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.
14/739,975	06/15/2015	Adam Rykowski	W205.01 (500102-1950)	8119

152577 7590 01/28/2020
Thomas | Horstemeyer, LLP (VMW)
3200 Windy Hill Road, SE
Suite 1600E
Atlanta, GA 30339

EXAMINER	
MCCOY, RICHARD ANTHONY	
ART UNIT	PAPER NUMBER
2431	
NOTIFICATION DATE	DELIVERY MODE
01/28/2020	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):

docketing@thomashorstemeyer.com
ipadmin@vmware.com
uspatents@thomashorstemeyer.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte ADAM RYKOWSKI, ASHISH JAIN, DALE ROBERT OLDS,
EMILY HONG XU, KABIR BARDAY, KYLE AUSTIN, SRIDHARA
BABU KOMMIREDDY, JONATHAN BLAKE BRANNON,
and CAMILO LOTERO

Appeal 2019-000436
Application 14/739,975
Technology Center 2400

Before JOHN A. JEFFERY, JUSTIN BUSCH, and CARL L. SILVERMAN, *Administrative Patent Judges*.

JEFFERY, *Administrative Patent Judge*.

DECISION ON APPEAL

Under 35 U.S.C. § 134(a), Appellant[1] appeals from the Examiner's decision to reject claims 1–20. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.

[1] We use the word "Appellant" to refer to "applicant" as defined in 37 C.F.R. § 1.42. Appellant identifies the real party in interest as AirWatch LLC. Appeal Br. 2.

STATEMENT OF THE CASE

Appellant's invention enables single-sign on using managed mobile devices. After receiving an identity assertion request from a client device application, an identity provider service detects a platform associated with the client device, and sends a response to the request based on the platform, where the response requests authentication by a management credential. Data generated by the management credential is received from the client device, and the credential is determined to be valid for the identity assertion. The identity assertion is then sent to the client device responsive to this determination. *See* Abstract. Claim 1 is illustrative:

> 1. A non-transitory computer-readable medium embodying a program executable in a server computing device, the program, when executed by the server computing device, being configured to cause the server computing device to at least:
>
> receive a request for an identity assertion from an application executed in a mobile device;
>
> detect that the mobile device is associated with a specific platform of a plurality of platforms;
>
> identify a specific platform adapter corresponding to the specific platform, the specific platform adapter being associated with a type of management credential;
>
> send to the mobile device a response to the request that is generated by the specific platform adapter for the type of management credential, the response requesting authentication by a management credential;
>
> receive data generated by the management credential from the mobile device;
>
> determine that the management credential is valid for the identity assertion; and
>
> send the identity assertion to the mobile device in response to determining that the management credential is valid for the identity assertion.

THE REJECTIONS

The Examiner rejected claims 1–6, 12–17,[2] and 20 under 35 U.S.C. § 103 as unpatentable over Moore (US 2013/0049928 A1; published Feb. 28, 2013), Matsumura (US 2010/0318636 A1; published Dec. 16, 2010), and Lamoureux (US 2014/0279622 A1; published Sept. 18, 2014). Final Act. 13–18.[3]

The Examiner rejected claims 7, 9, and 10 under 35 U.S.C. § 103 as unpatentable over Moore, Hyland (US 2014/0310792 Al; published Oct. 16, 2014), and Shao (US 2014/0376403 Al; published Dec. 25, 2014). Final Act. 19–21.

The Examiner rejected claim 8 under 35 U.S.C. § 103 as unpatentable over Moore, Hyland, Shao, Matsumura, and Lamoureux. Final Act. 22–23.

The Examiner rejected claim 11 under 35 U.S.C. § 103 as unpatentable over Moore, Hyland, Shao, and Rudraraju (US 2015/0052584 Al; published Feb. 19, 2015). Final Act. 24.

The Examiner rejected claim 18 under 35 U.S.C. § 103 as unpatentable over Moore, Matsumura, Lamoureux, and Rudraraju. Final Act. 25.

[2] Although the Examiner omits claim 14 from the statement of the rejection, this claim is nonetheless included in the corresponding discussion. *Compare* Final Act. 13 *with* Final Act. 18. We, therefore, include claim 14 here to clarify the record, and treat the Examiner's error in this regard as harmless.

[3] Throughout this opinion, we refer to (1) the Final Rejection mailed December 27, 2017 ("Final Act."); (2) the Appeal Brief filed May 25, 2018 ("Appeal Br."); (3) the Examiner's Answer mailed August 23, 2018 ("Ans."); and (4) the Reply Brief filed October 17, 2018 ("Reply Br.").

The Examiner rejected claim 19 under 35 U.S.C. § 103 as unpatentable over Moore, Matsumura, Lamoureux, and Chung (US 2002/0078153 Al; published June 20, 2002). Final Act. 26.

THE REJECTION OVER MOORE, MATSUMURA, AND LAMOUREUX

Regarding independent claim 1, the Examiner finds that Moore discloses a computer-readable medium with a program causing a server computing device to (1) receive a request for an identity assertion from an application executed in a mobile device; (2) send a response to the request to the mobile device, where the response requests authentication by a management credential; (3) receive data generated by the management credential from the mobile device; (4) determine that the management credential is valid for the identity assertion; and (5) send the identity assertion to the mobile device responsive to determining the credential's validity. Final Act. 13. Although the Examiner acknowledges that Moore does not detect that the mobile device is associated with a specific platform of plural platforms, the Examiner cites Matsumura as teaching this feature. *Id.* 14. The Examiner also acknowledges that Moore and Matsumura do not identify a specific platform adapter corresponding to the specific platform, but cites Lamoureux for teaching that feature. *Id.* 15. The Examiner adds that Moore and Matsumura collectively teach (1) associating the adapter with a type of management credential, and (2) generating a request by the specific platform adapter. *Id.* Based on these collective teachings, the Examiner concludes that the claim would have been obvious. *Id.* 13–15.

Appellant argues that the cited prior art fails to disclose (1) receiving a request for an identity assertion from an application executed in a mobile device; (2) detecting that the mobile device is associated with a specific platform of plural platforms; (3) identifying a specific platform adapter corresponding to the specific platform, where the adapter is associated with a type of management credential; and (4) sending to the mobile device a response to the request that is generated by the specific platform adapter for the type of management credential, where the response requests authentication by a management credential. Appeal Br. 6–21; Reply Br. 4–20. According to Appellant, Moore does not receive a request for an identity assertion from a mobile device application, let alone disclose a management credential that is provisioned to devices, but rather uses a single login form associated with a physical visitor check-in point that is part of a closed physical access system. Appeal Br. 7–13; Reply Br. 4–5, 8–9, 13–15. Appellant adds that Moore does not authenticate mobile devices with different platforms or identify a specific platform adapter, let alone generate messages based on that adapter. Appeal Br. 7.

Appellant also argues that the Examiner's reliance on Matsumura is misplaced because Matsumura is unrelated to authentication where different platforms with different management credentials request access, thus requiring different responses. Appeal Br. 13–15. According to Appellant, Matsumura's data format conversion is inapplicable to login forms, such as those used by Moore. Appeal Br. 14–15. Appellant adds that the Examiner's reliance on Lamoureux is likewise misplaced because not only are Lamoureux's employment search teachings unrelated to the claimed invention, Lamoureux does not identify a specific platform adapter associated with a management credential as claimed, but merely generates different user interfaces for different platforms. Appeal Br. 16–18; Reply Br. 11. Appellant argues other recited limitations summarized below.

ISSUES

I. Under § 103, has the Examiner erred by finding that Moore, Matsumura, and Lamoureux collectively would have taught or suggested:

(1)(a) receiving a request for an identity assertion from an application executed in a mobile device; (b) detecting that the mobile device is associated with a specific platform of plural platforms; (c) identifying as specific platform adapter corresponding to the specific platform, where the adapter is associated with a type of management credential; and (d) sending to the mobile device a response to the request that is generated by the specific platform adapter for the type of management credential, where the response requests authentication by a management credential as recited in claim 1?

(2) the management credential corresponds to a secure certificate or a Kerberos profile as recited in claim 12?

II. Is the Examiner's proposed combination of the cited references supported by articulated reasoning with some rational underpinning to justify the Examiner's obviousness conclusion?

ANALYSIS

Claims 1–6

As noted above, a key aspect of the claimed invention involves identifying a specific platform adapter corresponding to a specific platform, where the adapter is associated with a type of *management* credential. Our emphasis underscores a key term in this dispute, for Appellant emphasizes this qualifier in arguing that the cited prior art lacks such a credential, and that the Examiner allegedly ignored the term “management” in the term “management credential” as claimed. *See* Appeal Br. 10; Reply Br. 5, 15. We, therefore, begin by construing the term “management credential.”

The Specification does not define the term, but does note that upon authentication with device management service 204 in Figure 2, the client device’s management application 221 is able to obtain management credentials 225 that allow the client applications 224 to request identity assertions from identity provider 206 to authenticate the client applications with the respective service providers. Spec. ¶ 32. This process is shown in steps 315 to 330 of Figure 3, where a client application obtains a management credential from the device management service after the management application obtains the user’s security credentials in step 318. *See* Spec. ¶¶ 36–38.

As shown in step 408 of Figure 4, identity provider 206 requests authentication using a management credential 225 based on the client device’s detected platform. Spec. ¶ 43. According to the Specification, paragraph 43, different types of security credentials and certificates can be used depending on the client device’s platform. For example, the management credential can include (1) a secure certificate; (2) a Kerberos profile; or (3) *other credentials*. *Id.* Our emphasis underscores that the management credential is not limited to secure certificates or Kerberos profiles, but rather can also include other unspecified credentials.

Although this description informs our understanding of the recited “management credential,” the term is not so limited, particularly given the

Specification's lack of specificity regarding the "other" credentials that can be "management credentials" in paragraph 43. *Accord* Ans. 12 (noting the Specification's lack of guidance regarding the distinction between a "credential" and a "management credential"), 16 (noting that the term "other credential" is not narrower than the term "credential").

Given the scope and breadth of the term "management credential," we see no error in the Examiner's reliance on the credentials and other identifying information (4)[4] that are entered by a visitor in a login interface in Moore's Figure 3 for teaching the recited management credential. *See* Final Act. 13; Ans. 4, 12. Appellant's arguments regarding Moore's lacking a management credential, particularly in light of the distinction between user-entered credentials and management credentials in Appellant's Figure 3 (Appeal Br. 10–11; Reply Br. 13) are unavailing, for they are not commensurate with the scope of the claim. That Moore may not articulate the word "management" explicitly as Appellant contends (Reply Br. 5) is not dispositive. Notably, nothing in the claim precludes the Examiner's reliance on the credentials and other identifying information that comport with the non-limiting examples of management credentials in the Specification's paragraph 43 noted previously. Furthermore, Moore's credentials at least relate to managing access using various devices shown in Figure 3, including visitor access service 210, identity provider STS 220, and resource STS 230. Notably, these devices' functionality that, among

[4] Numerals indicated in parentheses correspond to various enumerated steps shown in ovals in Moore's Figure 3 that illustrate the flow of communications between various components in that figure. *See* Moore ¶¶ 40–44.

other things, generates and verifies tokens, is based partly on the identity provider STS 220 receiving the credentials (4). *See* Moore ¶¶ 43–46. In this sense, then, these credentials are at least related to device management, at least with respect to an authentication procedure that uses those devices in a particular way. Therefore, Appellant's arguments regarding Moore's alleged shortcomings regarding *device* management (Reply Br. 5) are unpersuasive even if the term "management credential" in claim 1 was somehow limited to device management—which it is not. To the extent that some exemplary management credentials in the Specification pertain to device management, we decline to import those particular device management examples into the claim. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1323 (Fed. Cir. 2005) (en banc) (citations omitted) ("[A]lthough the specification often describes very specific embodiments of the invention, we have repeatedly warned against confining the claims to those embodiments. . . . [C]laims may embrace different subject matter than is illustrated in the specific embodiments in the specification.") (citations and internal quotation marks omitted).

Nor do we find error in the Examiner's reliance on the functionality of Moore's Figure 3 for teaching (a) receiving a request, namely redirect message (2D), for an identity assertion from an application; and (b) sending a response to the request, namely the visitor organization's login form (3) that the identity provider STS 220 presents to the visitor, where the response requests authentication by a management credential. *See* Final Act. 13; Ans. 12.

As shown in Moore's Figure 3, after a visitor invokes a graphical user interface (GUI) of visitor access service 210 through visitor interface 208, such as through a browser window, the visitor can select a particular organization associated with that visitor, and then request access (1) under that organization. Moore ¶ 41. After several other steps, the visitor interface sends a redirect message (2D) with an access request to identity provider secure token service (STS) 220. Moore ¶ 42. The identity provider STS 220 then presents the user with the visitor organization's login form (3) within the visitor interface. Moore ¶ 43; Figs. 3–4. The credentials or other identifying information (4) entered by the user in the organization's login interface within the visitor interface are then received by the identity provider STS 220 that then authenticates the visitor using the visitor's employer authentication credentials entered by the visitor. Moore ¶ 43. The identity provider STS 220 then creates a Security Assertion Markup Language (SAML) ID-token containing the visitor's authenticated identity and attribute assertions, where the token is signed and encrypted in accordance with the WS-Federation standard. *Id.*

Based on this functionality in Moore's Figure 3, we see no error in the Examiner's finding that Moore at least suggests receiving a request for an identity assertion, namely redirect message (2D), from an application executed in a device, namely the device providing the visitor interface. Although Moore does not say that this interface-providing device can be a mobile device, we nonetheless see no error in the Examiner's finding that providing this interface via a mobile device would have been at least an obvious variation for the reasons indicated by the Examiner, including enabling the user to use their own device to access the interface instead of standing in line at a kiosk, as well as leveraging the mobile device's memory and display capabilities. *See* Ans. 10 (noting the advantages to both the visitor and host organization of using mobile devices in connection with the visitor entering credentials in connection with Moore's paragraph 43).[5]

Even assuming, without deciding, that Moore's visitor check-in point 104 is limited to a fixed, physical device that displays the visitor interface, such as a kiosk, as Appellant seems to suggest (*see* Reply Br. 8), Appellant has still not shown that adapting Moore's system with its purported "controlled, physically installed check-in point" to use more modern electronic components, such as mobile devices, to provide the visitor interface to gain the commonly understood benefits of such an adaptation, would have been uniquely challenging or otherwise beyond the level of skill of ordinarily skilled artisans. Indeed, the Examiner's proposed adaptation to Moore's system is analogous to conventional electronic updates to mechanical devices that the court noted in *Leapfrog Enterprises, Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1161 (Fed. Cir. 2007)—a technological trend that was held to be common in the electronics industry. *See Leapfrog*, 485 F.3d at 1161 ("Applying modern electronics to older mechanical devices has been commonplace in recent years."). In short, the fact that Moore ostensibly uses a "controlled, physically installed check-in point" in connection with the visitor interface as Appellant contends is not dispositive here, particularly when considered in light of the teachings of Matsumura

[5] Although the Examiner cites an additional reference (i.e., Pradhan) in the Examiner's response to Appellant's arguments (Ans. 10–11), this reference was not cited in the rejection, nor will we consider it here. *See In re Hoch*, 428 F.2d 1341, 1342 n.3 (CCPA 1970) ("Where a reference is relied on to support a rejection, whether or not in a 'minor capacity,' there would appear to be no excuse for not positively including the reference in the statement of the rejection.").

and Lamoureux as the Examiner indicates. *See* Ans. 10 (citing Lamoureux Fig. 14 and Matsumura ¶ 7). That Matsumura's paragraph 7 notes that a company's employees possess mobile terminals as company equipment, and that a visitor in Moore is authenticated using the visitor's *employer* authentication credentials entered by the visitor in paragraph 43 only further bolsters the Examiner's conclusion that providing the visitor interface via mobile devices in Moore's Figure 3 would have been at least an obvious variation. *See* Ans. 13 (noting that the visitor in Moore could be an employee with an employer-issued mobile terminal, such as that described in Matsumura's paragraph 7).

To the extent that using mobile devices to provide the visitor interface in the system of Moore's Figure 3 to obtain the commonly understood benefits of such an adaptation as the Examiner proposes would have been uniquely challenging or otherwise beyond the skill level of ordinarily skilled artisans, there is no persuasive evidence on this record to substantiate such a contention. Rather, such an update is analogous to the conventional electronic updates to mechanical devices noted in *Leapfrog*, and reasonably comports with technological trends that are common in the electronics industry. *See Leapfrog*, 485 F.3d at 1161 ("Applying modern electronics to older mechanical devices has been commonplace in recent years.").

Appellant's arguments regarding Moore's alleged shortcomings in this regard (Appeal Br. 8–9; Reply Br. 8) are unavailing, for they do not show nonobviousness where, as here, the rejection is based on the cited references' collective teachings. *See In re Merck & Co.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986).

Nor are we persuaded of error in the Examiner's reliance on Matsumura for at least suggesting detecting that the mobile device used in connection with Moore's visitor interface is associated with a specific platform of plural platforms. *See* Final Act. 14; Ans. 5, 12, 17–18, 24. Matsumura's service management section 24 is a system interface that provides, among other things, adapter functions that (1) determine the type of accessing mobile terminal; (2) determine the type and version of the operating system (OS) running on the terminal; and (3) convert data to a format suitable for the terminal. *See* Matsumura ¶¶ 69, 78. By determining the *particular type and version* of the mobile terminal's operating system, Matsumura at least suggests detecting the terminal's specific platform of plural platforms. Despite Appellant's arguments to the contrary (Appeal Br. 13–16, 21), we see no reason why ordinarily skilled artisans could not provide such a capability in connection with mobile devices used in connection with Moore's visitor interface under the Examiner's proposed combination. Such an enhancement uses prior art elements predictably according to their established functions—an obvious improvement. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007).

Nor are we persuaded of error in the Examiner's reliance on Lamoureux for at least suggesting identifying a specific platform adapter corresponding to the specific platform. Final Act. 15; Ans. 6, 13–14, 17–19, 21. As shown in Lamoureux's Figure 8, Lamoureux's system includes a mobile interface 810 that supports *adapters* for each supported mobile platform, such as Android, iOS, etc. Lamoureux ¶ 123. The mobile interface includes a mobile translation interface that converts or translates information from the system into a mobile device operating system-friendly format and vice-versa. *Id.*

Given this multi-platform adapter support and data conversion functionality, we see no reason why this functionality could not be provided in connection with the Moore/Matsumura system as the Examiner proposes, particularly in light of Matsumura's *adapter* functions that (1) determine the type of accessing mobile terminal; (2) determine the type and version of the operating system (OS) running on the terminal; and (3) convert data to a format suitable for the terminal. *See* Matsumura ¶¶ 69, 78. The Examiner's articulated rationale for the combination, namely to organize Matsumura's conversion software as a set of adapters in light of Lamoureux, where each adapter is associated with a particular platform (Ans. 6), has at least a rational basis on this record and has not been persuasively rebutted.

Given this functionality, the cited prior art also at least suggests sending to the mobile device a response, namely Moore's login form (3), to the request, namely redirect message (2D), that, in light of Lamoureux, would be generated by a specific identified platform adapter as the Examiner proposes. *See* Final Act. 13–15; Ans. 6, 12–13, 17–21. Appellant's arguments regarding Matsumura's and Lamoureux's individual shortcomings in this regard (Appeal Br. 13–21; Reply Br. 6, 9–11, 16–20) do not show nonobviousness where, as here, the rejection is based on the cited references' collective teachings. *See Merck,* 800 F.2d at 1097.

Nor are we persuaded of error in the Examiner's articulated reason to combine the references. *See* Final Act. 14–15; Ans. 6, 10, 13–14. Prior art is analogous if it is (1) from the same field of endeavor regardless of the problem addressed, or (2) reasonably pertinent to the particular problem with which the inventor is involved. *In re Bigio*, 381 F.3d 1320, 1325 (Fed. Cir. 2004). Here, the cited references are at least reasonably pertinent to Appellant's problem because (1) Moore pertains to computer-based authentication as shown in Figure 3; (2) Matsumura's system provides mobile service that, among other things, authenticates the user as noted in the Abstract; and (3) Lamoureux's system uses an interface that supports different mobile platforms as noted in paragraph 123. That Lamoureux's system is used for employment searches as Appellant indicates (Appeal Br. 17; Reply Br. 6, 9) is of no consequence here, for Lamoureux's system nevertheless includes multi-platform functionality for mobile devices that is at least reasonably pertinent to Appellant's claimed invention. In short, we find the cited references constitute analogous art, and the Examiner's basis for combining their teachings is supported by articulated reasoning with rational underpinning to justify the Examiner's obviousness conclusion.

Therefore, we are not persuaded that the Examiner erred in rejecting claim 1, and claims 2–6 not argued separately with particularity.

Claims 12–17 and 20

We also sustain the Examiner's rejection of independent claim 12 reciting functions similar to those recited in claim 1, but adding that the management credential corresponds to a secure certificate or a Kerberos profile. *See* Final Act. 18 (rejecting claim 12 on the same basis as claims 1 and 5) Ans. 25 (explaining why Moore's management credential corresponds to a secure certificate in paragraph 43).

Despite Appellant's arguments to the contrary (Appeal Br. 21–36; Reply Br. 20–21), we are unpersuaded of error in the Examiner's reliance on

Moore, Matsumura, and Lamoureux for their respective teachings as well as their combinability for the reasons noted previously. Nor are we persuaded of error in the Examiner's reliance on the signed and encrypted token in Moore's paragraph 43 for at least suggesting that the management credential, namely the credentials or other identifying information (4), at least *corresponds to* a secure certificate, namely the corresponding ID-token (5) that is generated, signed, and encrypted in accordance with the WS-Federation standard responsive to the identity provider STS 220 receiving those credentials. *See* Moore ¶¶ 43–44; Fig. 3.

Appellant's contention that the Examiner improperly relied on the "Web Services Federation Language" Version 1.2 document, which, according to Appellant, was not properly cited nor designated as a new ground of rejection in the Answer (Reply Br. 21), is a petitionable matter that is not before us.[6] *See* 37 C.F.R. § 41.40(a) (noting that any request seeking review of the Examiner's failure to designate a new ground of rejection must be made via a petition filed before filing a Reply Brief). Where, as here, no such petition was filed, Appellant's arguments regarding any alleged new ground of rejection in the Answer are, therefore, waived. *See id.*; *see also* MPEP § 1208(I).

Appellant's contention that the cited prior art does not show or suggest receiving data generated by the management credential from the client device (Reply Br. 20–21) is likewise unavailing. First, this argument

[6] *See* MPEP § 706.01 ("[T]he Board will not hear or decide issues pertaining to objections and formal matters which are not properly before the Board."); *see also* MPEP § 1201 ("The Board will not ordinarily hear a question that should be decided by the Director on petition . . . .").

was raised for the first time in the Reply Brief and is, therefore, waived as untimely. *See* 37 C.F.R. § 41.41(b)(2); *compare* Appeal Br. 21–22 (arguing the three emphasized detecting, identifying, and sending limitations) *with* Reply Br. 20–21 (arguing the unemphasized receiving limitation that follows the emphasized sending limitation). Nor has good cause been shown to raise these new arguments in the first instance in the Reply Brief.

But even if these arguments in the Reply Brief were timely raised—which they were not—we still find them unpersuasive. Among other things, Appellant's new argument is apparently premised on the notion that the ID-token in Moore's paragraphs 43 and 44 is mapped to the recited management credential. *See* Reply Br. 20–21 (replacing the term "management credential" with "ID-token" in brackets in the disputed receiving clause). But as noted previously, the Examiner mapped the recited management credential to the credentials or other identifying information (4) in Moore's Figure 3 in rejecting claim 12. *See* Final Act. 18 (rejecting claim 12 on the same basis as claims 1 and 5); *see also* Final Act. 13 (mapping the recited "management credential" to the credentials or other identifying information (4) in Moore's Figure 3); Ans. 4, 12 (same).

As noted previously, these credentials in Moore at least *correspond to* a secure certificate, namely the corresponding ID-token (5) that is generated, signed, and encrypted responsive to the identity provider STS 220 receiving those credentials. *See* Moore ¶¶ 43–44; Fig. 3. Because Appellant's arguments do not persuasively rebut the Examiner's findings and conclusions in this regard, we are not persuaded of error in the Examiner's rejection for that additional reason.

Accordingly, we are not persuaded that the Examiner erred in rejecting claim 12, and claims 13–17 and 20 not argued separately with particularity.

THE REJECTION OVER MOORE, HYLAND, AND SHAO

Regarding independent claim 7, the Examiner finds that Moore discloses every recited element except for (1) the application corresponds to a webview of a native application, and (2) the received identity assertion request including a user-agent string that is examined to determine that the application corresponds to a webview of a native application rather than a browser. Final Act. 19–20. The Examiner, however, cites Hyland and Shao for curing the first and second deficiencies, respectively, in concluding that the claim would have been obvious. Final Act. 20.

Appellant argues that the Examiner's reliance on Hyland and Shao is misplaced because, among other things, Hyland's teaching that a native application may be substituted with a browser does not teach or suggest the recited determination, nor is a browser the same as a webview of a native application. Appeal Br. 36–38; Reply Br. 21–22. Appellant adds that Shao's user-agent string identifies the type of device, but is not sent in a request for an identity assertion, let alone used to determine that the application corresponds to a webview of a native application as claimed. Appeal Br. 38–39; Reply Br. 22–23.

Despite these contentions, we see no error in the Examiner's rejection based on the cited references' collective teachings. First, we see no reason why Moore's identity assertion request, namely redirect message (2D), could not include a user-agent string, such as the user-agent string in Shao's paragraph 24 as the Examiner proposes, to identify the type of device and/or *browser* that is used in connection with this request. On this record, we see no reason why this string-based identification functionality could not be provided in connection with Hyland's system in Figure 4 that can substitute a native application 436 with mobile browser 432 in operation as noted in paragraph 50 as the Examiner proposes. This proposed combination at least suggests a system that effectively determines that the application corresponds to a webview of a native application rather than a browser by examining the string. We reach this conclusion noting the Examiner's construing the term "determining" to include substitution—a substitution that must involve determining the things that are substituted, namely the browser and native application, as the Examiner indicates. *See* Ans. 26.

Although Hyland's paragraph 50 does not indicate explicitly that the mobile native application 436 has webview capabilities, ordinarily skilled artisans would nonetheless at least infer as much given that the native application is *substituted with a browser* that enables viewing web content. Providing commensurate capabilities with either alternative would have been at least an obvious variation to, among other things, retain the ability to view web pages regardless of whether the browser or native application was invoked. To the extent that Appellant contends that providing such viewing capabilities in connection with Hyland's native application would have been uniquely challenging or otherwise beyond the skill level of ordinarily skilled artisans (*see* Appeal Br. 39; Reply Br. 21–22), there is no persuasive evidence on this record to substantiate such a contention.

Therefore, we are not persuaded that the Examiner erred in rejecting claim 1, and claims 9 and 10 not argued separately with particularity.

THE OTHER OBVIOUSNESS REJECTIONS

We also sustain the Examiner's obviousness rejections of claims 8, 11, 18, and 19. Final Act. 22–26. Because these rejections are not argued separately with particularity (*see* Appeal Br. 39–40), we are not persuaded of error in these rejections for the reasons previously discussed.

CONCLUSION

In summary:

Claims Rejected	**35 U.S.C. §**	**Reference(s) /Basis**	**Affirmed**	**Reversed**
1–6, 12–17, 20	103	Moore, Matsumura, Lamoureux	1–6, 12–17, 20	
7, 9, 10	103	Moore, Hyland, Shao	7, 9, 10	
8	103	Moore, Hyland, Shao, Matsumura, Lamoureux	8	
11	103	Moore, Hyland, Shao, Rudraraju	11	
18	103	Moore, Matsumura, Lamoureux, Rudraraju	18	
19	103	Moore, Matsumura, Lamoureux, Chung	19	
Overall outcome			1−20	

TIME PERIOD FOR RESPONSE

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1).

AFFIRMED