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.
14/621,123	02/12/2015	Cristian Radu	P01729-US-UTIL (M01.308)	3632

125619 7590 06/30/2020
Mastercard International Incorporated
c/o Buckley, Maschoff & Talwalkar LLC
50 Locust Avenue
New Canaan, CT 06840

EXAMINER	
ST CYR, DANIEL	

ART UNIT	PAPER NUMBER
2876	

NOTIFICATION DATE	DELIVERY MODE
06/30/2020	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):

colabella@bmtpatent.com
martin@bmtpatent.com
szpara@bmtpatent.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte CRISTIAN RADU, JONATHAN JAMES MAIN, and
ERIC G. ALGER

Appeal 2019-002540
Application 14/621,123
Technology Center 2800

Before CATHERINE Q. TIMM, ELIZABETH M. ROESEL, and MICHAEL G. McMANUS, *Administrative Patent Judges.*

TIMM, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE

Pursuant to 35 U.S.C. § 134(a), Appellant[1] appeals from the Examiner's decision to reject claims 2–11, 13, 14, and 16–20. *See* Final Act. 1. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM IN PART.

[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 Mastercard International Incorporated. Appeal Br. 2.

CLAIMED SUBJECT MATTER

The claims are directed to a method (*see, e.g.*, claims 2 and 9) and apparatus (*see, e.g.*, claim 16) for streamlined digital wallet transactions. Claim 2, reproduced below, is illustrative of the claimed subject matter:

> 2. A method comprising:
>
> maintaining a digital wallet in a computer, the digital wallet storing a plurality of payment account entries associated with a user of the digital wallet, each of said payment account entries corresponding to a respective payment account that belongs to said user;
>
> receiving a request for a transaction;
>
> receiving and verifying, by the computer, user authentication data regarding the user and the requested transaction;
>
> verifying, by the computer, authentication of a device used by the user to initiate the transaction, said verifying authentication of the device including verification of a hash result calculated over identification data stored in the device, said identification data including at least one serial number assigned to a hardware or software component of the device; and
>
> in response to verifying the user authentication data, allowing the user to access any one of said payment accounts without requiring further user authentication.

Appeal Br. 14.

REFERENCES

The prior art relied upon by the Examiner is:

Name	Reference	Date
DiMartino	US 8,165,961 B1	Apr. 24, 2012
Griggs	US 2014/0114857 A1	Apr. 24, 2014
Bondesen	US 2015/0254655 A1	Sept. 10, 2015

REJECTIONS

The Examiner maintains the following rejections:

Claims 2–8 and 16–20 are rejected under 35 U.S.C. § 103 as being unpatentable over DiMartino in view of Bondesen.[2] Final Act. 2.

Claims 9–11, 13, and 14 are rejected under 35 U.S.C. § 103 as being unpatentable over DiMartino in view of Griggs. Final Act. 5.

OPINION

The Rejection of Claims 2–8 and 16–20 as obvious over DiMartino in view of Bondesen

In arguing against the rejection of claims 2–8 and 16–20 over DiMartino in view of Bondesen, Appellant focuses on claims 2, 3, 16, and 17. It will suffice for us to discuss claims 2, 16, and 17. The arguments for claim 3 need not be separately addressed given our disposition of the rejection of claim 2.

Claim 2

DiMartino discloses a system of completing a payment using an electronic wallet on a mobile device. DiMartino col. 1, l. 63–col. 2, l. 9. The Examiner acknowledges that DiMartino fails to disclose the step of verifying

[2] The Examiner lists claim 1 as rejected, but claim 1 was canceled.

the authentication of the device as required by claim 2 and turns to Bondesen to support the conclusion that it would have been obvious to verify the device as another layer of security. Final Act. 3–4.

Claim 2 requires that verifying authentication of the device include "verification of a hash result calculated over identification data stored in the device." The Examiner turns to paragraph 128 of Bondesen and finds that Bondesen's teaching of incorporating a validation of the user's mobile device into a unique identity score meets this limitation. Final Act. 4. Specifically, the Examiner finds that Bondesen's unique identity score is a hash result as the unique identity score is a numeric value that uniquely identifies the mobile device. *Id.*

Appellant contends that generating an identity score and calculating a hash result are two distinctly different processes and the former would not be considered to constitute a species of the latter. Appeal Br. 8.

Appellant has identified a reversible error in the Examiner's finding. The question of whether generating an identity score involves calculating a hash score requires us to consider the broadest reasonable meaning of "hash result" consistent with the Specification as it would be interpreted by one of ordinary skill in the art.

Turning to the Specification to discern the meaning of "hash result" we determine that the Specification equates a hash result with a cryptographic result. Spec. 15:8–11 ("the user/payment device 212 may calculate a hash or other cryptographic result over both a device fingerprint and user authentication data provided by the user"). Thus, we interpret "calculating a hash result" as using a mathematical function to convert the device identification data into a new value and thereby encrypt the device identification data.

The Examiner has not established that Bondesen verifies a hash result calculated over identification data stored in the device. Although Bondesen discloses identifying the mobile device using device identification information, Bondesen does not disclose calculating a cryptographic result, i.e., using a mathematical function to convert the device identification data into a new value to encrypt the data. Bondesen ¶ 128.

Bondesen gathers device identification information from the mobile device to generate the device's "fingerprint" or unique signature and then bases the level of user authorization in part on validating this device information. Bondesen ¶ 128. Bondesen incorporates this verification into a close network score or into a unique identity score that is combined with the close network score. *Id.* Taking the verification of the identity of the device and *adding* it to a unique identity score, on its face, is not the same as using a mathematical function to convert the device identification data into a new value to encrypt the data.

Because the Examiner fails to further explain how Bondesen's disclosure of incorporating the device verification data into the unique identity score meets the requirement of verifying a hash result calculated over the device's stored identification data, we agree with Appellant that the Examiner has not established that adding the device identification data to a score is the type of hashing required by claim 2.

For these reasons, we do not sustain the Examiner's rejection of claims 2–8.

Claim 16

Claim 16 is directed to an apparatus with a processor, memory, and program instructions on the processor that perform a digital wallet transaction. Claim 16 requires a step of verifying authentication of a device used by the user to initiate the transaction. The verifying step differs from that of claim 2. In claim 16, the step involves "verifying a result computed by the device based in part on a *challenge issued to the device by the server computer*." Claim 16 (emphasis added).

According to the Examiner, "[t]he challenge issued by the server is just [a] basic hand-shake protocol between electronic devices." Ans. 10. In other words, in the challenge, the mobile device is requesting access and the server is asking the mobile device to provide the credential before access is granted. *Id.*

Appellant contends that the Examiner has not addressed Appellant's argument that the prior art fails to disclose such a challenge. Reply Br. 2. According to Appellant, "Bondesen has some disclosure relating to device authentication, but fails to teach or suggest verification of device authentication that includes verifying a result computed by the device based in part on a challenge issued to the device by a wallet server." Appeal Br. 10.

Appellant's argument does not address the Examiner's finding that the challenge issued by the server is just a basic hand-shake protocol between the electronic devices. In order to carry out authentication, the wallet server and mobile device must speak to each other. *See, e.g.*, DiMartino col. 5, ll. 11–26. Appellant has not identified a reversible error in the Examiner's finding.

We sustain the Examiner's rejection of claims 16 and 18–20.

Claim 17

Appellant argues claim 17 separately in the grouping with claim 3. Because we did not sustain the rejection of claim 2, there was no need to address claim 3. We address claim 17 here.

Claim 17 depends from claim 16 and further requires the processor have program instructions to "set a consumer authentication status flag to a 'valid' state to indicate that the processor has verified the received user authentication data; wherein the processor does not receive a consumer authentication status flag value from said device used by the user."

In the rejection, the Examiner states that "the user information is required in order for the transaction to proceed, so setting flag or acknowledgement to indicate the user and/or device has been authenticated is obtained." Final Act. 4. In the Answer, the Examiner further explains that "[i]f a user is authenticated and allowed to gain access to the electronic wallet, that is an indication of a valid authentication status flag, while a user who is failed to authenticate and not allowed to gain access, that is an indication of invalid authentication status." Ans. 10.

The Examiner does not point to any particular teaching in either reference to support the findings. We, like Appellant, interpret the Examiner's finding as one of inherency, i.e., that granting access inherently results in setting a consumer authentication status flag to "valid." Reply Br. 2–3. But, as pointed out by Appellant, "access can be granted without setting a flag, and a flag can be set without granting access." Reply Br. 3. Although it is *possible* to set a flag to "valid" to indicate that the processor has verified the received authentication data, it is not *necessary*. Thus, it is not inherent.

We do not sustain the Examiner's rejection of claim 17.

The rejection of claims 9–11, 13, and 14 as obvious over DiMartino in view of Griggs

Claim 9 is an independent claim and requires a server computer receive and verify authentication data for the requested transaction and, "in response to verifying the authentication data by the server computer, triggering by the server computer generation of a cryptogram for the transaction, said cryptogram generated in accordance with an EMV (Europay-Mastercard-Visa) standard." Claims 10, 11, 13, and 14 depend from claim 9.

The Examiner relies on paragraph 68 of Griggs as teaching the step of triggering generation of the cryptogram. Final Act. 9–10. As stated by the Examiner,

> Griggs et al[.], in the field of transaction initiation modes (abstract), teach in response to verifying authentication data, triggering generation of a cryptogram for the transaction (chip cryptogram maybe different and can assist in determining transaction initiation mode, para 0068).

Final Act. 6–7. In the Answer, Examiner further explains that "the device is asking for access and the server computer is requesting credential information in order to grant access, which triggers the mobile device to generate the cryptogram data." Ans. 10.

Appellant contends that Griggs merely discloses a server that *receives* and *stores* a chip cryptogram and does not teach that the server *triggers generation* of the cryptogram. Appeal Br. 9; Reply Br. 2.

We agree with Appellant that paragraph 68 of Griggs teaches receiving and storing a chip cryptogram and does not disclose triggering the generation of the cryptogram. Griggs teaches a server 200 that includes an authentication database 240. Database 240 stores a table of data elements used to compare against a plurality of transaction specific data elements received from communication device 110 (e.g., a mobile device). Griggs ¶¶ 29, 68. The values within these data elements may be used to determine the transaction initiation mode, i.e., the type of transaction occurring between a consumer and merchant (magnetic stripe read, chip card, secure mobile near field communication (NFC), etc.). Griggs ¶¶ 46, 68. The chip cryptogram may be different for the credentials on a chip than for a secure mobile NFC transaction. Griggs ¶ 68. Thus, the value of the chip cryptogram may assist in determining the transaction initiation mode. *Id.*

The Examiner finds that Griggs teaches that the server triggers the mobile device to generate a cryptogram, but we do not find any disclosure of such a trigger in paragraph 68. The Examiner states that "the device is asking for access and the server computer is requesting credential information in order to grant access, which triggers the mobile device to generate the cryptogram data." Ans. 10. But paragraph 68 merely discusses storing a chip cryptogram in a table on the server. Paragraph 70 discloses receiving the data elements, which may include the chip cryptogram, from communication device 110, and comparing them with the stored data elements, but the Examiner does not rely on paragraph 70 and paragraph 70 does not disclose that the server triggers the mobile device to generate a cryptogram. Given the lack of explanation by the Examiner, we determine a preponderance of the evidence on this appeal record supports Appellant's argument that Griggs's server does not trigger generation of the cryptogram mentioned in paragraph 68 of Griggs.

We do not sustain the rejection of claims 9–11, 13, and 14.

CONCLUSION

The Examiner's decision to reject claims 16 and 18–20 affirmed, but the Examiner's decision to reject claims 2–11, 13, 14, and 17 is reversed.

DECISION SUMMARY

Claims Rejected	**35 U.S.C. §**	**Reference(s)/ Basis**	**Affirmed**	**Reversed**
2–8, 16–20	103	DiMartino, Bondesen	16, 18–20	2–8, 17
9–11, 13, 14	103	DiMartino, Griggs		9–11, 13, 14
Overall Outcome			16, 18–20	2–11, 13, 14, 17

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). *See* 37 C.F.R. § 1.136(a)(1)(iv) (2018).

AFFIRMED IN PART