *Sotera*, Paper 12 at 19.

There is no dispute that the parties in the parallel litigation are the same as those before us. Pet. 99; Prelim. Resp. 7. Accordingly, this factor weighs in favor of exercising our discretion to deny institution.

F. Other Circumstances, Including the Merits (Factor 6)

The sixth *Fintiv* factor takes into account other circumstances that may bear on the decision to exercise discretion to deny, such as the merits of

the patentability challenges. *See Fintiv*, Paper 11 at 14–16. If the merits “seem particularly strong on the preliminary record, this fact has favored institution,” whereas “if the merits of the grounds raised in the petition are a closer call, then that fact has favored denying institution when other factors favoring denial are present.” *Id.* at 14–15. We therefore address the question of whether the merits of this case are particularly strong.

As set forth in our discussion of the merits in Section III, *supra*, Petitioner has presented an element-by-element analysis of the challenged claims in light of the cited prior art references, supported by testimony from Dr. Martin, that is sufficient for institution of a trial,

In connection with this *Fintiv* factor, Patent Owner argues that “all the references cited in the petition are cumulative to the art already considered during prosecution.” Prelim. Resp. 8. For example, Patent Owner asserts that “during prosecution, the Examiner cited and relied on the teachings of Goss.”⁸ *Id.* (citing Ex. 2006). Patent Owner contends that “Bugiel is cumulative to the art already considered during prosecution of the ‘838 patent,” specifically, Goss. *Id.* Patent Owner makes similar arguments for Chou (“A similar architecture was disclosed in Goss.”), Tkacik, and TLS-1.2. *Id.* at 8–9.

Petitioner argues “[t]he art in the Petition is materially different and noncumulative of art the Office previously considered.” Prelim. Reply 8. Petitioner continues that Patent Owner “does not dispute that Bugiel, Chou, Tkacik, and TLS-1.2 were not before the Examiner and not cited in any office action during prosecution.” *Id.* (citations omitted).

⁸ US Patent Pub. No. 2005/0213766 A1 (Ex. 2005).

We agree that Patent Owner's argument is weak. To succeed on its only argument at the trial stage, Patent Owner will have to demonstrate more fully than it has so far the extent to which the cited references are cumulative of the references that were considered by the examiner during prosecution. Judging from the record presented thus far, this may be a heavy lift for Patent Owner. Focusing on Goss, Patent Owner relies on a November 16, 2015 Office Action. *See* Prelim. Resp. 8 (citing Ex. 2006 (Nov. 16, 2015 Office Action)); *see also* Ex. 1012, 273–287 (same as Ex. 2006). In that Office Action, the examiner rejected the then-pending claims based on Goss in combination with a Chou patent⁹ (different from the Chou reference cited in the Petition). *Id.* at 276–277. Patent Owner responded with an amendment, and the examiner withdrew reliance on Goss in the next Office Action. *Id.* at 215–230. Goss was not cited again during the prosecution, which ended with an allowance after additional amendments to the claims. *See id.* at 69–82 (amendment), 39–42 (allowance). Thus, while Goss was cited by the examiner early in the prosecution, Goss was never cited against the later-amended claims that are before us in this proceeding.

Patent Owner also points to Kumar,¹⁰ which was cited by the examiner later in the prosecution. *See* Prelim. Resp. 9; Ex. 1012, 215–230. In response, Petitioner asserts that during prosecution, the applicant argued that Kumar, relied upon by the examiner in a final rejection, fails to disclose “a security engine that is separate from a processor core of the system-on-a-chip,” a feature that is disclosed in Chou and Tkacik. Prelim. Reply 8–9

⁹ US Patent 7,966,646 B2 (Ex. 2009).

¹⁰ US Patent 8,364,975 B2 (Ex. 2007).

(citing Ex. 1012, 77–79). During prosecution, the claims were allowed over Kumar after this limitation was added by amendment. *See* Ex. 1012, 40, 70, 72, 74, 77–81. Patent Owner does not respond persuasively to Petitioner’s assertion that Kumar (unlike Chou and Tkacik) does not disclose a security engine “separate from a processor core.” Prelim. Reply 8–9; Prelim. Sur-reply 4–5.¹¹ Regarding Kumar, we agree with Petitioner that “[a]rt that was successfully distinguished from the claims is not cumulative of asserted art that includes these features.” Prelim. Reply 8.

Petitioner argues that “Patent Owner identifies no missing elements in Petitioner’s grounds, nor does it contest any of Petitioner’s rationales for combining the art.” Prelim. Reply 7. We agree. Patent Owner’s argument is limited to its claim that “cumulative” references were considered during prosecution. *See, generally*, Prelim, Resp. For the reasons given, we do not see this as a strong argument. In conclusion, taking into account Petitioner’s element-by-element analysis of the challenged claims supported by Dr. Martin’s testimony and Patent Owner’s weak response, we determine that at this stage and on this record, for the reasons given, Petitioner’s challenge is particularly strong.

¹¹ Attempting to show that this issue was before the examiner, Patent Owner cites an argument appearing at pages 95–96 of Exhibit 1012. Prelim. Sur-reply 5. This argument does not address the limitation added later by amendment that led to allowance. *See* Ex. 1012, 70. That amendment recites “a security engine that is separate from a processor core of the system-on-a-chip.” *Id.* The argument cited by Patent Owner addresses the limitation “a secure memory accessible only by the security engine,” but not the separate security engine limitation that was added later.

G. Conclusion – Fintiv Analysis

We have considered the facts and circumstances before us in view of the *Fintiv* factors. The *Sotera* stipulation weighs against denial of institution. The merits of Petitioner’s challenges are strong, especially in light of Patent Owner’s lack of a response that addresses the details of Petitioner’s element-by-element analysis or the motivation to combine references. This factor therefore weighs strongly against denial of institution. However, the other factors are neutral or weigh in favor of denial, especially the trial date factor. In summary, *Fintiv* factors 1 and 3 are neutral; factors 2 and 5 favor discretionary denial; and factors 4 and 6 do not favor discretionary denial. The particularly strong merits of Petitioner’s case and the *Sotera* stipulation, however, lead us to conclude that the trial date and other factors favoring denial are outweighed. We, therefore, decline to exercise discretion under 35 U.S.C. § 314(a) to deny institution of *inter partes* review.

V. CONCLUSION

For the foregoing reasons, we determine that Petitioner has demonstrated a reasonable likelihood that Petitioner would prevail in showing at least one of the challenged claims of the ’838 patent is unpatentable. Furthermore, we are not persuaded to exercise our discretion to deny institution under 35 U.S.C. ¶ 314(a).

VI. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 1–24 of the '838 patent is instituted with respect to all grounds set forth in the Petition; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4(b), *inter partes* review of the '838 patent shall commence on the entry date of this Order, and notice is hereby given of the institution of a trial.

IPR2025-00100
Patent 9,887,838 B2

For PETITIONER:

Cory Bell
Joseph Long
Alexander Boyer
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP
cory.bell@finnegan.com
jp.long@finnegan.com
alexander.boyer@finnegan.com

For PATENT OWNER:

Tarek Fahmi
Jonathan Tsao
ASCENDA LAW GROUP, PC
tarek.fahmi@ascendalaw.com
jonathan.tsao@ascendalaw.com