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.
12/816,356	06/15/2010	Robert O. Carr	0180-002	3130

120491 7590 03/02/2020

Leffler Intellectual Property Law, PLLC
8300 Boone Boulevard
5th Floor
Vienna, VA 22182

EXAMINER	
WINTER, JOHN M	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
03/02/2020	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):

info@leffleriplaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte ROBERT O. CARR, STEVE ELEFANT, SARAH McCRARY, and PAUL MINUTILLO

Appeal 2019-003977
Application 12/816,356
Technology Center 3600

Before ST. JOHN COURTENAY III, LARRY J. HUME, and PHILLIP A. BENNETT, *Administrative Patent Judges.*

BENNETT, *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 1, 3, 4, 10, 12, and 13. Claims 2 and 11 are canceled. Claims 5–9 and 14–20 are withdrawn. We have jurisdiction under 35 U.S.C. § 6(b).We reverse.

[1] We use the word "Appellant" to refer to the applicant as defined in 37 C.F.R. § 1.42(a). Appellant identifies the real party in interest as Heartland Payment Systems, LLC. Appeal Br. 2.

CLAIMED SUBJECT MATTER

The claims are directed to methods and systems that enable products and services to be purchased by means of electronic payment transactions, such as by means of credit and debit card transactions, and more particularly to methods and apparatuses that protect the data communicated in such transactions against unauthorized access. Spec. 1, ll. 10–14. Claim 1, reproduced below, is illustrative of the claimed subject matter:

> 1. A method of securely communicating data in a communication network, the method comprising:
>
> a gateway device receiving a key transmission block from a first device, wherein the key transmission block includes an encrypted copy of a first device-specific decrypting key and one or more key-related parameters;
>
> the gateway device using the one or more key-related parameters to derive a decrypting key that is associated with the gateway device;
>
> the gateway device using the decrypting key that is associated with the gateway device to decrypt the encrypted copy of the first device-specific decrypting key;
>
> the gateway device receiving first encrypted transaction data from the first device, wherein the first encrypted transaction data is encrypted by means of a first device-specific encrypting key;
>
> the gateway device producing decrypted transaction data by using the first device specific decrypting key to decrypt the first encrypted transaction data;
>
> the gateway device deriving second encrypted transaction data from at least a portion of the decrypted transaction data, wherein the second encrypted transaction data is encrypted by means of a host-specific encrypting key; and
>
> the gateway device communicating the second encrypted transaction data to another host device.

Appeal Br. 25 (Claims Appendix).

REFERENCES

The prior art relied upon by the Examiner as evidence is:

Name	Reference	Date
Johnson et al.	US 5,448,638	Sept. 5, 1995
Schipper et al.	US 2007/0133797 A1	June 14, 2007
Hammad et al.	US 2008/0103982 A1	May 1, 2008

REJECTION[2]

Claims 1, 3, 4, 10, 12, and 13 stand rejected under pre-AIA 35 U.S.C. § 103(a) as being unpatentable over the combination of Hammad, Johnson, and Schipper. Final Act. 7.

ISSUE

Has the Examiner erred in finding Hammad and Schipper teach or suggest a gateway device receiving both a "encrypted copy of a first device-specific decrypting key" and also "one or more key-related parameters" which are subsequently used "to derive a decrypting key that is associated with the gateway device," as recited in claim 1?

ANALYSIS

Claim 1 recites the limitations:

> a gateway device receiving a key transmission block from a first device, wherein the key transmission block includes an encrypted copy of a first device-specific decrypting key *and one or more key-related parameters;*

[2] The Examiner has withdrawn the previous rejection of claims 1, 3, 4, 10, 12, and 13 under 35 U.S.C. § 101. Ans. 3.

> the gateway device using *the one or more key-related parameters to derive a decrypting key that is associated with the gateway device*;

Appeal Br. 25 (Claims Appendix). In rejecting claim 1, the Examiner finds Hammad's use of stored public keys to create point-of-sale access device-specific symmetric keys teaches a "gateway device receiving . . . one or more key-related parameters," and additionally finds Schipper's use of control words also teaches this limitation. Non-Final Act. 7 (citing Hammad ¶¶ 35, 36, 50, and 53), Ans. 3–4 (additionally citing Hammad ¶ 54), Ans. 4–5 (citing Schipper ¶¶ 2, 3).

With respect to Hammad, the Examiner finds Hammad's issuer corresponds to the recited "gateway device," and that the public-key encrypted, terminal-specific key sent to the issuer corresponds to the recited "key transmission block." Ans. 3–4 (citing Hammad ¶ 52). The Examiner further finds that the Hammad's public key corresponds to the "one or more key related parameters."

Appellant argues Hammad's public key does not teach "a gateway device receiving . . . one or more key-related parameters" because

> Hammad does not disclose that the public key is communicated along with the encrypted terminal-specific symmetric key, nor is there any reason why it would be. It is well known in the art that in asymmetric encryption strategies, one key (the so-called "public" key) is distributed to the public (i.e., not kept secret) and is used to encrypt data. The recipient retains the counterpart of the public key, that is, the so called "private" key, which (as the name suggests) is kept private with the owner of the public/private key pair. Notably, public keys are useful for encrypting data, but this is a one-way operation; public keys cannot be used decrypt the data that they have encrypted. Instead, only the counterpart private key can do the decrypting.

> With this as well-known background, it is not understood on what basis the Examiner can correctly assert that "a key related parameter is taught by the public key of Hammad et al." For one thing, as already-mentioned, there is no disclosure of it being communicated along with the encrypted terminal-specific symmetric key, so right away it fails to satisfy the terms of Appellant's claims. But for the sake of argument, *even if the public key were communicated with the encrypted key,* ***the recipient would not be able to use it to decrypt the encrypted key, or to derive another key that can.*** So again, there is ***no rational basis*** for concluding that Hammad's disclosure of a "public key" corresponds to Appellant's claimed "key related parameters."

Reply Br. 6.

We agree with Appellant. Hammad describes sending a public-key encrypted, terminal-specific key from a merchant computer to an issuer. Hammad ¶ 52, 54. The Examiner finds that Hammad's issuer corresponds to the recited "gateway receiving device" and that the public key corresponds to the recited "key-related parameters." However, Hammad does not describe including the public key in the transmission of the terminal-specific key to the issuer. The public key is used to encrypt the terminal-specific key, but it is not sent to the issuer along with the terminal-specific key. As such, we agree with Appellant that the public key described in Hammad is not a "key-related parameter" within the meaning of claim 1. We further agree with Appellant that even if the public key were sent to the issuer, it would not meet the claim 1's requirement of "the gateway device using the one or more key-related parameters to derive a decrypting key that is associated with the gateway device." As explained by Appellant, a public key cannot be used to decrypt data encrypted by that same public key. As

such, mapping Hammad's public key to the recited "key-related parameter" is insufficient to teach or suggest the disputed limitations.

Appellant also argues Schipper's control word does not teach "the gateway device using *the one or more key-related parameters to derive a decrypting key that is associated with the gateway device*" because Schipper's control word is communicated in encrypted form and is used for decrypting data, not used as a parameter to "derive a decrypting key that is associated with the gateway device." Reply Br. 7. We agree that Schipper's control words used to decrypt video data do not teach or suggest "key-related parameters to derive a decrypting key that is associated with the gateway device" because Schipper's control words are not used to *derive a decrypting key* associated with a gateway device. The cited portions of Schipper do not show how control words are key-related parameters used to derive a decrypting key associated with a gateway device. *See e.g.*, Schipper Abst., Fig. 3, ¶¶ 2,3.

Accordingly, we are persuaded the Examiner erred, and we reverse the rejection of claim 1 under 35 U.S.C. § 103(a). For the same reasons, we also reverse the rejection of independent claim 10, which recites similar limitations, as well as of the remaining claims which depend therefrom.[3]

[3] Because we find this argument persuasive and dispositive of the rejections made under § 103, we do not address Appellant's other § 103 arguments herein.

CONCLUSION[4]

We reverse the Examiner's rejection of claims 1, 3, 4, 10, 12, and 13 under pre-AIA 35 U.S.C. § 103(a).

DECISION SUMMARY

Claims Rejected	**35 U.S.C. §**	**Reference(s)/Basis**	**Affirmed**	**Reversed**
1, 3, 4, 10, 12, 13	103	Hammad, Johnson, Schipper		1, 3, 4, 10, 12, 13

REVERSED

[4] In the event of further prosecution, including any pre-allowance review, we direct the attention of the Examiner and Appellant to the incorrect dependencies of claims 3 and 12, which erroneously depend from cancelled claims 2 and 11, respectively. We leave it to the Examiner and Appellant to determine whether these claims should be amended to depend from independent claims 1 and 10, respectively, in order to comply with the requirements of pre-AIA 35 U.S.C. § 112, ¶¶ 2, 4.