



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.
17/123,018	12/15/2020	Bjorn Markus Jakobsson	MJAKP026	1102
21912 7590 01/28/2022 VAN PELT, YI & JAMES LLP 10050 N. FOOTHILL BLVD #200 CUPERTINO, CA 95014			EXAMINER STEINLE, ANDREW J	
			ART UNIT 2497	PAPER NUMBER
			NOTIFICATION DATE 01/28/2022	DELIVERY MODE 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):

usptocorrespondence@ip-patent.com

DETAILED ACTION

Notice of Pre-AIA or AIA Status

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

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 claims at issue 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); and *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 a nonstatutory double patenting ground provided the reference application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of

activities undertaken within the scope of a joint research agreement. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO internet Web site contains terminal disclaimer forms which may be used. Please visit <http://www.uspto.gov/forms/>. The filing date of the application will determine what form 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 <http://www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp>.

Claims 1-22 are provisionally rejected on the ground of nonstatutory double patenting as being unpatentable over **Claims 1-5, 8-11, 13, 16-17, 19, 21 of U.S. Patent 9,294,452, Claims 2, 4-5, 8, 10-11, 13-15, 17, 19-22, and 24-41 of U.S. Patent 10,360,351, Claims 2-26 of U.S. Patent 10,521,568, and Claims 1-21 of U.S. Patent 10,929,512**. Although the claims at issue are not identical, they are not patentably distinct from each other because aside from a few minor differences, these claims contain the same limitations and perform the same functions.

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

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 negated by the manner in which the invention was made.

In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

Claims 1-3, 7-9, 11-14, and 17-22 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Shah et al., (US 20080059804 A1) **hereinafter referred to as Shah** in view of Johansson (US 8776214 B1) **hereinafter referred to as Johansson**.

Regarding **Claims 1, 17, and 18**, Shah discloses ***A system, comprising: one or more processors configured to: receive, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;*** [paragraph 0014, After the initial setup, users can sign into their workstation, either as they did before, or through a new E-SSO software interface. When users request to connect to applications using their workstation, the E-SSO software automatically populates the user ID and password fields of the applications' login pages]

access at least one record stored on the first device, [paragraph 0014, To implement E-SSO, a copy of the E-SSO software must be installed on each WTRU. User ID and password for every system and application are stored in a local file]

the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, [paragraph 0014, After the initial setup, users can sign into their workstation, either as they did before, or through a new E-SSO software interface. When users request to connect to applications using their workstation, the E-SSO software automatically populates the user ID and password fields of the applications' login pages]

receive authentication input from the user; [paragraph 0016, Some E-SSO systems support the use of authentication technologies other than passwords to sign into the workstation and to access a user's credential profile, including smart cards, authentication tokens or biometric samples – user authenticates to the E-SSO system]

determine that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device; [Claim 1, for comparing said received user authentication data to the stored user authentication data, and forwarding said stored user specific login information if said comparison is positive]

retrieve at least a portion of the credential information from the at least one record stored on the first device; [paragraph 0014, After the initial setup, users can sign into their workstation, either as they did before, or through a new E-SSO software interface. When users request to connect to applications using their workstation, the E-SSO software automatically populates the user ID and password fields of the applications' login pages]

facilitate access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; [paragraph 0014, When users request to connect to applications using their workstation, the E-SSO software automatically populates the user ID and password fields of the applications' login pages]

Shah does not explicitly teach ***wherein the credential information comprises a cryptographic key; and initiate a backup, to a second device, of at least a portion of the at least one record; and a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.***

Johansson teaches ***wherein the credential information comprises a cryptographic key;*** [Column 5, lines 17-23, For example, the user may provide to the authentication manager 124 existing security credentials such as, for example, usernames, passwords, security keys, certificates, and/or other security credentials along with identifying information for the network sites 140 and/or uniform resource locators (URLs) associated with the security credentials – the credential information includes “security keys”]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Johansson with the disclosure of Shah. The motivation or suggestion would have been to include multiple credential options. (Column 5, lines 12-27)

and initiate a backup, to a second device, of at least a portion of the at least one record; and a memory coupled to the one or more processors and configured to provide the one or more processors with instructions. [Column 5, lines 30-34, the authentication manager 124 may back up the account information to account data 160 located on the remote data server 106, account data 163 located on in the portable data store 118, and/or another location]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Johansson with the disclosure of Shah. The motivation or suggestion would have been to include multiple credential options. (Column 5, lines 12-27)

Regarding Claim 2, Shah does not explicitly teach ***wherein the second device is used to authenticate the user to one or more external resources.***

Johansson teaches ***wherein the second device is used to authenticate the user to one or more external resources.*** [Column 4, lines 59-63, The portable data store 118 may be configured to store account data 163. The account data 163 may include, for example, security credentials used to access various network sites 140 or network pages 145, information regarding authentication endpoints 139, and/or other information]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Johansson with the disclosure of Shah. The motivation or suggestion would have been to provide redundancy and to mitigate loss of data.

Regarding Claim 3, Shah does not explicitly teach *wherein the backup is completed after the first device has performed a verification that the second device conforms to a policy associated with the at least one record stored on the first device.*

Johansson teaches *wherein the backup is completed after the first device has performed a verification that the second device conforms to a policy associated with the at least one record stored on the first device.* [Column 5, lines 30-36, the authentication manager 124 may back up the account information to account data 160 located on the remote data server 106, account data 163 located on in the portable data store 118, and/or another location. In some embodiments, the authentication manager 124 may not store the account information on the client 103 at all and may only use other locations – the policy is that the backup cannot be stored on the client]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Johansson with the disclosure of Shah. The motivation or suggestion would have been to provide redundancy and to mitigate loss of data.

Regarding Claim 7, Shah does not explicitly teach *wherein subsequent to completion of the backup, the second device comprises a first profile associated with the user of the first device, and a second profile associated with a second user different from the user of the first device.*

Johansson teaches *wherein subsequent to completion of the backup, the second device comprises a first profile associated with the user of the first*

device, and a second profile associated with a second user different from the user of the first device. [Column 5, lines 43-56, Security credentials may be shared among multiple users of the authentication manager 124. As a non-limiting example, several users in an organization may share an online banking account. A first user may create a username and password for the account using the authentication manager 124. The first user may mark the account as shared and provide a list of users that are authorized to access the account, including a second user. When the account is distributed to account data 130, 160, it is secured such that only the authorized users can access it. When the second user next uses the authentication manager 124, the second user may be given the opportunity to synchronize the new account with account data 163 located in the portable data store 118 belonging to the second user or in some other location] [Column 5, lines 30-34, the authentication manager 124 may back up the account information to account data 160 located on the remote data server 106, account data 163 located on in the portable data store 118, and/or another location]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Johansson with the disclosure of Shah. The motivation or suggestion would have been to include multiple credential options. (Column 5, lines 12-27)

Regarding Claim 8, Shah does not explicitly teach *wherein the one or more processors are further configured to: determine that the authentication input from the user does not match authentication information of a first profile; and subsequent to determining that the authentication input from the user does not match the authentication information of the first profile, determine that the*

authentication input from the user matches authentication information of a second profile, wherein the first profile is associated with a different user than the second profile.

Johansson teaches ***wherein the one or more processors are further configured to: determine that the authentication input from the user does not match authentication information of a first profile; and subsequent to determining that the authentication input from the user does not match the authentication information of the first profile, determine that the authentication input from the user matches authentication information of a second profile, wherein the first profile is associated with a different user than the second profile.*** [Column 10, lines 8-15, the authentication manager 124 may give an indication of success or failure and may provide another authentication button 218 in order to log out of the network site 140. If multiple user accounts are present for the network site 140, the authentication manager 124 may provide a drop-down box or other user interface element allowing the user to select one of the accounts for authentication]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Johansson with the disclosure of Shah. The motivation or suggestion would have been to include multiple credential options. (Column 5, lines 12-27)

Regarding Claim 9, Shah discloses wherein the at least one record stored on the first device is stored in a secure storage, and where the one or more processors are configured to access the record stored on the secure storage using a restricted interface. [paragraph 0064, The TPM/TSS 815 interacts with both

the SASO proxy unit 810 and the WAA 820 to provide a secure, trusted mechanism to generate, store, and retrieve passwords and SSO credentials]

Regarding Claim 11, Shah discloses *wherein the restricted interface comprises an application programming interface*. [paragraph 0064, The TPM/TSS 815 interacts with both the SASO proxy unit 810 and the WAA 820 to provide a secure, trusted mechanism to generate, store, and retrieve passwords and SSO credentials]

Regarding Claim 12, Shah does not explicitly teach *wherein the backup causes a certificate to be transmitted to the second device*.

Johansson teaches *wherein the backup causes a certificate to be transmitted to the second device*. [Column 5, lines 30-34, the authentication manager 124 may back up the account information to account data 160 located on the remote data server 106, account data 163 located on in the portable data store 118, and/or another location]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Johansson with the disclosure of Shah. The motivation or suggestion would have been to include multiple credential options. (Column 5, lines 12-27)

Regarding Claim 13, Shah discloses *wherein the certificate is generated at least in part by the first device*. [paragraph 0072, The USIM could also be configured to generate and store of high-entropy site-specific passwords and also to store SSO password and SSO credentials]

Regarding Claim 14, Shah discloses *wherein the authentication input from the user is received using a biometric user input element*. [paragraph 0016, Some

E-SSO systems support the use of authentication technologies other than passwords to sign into the workstation and to access a user's credential profile, including smart cards, authentication tokens or biometric samples]

Regarding Claims 19 and 21, Shah does not explicitly teach *wherein the one or more processors are configured to access records associated with at least two different users.*

Johansson teaches *wherein the one or more processors are configured to access records associated with at least two different users.* [Column 10, lines 8-15, the authentication manager 124 may give an indication of success or failure and may provide another authentication button 218 in order to log out of the network site 140. If multiple user accounts are present for the network site 140, the authentication manager 124 may provide a drop-down box or other user interface element allowing the user to select one of the accounts for authentication]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Johansson with the disclosure of Shah. The motivation or suggestion would have been to include multiple credential options. (Column 5, lines 12-27)

Regarding Claims 20 and 22, Shah does not explicitly teach *wherein the records associated with the at least two different users are stored on the first device.*

Johansson teaches *wherein the records associated with the at least two different users are stored on the first device.* [Column 5, lines 43-48, Security credentials may be shared among multiple users of the authentication manager 124. As

a non-limiting example, several users in an organization may share an online banking account. A first user may create a username and password for the account using the authentication manager 124] [Column 5, lines 34-36, In some embodiments, the authentication manager 124 may not store the account information on the client 103 at all and may only use other locations – indicates that only in “some embodiments”, the authentication manager cannot store account information on the client or the device which means that in other embodiments, it is able to do this]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Johansson with the disclosure of Shah. The motivation or suggestion would have been to include multiple credential options. (Column 5, lines 12-27)

Claims 4-6 and 10 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Shah in view of Johansson, as applied to **Claims 1, 17, and 18**, respectively, above, and further in view of Owen et al., (US 20070257104 A1) **hereinafter referred to as Owen.**

Regarding Claim 4, the combination of Shah and Johansson does not explicitly teach *wherein the backup is completed after a secure channel is established by at least one of the first device and the second device.*

Owen teaches *wherein the backup is completed after a secure channel is established by at least one of the first device and the second device.* [paragraph 0162, Then, at block 1430, the secure internet portal 70 initiates a private connection 65 with the remote computer 55 by, for example, forming an encrypted VPN connection

between the two computers. In certain embodiments, the encryption level of the connection can be scaled according to the bandwidth of the transmission channel between the two computers]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Owen with the disclosures of Shah and Johansson. The motivation or suggestion would have been to ensure a secure connection between devices in order to mitigate against nefarious actions]

Regarding Claim 5, the combination of Shah and Johansson does not explicitly teach ***wherein the first device and the second device are configured to complete a pairing process.***

Owen teaches ***wherein the first device and the second device are configured to complete a pairing process.*** [paragraph 0162, Then, at block 1430, the secure internet portal 70 initiates a private connection 65 with the remote computer 55 by, for example, forming an encrypted VPN connection between the two computers. In certain embodiments, the encryption level of the connection can be scaled according to the bandwidth of the transmission channel between the two computers]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Owen with the disclosures of Shah and Johansson. The motivation or suggestion would have been to ensure a secure connection between devices in order to mitigate against nefarious actions]

Regarding Claim 6, the combination of Shah and Johansson does not explicitly teach ***wherein the pairing process comprises a comparison of data generated from one or more authentication inputs.***

Owen teaches ***wherein the pairing process comprises a comparison of data generated from one or more authentication inputs.*** [paragraph 0162, Then, at block 1430, the secure internet portal 70 initiates a private connection 65 with the remote computer 55 by, for example, forming an encrypted VPN connection between the two computers. In certain embodiments, the encryption level of the connection can be scaled according to the bandwidth of the transmission channel between the two computers]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Owen with the disclosures of Shah and Johansson. The motivation or suggestion would have been to ensure a secure connection between devices in order to mitigate against nefarious actions]

Regarding Claim 10, the combination of Shah and Johansson does not explicitly teach ***wherein the restricted interface comprises a dedicated physical connection.***

Owen teaches ***wherein the restricted interface comprises a dedicated physical connection.*** [paragraph 0054, the biometrically-secured device is a portable device similar in appearance to a flash drive (e.g., a "jump drive" or a "thumb drive")]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Owen with the disclosures of Shah and Johansson. The motivation or suggestion would have been to

ensure a secure connection between devices in order to mitigate against nefarious actions]

Claim 15 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Shah in view of Johansson, as applied to **Claim 1**, above, and further in view of Gardner et al., (US 20140250079 A1) **hereinafter referred to as Gardner**.

Regarding Claim 15, the combination of Shah and Johansson does not explicitly teach ***wherein the backup comprises copying a modified version of a vault to the second device.***

Gardner teaches ***wherein the backup comprises copying a modified version of a vault to the second device.*** [paragraph 0004, Using this approach, individual files are backed up if they have been modified since the previous backup]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Gardner with the disclosures of Shah and Johansson. The motivation or suggestion would have been to ensure the latest files are backed up. (paragraph 0004)

Allowable Subject Matter

Claim 16 is but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims and if the Double Patenting rejection was obviated.

The following is an examiner's statement of reasons for allowance:

Regarding Claim 16, none of the closest prior art of record explicitly teaches nor suggests in detail ***wherein the backup is performed in response to a determination that the first device is of a same brand as the second device*** in view of other limitations of the intervening claims.

Thus the prior arts of record taking singly or in combination do not teach or suggest the above-stated limitations taking wholly in combination with all the elements of each independent claim.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW J STEINLE whose telephone number is (571)272-9923. The examiner can normally be reached M-F 10am-6pm CT.

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, Eleni Shiferaw can be reached on (571) 272-3867. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: <https://patentcenter.uspto.gov>. Visit <https://www.uspto.gov/patents/apply/patent->

center for more information about Patent Center and
<https://www.uspto.gov/patents/docx> for information about filing in DOCX format. For
additional questions, contact the Electronic Business Center (EBC) at 866-217-9197
(toll-free). If you would like assistance from a USPTO Customer Service
Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ANDREW J STEINLE/
Primary Examiner, Art Unit 2497