



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.
13/622,534	09/19/2012	VINCENT CEDRIC COLNOT	81527567US01	7715

65913 7590 11/30/2016  
Intellectual Property and Licensing  
NXP B.V.  
411 East Plumeria Drive, MS41  
SAN JOSE, CA 95134

EXAMINER
----------

DESROSIERS, EVANS

ART UNIT	PAPER NUMBER
----------	--------------

2491

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

11/30/2016

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):

ip.department.us@nxp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

*Ex parte* VINCENT CEDRIC COLNOT

---

Appeal 2015-008080  
Application 13/622,534  
Technology Center 2400

---

Before DEBRA K. STEPHENS, JEREMY J. CURCURI, and  
MICHAEL J. ENGLE, *Administrative Patent Judges*.

STEPHENS, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellant appeals under 35 U.S.C. § 134 from a Final Rejection of claims 1–26. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM-IN-PART.

## STATEMENT OF THE INVENTION

According to Appellant, the claims are directed to a method and system for securely updating firmware in a computing device (Abstract). Claims 1 and 22, reproduced below, are exemplary of the claimed subject matter:

1. A method for updating firmware in a computing device, the computing device including a host processor and a non-volatile memory, the method comprising:

receiving a double-encrypted firmware image from an external firmware source, wherein the double-encrypted firmware image is generated from firmware that is encrypted a first time using a first crypto-key and then encrypted a second time using a second crypto-key;

receiving the second crypto-key from an external key source;

decrypting the double-encrypted firmware image using the second crypto-key to produce an encrypted firmware image;

storing the encrypted firmware image in the non-volatile memory of the computing device;

reading the encrypted firmware image from the non-volatile memory of the computing device;

decrypting the encrypted firmware image using the first crypto-key to produce the firmware; and

executing the firmware on the computing device.

22. A method for confirming the presence of a secure element in a computing device, the computing device including a host processor and a non-volatile memory, the method comprising:

receiving an encrypted random number at the secure element, wherein the random number is encrypted using a crypto-key;

receiving the crypto-key from an external key source;

decrypting the encrypted random number at the secure element using the cryptokey to produce a decrypted random number;

storing the decrypted random number in the non-volatile memory of the computing device;

reading the decrypted random number from the non-volatile memory of the computing device;

comparing the decrypted random number to a stored version of the random number; and

confirming the presence of the element if the decrypted random number matches the stored random number.

#### REFERENCES

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Wang	US 2008/0072068 A1	Mar. 20, 2008
de Cesare	US 2009/0257595 A1	Oct. 15, 2009
Kim	US 2011/0239211 A1	Sep. 29, 2011
Catrein	US 2011/0261957 A1	Oct. 27, 2011
Leclercq	US 2012/0198224 A1	Aug. 2, 2012

#### REJECTIONS

Claims 1, 6, and 7 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wang and Catrein (Final Act. 3–6).

Claims 2–4, 9, and 11 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wang, Catrein, and Leclercq (Final Act. 6–9).

Claims 5 and 12–14 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wang, Catrein, Leclercq, and de Cesare (Final Act. 10–12).

Claim 8 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Wang, Catrein, and Kim (Final Act. 12–13).

Claim 10 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Wang, Catrein, Leclercq, and Kim (Final Act. 13–14).

Claim 15 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Wang, Catrein, Leclercq, de Cesare, and Kim (Final Act. 14–15).

Claim 16 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Wang and Leclercq (Final Act. 15–17).

Claims 17–19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wang, Leclercq, and de Cesare (Final Act. 17–19).

Claims 20 and 21 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wang, Leclercq, and Kim (Final Act. 19–20).

Claims 22, 23, 25, and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wang, Catrein, Leclercq, and Kim (Final Act. 21–24).

Claim 24 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Wang, Catrein, Leclercq, Kim, and de Cesare (Final Act. 25–26).

## ISSUE 1

### *35 U.S.C. § 103(a): Claims 1, 6, and 7*

Appellant contends their invention as recited in claims 1, 6, and 7 is not obvious over Wang and Catrein (App. Br. 9–14). The issue presented by the arguments is:

*Issue 1:* Has the Examiner shown the combination of Wang and Catrein teaches, suggests, or otherwise renders obvious “storing the encrypted firmware image in the non-volatile memory of the computing device,” as recited in claim 1?

#### ANALYSIS

We disagree with Appellant’s conclusions and adopt as our own: (1) the findings and reasons set forth by the Examiner in the action from which this appeal is taken; and (2) the reasons set forth by the Examiner in the Answer in response to the Appeal Brief. With respect to the claims argued by Appellant, we highlight and address specific findings and arguments for emphasis as follows.

Appellant argues Wang fails to teach an encrypted firmware image is stored in *non-volatile* memory of the computing device because Wang teaches the firmware image is stored in DRAM, a well-known form of *volatile* memory (App. Br. 10–11; Reply Br. 3). Although “Appellant agrees that storing data in volatile and non-volatile memory is known” and “it is known to store an encrypted firmware image in non-volatile memory” (Reply Br. 3 (citing Spec. ¶ 28, Fig. 1A) (emphasis omitted)), Appellant asserts the combination of Wang and Catrein does not teach the double-encryption technique in which encrypted firmware is stored in non-volatile memory after already once having been decrypted from double-encrypted firmware to encrypted firmware (Reply Br. 3–4). Additionally, Appellant argues Catrein does not teach this limitation (*id.* at 12).

We are not persuaded by Appellant’s arguments. Appellant acknowledges it is known to store an encrypted firmware image in non-volatile memory (Ans. 3; Spec. ¶ 28). Additionally, as noted by the

Examiner, Wang teaches the step of storing data in either a non-volatile memory (Wang ¶ 40) or a volatile memory (Wang ¶ 54) (Ans. 7). We agree with the Examiner that “one ordinarily skilled in the relevant art[] will recognize that the step of storing data can be made either in a ‘non-volatile memory’ . . . or in a ‘volatile memory’” (*id.*). Moreover, the argument that storing in non-volatile memory “is important because it allows the computing device (e.g., smartphone) to be re-booted from the encrypted firmware image that is stored in the non-volatile memory” (Reply Br. 4) is not persuasive because re-booting from the encrypted firmware image stored in the non-volatile memory, is not recited in the claim. Furthermore, we determine a skilled artisan would readily consider non-volatile memory as an alternative storage option as further explained below.

A skilled artisan is “a person of ordinary creativity, not an automaton” (*KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 420–21 (2007)). Appellant has not presented sufficient evidence or argument to persuade us that using non-volatile memory as the memory to store data (i.e., the encrypted firmware image) would have been “uniquely challenging or difficult for one of ordinary skill in the art” or “represented an unobvious step over the prior art” (*See Leapfrog Enters., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1162 (Fed. Cir. 2007)). Accordingly, we are not persuaded the combination of Wang and Catrein fails to teach, suggest, or otherwise renders obvious “storing the encrypted firmware image in the non-volatile memory of the computing device,” as recited in claim 1.

With respect to claim 7, Appellant argues Wang teaches a fully decrypted version of the firmware image is stored in the non-volatile memory but does not teach “the double-encrypted firmware image is first

stored in non-volatile memory and then read from the non-volatile memory and decrypted using the second crypto-key,” as recited. As set forth above, Appellant has not persuaded us that an ordinarily skilled artisan would not have found it obvious to store the double-encrypted firmware image in non-volatile memory.

Separate arguments were not set forth for claim 6 (App. Br. 13).

Accordingly, we are not persuaded the combination of Wang and Catrein fails to teach, suggest, or otherwise render obvious the limitations as recited in claims 1, 6, and 7. Therefore, we sustain the rejection of claims 1, 6, and 7 under 35 U.S.C. § 103(a) for obviousness over Wang and Catrein.

## ISSUE 2

### *35 U.S.C. § 103(a): Claims 2–4, 9, and 11*

Appellant contends the invention as recited in claims 2–4, 9, and 11, is not obvious over Wang, Catrein, and Leclercq (App. Br. 15–18). The issue presented by the arguments is:

*Issue 2:* Has the Examiner shown the combination of Wang, Catrein, and Leclercq teaches, suggests, or otherwise renders obvious

- (i) “a secure element located in a data path between the host processor and the non-volatile memory,” and
- (ii) “a crypto-engine . . . being configured to decrypt the double-encrypted firmware image . . . to provide the encrypted firmware image to the non-volatile memory of the computing device for storage,”

as recited in claim 11?

## ANALYSIS

For claim 11, Appellant first contends the similar limitations are not taught by Wang for the reasons set forth with respect to claim 1 (App. Br. 15). Appellant has not persuaded us Wang fails to teach or suggest the disputed limitations of claim 1; accordingly, for the reasons set forth above with respect to claim 1, we are not persuaded by Appellant's arguments.

Appellant next argues Leclercq fails to teach "a secure element located in a data path between the host processor and the non-volatile memory," as recited in claim 11 (App. Br. 15–17). The Examiner finds, and we agree, Leclercq teaches a secure element located in a data path between the host processor and the non-volatile memory (Ans. 13; Final Act. 9; Leclercq ¶¶ 51, 56, Fig. 4). Appellant additionally argues Leclercq, in Figure 4, does not teach a secure element having a crypto-engine, as recited, but instead, teaches a secure element that performs an authentication operation and a control word generation operation (App. Br. 15–16). However, Appellant does not address the Examiner's finding that paragraph 56 of Leclercq teaches the recited crypto-engine (Final Act. 9; Ans. 13). Indeed, Leclercq teaches the secure element uses the stored key to decrypt the encrypted data file (Leclercq ¶ 56). Thus, Appellant has not persuaded us the Examiner's findings are in error.

With respect to claim 2, Appellant argues Leclercq teaches a secure element that includes crypto hardware but does not teach the secure element is located between a host processor and a non-volatile memory (App. Br. 17). As set forth above, we are not persuaded by Appellant's arguments.

Claims 3, 4, and 9 were not separately argued (App. Br. 18). Accordingly, we are not persuaded the Examiner failed to show the

combination of Wang, Catrein, and Leclercq teaches, suggests, or otherwise renders obvious the limitations as recited in claims 2–4, 9, and 11.

Therefore, we sustain the rejection of claims 2–4, 9, and 11 under 35 U.S.C. § 103(a) for obviousness over Wang, Catrein, and Leclercq.

### ISSUE 3

#### *35 U.S.C. § 103(a): Claims 5 and 12–14*

Appellant contends the invention as recited in claims 5 and 12–14, is not obvious over Wang, Catrein, Leclercq, and de Cesare (App. Br. 18–20).

The issue presented by the arguments is:

*Issue 3:* Has the Examiner shown the combination of Wang, Catrein, Leclercq, and de Cesare teaches, suggests, or otherwise renders obvious “the secure element is configured to apply decryption to data addressed to code blocks in the non-volatile memory and to pass without decryption data addressed to data blocks in the non-volatile memory,” as recited in claim 5?

### ANALYSIS

Appellant contends de Cesare teaches a technique for verifying if a code image is trusted and for determining if the trusted code image is compatible with the device (App. Br. 20). However, according to Appellant, de Cesare does not teach a distinction between data addressed to code blocks and data addressed to data blocks in a non-volatile memory (*id.*).

The Examiner finds de Cesare teaches a trusted code image is verified before decrypting the code image and bypassing the decrypting if the trusted code image is not compatible (Final Act. 10; Ans. 18 (citing de Cesare ¶¶ 73–74)). However, the Examiner has not shown how the trusted code that is compatible and the trusted code that is not compatible teaches,

suggests, or otherwise renders obvious distinguishing between data addressed to code blocks and data addressed to data blocks.

Accordingly, we are unable to sustain the rejection of claims 5 and 12–14 under 35 U.S.C. § 103(a) for obviousness over Wang, Catrein, Leclercq, and de Cesare.

#### ISSUE 4

##### *35 U.S.C. § 103(a): Claim 8*

Appellant contends the invention as recited in claim 8, is not obvious over Wang, Catrein, and Kim (App. Br. 20 and 21). The issue presented by the arguments is:

*Issue 4:* Has the Examiner shown the combination of Wang, Catrein, and Kim teaches, suggests, or otherwise renders obvious “the first crypto-key is a group key (GK1), which is the same for a group of computing devices, and wherein the second crypto-key is a group key (GK2), which is the same for a particular version of the firmware,” as recited in claim 8?

#### ANALYSIS

Appellant contends Kim teaches that a user group key is used to decrypt the firmware encryption key (FEK); however, Kim does not teach the user group key is used to decrypt the firmware itself (App. Br. 21).

We do not agree with Appellant’s contention. Specifically, the Examiner relies on Kim as teaching the first crypto-key being a group key which is the same for a group of computing devices, and the second crypto-key being a group key which is the same for a particular version of the firmware (Final Act. 8–9; Ans. 19–20). Appellant’s argument that Kim does not teach the user group key is used to decrypt the firmware itself, is arguing

the references individually. Specifically, the Examiner relies on Wang to teach using the first crypto-key to decrypt the encrypted firmware (Final Act. 4) and Kim to teach the two different group keys (Final Act. 12–13; Ans. 19–20).

Accordingly, we are not persuaded the Examiner erred in finding the combination of Wang, Catrein, and Kim teaches, suggests, or otherwise renders obvious the limitations as recited in claim 8. Therefore, we sustain the rejection of claim 8 under 35 U.S.C. § 103(a) for obviousness over Wang, Catrein, and Kim.

#### ISSUE 5

*35 U.S.C. § 103(a): Claims 10 and 15–21*

Claims 10 and 15–21 are not separately argued, relying on previously presented arguments (App. Br. 21–24). As set forth above, we are not persuaded of error in the Examiner’s findings and reasoning. It follows, we sustain the rejection of claims 10 and 15–21 under 35 U.S.C. § 103(a) for obviousness over Wang, Catrein, and Kim.

#### ISSUE 6

*35 U.S.C. § 103(a): Claims 22, 23, 25, and 26*

Appellant contends the invention as recited in claims 22, 23, 25, and 26 is not obvious over Wang, Catrein, Leclercq, and Kim (App. Br. 24–28). The issue presented by the arguments is:

*Issue 6:* Has the Examiner shown the combination of Wang, Catrein, Leclercq, and Kim teaches, suggests, or otherwise renders obvious

“storing the decrypted random number in the non-volatile memory of the computing device,”

“reading the decrypted random number from the non-volatile memory of the computing device,” and

“confirming the presence of the element if the decrypted random number matches the stored random number,”

as recited in claim 22?

#### ANALYSIS

Appellant again argues Wang fails to teach “storing the decrypted random number in the non-volatile memory of the computing device” (App. Br. 25). According to Appellant, Wang does not teach storing a decrypted random number in the non-volatile memory (*id.*). Appellant next argues Wang fails to teach “reading the decrypted random number from the non-volatile memory of the computing device” because although Wang teaches a decrypted firmware image is stored in and read from non-volatile memory, Wang fails to teach a decrypted random number is stored in the non-volatile memory (App. Br. 25).

We are not persuaded of error in the Examiner’s findings and reasoning (Final Act. 21; Ans. 27–28). Additionally, we determine storing and reading a decrypted random number as recited would not have been uniquely challenging or difficult for an ordinarily skilled artisan in light of Wang’s teachings. Indeed, Wang teaches storing and reading decrypted data and thus, in light of the teachings and suggestions of the references, as well as Appellant’s arguments, we are not persuaded the combination fails to teach, suggest, or otherwise render obvious the disputed limitations.

Appellant further argues “confirming the presence of the element if the decrypted random number matches the stored random number” is not

taught by Kim (App. Br. 25). Instead, Appellant contends, Kim teaches an apparatus that can generate a random number to be used to generate an encryption key (*id.*).

We agree with Appellant that the Examiner has failed to show where Kim teaches the generated random number is compared to any other random number and specifically, confirming the presence of the element if the two random numbers match. Accordingly, we are persuaded the Examiner has not shown the combination of Wang, Catrein, and Kim teaches, suggests, or otherwise renders obvious the limitations as recited in claim 22. Claims 23, 25, and 26 depend from claim 22 and thus, stand with claim 22. Therefore, we cannot sustain the rejection of claims 22, 23, 25, and 26 under 35 U.S.C. § 103(a) for obviousness over Wang, Catrein, Leclercq, and Kim.

#### ISSUE 7

##### *35 U.S.C. § 103(a): Claim 24*

Claim 24 depends from claim 22 and thus, stands with claim 22. Accordingly, we cannot sustain the rejection of claim 24 under 35 U.S.C. § 103(a) for obviousness over Wang, Catrein, and Kim.

#### DECISION

The Examiner's rejection of claims 1, 6, and 7 under 35 U.S.C. §103(a) as being unpatentable over Wang and Catrein is affirmed.

The Examiner's rejection of claims 2–4, 9, and 11 under 35 U.S.C. §103(a) as being unpatentable over Wang, Catrein, and Leclercq is affirmed.

The Examiner's rejection of claims 5 and 12–14 under 35 U.S.C. §103(a) as being unpatentable over Wang, Catrein, Leclercq, and de Cesare is reversed.

The Examiner's rejection of claim 8 under 35 U.S.C. §103(a) as being unpatentable over Wang, Catrein, and Kim is affirmed.

The Examiner's rejection of claim 10 under 35 U.S.C. §103(a) as being unpatentable over Wang, Catrein, Leclercq, and Kim is affirmed.

The Examiner's rejection of claim 15 under 35 U.S.C. §103(a) as being unpatentable over Wang, Catrein, Leclercq, de Cesare, and Kim is affirmed.

The Examiner's rejection of claim 16 under 35 U.S.C. §103(a) as being unpatentable over Wang and Leclercq is affirmed.

The Examiner's rejection of claims 17–19 under 35 U.S.C. §103(a) as being unpatentable over Wang, Leclercq, and de Cesare is affirmed.

The Examiner's rejection of claims 20 and 21 under 35 U.S.C. §103(a) as being unpatentable over Wang, Leclercq, and Kim is affirmed.

The Examiner's rejection of claims 22, 23, 25, and 26 under 35 U.S.C. §103(a) as being unpatentable over Wang, Catrein, Leclercq, and Kim is reversed.

The Examiner's rejection of claim 24 under 35 U.S.C. §103(a) as being unpatentable over Wang, Catrein, Leclercq, Kim, and de Cesare is reversed.

Appeal 2015-008080  
Application 13/622,534

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)(iv).

AFFIRMED-IN-PART