

United States Patent and Trademark Office
Before the Patent Trial and Appeal Board

***Mastercard Incorporated and
Mastercard International Incorporated***

(Petitioner)

v.

OV Loop, Inc.

(Patent Owner)

Hearing

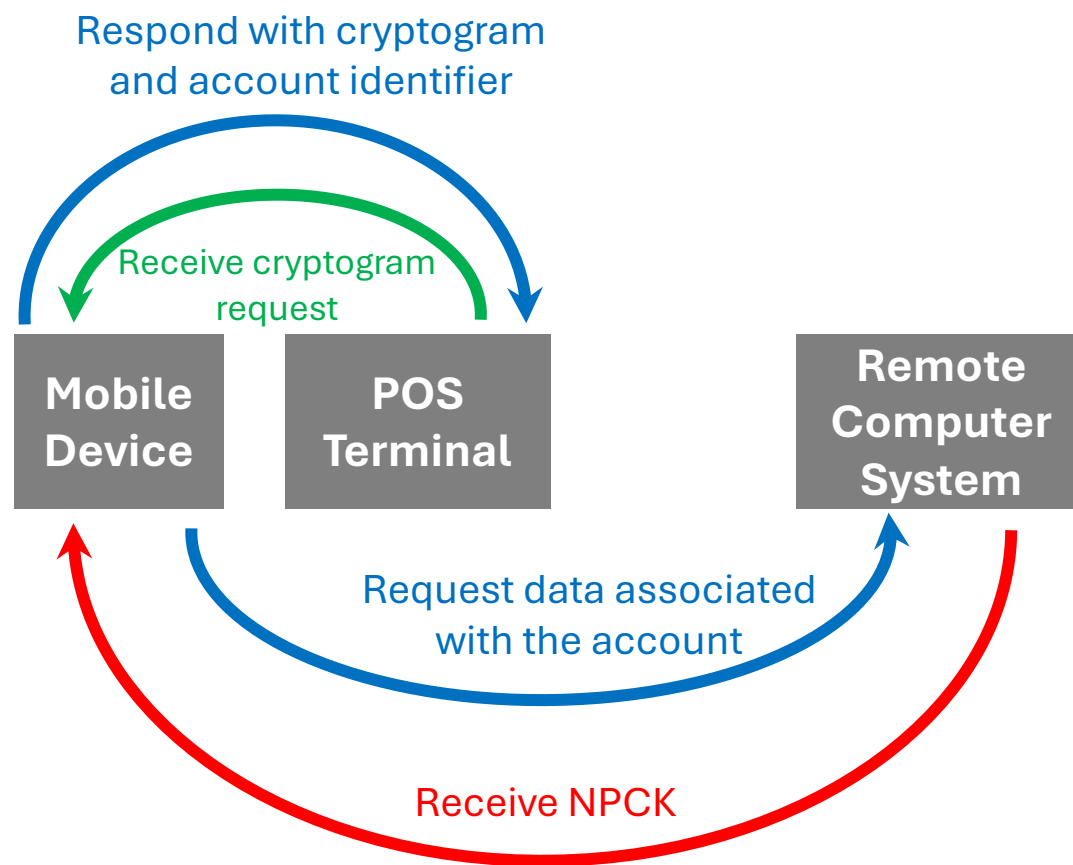
No. IPR2023-01289 | U.S. Patent No. 10,032,171

Patent Owner's Demonstrative Exhibits

Ex. 2039

December 13, 2024

Overview of Payment Process



U.S. Pat. No. 10,032,171

1. A method for secure application-based participation in a payment card transaction authorization process by a mobile device, the method comprising:

at a mobile device, executing an application in an operating system of the mobile device

...

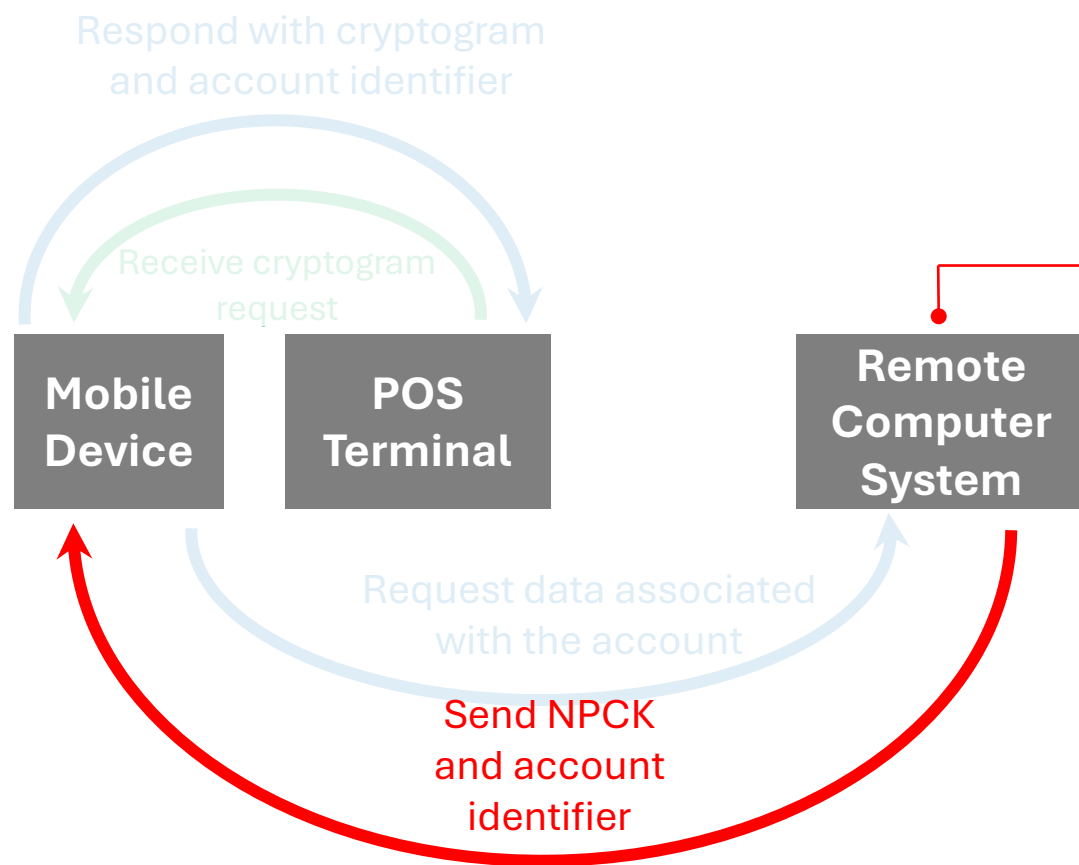
configured to request, from a remote computer system hosting the corresponding digital credential, over a wireless network that is separate from the first communications channel

...

participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device comprising:

...

Overview of Payment Process



U.S. Pat. No. 10,032,171

8. The method of claim 1, further comprising, at the remote computer system:

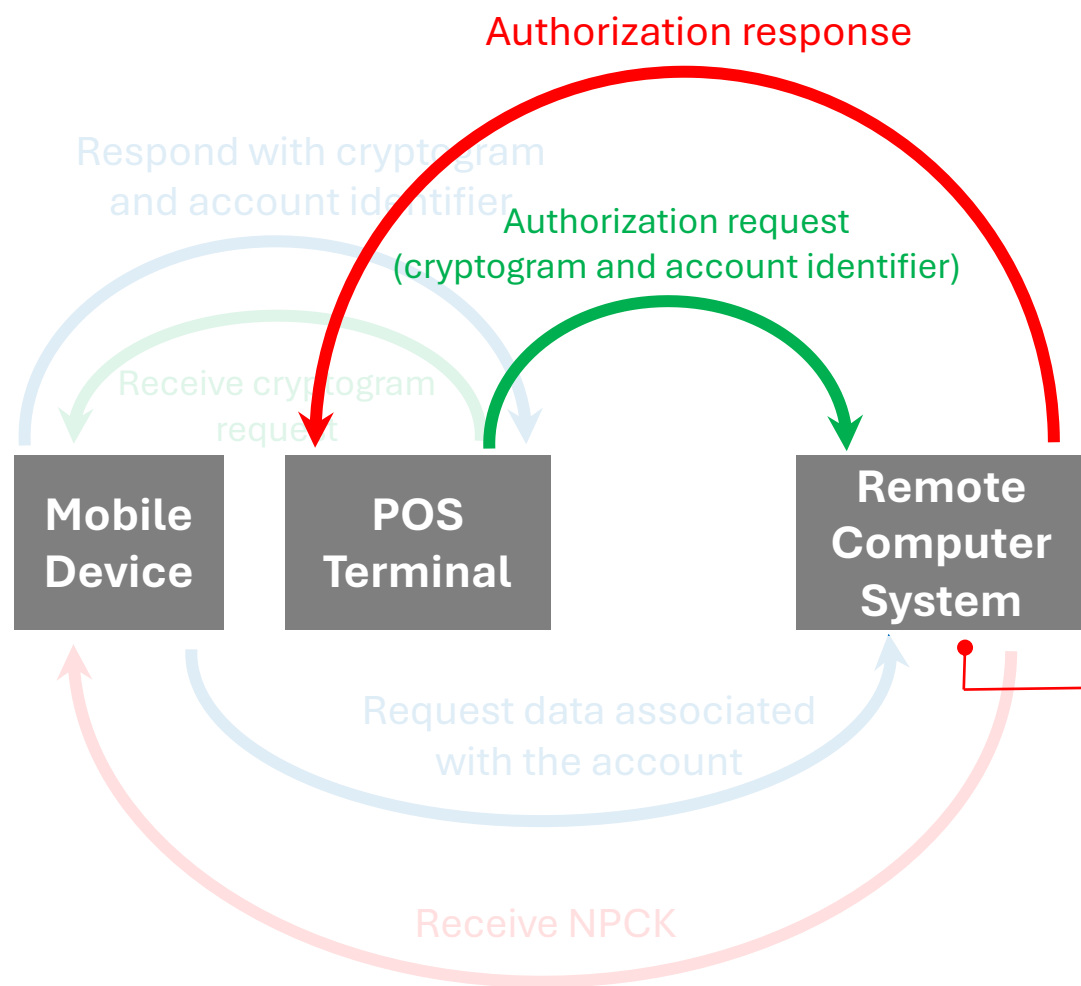
prior to the interrogation, **generating the first non-permanent cryptographic key** at the remote computer system,

associating the first non-permanent cryptographic key with the account, and

sending the first non-permanent cryptographic key and the account identifier to the mobile device over the wireless network;

...

Overview of Payment Process



U.S. Pat. No. 10,032,171

10. The method of claim 1, further comprising, **at the remote computer system**, performing an authorization process comprising:

receiving an authorization request to authorize the transaction **from the POS terminal**, ... wherein the authorization data comprises the response cryptogram and the account identifier;

determining a current non-permanent cryptographic key associated with the account using the account identifier;

calculating a calculated cryptogram using the current non-permanent cryptographic key associated with the account;

verifying a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram; and

sending an authorization response to the POS terminal ...

Grounds 1 & 2 – Collinge

“remote computer system”

(Claims 1/17, 10/27)

Claims 1 and 10

U.S. Pat. No. 10,032,171

1. A method for secure application-based participation in a payment card transaction authorization process by a mobile device, the method comprising:

at a mobile device, executing an application in an operating system of the mobile device...

configured to request, from **a remote computer system**  **hosting** the corresponding digital credential, over a wireless network that is separate from the first communications channel...

requesting by the application, from **the remote computer system**, over the wireless network, a first set of data associated with the account;...

receiving by the application, from **the remote computer system**, over the wireless network, the first set of data associated with the account...

EX1001, 50:61-51:18

U.S. Pat. No. 10,032,171

10. The method of claim 1, further comprising, **at the remote computer system**, performing an authorization process comprising:

receiving an authorization request to authorize the transaction from the POS terminal, ... wherein the authorization data comprises the response cryptogram and the account identifier;

determining a current non-permanent cryptographic key associated with the account using the account identifier;

calculating a calculated cryptogram using the current non-permanent cryptographic key associated with the account;

verifying a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram; and

sending an authorization response to the POS terminal
...

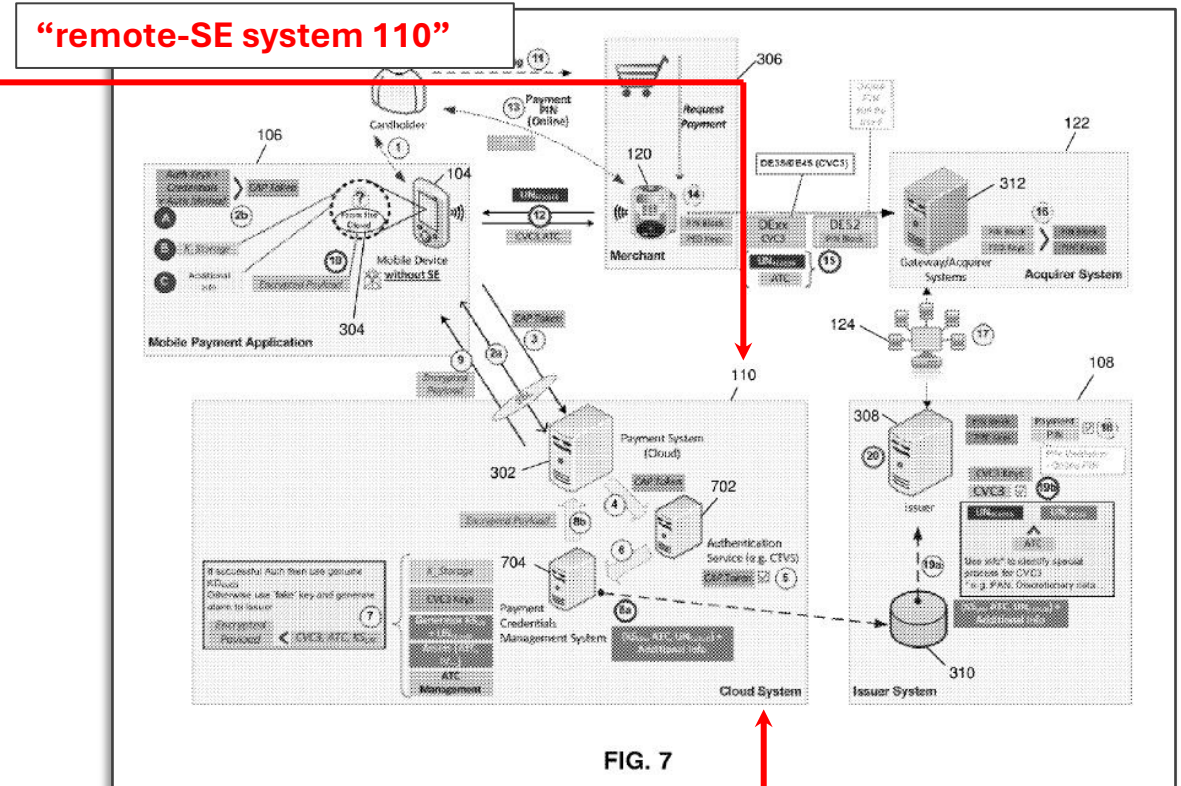
EX1001, 52:42-61

Petition identifies “remote-SE system 110” as a *remote computer system*

Claim 1

Petition – “a remote computer system” (claim 1)

Collinge discloses that “[p]ayment credentials corresponding to the payment account may be stored in a remote-SE (remote-secure-element) system 110 for provisioning to the mobile device.” Ex[1011], [0042], [0071], Fig. 7; *see also* Ex[1009], [0061] (Table 1, Steps 1-2). Further, “the mobile payment application 106 may transmit [a] CAP token to the remote-SE system 100,” Ex[1011], [0081], which causes the remote-SE system to generate and return payment credentials in an encrypted payload after verification of CAP token, *id.* at [0082]-[0083], [0085]. A POSA would understand that sending of CAP token initiates, and thus constitutes a request for server to return payment credentials. Ex[1006] ¶ 87. Further, as shown in Collinge Fig. 7, the communication between the remote/cloud system to the phone is a different (second) communication channel (*e.g.*, SSL/TLS) from the channel used to communicate with the POS reader/merchant (first communication channel.



EX1011, Fig. 7

Pet. 38-39

“Cloud System”

Petitioner's expert confirms reliance on "remote-SE system 110"

Claim 1

Petitioner's Expert – Deposition

Q: So it is remote-SE system 110 that you are identifying as the remote computer system from the claim; right?

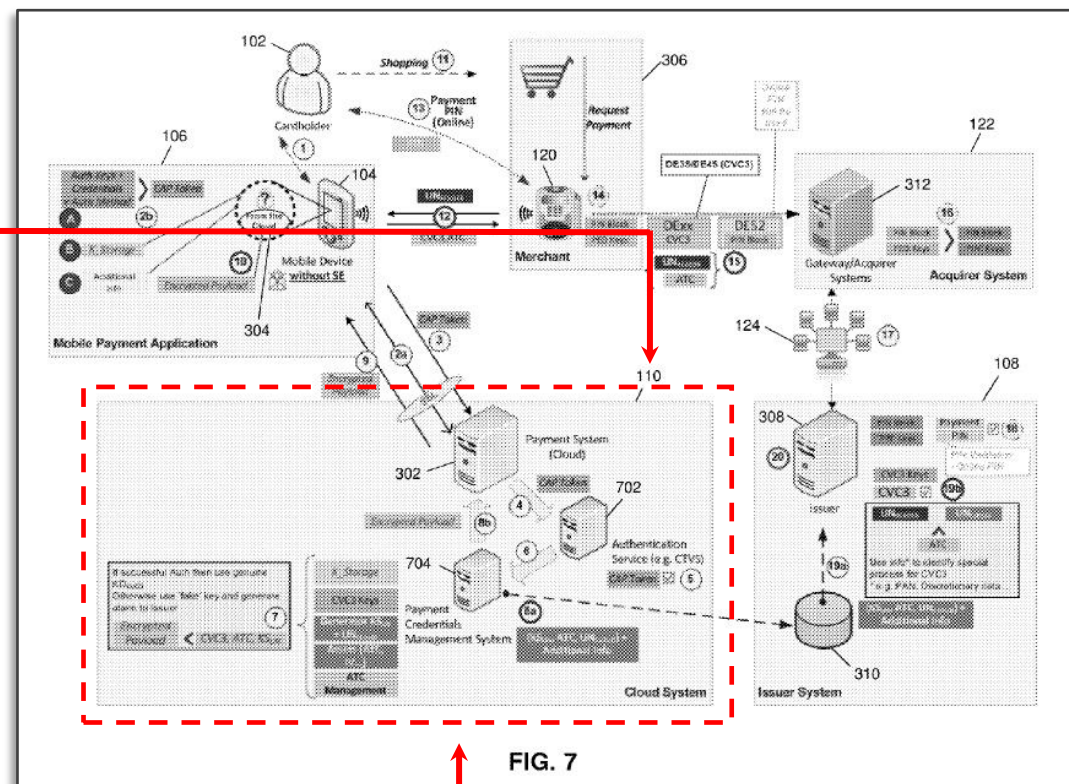
A: Yes. And in that sentence, which uses 100, it's actually talking about transmitting the generated CAP token... which is within 110. So yes, I'm pretty convinced that's a typo.

...

Q: So in the figure we see 110, which is essentially pointing to sort of a gray box in the lower left quadrant of Figure 7; right?

A: Yes.

Collinge



EX1011, Fig. 7

Petition does not allege that “remote-SE system 110” performs steps recited in claim 10

10. The method of claim 1, further comprising, at the remote computer system, performing an authorization process comprising:

To the extent the preamble is limiting, Collinge discloses this limitation. For example, Collinge discloses performing an authorization process at a payment network. Ex[1011], [0045], [0056]-[0057], [0086]-[0087]; *see also* Ex[1009], [0061] (Table 1, Steps 14-15).

Pet. 58

... determining a current non-permanent cryptographic key associated with the account using the account identifier;

Collinge discloses that “the issuer processing server 308 may validate the payment CVC3 value using at least the UN_{READER} , UN_{CLOUD} , and application transaction counter,” by retrieving (“determining”) the UN_{CLOUD} and KS_{UN} (hence the session key associated with the account and unique to transaction, as explained in [1.A-3]) values that were used by the Payment Credential Management System to generate (“calculating”) the CVC3 value. Ex[1011], [0087]; *see also* Ex[1009], [0061] (Table 1, Step 19a-19b). Because this CVC3 value is calculated using the

Pet. 59

Collinge

[0056] An acquirer processing server 312 may receive the information at the acquirer 122 and may generate and submit an authorization request for the financial transaction including the payment credentials and dynamic card validation code to the payment network 124. The payment network 124 may forward relevant information to the issuer 108 for authorization of the transaction for a specific transaction amount. The issuer 108 may include an issuer processing server 308. The

EX1011, [0056]

[0045] The acquirer 122 may submit an authorization request for the payment transaction to a payment network 124. The payment network 124 may be configured to process the authorization request, such as by querying the issuer 108 for approval of the payment transaction (e.g., based on funds or credits in the payment account). The payment network 124 may then submit an authorization response to the acquirer 122 and/or the merchant, who may then finalize the payment transaction with the user 102. Methods and systems suitable for the processing of a financial transaction will be apparent to persons having skill in the relevant art.

EX1011, [0045]

database 310. At stage 19b, the issuer processing server 308 may validate the payment CVC3 value using at least the UN_{READER} , UN_{CLOUD} , and application transaction counter. Methods for validating a CVC3 will be apparent to persons having skill in the relevant art. At stage 20, the issuer 108 may submit a response based on the validation, and the method may proceed accordingly as in traditional payment transactions.

EX1011, [0087]

Petition relies on elements outside of “remote-SE system 110”

Collinge

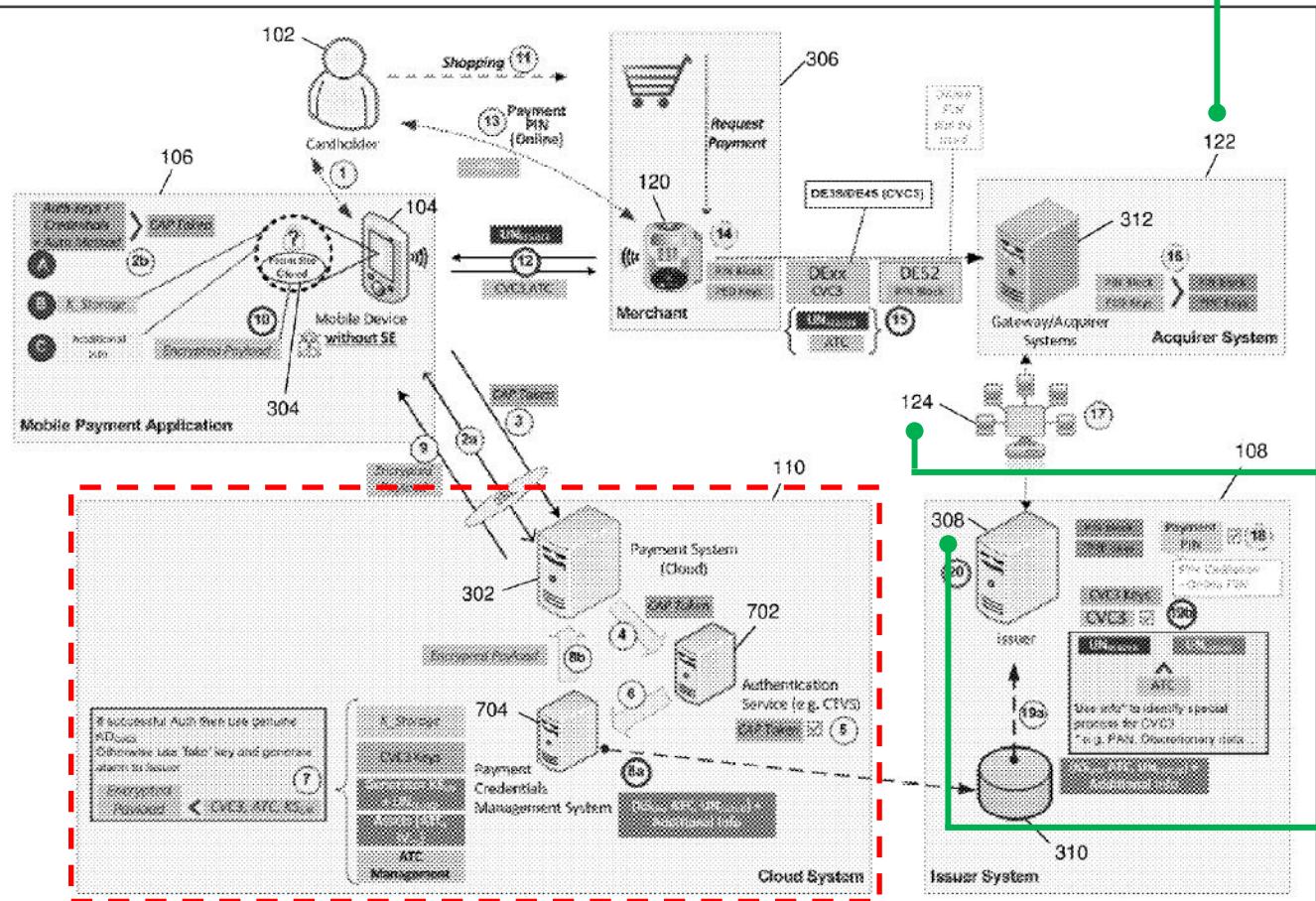


FIG. 7

EX1011, Fig. 7

Demonstrative Exhibit - Not Evidence

[0056] An acquirer processing server 312 may receive the information at the acquirer 122 and may generate and submit an authorization request for the financial transaction including the payment credentials and dynamic card validation code to the payment network 124. The payment network 124 may forward relevant information to the issuer 108 for authorization of the transaction for a specific transaction amount. The issuer 108 may include an issuer processing server 308. The

EX1011, [0056]

[0045] The acquirer 122 may submit an authorization request for the payment transaction to a payment network **124**. The payment network 124 may be configured to process the authorization request, such as by querying the issuer **108** for approval of the payment transaction (e.g., based on funds or credits in the payment account). The payment network 124 may then submit an authorization response to the acquirer **122** and/or the merchant, who may then finalize the payment transaction with the user **102**. Methods and systems suitable for the processing of a financial transaction will be apparent to persons having skill in the relevant art.

EX1011, [0045]

database 310. At stage 19b, the issuer processing server 308 may validate the payment CVC3 value using at least the UN_{READER}, UN_{CLOUD}, and application transaction counter. Methods for validating a CVC3 will be apparent to persons having skill in the relevant art. At stage 20, the issuer 108 may submit a response based on the validation, and the method may proceed accordingly as in traditional payment transactions.

EX1011, [0087]

Petitioner's Reply identifies a different alleged *remote computer system*

Collinge

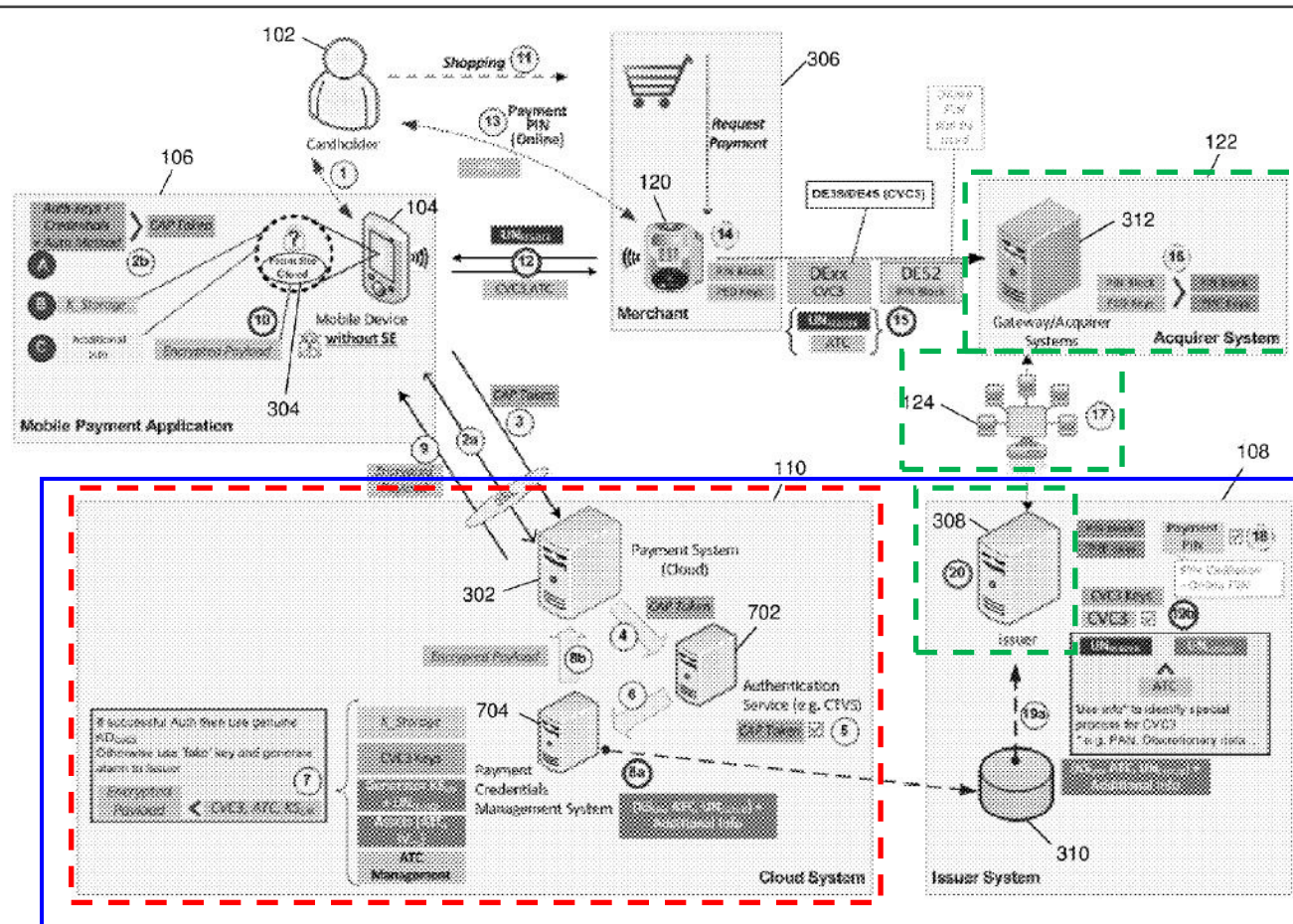


FIG. 7

EX1011, Fig. 7

Demonstrative Exhibit - Not Evidence

Petitioner's Reply

POR, 31. However, the Petition never limited the mapping of the claimed “remote computer system” to PO’s red box. To the contrary, the Petition mapped functionality performed in at least the structures identified below in the blue box (which are expressly stated and shown to share a “connection 178” therebetween) as corresponding to the functions of the remote computer system:

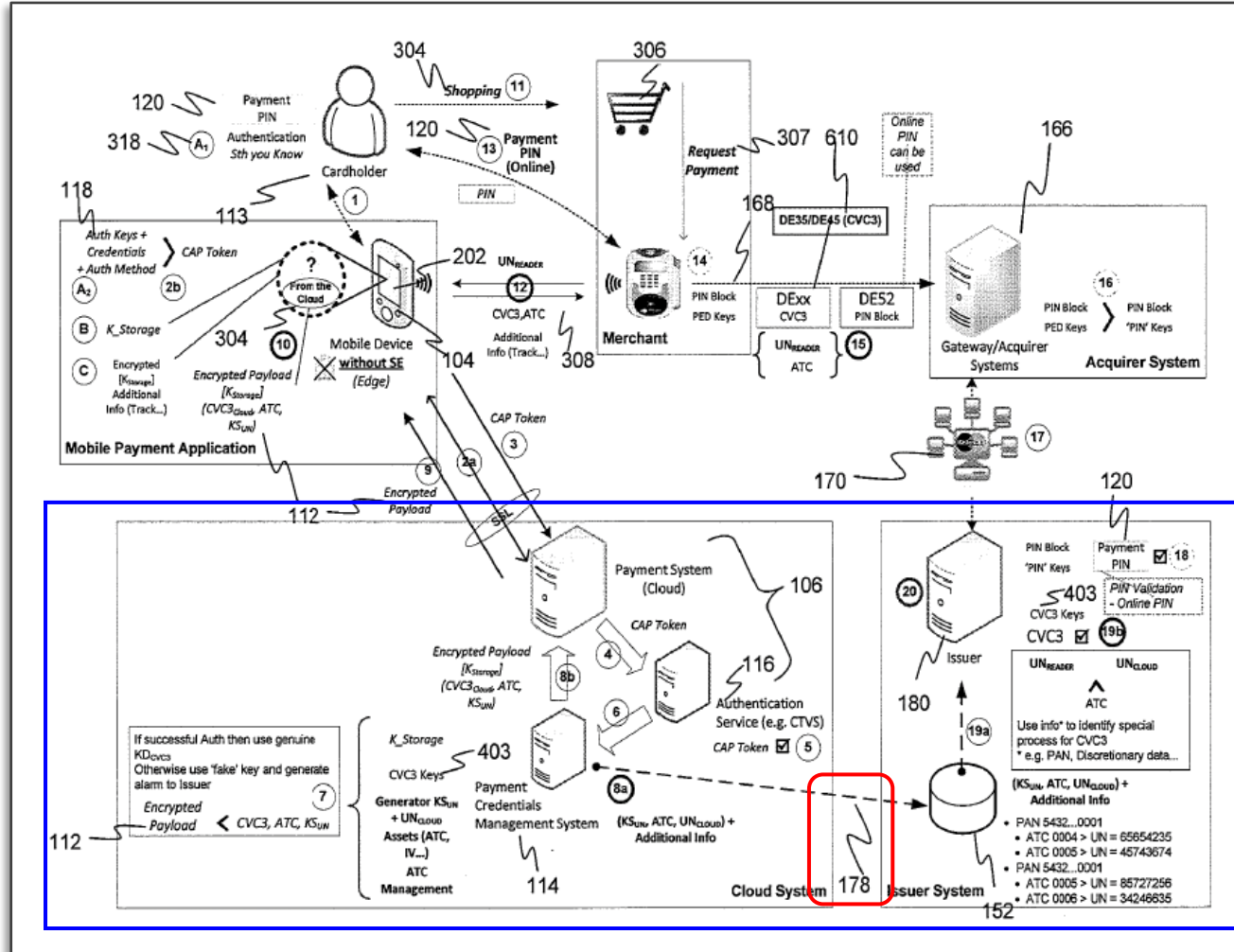
...

Ex[1009] [0046] and Fig. 7; Pet., 38-41 (mapping functions of claim 1 performed by the “remote computer system” to the “remote system” on the bottom of the figure), 58-59 (mapping functions of claim 10 performed by the “remote computer system” to the part of the “payment network” that allows the “issuer to authorize the transaction and associate it with the correct account” which is in the blue-boxed portion).

Reply 16-17

Petitioner has not shown that its “blue box” elements are part of the same *remote computer system*

Collinge Provisional



Petitioner's Reply

POR, 31. However, the Petition never limited the mapping of the claimed “remote computer system” to PO’s red box. To the contrary, the Petition mapped functionality performed in at least the structures identified below in the blue box (which are expressly stated and shown to share a “connection 178” therebetween) as corresponding to the functions of the remote computer system:

Reply 16

- No argument in Petition that “blue box” elements are part of a single *remote computer system*
- Any argument on Reply that these elements are part of a single remote computer system in not responsive to any issue raised in the POR
- Reply is still ambiguous as to the elements within the alleged *remote computer system*

EX1009, Fig. 7

POR 11-16

Grounds 1 & 2 – Collinge

**“determining a current non-
permanent cryptographic key ...using
the account identifier”**

(Claims 10/27)

No evidence that PAN (alleged *account identifier*) is used to determine current NPCK

10.C determining a current non-permanent cryptographic key associated with the account using the account identifier;

Petition

Collinge discloses that “the issuer processing server 308 may validate the payment CVC3 value using at least the UN_{READER}, UN_{CLOUD}, and application transaction counter,” by retrieving (“determining”) the UN_{CLOUD} and KS_{UN} (hence the session key associated with the account and unique to transaction, as explained in [1.A-3]) values that were used by the Payment Credential Management System to generate (“calculating”) the CVC3 value. Ex[1011], [0087]; *see also* Ex[1009], [0061] (Table 1, Step 19a-19b). Because this CVC3 value is calculated using the

Pet. 59

- New inherency theory, not presented in Petition
- Collinge Provisional says the ATC is used to “retrieve” KS_{UN}, not “re-calculate” it
- No reason PAN must be used

Collinge Provisional

- | | |
|------------|---|
| 19a | The Issuer has a mean to identify transaction that requires additional processing for CVC3 validation when the solution using SE-less Mobile Contactless Payment is used.
<u>Using the ATC provided in the Payment Transaction, the Issuer is able to retrieve the UN_{CLOUD} and KS_{UN} values that were used by the Payment Credential Management System to generate the CVC3 value.</u>
Detection of unsuccessful authentication can also take place at this stage. |
| 19b | A standard process applies for the CVC3 validation using the UN _{CLOUD} and KS _{UN} values. |

EX1009 [0061]

Petitioner's Reply

Contrary to POR's assertions, POR 34-35, Collinge Provisionals do not teach that retrieval of KS_{UN} is done using *only* the ATC. Ex[1009] 23. A POSITA would understand that the issuer must use an account identifier such as a PAN to retrieve or re-calculate (“determine”) the correct key because, as explained, KS_{UN} is generated uniquely with and for a PAN and is specific to a PAN. *Supra* §IV.A.1.b; Ex[1050] ¶45.

POR 34-35, Sur-reply 16-17

Reply 18

Grounds 1 & 2 – Collinge

**“sending ... the account identifier to
the mobile device”**

(Claims 8 & 25)

No evidence in Collinge of sending *the account identifier to the mobile device*

8. The method of claim 1, further comprising, **at the remote computer system**: prior to the interrogation, generating the first non-permanent cryptographic key at the remote computer system, associating the first non-permanent cryptographic key with the account, and **sending the first non-permanent cryptographic key and the account identifier to the mobile device** over the wireless network; and...

Petition

8. Claim 8

a. [8.PRE]

See §§ X.A.1.b , X.A.1.d ([1.A-1], [1.A-3]).

b. [8.A]

See §§ X.A.1.d, X.A.1.f, X.A.1.g, X.A.1.i(3) ([1.A-3], [1.B], [1.C], [1.E-3]).

c. [8.B]

See §§ X.A.1.j ([1.F]-[1.G]).

No evidence in Collinge of sending *the account identifier to the mobile device*

Petition

b. [8.A]

See §§ X.A.1.d, X.A.1.f, X.A.1.g, X.A.1.i(3) ([1.A-3] [1.B], [1.C], [1.E-3].

Pet. 57

Petition (1.B)

As explained in [1.A-3] above, Collinge discloses this element, where a first set of data is a digital credential associated with the account.

A POSA would also have found it obvious to configure the mobile application to make a request, either together with transmitting a CAP token or separately (e.g., before transmission), for purposes of efficiency and resources, as explained in [1.A-3].

Pet. 42

- Request from the mobile application
- Petition argues that encrypted payload includes a “single use key,” which is not an account identifier

POR 37-39

Petition (1.C)

As explained in [1.A-3] above, Collinge discloses that the mobile payment application can receive an encrypted payload and payment credentials from the cloud system over a wireless network. Ex[1011], [0009], [0013], [0083], [0141].
The encrypted payload can include a “single use key” including a generating key for generation of a CVC3 cryptogram or Application Cryptogram. Ex[1011], [0050].

Pet. 43

No evidence in Collinge of sending *the account identifier to the mobile device*

Petition

b. [8.A]
See §§ X.A.1.d, X.A.1.f, X.A.1.g, X.A.1.i(3) [1.A-3] [1.B], [1.C], [1.E-3].

Pet. 57

- No evidence or argument that encrypted payload includes the PAN

POR 38-39

Petition (1.A-3)

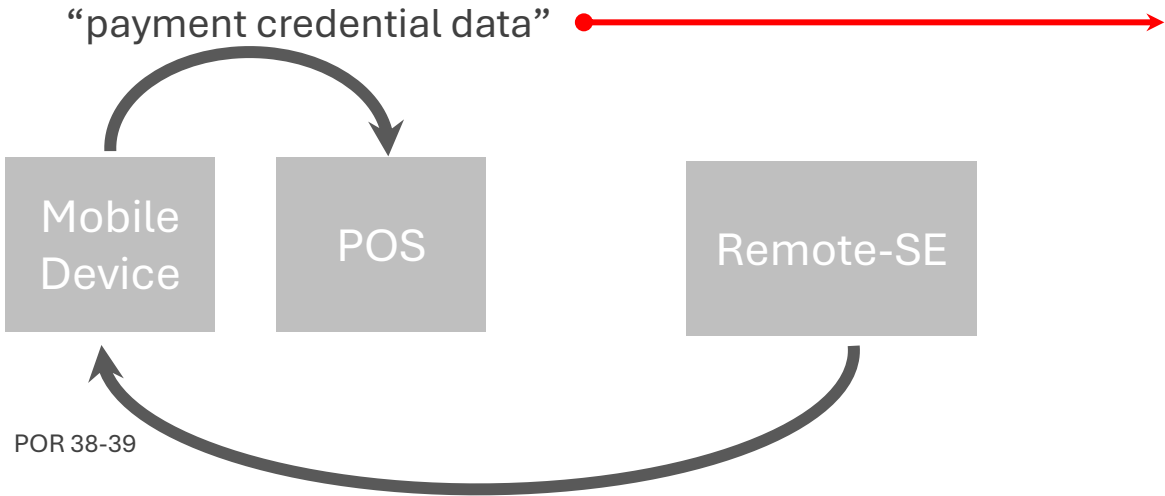
Collinge discloses that “[p]ayment credentials corresponding to the payment account may be stored in a remote-SE (remote-secure-element) system 110 for provisioning to the mobile device.” Ex[1011], [0042], [0071], Fig. 7; see also Ex[1009], [0061] (Table 1, Steps 1-2). Further, “the mobile payment application 106 may transmit [a] CAP token to the remote-SE system 100,” Ex[1011], [0081], which causes the remote-SE system to generate and return payment credentials in an encrypted payload after verification of CAP token, *id.* at [0082]-[0083], [0085]. A

Pet. 38-39

Petition (1.E-3)

As explained in [1.A-2], [1.E-1], and [1.E-2], Collinge discloses that the mobile device sends payment credential data, which a POSA would understand to include generated payment cryptogram and other “common payment credential information” such as account information (*e.g.*, PAN)⁶ to the POS terminal in response to a POS communication. See *supra* §§ X.A.1.c, X.A.1.i(1), X.A.1.i(2); see also Ex[1011], [0044], [0055], [0070], [0077]; Ex[1009], [0061] (Table 1, Step 15), [0064]. A POSA would understand that this can be implemented in the manner

Pet. 48



POR 38-39

No evidence in Collinge of sending *the account identifier to the mobile device*

Petitioner's Reply

a. [8.A]:

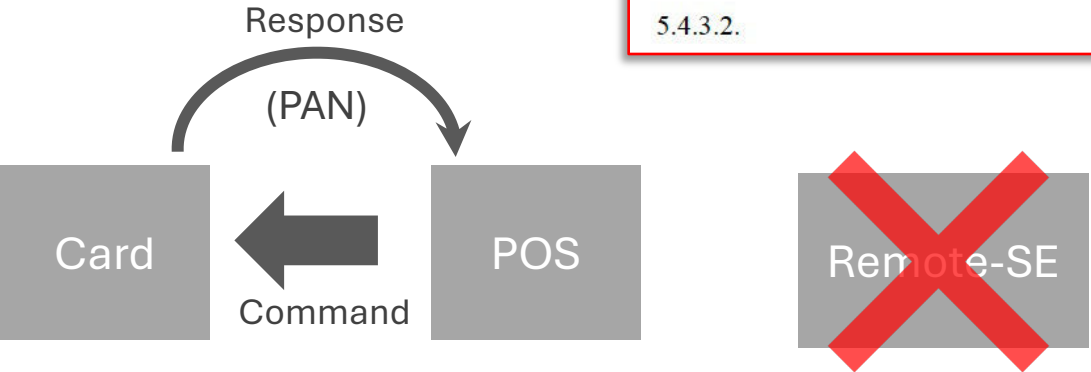
PO argues that Collinge does not explicitly mention the PAN as part of the encrypted payload. *Id.* 38-39. As explained in the Petition, Collinge discloses receiving from a remote-SE all necessary “payment credentials” to create a transaction request message including “account information (e.g. PAN)” (Pet., 38-39). Indeed, the Petition specifically cites to Collinge [0009] as explaining what “payment credentials” are received from the remote computer system. Pet., 43. That paragraph also suggests that the remote system sends “static payment credentials” (which a POSITA would understand include the account number) as well as the dynamic KS_{UN}.

Reply 19-20

Petition (1.A-2)

As explained, a POSA reading Collinge will understand that it discloses contactless payment techniques compatible with EMV infrastructure. Ex[1006] ¶ 73. It was well known that in an EMV transaction, a “card application” runs in a payment “Card,” and the POS terminal’s application “sends commands as a client to the card application, which responds as a server.” Ex[1006] ¶ 86; Ex[1037] at 47-48. The POS will select an application on a “Card,” such as a Mastercard or Visa transaction, Ex[1023] § 5.8.2; Ex[1026] § 2.3.3-2.3.4; Ex[1027] § 2.4.1, and the application on the “Card” will return “digital credential data”—data necessary for approval of a transaction, Ex[1001], 7:3-7, including account information (e.g., PAN) and MAC/cryptogram (CVC3 or Application Cryptogram). Ex[1026] §§ 3.4.2, 3.8.1–3.8.3, 5.2, 5.3; Ex[1021] Part III, § 7.2, Ex[1027] §§ 2.4.1, 5.2.2.3, 5.4.3.2.

Pet. 38



POR 37-39

No evidence in Collinge of sending *the account identifier* to the mobile device

Petitioner's Reply

a. [8.A]:

PO argues that Collinge does not explicitly mention the PAN as part of the encrypted payload. *Id.* 38-39. As explained in the Petition, Collinge discloses receiving from a remote-SE all necessary “payment credentials” to create a transaction request message including “account information (e.g. PAN)” (Pet., 38-39). Indeed, the Petition specifically cites to Collinge [0009] as explaining what “payment credentials” are received from the remote computer system. Pet., 43. That paragraph also suggests that the remote system sends “static payment credentials” (which a POSITA would understand include the account number) as well as the dynamic KS_{UN} .

Reply 19-20

- Pure speculation by counsel for Petitioner. No evidence as to how “static payment credentials” would have been understood in Collinge.
- “Suggestion” is not literal disclosure
- If Petitioner wanted to allege that “static payment credentials” would include the account number, the Petition should have said so

Sur-reply 19-20

No evidence in Collinge of sending *the account identifier* to the mobile device (Claim 8)

Petitioner's Reply

Moreover, because the non-permanent cryptographic key is specific to an account and only usable for the associated account, *see also supra* §IV.A.1.b, it would be obvious to send an account identifier along with the key, so that the mobile device knows which account's key it is receiving, which a POSITA would understand would be useful when designing a card capable of being used with multiple accounts or a credential wallet usable with multiple accounts. Ex[1050] ¶48.

Reply 20

- Improper new theory of obviousness
- Petition did not present any obviousness theory for claim 8
- Reply does not cite to any part of the Petition

Sur-reply 20



“The declaration raises a new obviousness argument for this limitation that could have been made in the petition. The Board correctly noted this argument was not made in the petition, which proposed that Shoubridge rendered obvious a number of other claim limitations. Blizzard, as petitioner, had an opportunity to present this argument in its petition, but chose not to.” *Acceleration Bay, LLC v. Activision Blizzard Inc.*, 908 F.3d 765, 775 (Fed. Cir. 2018)



“A reply may only respond to arguments raised in the corresponding opposition or patent owner response Once the Board identifies new issues presented for the first time in reply, neither this court nor the Board must parse the reply brief to determine which, if any, parts of that brief are responsive and which are improper.” *Intelligent Bio-Systems, Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369 (Fed. Cir. 2016) (internal quotations removed).

No evidence in Collinge of sending *the account identifier* to the mobile device (Claim 8)

Petitioner's Reply

Moreover, because the non-permanent cryptographic key is specific to an account and only usable for the associated account, *see also supra* §IV.A.1.b, it would be obvious to send an account identifier along with the key, so that the mobile device knows which account's key it is receiving, which a POSITA would understand would be useful when designing a card capable of being used with multiple accounts or a credential wallet usable with multiple accounts. Ex[1050] ¶48.

Reply 20

- No prior art disclosure of sending the first NPCK and the account identifier
- Modification of Collinge based on improper hindsight
- No mention in Collinge of multiple accounts. Mobile payment application is specific to a particular payment account.
- Even if an account identifier were sent, there is no basis for choosing the PAN instead of other account identifiers.

Sur-reply 21

Grounds 3 & 4 – Fiske

**“sending ... the account identifier to
the mobile device”**

(Claims 8 & 25)

No evidence in Fiske of sending the account identifier to the mobile device

Petition (Grounds 3/4)

8. Claim 8

a. [8-PRE]

See § [1.A].

b. [8-A]

See § [1.B]-[1.C].

c. [8-B]

See § [1.F]-[1.G].

Pet. 78

- No discussion of any account identifier.
- Only information allegedly received by user device is ICC Session Key, which is NOT an account identifier.
- No assertion that claim 8 would have been obvious.

Petition (1.B)

f. [1.B]

As explained in [1.A-3], Fiske discloses or renders obvious this element, where data associated with the account includes the single- use payment keys such as the ICC Session Key. Ex[1012], 12:45-52, 12:50-57, 13:17-24, 13:20-31, 13:63-67.

Pet. 69

Petition (1.C)

g. [1.C]

As explained in [1.A-3] and [1.B], Fiske discloses that the user device receives from remote servers a first set of data associated with the account, such as one or more single-use payment keys, specifically, an ICC Session Key, which are associated with an account at the issuing bank. Ex[1012], 12:45-52, 12:50-57, 13:17-24. Fiske discloses that the user device can communicate with the issuing bank via a communications interface, which can be wireless. Ex[1012], 11:49-50, 11:53-57, 13:59-67, 17:52-61.

Pet. 70

POR 51-53

No evidence in Fiske of sending the account identifier to the mobile device (Claim 8)

Petitioner's Reply

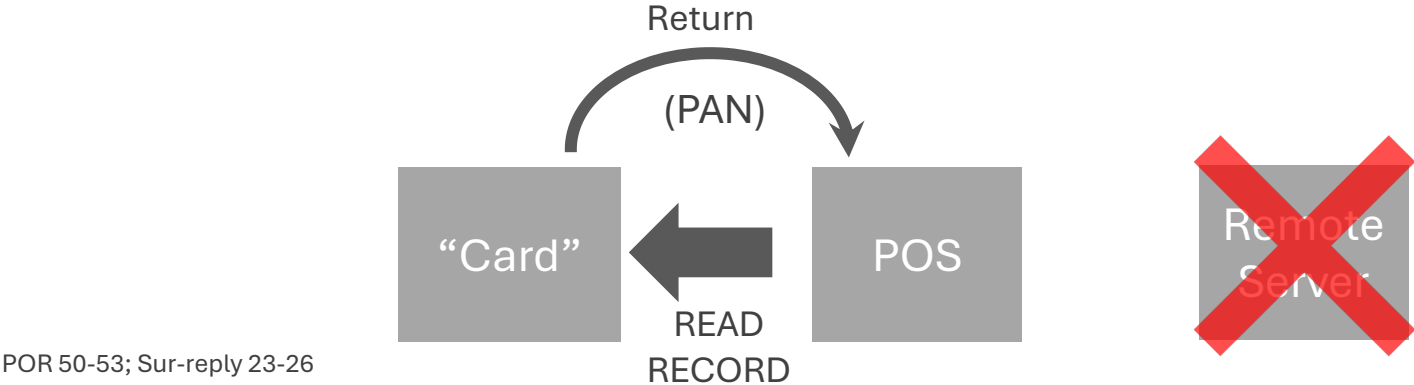
PO's argument that Fiske does not disclose sending the account identifier to the mobile device is without merit. The Petition expressly notes that Fiske (like Collinge in Ground 1), involves receiving “digital credential data” required for authorization including the “primary account number (PAN)” from the remote server. Pet., 66-67. Moreover, the Petition explains how this PAN would be included with the cryptogram by the card when requesting payment authorization. See Pet., 50, 72-73; Ex[1012] at 11:34-44 (discussing provisioning the user device with data sufficient to make a purchase); 3:44-46 (discussing PAN sent to terminal from the mobile application); 4:49-41 (discussing the mobile application sending the account number to the terminal during a transaction).

Reply 23

Petition

65. Also, as explained in Grounds 1-2, the application on the “Card” will return “digital credential data” required for authorization of transaction. Ex[1001], 7:3-7. Fiske's mobile application is interrogable by an electronic reader, such as the POS terminal, over a first communications channel (e.g., NFC) for digital credential data. See Ex[1012], 2:18-26, 11:38-40, 11:45-48, 12:9-24. Fiske describes the POS terminal issuing a “READ RECORD” command to the payment device to “read all of the transaction related data parameters” from the device, including the primary account number (PAN). Ex[1012], 3:26-46, 2:63-67, 5:28-30.

Pet. 66-67



POR 50-53; Sur-reply 23-26

No evidence in Fiske of sending the account identifier to the mobile device (Claim 8)

Petitioner's Reply

PO's argument that Fiske does not disclose sending the account identifier to the mobile device is without merit. The Petition expressly notes that Fiske (like Collinge in Ground 1), involves receiving "'digital credential data' required for authorization" including the "primary account number (PAN)" from the remote server. Pet., 66-67. Moreover, the Petition explains how this PAN would be included with the cryptogram by the card when requesting payment authorization. See Pet., 50, 72-73; Ex[1012] at 11:34-44 (discussing provisioning the user device with data sufficient to make a purchase); 3:44-46 (discussing PAN sent to terminal from the mobile application); 4:49-41 (discussing the mobile application sending the account number to the terminal during a transaction).

Reply 23

POR 50-53; Sur-reply 23-26

Petition at 50

infrastructure. Ex[1006] ¶ 109. Under Construction 1, as explained above, a Mastercard transaction would satisfy this element. Further, in an EMV mode contactless Visa transaction, the POS Kernel issues a GPO command, and the "Card" may return a cryptogram as well as Track 2 Equivalent Data, which contains, among other things, a PAN (Application PAN). Ex[1027] § 2.4.1, Table E-6. The "Card" may return an ARQC Application Cryptogram in the *same message* in response to the GPO command. Ex[1027] §§ 2.4.1, 5.2.2.3, 5.4.3.2. Therefore, either a

Pet. 50

Petition at 72-73

Cryptogram. Ex[1012], 9:49-51; 15:67-16:10. Fiske also describes the POS terminal issuing a "READ RECORD" command to the payment device to "read all of the transaction related data parameters" from the device, including the primary account number (PAN), and that the mobile device would return an Application Cryptogram in response to a "GENERATE AC" command. Ex[1012], 3:26-46, 2:63-67; 5:28-30, 7:30-41. As explained in [1.E] and [1.E-1], responses from the

Pet. 72-73

Petitioner's Reply adds an improper new theory of obviousness for Claim 8

Petitioner's Reply

Like Collinge, the non-permanent cryptographic key in Fiske (ICC Session Key) is specific to an account and only usable for that account. Pet. 59-70; *see also* Ex[1012], 12:45-52, 12:50-57, 13:17-24. Therefore, a POSITA would find it obvious to send an account identifier to the mobile device along with the key, so that the mobile device knows which account's key it is receiving. Ex[1050] ¶60; *see supra* §IV.A.3.a.

- Improper new theory of obviousness.
- Petition did not present any obviousness theory for claim 8 in Grounds 3 & 4. (See Pet. 78.)
- Reply does not cite to any part of the Petition.

Sur-reply 23-26

Reply 23



“The declaration raises a new obviousness argument for this limitation that could have been made in the petition. The Board correctly noted this argument was not made in the petition, which proposed that Shoubridge rendered obvious a number of other claim limitations. Blizzard, as petitioner, had an opportunity to present this argument in its petition, but chose not to.” *Acceleration Bay, LLC v. Activision Blizzard Inc.*, 908 F.3d 765, 775 (Fed. Cir. 2018)



“A reply may only respond to arguments raised in the corresponding opposition or patent owner response Once the Board identifies new issues presented for the first time in reply, neither this court nor the Board must parse the reply brief to determine which, if any, parts of that brief are responsive and which are improper.” *Intelligent Bio-Systems, Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369 (Fed. Cir. 2016) (internal quotations removed).

No evidence in Fiske of sending *the account identifier* to the mobile device (Claim 8)

Petitioner's Reply

Like Collinge, the non-permanent cryptographic key in Fiske (ICC Session Key) is specific to an account and only usable for that account. Pet. 59-70; *see also* Ex[1012], 12:45-52, 12:50-57, 13:17-24. Therefore, a POSITA would find it obvious to send an account identifier to the mobile device along with the key, so that the mobile device knows which account's key it is receiving. Ex[1050] ¶60; *see supra* §IV.A.3.a.

Reply 23

- Fiske makes no reference to multiple accounts.
- Payment application in Fiske is specific to an issuing bank.
- Even if an account identifier were sent, there is no basis for choosing the PAN instead of other account identifiers.

Sur-reply 26

Fiske (EX1012)

According to embodiments of the invention, the payment keys, which are necessary for the use of the payment application, are provided subsequently to the installation of the payment application, under the control of the issuing bank. Equipping the user device with the payment keys in this manner has the effect of activating the payment application, thereby associating it with an account at the issuing bank, and enabling it to conduct EMV payment transactions.

EX1012 at 12:45-52

User device 502 is provisioned with a payment application associated with issuing bank 500. The user of device 502 can interact with a terminal 504 at a PoS via user device 502 in order to make a purchase from a merchant. The PoS terminal 504 can communicate with the acquiring bank 506, and the transaction is later settled between the issuing bank 500 and the acquiring bank 506, once the proper transfer of funds has been arranged.

EX1012 at 11:37-44

Grounds 3 & 4 – Fiske

**“at the remote computer system ...
receiving ... from the POS terminal ...
the account identifier”**

(Claims 10 & 27)

Petitioner ignores the recited account identifier in the receiving step

[10.A] [at the remote computer system]... **receiving** an authorization request to authorize the transaction from the POS terminal, the authorization request comprising authorization data, wherein the authorization data comprises the **response cryptogram and the account identifier**;

Petition (Entirety of [10.A] section in Grounds 3 & 4)

b. [10.A]/[27.A]

Fiske discloses that “[i]n response to receiving the Application Cryptogram, the terminal identifies the type of Application Cryptogram sent by the user device ... and forwards the ARQC [Authorization Request Cryptogram] to the issuer ... for authorization of the transaction.” Ex[1012], 16:6-10; *see also id.* at 7:30-60, Fig. 7.

- Not the **account identifier**
- No obviousness argument

POR 53-55

Pet. 78-79

Petitioner's Reply points to data received by the device, not the remote computer system

[10.A] [at the remote computer system]... **receiving** an authorization request to authorize the transaction from the POS terminal, the authorization request comprising authorization data, wherein the authorization data comprises the **response cryptogram and the account identifier**;

Petitioner's Reply

PO ignores the analysis of this element incorporated the analysis of claim 1. The Petition explains that the device receives all data necessary to perform a transaction, including the PAN (needed by the issuer to associate the transaction with an account for financial tracking) and the cryptogram/MAC (needed by the issuer to verify the request's authenticity). *See supra* §IV.B.1; Ex[1037] 57; Ex[1050] ¶¶61-62.

- Claim 10 recites receiving the account identifier **at the remote computer system**, which is different from what the “device receives”
- Petitioner's claim 10 analysis did not incorporate the analysis of claim 1

POR 53-55; Sur-reply 26-27

Reply 24

Grounds 3 & 4 – Fiske

**“determining a ... key ... using the
account identifier”**

(Claims 10 & 27)

Petitioner ignores the recited account identifier in determining an NPCK

[10.B] [at the remote computer system]... determining a current non-permanent cryptographic key associated with the account **using the account identifier**;

Petition (entirety of [10.B] section)

c. [10.B]/[27.B]

Fiske discloses that “[t]he issuer may identify which Session Key was used to generate the ARQC” Ex[1012], 17:13-14, Fig. 7.

Pet. 79

- No mention of the **account identifier**
- No obviousness argument as to limitations 10.a or 10.b

POR 55-57; Sur-reply 27-28

Reply

b. “determining a...key associated with the account”

The Petition noted that Fiske discloses that the issuer identifies “which Session Key was used” when determining whether to authorize the transaction. Pet., 79 (citing Ex[1012], 16¹⁶:13-14; Fig. 7). Figure 7, in turn, shows the issuer examining the received ARQC, an Application Cryptogram for authorization. This claim element requires nothing more. Ex[1050] ¶63.

Reply 24

- Petitioner ignores “using the account identifier”
- Petitioner cannot incorporate by reference arguments that do not appear in the Reply

Sur-reply 27-28

Grounds 3 & 4 – Fiske

**“the calculated cryptogram is
calculated using the unpredictable
data”**

(Claims 11, 12, 28, and 29)

Petitioner improperly relies on EMV Specifications for *unpredictable data*

[11] The method of claim 10, wherein: the set of inputs comprises unpredictable data; the authorization data comprises the unpredictable data; and the calculated cryptogram is calculated using the unpredictable data.

Petition (Claim 11 – Fiske)

The set of inputs, authorization data, and calculated cryptogram would comprise unpredictable data, because Fiske explicitly incorporates by reference EMV Specifications, which explicitly require that input data for generation of the response cryptogram include an “Unpredictable Number,” which is supplied by “[POS]Terminal.” Ex[1020] § 8.1.1.

...

To the extent these claim elements are not disclosed in Fiske, because Fiske explicitly refers to the invention as “for authorizing an EMV transaction,” a POSA would have deemed it obvious to implement Fiske in a manner compliant with the EMV Specification, as explained above. Ex[1006] ¶ 212.

Institution Decision

Ex. 1012 1:58–64. The mere identification of the acronym “EMV” in Fiske for purposes of more easily referring later in Fiske to “examples” of publicly available transaction protocols is not an “incorporation by reference” of those protocols because it does not clearly identify any publication that is explicitly “incorporated” by “reference.” To the extent Petitioner relies on

Institution Decision at 29; POR 59

Petitioner’s Expert

Q: So is it accurate, then, to say that a card could be compliant and compatible with the EMV specifications without adopting the methods that are provided in Section 8 as to the generation of the application cryptogram?

A: Correct. That’s what “not mandatory” means.

Pet. 80

EX2035 at 61:21-62:1; POR 59

Petitioner's Reply presents a new theory that also improperly relies on EMV Specifications for *unpredictable data*

Reply (Claim 11 – Fiske)

Also, regardless of whether the portions of the EMV specification are mandatory or merely suggested, they teach this claim element: listing “Unpredictable Number” among input data from the terminal used to generate the cryptogram (Ex[1020] §8.1.1), which is repeated by the issuer when verifying the cryptogram. Ex[1037] 57-58. Ex[1050] ¶66. A POSITA understands that the

Reply 25



“The Board has recognized that non-prior art evidence of what was known cannot be applied, independently, as teachings separately combinable with other prior art, but can be relied on for their proper supporting roles, e.g., indicating the level of ordinary skill in the art, what certain terms would mean to one with ordinary skill in the art, and how one with ordinary skill in the art would have under-stood a prior art disclosure.” *Yeda Rsch. v. Mylan Pharms. Inc.*, 906 F.3d 1031, 1041 (Fed. Cir. 2018) (emphasis added) (internal quotations omitted).

Sur-reply 29

Additional Slides

Provisional patent application disclosures must also be found in published application

We declined to institute trial because Lo I is neither a patent nor an application for patent published under 35 U.S.C. § 122(b), and, therefore, is not one of the two types of documents that may be relied upon under 35 U.S.C. § 102(e) to show that claims are unpatentable. Dec. 3. We also explained that we

...

In its Request for Rehearing, Petitioner contends that our statement of the holding in *Yamaguchi* overlooks language in that decision stating that a provisional application constitutes prior art under § 102(e) “for all that it teaches.” Req. Reh’g 6 (citing *Yamaguchi*, 88 USPQ2d at 1612). Petitioner, thus, argues that our Decision overlooked the full breadth of the holding in *Yamaguchi*. *Id.* at 7–8.

...

Thus, rather than analyzing the provisional application in isolation, the *Yamaguchi* decision ensured that the patent-defeating disclosures were present in both the patent which formed the basis of unpatentability under § 102(e), as well as the corresponding provisional application. The decision in *Yamaguchi* recognized, therefore, that in a ground of unpatentability under § 102(e), the patent-defeating disclosures in a provisional application must also be found in a document applicable as prior art under § 102(e), that is, either a patent or application for patent published under § 122(b). Accordingly, we are not persuaded that *Yamaguchi* held that a ground of unpatentability under § 102(e) may be predicated on a provisional application, without reference to a corresponding patent or application for patent published under § 122(b).

“Application for patent published under §122(b)” (U.S. Patent Pub. No. 2009/0029377)

DIAGNOSING FETAL CHROMOSOMAL ANEUPLOIDY USING MASSIVELY PARALLEL GENOMIC SEQUENCING

CLAIM OF PRIORITY

[0001] The present application claims priority from and is a non-provisional application of U.S. Provisional Application No. 60/951,438, entitled “DETERMINING A NUCLEIC ACID SEQUENCE IMBALANCE” filed Jul. 23, 2007 (Attorney Docket No. 016285-005200US), the entire contents of which are herein incorporated by reference for all purposes.

- Provisional application (“Lo I”) is incorporated by reference in its entirety



“It is undisputed that the provisional applications are not themselves prior art under § 102(e)(1) because they are not applications published under § 122(b).” *Amgen Inc. v. Sanofi, Aventisub LLC*, 872 F.3d 1367, 1380 n.5 (Fed. Cir. 2017)

Sequenom, Inc. v. Bd. of Trustees of Leland Stanford Junior

Univ., No. IPR2014-00337, Paper 14 at 3-4 (P.T.A.B. Sep. 23, 2014); Sur-reply 2.

Exhibits 1058 and 1059

Exhibit 1058 (“PayPass-Magstripe”)

The information contained in this document is proprietary and confidential to MasterCard International Incorporated, one or more of its affiliated entities (collectively “MasterCard”) or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of MasterCard.

EX1058 at 2

Proprietary and Confidential

EX1058 at 2

Exhibit 1059 (“PayPass-M/Chip”)

The information contained in this document is proprietary and confidential to MasterCard International Incorporated, one or more of its affiliated entities (collectively "MasterCard"), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of MasterCard.

EX1059 at 2