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. |
|---|---|---|---|---|
| 15/120,887 | 08/23/2016 | Michael BALDISCHWEILER | 19838.295 | 5939 |

22913 7590 09/30/2020

Workman Nydegger
60 East South Temple
Suite 1000
Salt Lake City, UT 84111

| EXAMINER |
|---|
| JONES, COURTNEY PATRICE |

| ART UNIT | PAPER NUMBER |
|---|---|
| 3685 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 09/30/2020 | 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):

Docketing@wnlaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

*Ex parte* MICHAEL BALDISCHWEILER,
CLAUS DIETZE, and MARTIN AUER

---

Appeal 2020-001868
Application 15/120,887
Technology Center 3600

---

Before RICHARD M. LEBOVITZ, ULRIKE W. JENKS, and RACHEL H. TOWNSEND, *Administrative Patent Judges*.

LEBOVITZ, *Administrative Patent Judge*.

DECISION ON APPEAL

The Examiner rejected claims 14–26 under 35 U.S.C. § 103 as obvious. Pursuant to 35 U.S.C. § 134(a), Appellant[1] appeals from the Examiner's decision to reject the claims. We have jurisdiction for the appeal under 35 U.S.C. § 6(b).

We REVERSE.

---

[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 Giesecke+Devrient Mobile Security Gmbh. Appeal Br. 2.

STATEMENT OF THE CASE

The Examiner rejected claims 14–26 in the Final Office Action ("Final Act.") as follows:

1. Claim 14–18, 20, 24, and 26 under 35 U.S.C. § 103 as obvious in view of Esplin et al., (US 2007/0194113 A1, published Aug. 23, 2007), ("Esplin") and Grigg et al., (US 2015/0227726 A1, published Aug. 13, 2015) ("Grigg"). Final Act. 9.

2. Claim 19 and 22 under 35 U.S.C. § 103 as obvious in view of Esplin, Griggs, and Boubion et al., (US 2007/0223685 A1, published Sept. 27, 2007), ("Boubion"). Final Act. 16.

3. Claim 21 under 35 U.S.C. § 103 as obvious in view of Esplin, Grigg, and Huang et al., (US 2014/0244456 A1, published Aug. 28, 2014), ("Huang"). Final Act. 18.

4. Claims 23 and 25 under 35 U.S.C. § 103 as obvious in view of Esplin, Grigg, and Su et al., (US 2015/0095228 A1, published Apr. 2, 2015), ("Su"). Final Act. 19.

Claim 14, the only independent claim on appeal, is reproduced below, and annotated with bracketed numbers for reference to the claim limitations:

> 14. A method for authorizing a transaction, the method comprising:
>
> [1] reading out a first code generated by a system for the transaction, by a first reader of a first mobile device, with the first code having been encrypted,
>
> [2] reading out a second code, which is dedicated to the system and has at least one information item for decrypting the first code, the second code being read out by a second reader of the first mobile device,
>
> [3] generating a first signature confirming the transaction by way of the system from the previously decrypted first code,
>
> [4] transmitting the first signature to the system, and

> [5] transmitting the first signature and a second signature identifying the system to a service facility in order to authorize the transaction.

REJECTION BASED ON ESPLIN AND GRIGG

The Specification describes the claimed method of authorizing a transaction as an improvement that "solves the known problems from the prior art and is further adapted for increasing the security in performing a mobile transaction" on a point-of-sale system, such as at a supermarket or gas station. Spec. ¶¶ 7, 8, 10, 21.

In the first step [1] of the claim, "a first code generated by a system for the transaction" is read by a first reader of a first mobile device. The code is defined in the Specification as "any kind of machine-readable code, in particular a QR code (Quick Response code), a code capable of being read out by means of a near-field communication interface (NFC according to ISO 14443), a 2D bar code, etc." Spec. ¶ 3. The code contains information about the "transaction" to be carried out, such as the payment information involved in a transaction between a buyer and a seller. Spec. ¶¶ 6, 11, 12 ("A 'transaction' as intended by the present invention is for example the performance of a payment with the first mobile device on the system. The payment can be debited to the account of the owner of the mobile device by bank transfer or be effected as a credit-card transaction."). The first code can be displayed on a display device of the system, such as on a display of a point-of-sale system at a grocery store; the mobile device is enabled to read the code displayed on the point-of-sale system. Spec. ¶ 30. The first code is required by the claim to be encrypted.

A "second code" is read by the mobile device in the second step [2] of the claim, using a second reader. The second code "is dedicated to the

system and has at least one information item for decrypting the first code." The Specification explains that the second code can be a static code on an NFC sticker, displayed on the point-of-sale device, which contains the information for decrypting the code. Spec ¶ 32. When the second code is on the point-of-sale device, the mobile device has to be in the vicinity of the point-of-sale device to decode the first code, providing additional security for the transaction. Spec. ¶ 16. The Specification explains that "[w]ithout the second code 29 it is not possible to utilize the first code 28, since only the second code contains an information item for decrypting the first code 28." Spec ¶ 32.

A signature is generated by the device confirming the transaction in step [3] of the claim and the signature is transmitted to the system (such as the point-of-sale device) in step [4]. The Specification discloses that the signature "might incorporate for example at least one element of the following list: account data, bank, age, photo, signature, telephone number, marital status, etc." that allows the point-of-sale device to authenticate the user. Spec. ¶ 34. In the last step [5] of the claim, "the first signature and a second signature identifying the system" are transmitted "to a service facility in order to authorize the transaction." "The service facility may be for example a financial institution, in particular a credit-card company." Spec. ¶ 36.

The Examiner found that Esplin describes a first code for a transaction as recited in step [1] of claim 14, but not using a second code to decrypt the first code. Final Act. 9–10. To meet this deficiency, the Examiner further cited Grigg. The Examiner explained:

> Grigg from same or similar field of endeavor teaches reading out a first code generated by a system for the transaction, by a first

> read-out device of a first mobile device (Paragraph 0065 teaches a device may comprise a camera (i.e., first read-out device) and be configured to sense (i.e., read) an image (i.e., first code)), with the first code having been encrypted (Paragraph 0065 teaches the image contains an embedded (i.e., encrypted) message), reading out a second code which is dedicated to the system and has at least one information item for decrypting the first code, the second code being read out by a second read-out device of the first mobile device (Paragraphs 0031 and 0065 teach a mobile device could comprise a camera and an NFC reader device (i.e., second read-out device), and the device could be configured to sense (i.e., read) an image containing an embedded message using the camera and a signal (i.e., second code used for decrypting the first code) emitted from a fob (i.e., dedicated to system) using the NFC reader to obtain a credential to grant access to transfer funds between account, or pay a bill).

Final Act. 11 (emphasis omitted).

The Examiner identified paragraph 65 of Grigg as describing steps [1] and [2] of claim 14 in which a mobile device reads a first encrypted code and a second code for decrypting the first code. Paragraph 65 is copied below:

> For example, a bank application may contain the functionality to view a bank statement, transfer funds between accounts, and pay a bill. A mobile device could comprise a camera and an NFC reader. The device could further be configured to sense an image containing an embedded message using the camera and a signal emitted from a fob using the NFC reader. The device could be configured to require a credential be obtained and authorized by sensing the image with the embedded message prior to granting access to view the bank statement. The device could be further be configured to require a credential to be obtained and authorized by sensing the message emitted from the fob prior to granting access to transfer funds between accounts, or pay a bill.

Grigg ¶ 65.

In paragraph 65 reproduced above, Grigg describes a mobile device for viewing a bank statement. Grigg teaches that the device has (1) a camera for reading an image containing an embedded message and (2) an NFC reader for reading a signal from a fob. The image in the embedded message is used in Grigg as a credential to authorize access to view a bank statement ("configured to require a credential be obtained and authorized by sensing the image with the embedded message prior to granting access to view the bank statement"). The signal from the fob is also used as a credential, but as a credential to transfer funds or pay a bill. While the image is characterized by Grigg as "an embedded message," there is no description in this paragraph that the message is encrypted as the claim requires the first code to be (step [1]), let alone that a second code is used to decrypt it (step [2]).

Grigg also teaches that the "first credential may be obtained by decoding the image of indicia, thereby resulting in a first credential," but Grigg does not disclose that the decoding is accomplished by reading a second code dedicated to the system as required in the second step of claim 14. Griggs ¶ 54.

Paragraph 31 of Grigg cited by the Examiner describes authentication, but not using a second code in the authentication process.

Grigg also describes encrypting the credential using a shared encryption key between an "apparatus" and a remote server, and then sending the encrypted credential to the remote server. Griggs ¶ 53. However, there is no disclosure of how the remote server decrypts the credential, nor of using a second code to do so as required by step [2] of rejected claim 14.

An examiner bears the initial burden of presenting a prima facie case of obviousness. *In re Huai-Hung Kao*, 639 F.3d 1057, 1066 (Fed. Cir. 2011). The Examiner did not meet the burden of establishing that steps [1] and [2] of claim 14, as discussed above, are rendered obvious by Esplin and Grigg. For the foregoing reasons, the rejection of claim 14 is reversed. Dependent claims 15–18, 20, 24, and 26 contain all the steps of claim 14 are reversed for the same reasons.

The additional references cited in the rejections of the remaining dependent claims are not described by the Examiner as meeting steps [1] and [2] of claim 14. Rejections 2–4 of claims 19, 21–23, and 25 are therefore reversed.

CONCLUSION

In summary:

| Claims Rejected | 35 U.S.C. § | Reference(s) | Affirmed | Reversed |
|---|---|---|---|---|
| 14–18, 20, 24, 26 | 103 | Esplin, Griggs | | 14–18, 20, 24, 26 |
| 19, 22 | 103 | Esplin, Griggs | | 19, 22 |
| 21 | 103 | Esplin, Griggs | | 21 |
| 23, 25 | 103 | Esplin, Griggs | | 23, 25 |
| **Overall Outcome** | | | | 14–26 |

REVERSED