UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/597,773	10/09/2019	Scott MacDonald WARD	5061-0041CON	8373

39083 7590 09/18/2020

KENEALY VAIDYA LLP
3050 K Street, N.W.
Suite 302
Washington, DC 20007

EXAMINER	
HENNING, MATTHEW T	

ART UNIT	PAPER NUMBER
2491	

NOTIFICATION DATE	DELIVERY MODE
09/18/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

avaidya@kviplaw.com
uspto@kviplaw.com

Office Action Summary	Application No. 16/597,773	Applicant(s) WARD et al.	
	Examiner MATTHEW T HENNING	Art Unit 2491	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 7/13/2020.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☑ This action is **FINAL.** 2b) ☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-28 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-28 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 10/9/2019 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

The present application is being examined under the pre-AIA first to invent provisions.

This action is in response to the communication filed on 7/13/2020.

DETAILED ACTION

The examiner has considered the applicants' arguments and does not find them sufficient to overcome all objections and rejections.

The amendments to claim 5 have overcome the rejection under 35 USC 112.

The applicants' argument regarding the use of means plus function language are not found persuasive. While the language of the specification does describe structure, the specification does not clearly link the structure, material, or acts to the claimed functions. As such, the person having ordinary skill in the art would not be able to ascertain the scope of the claimed invention. Therefore, the rejections of claim 23-25 are maintained.

On page 13 of the response, the applicants make an incorrect allegation that in Proudler "clearly the address spaces of the trusted device 24 and of main processor 21 are the same", based on the description of Fig. 7 of Proudler. The examiner suggests that all the cited portion makes clear is that the trusted device is addressable, and this is not necessarily always true because this was just one possible solution Proudler presented for how the trusted device controls the processor before the BIOS is able to control the processor.

The examiner notes that Paragraph 0033 explicitly states that the trusted device contains processes which are inaccessible to other platform functions, thereby providing an environment which is substantially immune to unauthorized modification.

The applicants allege that Proudler does not teach "a separate processing environment inaccessible to said operating system". In Proudler, the trusted device is a separate operating environment which runs authentication software and is independent from and inaccessible to the

operating system. This is evidenced throughout the specification of Proudler. Paragraphs 0033, and 0044-0048 provide an overview of the trusted device, including that the device is tamperproof and its contents are inaccessible outside of the trusted device 24 (which is a part of the trusted computing platform, and therefore "inside". This meets the contested limitation. Fig. 11 and paragraphs 0070-0071 clearly show there are two different spaces, the user space 400 and the trusted space 401. The user space is under control of the operating system while the trusted space is supported by the processor and memory within trusted device 24. As such, the examiner does not find the allegation persuasive.

The applicants allege that Proudler does not teach "a memory being a secure part of a BIOS system or any other secure location in said electronic device, wherein said memory is inaccessible to the operating system". In Proudler, the trusted device is a separate operating environment which runs authentication software, stores secure data such as private keys, integrity measurements, etc. and is independent from and inaccessible to the operating system. This is evidenced throughout the specification of Proudler. Paragraphs 0033, and 0044-0048 provide an overview of the trusted device, including that the device is tamperproof and its contents are inaccessible outside of the trusted device. Proudler further teaches main memory 22 which is accessible by the operating system. This meets the contested limitation. Fig. 11 and paragraphs 0070-0071 clearly show there are two different spaces, the user space 400 and the trusted space 401. The user space is under control of the operating system while the trusted space is supported by the processor and memory within trusted device 24. As such, the examiner does not find the allegation persuasive.

The applicants allege that Proudler does not teach "providing authentication data or authentication software inaccessible to said operating system". In Proudler, the trusted device is a separate operating environment which runs authentication software, stores secure data such as private keys, integrity measurements, etc. and is independent from and inaccessible to the operating system. This is evidenced throughout the specification of Proudler. Paragraphs 0033, and 0044-0048 provide an overview of the trusted device, including that the device is tamperproof and its contents are inaccessible outside of the trusted device. Proudler further teaches main memory 22 which is accessible by the operating system. This meets the contested limitation. Fig. 11 and paragraphs 0070-0071 clearly show there are two different spaces, the user space 400 and the trusted space 401. The user space is under control of the operating system while the trusted space is supported by the processor and memory within trusted device 24. As such, the examiner does not find the allegation persuasive.

The applicants' allegation that "Proudler repeatedly suggests that processor 21 needs access to the memory of trusted device 24…" is merely an allegation without support and further without addressing the rejection as the examiner has presented it. The applicants' conclusory allegations based off of language which does not teach what is being alleged will not be found persuasive. If the applicants wish to argue that Proudler teaches that memory 24 must be accessible by the main processor 21, then the applicants need to point to the specific language of Proudler that states as such. The examiner will not find the applicants' mere allegations to be persuasive. The examiner has already shown that protected device 24, for example as recited in paragraph 0033 of Proudler, "a most desirable implementation would be to make the trusted device tamperproof, to protect secrets by making them inaccessible to other platform functions and provide an environment that is substantially immune to unauthorised modification."

The applicants' seem to be misunderstanding the teachings of Proudler. While Proudler teaches the main processor 21 treating the trusted device 24 as a memory, in that the device is addressable by the main processor 21, this is not the same as the main processor 21 accessing the internal memory of the trusted device 24. The internal memory of trusted device 24 is not accessible to the main processor 21. It is only accessible to the trusted device 24. As such, the examiner does not find the arguments persuasive.

Regarding the combination of Proudler and Constable, the applicants allege that it would not be possible to combine the teachings of Constable with the system of Proudler because "since Proudler suggests a system from which the machine can be booted [while Constable] presupposes that booting is already done", the examiner does not find the argument persuasive. Proudler Fig. 11 and Paragraphs 0069-0071 make very clear that the system of Proudler operates both a user space and a trusted space (in the trusted device) simultaneously. This presupposes that booting has already occurred. Constable is simply teaching that the isolated environments should hide their memory spaces from each other. As such, the examiner does not find the argument persuasive.

The applicants' allegation that Dryer cannot be combined with Proudler is not found persuasive. The applicant' appear to be attacking different teachings of Dryer than relied upon by the examiner. The examiner is merely relying upon the teachings of Dryer which suggest that all data for storage can be transparently encrypted. The applicants have not addressed this combination, and as such the examiner does not find the argument persuasive.

Regarding the applicants' arguments that Proudler does not teach that the stored authentication data is encrypted, the examiner reminds the applicants that Proudler is not being

relied upon as teaching this limitation, and as such the examiner does not find the argument persuasive.

Because the examiner does not find the arguments persuasive, the rejections have been maintained below.

All objections and rejections not set forth below have been withdrawn.

The examiner notes that if rewritten in independent form, including all limitations from their parent claims, claims 11, 15, and 16 would be allowable, assuming copending application umber 10/560,579 has not been allowed.

Claims 1-28 have been examined.

Claim Rejections - 35 USC § 112

The following is a quotation of 35 U.S.C. 112(f):

> (f) Element in Claim for a Combination. – An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

The following is a quotation of pre-AIA 35 U.S.C. 112, sixth paragraph:

> An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

Claims 23-25 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

Regarding claims 23-25, claim limitations "means for providing…", "means for activating…" invoke 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph. However, the written description fails to disclose the corresponding structure, material, or acts for performing

the entire claimed function and to clearly link the structure, material, or acts to the function. Therefore, the claim is indefinite and is rejected under 35 U.S.C. 112(b) or pre-AIA 35 U.S.C. 112, second paragraph.

Applicant may:

(a) Amend the claim so that the claim limitation will no longer be interpreted as a limitation under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph;

(b) Amend the written description of the specification such that it expressly recites what structure, material, or acts perform the entire claimed function, without introducing any new matter (35 U.S.C. 132(a)); or

(c) Amend the written description of the specification such that it clearly links the structure, material, or acts disclosed therein to the function recited in the claim, without introducing any new matter (35 U.S.C. 132(a)).

If applicant is of the opinion that the written description of the specification already implicitly or inherently discloses the corresponding structure, material, or acts and clearly links them to the function so that one of ordinary skill in the art would recognize what structure, material, or acts perform the claimed function, applicant should clarify the record by either:

(a) Amending the written description of the specification such that it expressly recites the corresponding structure, material, or acts for performing the claimed function and clearly links or associates the structure, material, or acts to the claimed function, without introducing any new matter (35 U.S.C. 132(a)); or

(b) Stating on the record what the corresponding structure, material, or acts, which are implicitly or inherently set forth in the written description of the specification, perform

the claimed function. For more information, see 37 CFR 1.75(d) and MPEP §§ 608.01(o) and 2181.

Claim Rejections - 35 USC § 103

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-10, 12-14, and 21-28 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Proudler (US Patent Application Publication Number 2003/0041250), and further in view of Constable et al. (US Patent Application Publication Number 2002/0095557) hereinafter referred to as Constable, and further in view of Dryer (US Patent Application Publication Number 2002/0099666).

Regarding claims 1, 23, 24, and 26-28, Proudler disclosed a method for performing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party (Proudler Figs. 10 and 12 and Paragraphs 0058-0064 and 0134-0135), the electronic device having an operating system creating a run-time environment for user applications (Proudler Fig. 11 and Paragraphs 0070-0071 and 0075), the method comprising: providing authentication data in a memory of said electronic device, said memory being a secure part of a Basic In Out System or any other secure location in said electronic device (Proudler Fig. 11 and Paragraphs 0070-0071 and 0075), which authentication

data are inaccessible to a user of said electronic device (Proudler Fig. 11 and Paragraphs 0070-0071 and 0075), wherein said memory is inaccessible to said operating system of said electronic device, thereby rendering the authentication data inaccessible to said user (Proudler Fig. 11 and Paragraphs 0070-0071 and 0075); providing authentication software in said electronic device, the authentication data being accessible to said authentication software, wherein authentication software is stored in said secure memory inaccessible to said operating system (Proudler Figs. 10 and 12 and Paragraphs 0058-0064 and 0134-0135); activating the authentication software to generate a digital signature from the authentication data, wherein the authentication software is run in a secure processing environment inaccessible to said operating system (Proudler Figs. 10 and 12 and Paragraphs 0058-0064 and 0134-0135); providing the digital signature to the second transaction party (Proudler Figs. 10 and 12 and Paragraphs 0058-0064 and 0134-0135), but Proudler did not explicitly teach that the secure storage locations are not reported to the operating system.

Constable taught a system where physical memory is shared amongst various isolated environments, but that each isolated environment hides its physical memory space from the others (Constable Paragraph 0075).

It would have been obvious to the person having ordinary skill in the art before the effective filing date of the invention to have employed the teachings of Constable in the trusted computing environment of Proudler by having each environment hide their physical memory space from the other environments. This would have been obvious because the person having ordinary skill in the art would have been motivated to protect the memory subsystems from unwanted corruption or destruction.

Proudler and Constable further did not explicitly teach that the authentication data are encrypted when the authentication data are stored in said memory, a decryption key for decrypting the authentication data being incorporated in the electronic device, and said decryption key being inaccessible to said user, to any user-operated software and to said operating system.

Dryer taught a storage system which transparently encrypted all data for storage (Dryer Paragraph 0011 for example).

It would have been obvious to the person having ordinary skill in the art at the time of invention to have employed the teachings of Dryer in the system of Proudler and Constable by encrypting all data being stored and decrypting the data when it is retrieved. This would have been obvious because the person having ordinary skill in the art would have been motivated to further protect the data being stored from illicit access.

Further in this combination, it would have been obvious that the encryption key for encrypting the data would be available on the device and inaccessible, as Proudler already disclosed that the cryptographic operations and materials are contained in secure storage inaccessible from the outside (Proudler Paragraphs 0033, 0080, and 0103 for example).

Regarding claim 2, Proudler, Constable, and Dryer taught that the authentication data are provided by the second transaction party, which stores the authentication data together with data identifying the first transaction party (Proudler Figs. 10 and 12 and Paragraphs 0058-0065 and 0134-0135).

Regarding claim 3, Proudler, Constable, and Dryer taught that the second transaction party uses the stored authentication data to obtain transaction specific authentication data

according to a specific algorithm (Proudler Figs. 10 and 12 and Paragraphs 0058-0064 and 0134-0135).

Regarding claim 4, Proudler, Constable, and Dryer taught that the second transaction party verifies the digital signature provided by the first transaction party using the authentication data stored at the second transaction party (Proudler Figs. 10 and 12 and Paragraphs 0058-0064 and 0134-0135).

Regarding claim 5, Proudler, Constable, and Dryer taught that the authentication software has its own unique serial number, software ID and/or private encryption key (Proudler Paragraph 0046 and 0048).

Regarding claim 6, Proudler, Constable, and Dryer taught that the authentication data are encrypted by the second transaction party using an encryption key before the authentication data are provided to the first transaction party (Proudler Paragraph 0071).

Regarding claim 7, Proudler, Constable, and Dryer taught that the authentication software retrieves a decryption key associated with the encryption key and decrypts the authentication data at its first use (Proudler Paragraph 0044 and 0136).

Regarding claim 8, Proudler, Constable, and Dryer taught that the authentication software is installed in an application environment in the secure area such that it may obtain the authentication data without passing through an unsecured part of said electronic device (Proudler Paragraph 0071 and Constable Paragraph 0075).

Regarding claim 9, while Proudler, Constable, and Dryer did not explicitly teach that the authentication data are encrypted using at least two encryption layers, it was well known in the art of information security for a sender to encrypt data being transmitted using both the private

key of the sender and the public key of the recipient, allowing the data to be authenticated as sent by the sender as well as only decryptable by the receiver. As such, it would have been obvious to the person having ordinary skill in the art before the effective filing date of the invention to have done so in the system of Proudler and constable. This would have been obvious because the person having ordinary skill in the art would have been motivated to both protect the challenge from being intercepted, as well as to authenticate that the challenge came from the user.

Regarding claim 10, Proudler, Constable, and Dryer taught that the authentication data are encrypted using an encryption key which is associated with a hardware device serial number (Proudler Paragraph 0046 and 0048).

Regarding claim 12, Proudler, Constable, and Dryer taught that the decryption key is associated with one or more serial numbers of hardware components of said electronic device (Proudler Paragraph 0046 and 0048).

Regarding claim 13, Proudler, Constable, and Dryer taught that the authentication data is decrypted by the authentication software (Proudler Paragraphs 0044 and 0071 and the rejection of claim 9 above).

Regarding claim 14, Proudler, Constable, and Dryer taught that the authentication data is decrypted by an application stored in the electronic device using a device specific encryption key (Proudler Paragraph 0044, 0046, 0048, and 0071).

Regarding claim 21, Proudler, Constable, and Dryer taught identifying the user of the electronic device before activating the authentication software (Proudler Paragraph 0032).

Regarding claim 22, Proudler, Constable, and Dryer taught that the authentication software has a private encryption key for encrypting digital data (Proudler Paragraph 0046 and 0048).

Regarding claim 25, Proudler, Constable, and Dryer taught that the electronic device is a personal computer, a cellular phone, a hand-held personal digital assistant with wireless communication capabilities, or a device containing a BIOS (Proudler Paragraph 0037).

Claims 17-20 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Proudler and Constable, and further in view of Unicate (WO 00/67143).

Regarding claim 17-20, Proudler, Constable, and Dryer did not explicitly teach that the authentication data include an authentication table.

Unicate teaches an authentication system wherein the authentication data comprise an authentication table, wherein the authentication table is generated from a bit string which is generated from fixed data and variable data, wherein the fixed data are at least part of a serial number of a hardware device, wherein the fixed data are at least part of a device specific software identification code of the authentication software, wherein the variable data comprise a random table, wherein the random table is calculated from a random two-dimensional or three-dimensional pattern, or wherein the authentication table is generated from fixed data, variable data and a bit string, which bit string is specific to a trusted third party that provides the authentication data (Unicate Page 13 Line 34 – Page 15 Line 2). Unicate further teaches that to use the authentication data to generate a signature of content, hashing the content resulting in reference numbers referring to positions in authentication data stored in the electronic device;

and generating the digital signature using data components from the authentication data at said positions (Unicate Page 14 Lines 7-22).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Unicate in the content player system of Proudler and Constable by employing the authentication table for generating the signatures. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a secure transaction without the need for cryptography.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on nonstatutory double patenting provided the reference application or patent either is shown to be commonly owned with the

examined application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. See MPEP § 717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP § 2159. See MPEP §§ 706.02(l)(1) - 706.02(l)(3) for applications not subject to examination under the first inventor to file provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www.uspto.gov/patent/patents-forms. The filing date of the application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

Claims 1-28 are provisionally rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-2, 4, 7-8, 10-11, 13-25, 29, 33-38, and 42-43 of copending Application No. 10/560,579. Although the claims at issue are not identical, they are not patentably distinct from each other because the instant claims are essentially anticipated by the copending claims. The main difference regarding the encryption of the authentication data and the secure storage of the decryption key, which has been shown above to be obvious.

This is a provisional nonstatutory double patenting rejection because the patentably indistinct claims have not in fact been patented.

Allowable Subject Matter

Claims 11, 15, and 16 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims, assuming that copending application 10/560,579 is not allowed before such an amendment is made.

Conclusion

Claims 1-28 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW T HENNING whose telephone number is (571)272-3790. The examiner can normally be reached on M-F 8-4 EST.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ashok Patel can be reached on (571)272-3972. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see https://ppair-my.uspto.gov/pair/PrivatePair. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MATTHEW T HENNING/
Primary Examiner, Art Unit 2491

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16597773
Filing Date	2019-10-09
First Named Inventor	Scott MacDonald WARD
Art Unit	2491
Examiner Name	Matthew T. HENNING
Attorney Docket Number	5061-0041CON

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.T.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16597773
Filing Date	2019-10-09
First Named Inventor	Scott MacDonald WARD
Art Unit	2491
Examiner Name	Matthew T. HENNING
Attorney Docket Number	5061-0041CON

	1	"BIOS Boot Specification, Compaq Computer Corporation," Phoenix Technologies Ltd., Intel Corporation, Version 1.01, January 11, 1996, pp. 1-46.	
	2	"Phoenix Technologies and Orbid Corporation Partner in Development of Secure Digital Rights Management Solution," Phoenix Technologies, 2003, 2 pages.	
	3	"What Is The BIOS?," Computing Basics, Vol. 5 Issue 7, July 1994, 8 pages.	
	4	"Federal Communications Commission Radio Frequency Interference Statement," Technical Reference, IBM Personal Computer XT Hardware Reference Library, 1983, 215 pages.	
	5	B. YEE, "Using Secure Coprocessors," School of Computer Science, Carnegie Mellon University, May 1994, 104 pages.	
	6	G. J .POPEK et al, "Encryption and Secure Computer Networks," Computing Surveys, Vol. 11, No. 4, December 1979, pp. 331- 356.	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/MATTHEW T HENNING/	Date Considered	09/14/2020

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.T.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16597773
Filing Date	2019-10-09
First Named Inventor	Scott MacDonald WARD
Art Unit	2491
Examiner Name	Matthew T. HENNING
Attorney Docket Number	5061-0041CON

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Eric D. Morehouse/	Date (YYYY-MM-DD)	2020-08-11
Name/Print	Eric D. Morehouse	Registration Number	38565

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.T.H/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.T.H/