

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROCHIP TECHNOLOGY INC.,
Petitioner,

v.

HD SILICON SOLUTIONS LLC,
Patent Owner.

IPR2021-01567
Patent 7,810,002 B2

Before FRANCES L. IPPOLITO, NATHAN A. ENGELS, and
ARTHUR M. PESLAK, *Administrative Patent Judges*.

ENGELS, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

Petitioner Microchip Technology, Inc. filed a Petition (Paper 2, “Pet.”) requesting *inter partes* review of claims 1–6, 8, 9, 11, 12, and 15–19 of U.S. Patent No. 7,810,002 B2 (Ex. 1001, “the ’002 patent”). Patent Owner HD Silicon Solutions LLC filed a Preliminary Response. Paper 7 (“Prelim. Resp.”). The Board issued a Decision Granting Institution of *Inter Partes* Review. Paper 12.

After institution, Patent Owner filed a Response (Paper 15, “PO Resp.”), Petitioner filed a Reply (Paper 17), and Patent Owner filed a Sur-reply (Paper 20). Both parties presented oral arguments at a hearing, and a copy of the hearing transcript is in the record. Paper 25.

Based on the complete record in this proceeding, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–6, 8, 9, 11, 12, and 15–19 of the ’002 patent are unpatentable.

A. *Real Parties in Interest*

Petitioner identifies Microchip Technology Inc. as the real party-in-interest. Pet. 1. Patent Owner identifies HD Silicon Solutions LLC as the real party-in-interest. Paper 4, 2.

B. *Related Matters*

The parties state that the ’002 patent was asserted in *HD Silicon Solutions LLC v. Microchip Technology Inc.*, No. 6:20-cv-01092 (W.D. Tex.). Pet. 1; Paper 4, 2. That case has been transferred to *HD Silicon Solutions LLC v. Microchip Technology Inc.*, No. 3:21-cv-08295-SK (N.D. Cal.). Paper 6, 2; Ex. 2003 (order granting transfer to N.D. Cal.).

C. *The ’002 Patent*

Titled “Providing Trusted Access to a JTAG [“Joint Test Action Group”] Scan Interface in a Microprocessor,” the ’002 patent describes a

method of securing scan chain architecture by performing an authentication operation through a trusted software layer to authorize use of a protected scan chain. Ex. 1001, 1:42–45, codes (54), (57). According to the '002 patent, when a processor contains processor-specific secrets, interfaces that support debugging the chip can put those secrets at risk. Ex. 1001, 1:24–38. To protect against those risks, the '002 patent describes restricting access to a processor's resources (e.g., internal registers, caches, etc.) to only a trusted software layer. Ex. 1001, 5:44–52.

The '002 patent states that embodiments can be implemented on software running on a computer system, where the software is operable for securing a scan chain architecture by performing an authentication operation through a software layer to authorize use of a JTAG scan interface. Ex. 1001, 2:23–31. Figure 4, reproduced below, illustrates an embodiment of the '002 patent.

400

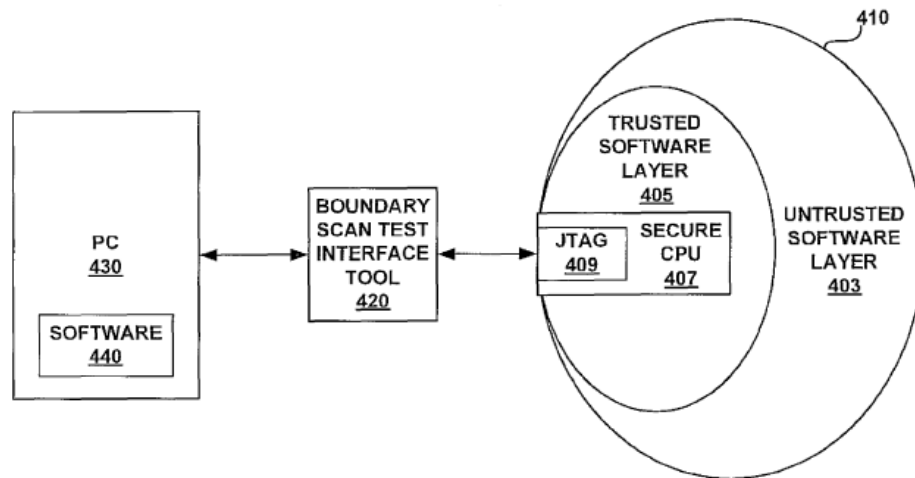


FIGURE 4

Figure 4 of the '002 patent is a block diagram of a system implementing a JTAG scan interface. Ex. 1001 1:61–62. Figure 4 depicts PC 430 having software 440. Separate from PC 430, Figure 4 depicts secure CPU 407 having a JTAG 409. Trusted software layer 405 surrounds secure CPU 407 and untrusted software layer 403 surrounds trusted software layer 405. Between PC 430 and secure CPU 407 is boundary scan test interface tool 420. PC 430 is communicatively coupled to JTAG scan interface tool 420, and JTAG scan interface tool 420 is communicatively coupled to JTAG scan test interface 409. Ex. 1001, 6:4–6. PC 430 and software 440 provide a user interface with JTAG scan interface tool 420 and allow for debugging secure CPU 407. Ex. 1001, 6:9–14.

Describing Figure 4, the '002 patent's specification states secure CPU 407 is only accessible through trusted software layer 405, and “[t]he trusted software layer provides executable instructions which are sent to the secure CPU for processing.” Ex. 1001, 5:35–39. More specifically:

the trusted software layer 405 is capable of interfacing with permitted resources in the secure CPU 407 that the secure CPU 407 grants access. As such, the trusted software layer 405 has complete and total control over the hardware code and resources in the secure CPU 407 that the trusted software layer 405 has permission to access. In contrast, the untrusted software layer 403 does not have any access to the resources (e.g., internal registers, caches, etc.) of the secure CPU 407.

Ex. 1001, 5:44–51 (emphasis omitted).

D. Illustrative Claims

Of the challenged claims, claims 1, 11, and 17 are independent claims. Claim 1, reproduced below with bracketed labels added corresponding to the numbering in the Petition, is illustrative.

1. A method for securing a scan chain architecture, said method comprising:
 - [1.a] disabling a scan interface in a system comprising a secure processor and a software layer, wherein said software layer is authorized to access trusted resources in said secure processor;
 - [1.b] receiving authentication information at the software layer, wherein said authentication information if valid provides access to said scan interface;
 - [1.c] verifying whether said authentication information is valid using said software layer; and
 - [1.d] allowing access to said scan interface if said authentication information is valid.

E. Alleged Grounds of Unpatentability

Petitioner asserts that claims 1–6, 8, 9, 11, 12, and 15–19 would have been unpatentable on the following grounds (Pet. 4–5):

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–6, 8, 9, 11, 12, 15–19	103	Giles ¹
1, 2, 5, 6, 8, 9, 11, 15–17, 19	103	Moyer ²
3, 4, 12, 18	103	Moyer, Giles
1, 2, 5, 6, 8, 9, 11, 15–17, 19	103	Moyer, Giles

II. ANALYSIS

A. Obviousness

The Supreme Court set out a framework for assessing obviousness under § 103 that requires consideration of four factors: (1) the “level of

¹ U.S. Patent No. 7,228,440 B1, issued June 5, 2007 (Ex. 1008).

² U.S. Patent No. 7,248,069 B2, issued July 24, 2007 (Ex. 1009).

ordinary skill in the pertinent art,” (2) the “scope and content of the prior art,” (3) the “differences between the prior art and the claims at issue,” and (4) “secondary considerations” of non-obviousness such as “commercial success, long felt but unsolved needs, failure of others, etc.”³ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). We address the level of ordinary skill below, followed by an analysis of the prior art and challenged claims. On the current record, there is no evidence or argument relating to secondary considerations of non-obviousness.

1. Level of Ordinary Skill in the Art

In determining the level of skill in the art, we consider the type of problems encountered in the art, the prior art solutions to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the educational level of active workers in the field. *Custom Accessories, Inc. v. Jeffrey-Allan Indus., Inc.*, 807 F.2d 955, 962 (Fed. Cir. 1986); *Orthopedic Equip. Co. v. U.S.*, 702 F.2d 1005, 1011 (Fed. Cir. 1983).

Petitioner contends a person of ordinary skill in the art at the time of the invention (“POSITA”) would have “possessed at least a bachelor’s degree in electrical engineering, computer engineering, or computer science, with at least two years of experience in computer system development, including experience using hardware interfaces to debug computer systems.” Pet. 6. Petitioner further states that a person could also have qualified as a person of ordinary skill in the art “with some combination of (1) more formal education (such as a master’s of science degree) and less technical

³ The record does not include any evidence of secondary considerations of non-obviousness.

experience or (2) less formal education and more technical or professional experience in the fields listed above.” Pet. 6 (citing Ex. 1002 ¶ 26).

Patent Owner does not address the level of skill in the art. We apply the level of ordinary skill advanced by Petitioner except that we omit the “at least” qualifiers, which would render the level of skill open-ended and inclusive of expertise beyond the level of ordinary skill.

2. *Claim Construction*

We construe claims using the principles set forth in *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–17 (Fed. Cir. 2005) (en banc) and related cases. 37 C.F.R. § 42.100(b) (2021). Under that precedent, the words of a claim are generally given their “ordinary and customary meaning,” which is the meaning the term would have to a person of ordinary skill at the time of the invention, in the context of the entire patent including the specification. *Phillips*, 415 F.3d at 1312–13.

Petitioner states that all claim terms should be accorded their plain and ordinary meanings (Pet. 13), and Petitioner contends the plain and ordinary meaning of the claim term “software layer” is “software code at a particular level” (Reply 2 (citing Ex. 1041 ¶ 7; Ex. 1034)). Patent Owner contends “software layer” should be construed as “computer program code executed on a processor that comprises one level of a hierarchy of functional components that interfaces with neighboring levels.” PO Resp. 26 (citing Ex. 2007 ¶ 76); Sur-reply 4.

According to Patent Owner, a person of ordinary skill would have understood that in “software architecture and software engineering arts, there is a practice of classifying styles of implementations according to the structural organization of the system.” PO Resp. 27 (citing Ex. 2007 ¶ 65).

Patent Owner contends its construction is supported by intrinsic and extrinsic evidence. PO Resp. 27–31; Sur-reply 4–7.

First, citing extrinsic evidence relating to software architecture and expert testimony, Patent Owner contends that “layers” is a concept that is fundamental to the field of software architecture and engineering and widely recognized and understood by a person of ordinary skill in the art. PO Resp. 27 (citing Ex. 2007 ¶¶ 65–69; Ex. 2002, 42, 46; Ex. 2010, 20, 39; Ex. 2011, 100). Patent Owner also contends the ’002 patent’s specification uses the term software layer consistent with that evidence. PO Resp. 28.

Among other things, Patent Owner notes that the ’002 patent’s specification uses the terms “software layers, secure software layers, trusted software layers and untrusted software layers,” and Patent Owner cites Figure 4 which depicts “software” on a PC distinct from a trusted software layer and an untrusted software layer at a secure CPU. PO Resp. 32; Sur-reply 5.

We agree with Petitioner that “software layer” should be given its plain and ordinary meaning. Nothing in the specification specifically defines software layer, and as Patent Owner notes, evidence of record indicates that a person of ordinary skill would be familiar with the concept of layers in software architecture, which is consistent with applying the plain and ordinary meaning. *See* PO Resp. 27 (citing Ex. 2007 ¶¶ 65–69; Ex. 2002, 42, 46; Ex. 2010, 20, 39; Ex. 2011, 100).

Further, we do not find support for the language of Patent Owner’s proposed construction. First, Patent Owner’s suggestion that the code is “executed on a processor” is unwarranted and potentially unclear. Among other problems, it is not clear whether “a processor” in Patent Owner’s

proposed definition refers to the claimed secure processor or some other processor.

We also do not find support for Patent Owner’s proposed language requiring “a hierarchy of functional components” and “interfaces with neighboring levels.” The claim language refers to a single “software layer.” Contrary to Patent Owner’s arguments, the fact that the specification refers to “software layers, secure software layers, trusted software layers, and untrusted software layers,” evidences that the patentee could have claimed multiple different layers but chose not to. Moreover, certain embodiments disclosed in the ’002 patent refer only to a single, trusted software layer. *See* Ex. 1001, Figs. 5–7.

The claim language itself requires that the software layer “is authorized to access trusted resources in [a] secure processor” and that the software layer receives and verifies authentication information. We note that each party refers to “code” as part of its definitions of “software layer”—“software code” in Petitioner’s definition, and “computer program code” in Patent Owner’s definition—and it follows that it is code that performs the recited functions. *See* Paper 25, 37:25–38:2 (Patent Owner noting that both parties’ proposed constructions use the word “levels” and “code”; stating “the main difference [between the parties’ constructions] is . . . that [Patent Owner] contend[] there’s more than one layer of software, whereas Petitioner’s construction does not allow for that”).

With those clarifications, we apply the plain meaning of “software layer” as articulated by Petitioner.

3. *Ground 1: Giles*

a) *Claim 1*

[1.p] A method for securing a scan chain architecture, said method comprising:

Petitioner contends that to the extent the preamble is limiting, Giles satisfies the preamble with its disclosures of a boundary scan disable mechanism on a secure device. Pet. 25 (citing Ex. 1008, 1:17–19). Among other things, Petitioner contends Giles describes a method for authentication and disabling an Extended Joint Test Action Group (“EJTAG”) debug interface. Pet. 25–26 (citing Ex. 1008, 1:42–48; Ex. 1002 ¶ 66).

Patent Owner does not address Petitioner’s showing for the preamble, and we determine Petitioner has shown that the preamble is satisfied.

[1.a] disabling a scan interface in a system comprising a secure processor and a software layer, wherein said software layer is authorized to access trusted resources in said secure processor;

Petitioner contends Giles satisfies this limitation with its disclosures of authentication and disabling an EJTAG debug interface which includes a secure component and code stored on a boot ROM module 162. Pet. 29 (citing Ex. 1008, 1:46–47, 3:28–31, 5:57–58, 6:32–44, Figs. 1, 4). Specifically, Petitioner states that “Giles discloses secure component 102 . . . , which is the claimed ‘secure processor,’ and code 163 (stored in boot ROM module 162) which is the claimed ‘software layer.’” Pet. 29 (citing Ex. 1008, 3:28–31, 5:57–58. Fig. 1; Ex. 1002 ¶ 73).

According to Petitioner, Giles’s secure component 102 includes One-Time Programmable (“OTP”) memory 122 and decoder circuit 120 which includes CPU module 174, with the OTP 122 and circuit 120 collectively

forming a secure processor. Pet. 30 (citing Ex. 1008, 2:52–60, 3:40–41, 3:63, Fig. 1; Ex. 1002 ¶¶ 73–74). Further, Petitioner states:

A POSITA would understand that code 163 includes all the characteristics of the recited software layer. For example, code 163 is authorized to access trusted resources within core processor circuit 124 or secure component 102, such as central processing unit 174 (*e.g.*, via the booting sequence) and OTP memory module 122, and perform secure operations like authentication and decryption operations.

Pet. 31–32 (citing Ex. 1008, 6:53–56; Ex. 1002 ¶ 76).

With arguments premised on Patent Owner’s proposed construction of “software layer,” Patent Owner argues Giles’s Boot ROM code 163 is not a software layer, would need to be combined with other software components to become a software layer, does not interface with neighboring software, and is nothing more than the code that initializes the hardware. PO Resp. 32 (citing Ex. 2007 ¶¶ 79–80); Sur-reply 8–9 (citing Ex. 1036, Fig. 3; Ex. 2007 ¶ 81; Ex. 2012, 29:2–10). Further, Patent Owner argues that because the Boot ROM code 163 is not a software layer, it does not satisfy the claim’s requirements of the software layer being authorized to access trusted resources, receiving authentication information at the software level, and verifying the authentication information in the software level. PO Resp. 32 (citing Ex. 2007 ¶ 81). Patent Owner also argues that Giles is like prior art distinguished during prosecution of the ’002 patent (Milne⁴) because Giles “relates to preventing unauthorized access to data being stored in memory and does not disclose or meet the limitation ‘a software layer is authorized to access trusted resources in said secure processor.’” PO Resp. 33 (citing

⁴ US 2006/0282734 A1; published Dec. 14, 2006. Ex. 1037.

Ex. 1004, 10; Ex. 2007 ¶ 85); Sur-reply 10 (citing Ex. 1004, 10; Ex. 2007 ¶¶ 84, 85).

We disagree with Patent Owner’s proposed construction of software layer for the reasons explained above, and we agree with Petitioner that Giles discloses a software layer, as claimed. Specifically, Petitioner contends, and Patent Owner does not rebut, that Giles teaches that its code 163 has access to OTP memory module 122 within a secure processor, secure component 102. In fact, Patent Owner acknowledges that “Giles describes that software 163 ‘may have privileged status as a Secure Privileged mode device, with full access to the entire map of the component 102.’” PO Resp. 21 (quoting Ex. 1008, 11:63–66).

Regarding Patent Owner’s arguments that Giles is like Milne in that both references relate to protecting data from memory (PO Resp. 33; Sur-reply 10), we note that Patent Owner has not shown that the prosecution history amounts to a clear and unmistakable disclaimer that affects claim scope. *See Mass. Inst. Of Tech. v. Shire Pharms.*, 839 F.3d 1111, 1119 (Fed. Cir. 2016) (“The party seeking to invoke prosecution history disclaimer bears the burden of proving the existence of a clear and unmistakable disclaimer that would have been evident to one skilled in the art.”) (citation and quotation marks omitted). Even if Giles and Milne both disclose protecting data from memory, those arguments do not rebut Petitioner’s contentions that Giles’s code 163 is authorized to access trusted resources in a secure processor.

Further, we agree with Petitioner that Giles discloses disabling a scan interface with its disclosures of systems and procedures for authenticating and disabling an EJTAG debug interface of secure component 102 using code 163 stored on boot ROM module 162. Ex. 1008, 1:46–47, 3:28–31,

5:57–58, 6:32–44, Figs. 1, 4. Giles discloses that boot ROM code 163 reads the values of security flag registers for the EJTAG enables from the OTP memory, performs authentication procedures, and enables the EJTAG probe upon successful authentication. Ex. 1008, 6:50–7:2.

Based on the entire record, we determine Giles satisfies limitation [1.a].

[1.b] receiving authentication information at the software layer, wherein said authentication information if valid provides access to said scan interface;

Petitioner contends Giles discloses this limitation with its authentication process used to enable access to the ETJAG features. Pet. 32–33. Patent Owner does not specifically rebut Petitioner’s showing for this limitation beyond the arguments addressed above, and we agree with Petitioner that Giles satisfies this limitation.

Giles describes authentication protocols in which boot ROM code 163 reads the security flag values for the EJTAG enables, and if an EJTAG enable is allowed via authentication, the boot ROM code 163 may execute a challenge portion of the EJTAG authentication procedure. Ex. 1008, 6:25–33, 6:53–7:2. Dr. Alpert states a person of ordinary skill would have understood that Giles’s code 163 executes the authentication procedures upon receiving authentication information from universal asynchronous receiver/transmitter (“UART”) interface 110 (Ex. 1002 ¶¶ 79–81), which is consistent with Giles’s teachings (Ex. 1006, 6:25–7:2).

Based on the complete record, we determine Giles satisfies limitation [1.b].

[1.c] verifying whether said authentication information is valid using said software layer; and

Petitioner contends Giles teaches this limitation with its authentication procedure discussed above regarding limitation [1.b]. Pet. 33–34.

According to Petitioner, a person of ordinary skill would understand that because boot ROM code 163 executes the EJTAG authentication procedure, it follows that the authentication information is verified by boot ROM code 163. Pet. 33–34 (citing Ex. 1002, ¶ 83).

Patent Owner does not specifically rebut Petitioner’s showing for this limitation beyond the arguments addressed above, and we agree with Petitioner that Giles satisfies this limitation. As noted above, Giles states that the authentication protocols, including a challenge/response-based authentication via the UART port 110, may be implemented by firmware, code, or software. Ex. 1008, 6:28–7:2. Petitioner has shown that Giles satisfies this limitation based on Giles’s discussion of the authentication protocols and Dr. Alpert’s testimony that a person of ordinary skill would have understood that the authentication information is verified by boot ROM code 163.

Based on the complete record, we determine Giles satisfies limitation [1.c].

[1.d] “allowing access to said scan interface if said authentication information is valid.”

Petitioner contends Giles satisfies this limitation with its disclosures that upon successful authentication, the EJTAG probe may be enabled. Pet. 34 (citing Ex. 1008, 6:66–7:2). Patent Owner does not specifically rebut Petitioner’s showing for this limitation.

We agree with Petitioner that Giles satisfies this limitation with its teachings of enabling the EJTAG probe upon successful authentication. Based on the complete record, we determine Giles satisfies limitation [1.d].

b) Conclusion Regarding Claim 1

Based on the complete record, we determine Petitioner has shown by a preponderance of the evidence that claim 1 is unpatentable as obvious in view of Giles.

c) Claim 2

2. The method of claim 1, wherein said disabling further comprises: disabling said scan interface upon booting up said secure processor.

Petitioner contends Giles discloses claim 2 with its teachings that boot ROM module 162 is used to bootstrap processor module 132, which is an integral part of component 102, the claimed secure processor. Pet. 34 (citing Ex. 1008, 4:28–30; Ex. 1002 ¶ 87). Petitioner states that Giles discloses that at the start of initializing the EJTAG security flags, the EJTAG interface is disabled and can remain disabled when the EJTAG security mode is set to “LOCKED” or the authentication fails in “AUTHENTICATE” mode. Pet. 35 (citing Ex. 1008 6:50–7:9, Fig. 4, Table III; Ex. 1002 ¶ 87).

Patent Owner does not rebut Petitioner’s showings, and we agree with Petitioner that the cited portions of Giles teach disabling the scan interface upon booting up the secure processor, as claimed.

Based on the complete record, we determine Petitioner has shown by a preponderance of the evidence that claim 2 is unpatentable as obvious in view of Giles.

d) Claim 3

3. The method of claim 1, wherein said disabling further comprises: setting a register to a first state that disables said

scan interface, wherein said register is internal to said secure processor.

Petitioner contends Giles discloses or renders obvious the limitations of claim 3 with its teachings of a Security Resource Control (“SRC”) register 292 that can be used to disable the EJTAG interface when an EJTAG Disable (“EDIS”) flag in SRC register 292 is in an appropriate state. Pet. 36 (citing Ex. 1008, 7:59–62; Ex. 1002 ¶ 89). Further, Petitioner states that Giles discloses that SRC register 292, including the EDIS field, may be implemented in Security Flags Block 146, which is an integral part of the secure component 102. Pet. 36 (citing Ex. 1008, 7:36–38, 14:8–15). Petitioner additionally cites details in Giles regarding how the flag EDIS bits in SRC register 292 can be modified to disable or enable the JTAG interface. Pet. 36–37 (citing Ex. 1008, 8:55–9:7, Tables VII, VIII; Ex. 1002 ¶ 90).

Patent Owner does not rebut Petitioner’s showings, and we agree with Petitioner that the cited portions of Giles teach setting a register internal to the secure processor to a first state that disables the scan interface.

Based on the complete record, we determine Petitioner has shown by a preponderance of the evidence that claim 3 is unpatentable as obvious in view of Giles.

e) Claim 4

The method of claim 3, wherein said allowing access to said scan interface further comprises: setting said register to a second state that enables said scan interface.

Petitioner contends that Giles discloses the additional limitation of claim 3 because Giles’s Table VII describes two states that can be used to enable and disable the EJTAG probe such that setting the EDIS flag of the SRC register 292 to the appropriate state will enable the EJTAG interface. Pet. 38 (citing Ex. 1008, 8:55–67, Table VII; Ex. 1002 ¶ 93).

Patent Owner does not rebut Petitioner's showings, and we agree with Petitioner that the cited portions of Giles teach setting a register internal to the secure processor to a second state that disables the scan interface.

Based on the complete record, we determine Petitioner has shown by a preponderance of the evidence that claim 4 is unpatentable as obvious in view of Giles.

f) Claim 5

5. The method of claim 1, wherein said receiving said authentication information further comprises: receiving said authentication information through a communication buffer that provides an interface to said software layer for authentication purposes, wherein said authentication information is a message.

Petitioner contends Giles discloses or renders obvious the limitations of claim 5 because a person of ordinary skill would have understood that code 163 in ROM module 162 executes the recited authentication upon receiving authentication information via UART interface 110. Pet. 38 (citing Ex. 1002 ¶ 95). Petitioner further contends that a person of ordinary skill would have understood that the UART would include a communication buffer for receiving the serial communication and transforming it to the appropriate data width used by the processor module 132 (e.g., 8-, 16-, 32-, or 64-bit width). Pet. 38–39 (citing Ex. 1008, 6:27–30; Ex. 1002 ¶¶ 95, 96). Further, Petitioner contends a person of ordinary skill would have understood that UART interface 110 can receive information, including authentication information in the form of a message used during an authentication process by boot ROM code 163. Pet. 39 (citing Ex. 1002, 2:19–20; Ex. 1002 ¶ 97). Petitioner additionally cites evidence that UART interfaces were well known to include receiver buffer registers that

correspond to the claimed communications buffer that provides an interface to the software layer for authentication purposes. Pet. 39–40 (citing Ex. 1011, 151, 153 Fig. 6.6, Ex. 1002 ¶ 98).

Patent Owner does not rebut Petitioner’s showings, and we agree with Petitioner that the cited portions of Giles teach receiving an authentication message through a communications buffer that provides an interface to the software layer for authentication purposes, as claimed.

Based on the complete record, we determine Petitioner has shown by a preponderance of the evidence that claim 5 is unpatentable as obvious in view of Giles.

g) Claim 6

6. The method of claim 1, wherein said verifying said authentication information further comprises: verifying whether said authentication information is in a proper format.

Petitioner contends Giles discloses or renders obvious claim 6. Pet. 41. Citing Dr. Alpert and other evidence, Petitioner contends a person of ordinary skill would have understood that verifying whether a response to a challenge is valid also involves verifying that the authentication information is in a proper format. Pet. 41 (citing Ex. 1002 ¶¶ 99, 100; Ex. 1014, 17 (“The interoperability of different implementations of the authentication protocols will rely, to some extent, on how tokens and messages (*e.g.*, the authentication information) are formatted and encoded.”)).

Patent Owner does not rebut Petitioner’s showings, and we agree with Petitioner that it would have been obvious to a person of ordinary skill that verifying the authentication information includes verifying whether the authentication information is in a proper format, as claimed.

Based on the complete record, we determine Petitioner has shown by a preponderance of the evidence that claim 6 is unpatentable as obvious in view of Giles.

h) Claim 8

8. The method of claim 1, wherein said authentication information is encrypted.

Among other things,⁵ Petitioner also argues that “a POSITA would have found it obvious in light of his or her knowledge, or in light of other references provided below, that challenge/response-based authentication could be practiced with encryption due to its benefits.” Pet. 42 (citing Ex. 1002 ¶ 103). Petitioner additionally cites Dr. Alpert and additional evidence to argue that the benefits of using encryption with challenge-response authentication protocols were well known. Pet. 42–43 (citing Ex. 1002 ¶¶ 103–105; Ex. 1014, 1; Ex. 1015, 397); Reply 11–12 (citing Ex. 1041 ¶ 38). “In light of these disclosures, and/or his or her own knowledge, a POSITA would have understood that authentication information could be encrypted, and would have been motivated to do so, given the known benefits of securing authentication information through encryption.” Pet. 43 (citing Ex. 1002 ¶ 105).

⁵ Petitioner alternately argues that Giles discloses or renders obvious claim 8 because “Giles discloses that ‘in the Secure Disabled mode, *decryption operations may be disabled*’ from which a POSITA would understand that authentication information in Giles can be encrypted and decrypted.” Pet. 42 (quoting Ex. 1008, 5:1–2 (emphasis added)) (citing Ex. 1002 ¶ 103). Petitioner argues that Giles’s secure processor has decryption operations which were at least used for decrypting video channels of Giles’s set-top box and for adding new security features on the chip. Pet. 42 (citing Ex. 1008, 5:25–30, 5:33–37; Ex. 1003 ¶ 103). We need not reach Petitioner’s alternate contentions or Patent Owner’s arguments for the reason discussed below.

Patent Owner argues Petitioner’s reasoning is conclusory and guided in improper hindsight. PO Resp. 35–37; Sur-reply 11–12. Dr. Przybylski merely parrots the Petition on this point. Ex. 2007 ¶ 87. Further, according to Patent Owner, Giles’s teachings of disabling the decryption operation for channels in its set-top-box “teach away from the idea of using the ‘existing decryption functionality (in) the authentication process.’” Sur-reply 11 (citing Ex. 1002 ¶ 103; Ex. 2007 ¶ 89); *see* Ex. 2009, 46:10–20.

We note that Dr. Przybylski’s testimony focuses on Petitioner’s arguments relating to disabling decryption (Ex. 2007 ¶¶ 88, 89), not on Petitioner’s arguments that the benefits of encryption for challenge-response authentication were well known. Nor does Dr. Przybylski explain with evidence why Petitioner’s reasoning is conclusory. We credit Dr. Alpert’s testimony and evidence of the known benefits of encryption in authentication processes like Giles’s challenge-response authentication. Ex. 1002 ¶¶ 104, 105; Ex. 1014, 1; Ex. 1015, 397; Ex. 1038, code (57); Ex. 1039, 8:30–32; Ex. 1041 ¶ 39). Giles expressly discloses that “the EJTAG debug port module 176 may undergo a challenge/response-based authentication via the UART port 110,” and the weight of the evidence establishes that it was well known to use encryption with challenge-response authentication processes. Thus, Petitioner has shown that a person of ordinary skill would have been motivated to encrypt the authentication information in Giles’s authentication process, and we determine Petitioner has shown by a preponderance of the evidence that claim 8 is unpatentable as obvious in view of Giles.

i) Claim 9

9. The method of claim 1, wherein said verifying said authentication information further comprises: verifying a password.

Petitioner contends Giles discloses or renders obvious claim 9 because Giles uses challenge-response authentication and verification process and “[a] POSITA would understand that even though a challenge-response authentication and verification process, if used, does not need to involve passwords, verifying the authentication information (*e.g.*, the identity of a user) by verifying a password is a common practice for a system to identify a user and allow access to its resources.” Pet. 44 (citing Ex. 1002 ¶ 107; Ex. 1015, 388–89). Petitioner additionally states that “[a]dditionally or alternatively, use of a password with a challenge-response was well known at the time and would have been obvious.” Pet. 44 (citing Ex. 1002 ¶ 107; Ex. 1016, 2029–30). Petitioner additionally argues that authentication by verifying a password was well known for challenge-response authentication techniques. Reply 13 (citing Ex. 1041 ¶ 42; Ex. 1038, code (57); Ex. 1039, 8:30–32).

Patent Owner states “Giles does not disclose the use of a password in connection with securing scan chain architecture. Dr. Alpert acknowledges that Giles does not disclose the use of a password.” PO Resp. 36 (citing Ex. 2009, 47:5–10; Ex. 2007 ¶ 91); *accord* Sur-reply 12; Ex. 2007 ¶ 91.

We note Patent Owner and Dr. Przybylski state only that Giles does not “disclose” the use of a password in connection with securing scan chain architecture without substantively addressing whether the use of a password in connection with securing scan chain architecture would have been obvious to a person of ordinary skill at the time of the invention. We credit

Dr. Alpert’s testimony and cited evidence that verifying a password would have been well known and obvious to a person of ordinary skill in implementing Giles’s challenge-response authentication. Ex. 1002 ¶ 107; Ex. 1015, 388–89; Ex. 1016, 2029–30; Ex. 1041 ¶ 42; Ex. 1038, code (57); Ex. 1039, 8:30–32.

Thus, Petitioner has shown that it would have been obvious to a person of ordinary skill to verify a password as part of Giles’s authentication process, and we determine Petitioner has shown by a preponderance of the evidence that claim 9 is unpatentable as obvious in view of Giles.

j) Claims 11 & 17

Independent claim 11 recites a system having limitations substantively equivalent⁶ to the method of independent claim 1, and independent claim 17 recites computer-executable instructions that cause a computing device to perform operations substantively equivalent to the method of claim 1. The parties rely on the same evidence and arguments addressed above regarding claim 1 for claims 11 and 17. Pet. 44–47 (addressing claim 11 with reference to Petitioner’s showings for claim 1), 51–53 (addressing claim 17 with reference to Petitioner’s showings for claim 1); PO Resp. 37 (stating “Petitioner advances the same arguments as asserted in connection with [c]laim 1”; arguing Giles does not disclose the limitations of claims 11 and 17 “for the reasons explained above” regarding claim 1).

⁶ Claim 11 recites a “software module” instead of the “software layer” recited in 1. The parties use the terms interchangeably. *See* Pet. 45 (“the ‘software module’ recited in claim 11 corresponds to the ‘software layer’ recited in claim 1”); PO Resp. 37 (arguing Giles does not contain “a software layer (or software module) and acknowledging that the Petition treats the terms interchangeably).

For the same reasons explained above, we determine Petitioner has shown by a preponderance of the evidence that claims 11 and 17 are unpatentable as obvious in view of Giles.

k) Claim 12

12. The system of claim 11, wherein said secure processor further comprises: an internal register for granting access to said scan interface, wherein said internal register is set if said authentication information is valid.

Petitioner relies on the same arguments and evidence addressed above for claims 3 and 4 to argue claim 12 is unpatentable. Pet. 48. Patent Owner does not separately address Petitioner's showings for claim 12, and we agree with Petitioner that the cited portions of Giles teach an internal register for granting access to the scan interface if the authentication information is valid, as claimed.

Based on the evidence of record, we determine Petitioner has shown by a preponderance of the evidence that claim 12 is unpatentable as obvious in view of Giles.

l) Claim 15

15. The system of claim 11, wherein access to said scan interface is denied by default upon bootstrapping said secure processor.

Claim 15 is substantively equivalent to claim 2, and Petitioner relies on the same arguments and evidence addressed above for claim 2 to argue claim 15 is unpatentable. Pet. 48. Patent Owner does not separately address Petitioner's showings for claim 15, and we agree with Petitioner that the cited portions of Giles teach that the scan interface is denied by default upon bootstrapping the secure processor, as claimed.

Based on the evidence of record, we determine Petitioner has shown by a preponderance of the evidence that claim 15 is unpatentable as obvious in view of Giles.

m) Claim 16

16. The system of claim 11 further comprising:

[16.a] a communication buffer for receiving said authentication information, wherein said communication buffer provides an interface to said software module for authentication purposes; and

The limitations of [16.a] are substantively similar to the limitations of claim 5, and Petitioner relies on the same arguments and evidence discussed above regarding claim 5. Patent Owner does not separately address this limitation, and we agree with Petitioner that the cited portions of Giles teach the limitations of [16.a] for the same reasons addressed above for claim 5.

[16.b] an authentication link that communicatively couples said communication buffer to said software module.

In addition to Petitioner's showing for claim 5, Petitioner contends Giles inherently discloses or renders obvious the claimed authentication link with its disclosure of a communication buffer that temporarily stores the response to the authentication challenge "to communicate at least the response from the communications buffer to the software module." Pet. 50. Patent Owner does not separately address claim 16, and we agree with Petitioner that it necessarily follows and would have been obvious that Giles uses or suggests a authentication link that communicatively couples the communication buffer and the software module, as claimed.

Based on the evidence of record, we determine Petitioner has shown by a preponderance of the evidence that claim 16 is unpatentable as obvious in view of Giles.

n) Claim 18

18. The computer-readable medium of claim 17, wherein said disabling further comprises: setting a register to a first state that disables said scan interface upon booting up said secure processor, wherein said register is internal to said secure processor.

Claim 18 includes limitations substantially similar to the limitations of claims 2 and 3, and Petitioner relies on the same arguments and evidence asserted for claims 2 and 3. Patent Owner does not separately address Petitioner's showing for claim 18, and we agree with Petitioner that Giles teaches the limitations of claim 18.

Based on the evidence of record, we determine Petitioner has shown by a preponderance of the evidence that claim 18 is unpatentable as obvious in view of Giles.

o) Claim 19

19. The computer-readable medium of claim 17, wherein said verifying said authentication information further comprises: verifying whether said authentication information is in a proper format.

Claim 19 includes limitations substantially similar to the limitations of claim 6, and Petitioner relies on the same arguments and evidence asserted for claim 6. Patent Owner does not separately address Petitioner's showing for claim 19, and we agree with Petitioner that Giles teaches the limitations of claim 19.

Based on the evidence of record, we determine Petitioner has shown by a preponderance of the evidence that claim 19 is unpatentable as obvious in view of Giles.

4. *Conclusion Regarding Ground 1*

Based on the entire record, for the reasons explained above, we determine Petitioner has shown by a preponderance of the evidence that claims 1–6, 8, 9, 11, 12, and 15–19 are unpatentable as obvious in view of Giles. Because we determine that all challenged claims are unpatentable in view of Giles, we do not reach Petitioner’s challenges of Grounds 2, 3, or 4.

III. CONCLUSION

For the reasons set forth above, based on the complete record, we determine that Petitioner has proven by a preponderance of the evidence that claims 1–6, 8, 9, 11, 12, and 15–19 of the ’002 patent are unpatentable as obvious in view of Giles.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that Petitioner has shown by a preponderance of the evidence that claims 1–6, 8, 9, 11, 12, and 15–19 are unpatentable;

FURTHER ORDERED that, because this is a Final Written Decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

In summary⁷:

⁷ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner’s attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. See 37 C.F.R. § 42.8(a)(3), (b)(2)

Claims	35 U.S.C. §	Reference(s)/Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–6, 8, 9, 11, 12, 15–19	103	Giles	1–6, 8, 9, 11, 12, 15–19	
1, 2, 5, 6, 8, 9, 11, 15–17, 19 ⁸	103	Moyer		
3, 4, 12, 18	103	Moyer, Giles		
1, 2, 5, 6, 8, 9, 11, 15–17, 19	103	Moyer, Giles		
OVERALL OUTCOME			1–6, 8, 9, 11, 12, 15–19	

⁸ We do not reach this alternate ground. *See SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1359 (2018) (holding that a petitioner “is entitled to a final written decision addressing all of the claims it has challenged.”); *see also* 35 U.S.C. § 318(a).

IPR2021-01567
Patent 7,810,002 B2

FOR PETITIONER:

Sanjeet K. Dutta
Suhrid Wadekar
GOODWIN PROCTER LLP
sdutta@goodwinlaw.com
swadekar@goodwinlaw.com

FOR PATENT OWNER:

Justin J. Oliver
Sarah S. Brooks
Seth Boeshore
VENABLE LLP
joliver@venable.com
ssbrooks@venable.com
sboeshore@venable.com