(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 August 2008 (07.08.2008)

PCT

(10) International Publication Number
WO 2008/094328 A3

(51) International Patent Classification:
*H04K 1/00* (2006.01)

(21) International Application Number:
PCT/US2007/082903

(22) International Filing Date: 29 October 2007 (29.10.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

| | | |
|---|---|---|
| 60/887,307 | 30 January 2007 (30.01.2007) | US |
| 11/713,307 | 1 March 2007 (01.03.2007) | US |


(71) Applicant *(for all designated States except US)*: **VISA U.S.A. INC.** [US/US]; P.O. Box 8999, San Francisco, CA 94128-8999 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **DIXON, Phil** [US/US]; 7389 Juncus Ct., San Diego, CA 92129 (US). **HAMMAD, Ayman, A.** [US/US]; 6981 Corte Mercado, Pleasanton, CA 94566 (US). **THAW, William, Alexander** [CA/US]; 352 Avalon Drive, South San Francisco, CA 94080 (US). **AABYE, Christian** [DK/US]; 515 Trinidad Lane, Foster City, CA 94404 (US).

(74) Agent: **DESANDRO, Bradley, K.**; Quarles & Brady LLP, One Renaissance Square, Two North Central Ave, Phoenix, AZ 85004-2391 (US).


(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).


*[Continued on next page]*

(54) Title: SIGNATURE BASED NEGATIVE LIST FOR OFF LINE PAYMENT DEVICE VALIDATION

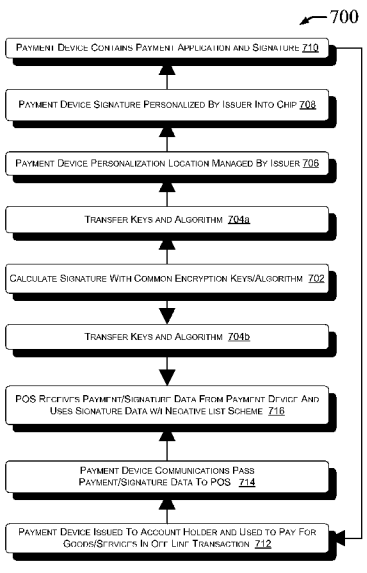


Figure 7

(57) Abstract: At each of a plurality of transit readers of a transit system, for each of a plurality of riders, where each rider seeks to conduct an access transaction with the transit system for access into the transit facility by using a payment device issued by an issuer in a payment system, data is read from the payment device. The data includes an encryption code that uniquely corresponds to the payment device and was created by the issuer using one or more encryption keys and a predetermined algorithm. A check will be performed, remotely and/or locally, of one or more lists of other encryption codes to determine if the encryption code is on the list. On the basis of whether the encryption code is on the list, the rider is permitted access to the facility of the transit system. The payment device need not be changed for the rider's fare. Decryption of the encryption code read from the payment device is not required to complete the access transaction.

WO 2008/094328 A3

**Published:**
— *with international search report*
— *with amended claims*

**(88) Date of publication of the international search report:**
6 November 2008

**Date of publication of the amended claims:** 24 December 2008

AMENDED CLAIMS
Received by the International Bureau
on 18 October 2008 (18.10.08)

1. A method comprising:

reading data at a point of service (POS) terminal at a merchant, wherein:

a payment device is presented to the POS terminal by a consumer seeking to conduct a transaction for a good or service from the merchant;

the payment device includes a Primary Account Number (PAN) issued by an issuer; and

the data read from the payment device includes a non-PAN signature that corresponds to the PAN;

checking a list of non-PAN signatures maintained by the POS terminal to determine if the non-PAN signature read from the data on the payment device is on the list; and

permitting, on the basis if whether the non-PAN signature is on the list, the consumer to complete the transaction with the merchant;

wherein the non-PAN signature is created by the issuer using one or more encryption keys and a predetermined algorithm.

2. (canceled)

3. The method as defined in Claim 1, wherein at least one said encryption key is a type selected from the group consisting of a symmetric type and an asymmetric type.

4. The method as defined in Claim 3, wherein the asymmetric type is a public key infrastructure.

5. The method as defined in Claim 1, wherein the predetermined algorithm produces a result selected from the group consisting of a hash, a certificate, a signature utilizing data stored on the payment device that is unique to that payment device.

6. The method as defined in Claim 1, wherein the predetermined algorithm includes one or more variables each of which is selected from the group consisting of the name of an account holder corresponding to the payment device, a partial PAN, expiry data of the payment device, and a service code of the payment processing system that corresponds to the PAN of the payment device.

7. The method as defined in Claim 6, wherein the one or more variables are stored in the payment device in Track 1 and/or Track 2 data fields in accordance with a magnetic stripe data (MSD) configuration.

8. The method as defined in Claim 1, wherein the non-PAN signature is static on the payment device.

9. The method as defined in Claim 1, wherein the reading data further comprises storing information for each said transaction.

10. The method as defined in Claim 9, wherein the information stored for each said transaction comprises the date and time thereof, an identification of the POS terminal of the merchant, and at least some of the data read from a data storage region of the payment device.

11. The method as defined in Claim 10, wherein the data read from the data storage region of the payment device is stored in a format selected from the group consisting of:

either Track 1 or Track 2 data fields of the payment device in accordance with a magnetic stripe data (MSD) configuration; and

a data track that is compatible with the payment processing system that processes data in accordance with a magnetic stripe data (MSD) configuration.

12. The method as defined in Claim 10, wherein the data read from the data storage region of the payment device is read contactlessly.

13. The method as defined in Claim 1, wherein the payment device is selected from the group consisting of a credit card, a debit card, a stored value card, a contactless payment device, and combinations thereof

14. The method as defined in Claim 1, wherein the payment device is within a mobile device selected from the group consisting of a personal digital assistant, a wireless telephone, and an expert system including a substrate having embedded therein a contactless element including a chip capable of use as a transaction payment mechanism for each said access transaction.

15. The method as defined in Claim 1, wherein the reading, the checking, and the permitting are all performed within a time period not exceeding one (1) second.

16. A computer readable medium comprising instructions which, when executed by a computer, performs the method of Claim 1.

17. A method comprising:

reading data at a transit system reader in a transit system, wherein:

a payment device is presented to the transit system reader by a rider seeking to conduct an access transaction for access to a facility of the transit system; and

the payment device includes a Primary Account Number (PAN) issued by an issuer in a payment processing system; and

the data read from the payment device includes encryption code;

and

without decrypting the encryption code:

checking, at the transit system reader, a list of other said encryption codes to determine if the encryption code is on the list; and

permitting, on the basis if whether the encryption code is on the list, the rider access to the facility of the transit system;

wherein the encryption code that uniquely corresponds to the payment device is created by the issuer using one or more encryption keys and a predetermined algorithm.

18. (canceled)

19. The method as defined in Claim 17, wherein at least one said encryption key is a type selected from the group consisting of a symmetric type and an asymmetric type.

20. The method as defined in Claim 19, wherein the asymmetric type is a public key infrastructure.

21. The method as defined in Claim 17, wherein the predetermined algorithm produces a result selected from the group consisting of a hash, a certificate, a signature utilizing data stored on the payment device that is unique to that payment device.

22. The method as defined in Claim 17, wherein the predetermined algorithm includes one or more variables each of which is selected from the group consisting of the name of a cardholder corresponding to the payment device, a partial PAN, expiry data of the payment device, and a service code of the payment device.

23. The method as defined in Claim 22, wherein the one or more variables are stored in the payment device in Track 1 and/or Track 2 data fields of the payment device in accordance with a magnetic stripe data (MSD) configuration.

24. The method as defined in Claim 17, wherein the encryption code read from the payment device is static on the payment device.

25. The method as defined in Claim 17, wherein the reading data further comprises storing information for each said access transaction.

26. The method as defined in Claim 25, wherein the information stored for each said access transaction comprises the date and time thereof, an identification of the POS terminal in the transit system, and at least some of the data read from a data storage region of the payment device.

27. The method as defined in Claim 17, wherein the data read from the payment device is stored in a format selected from the group consisting of:

either Track 1 or Track 2 data fields of the payment device in accordance with a magnetic stripe data (MSD) configuration; and

a data track that is compatible with the payment processing system that processes data in accordance with a magnetic stripe data (MSD) configuration.

28. The method as defined in Claim 17, wherein the data is contactlessly read from a data storage region of the payment device.

29. The method as defined in Claim 17, wherein the payment device is selected from the group consisting of a credit card, a debit card, a stored value card, a contactless payment device, and combinations thereof

30. The method as defined in Claim 17, wherein the payment device is within a mobile device selected from the group consisting of a personal digital assistant, a wireless telephone, and an expert system including a substrate having embedded therein a contactless element including a chip capable of use as a transaction payment mechanism for each said access transaction.

31. The method as defined in Claim 17, wherein the reading, the checking, and the permitting are all performed within a time period not exceeding one (1) second.

32. A computer readable medium comprising instructions which, when executed by a computer, performs the method of Claim 17.

33. A method comprising:

reading data at a transit reader in a transit system, wherein:

a payment device is presented to the transit system reader by a rider seeking to conduct an access transaction for access to a facility of the transit system;

the data is in the Track 1 and/or Track 2 data fields in accordance with an Magnetic Stripe Data (MSD) configuration;

the payment device includes a Primary Account Number (PAN) issued by an issuer in a payment processing system; and

the data read from the payment device includes encryption code that:

uniquely corresponds to the payment device;

is created by the issuer using at least one of:

one or more encryption keys; and

a predetermined algorithm;

checking, at the transit system reader, a list of other said encryption codes to determine if the encryption code is on the list; and

permitting, without decrypting the encryption code, the rider access to the facility of the transit system on the basis if whether the encryption code is on the list.

34. The method as defined in Claim 33, wherein at least one said encryption key is a type selected from the group consisting of a symmetric type and an asymmetric type.

35. The method as defined in Claim 34, wherein the asymmetric type is a public key infrastructure.

36. The method as defined in Claim 33, wherein the predetermined algorithm produces a result selected from the group consisting of a hash, a certificate, a signature utilizing data stored on the payment device that is unique to that payment device.

37. The method as defined in Claim 33, wherein the predetermined algorithm includes one or more variables each of which is selected from the group consisting of the name of a cardholder corresponding to the payment device, a partial PAN, expiry data of the payment device, and a service code of the payment device.

38. The method as defined in Claim 33, wherein the reading data further comprises storing information for each said access transaction.

39. The method as defined in Claim 38, wherein the information stored for each said access transaction comprises the date and time thereof, an identification of the POS terminal in the transit system, and at least some of the data read from a data storage region of the payment device.

40. The method as defined in Claim 33, wherein the data is contactlessly read from a data storage region of the payment device.

41. The method as defined in Claim 33, wherein the payment device is selected from the group consisting of a credit card, a debit card, a stored value card, a contactless payment device, and combinations thereof

42. The method as defined in Claim 33, wherein the payment device is within a mobile device selected from the group consisting of a personal digital assistant, a wireless telephone, and an expert system including a substrate having embedded therein a contactless element including a chip capable of use as a transaction payment mechanism for each said access transaction.

43. The method as defined in Claim 33, wherein the reading, the checking, and the permitting are all performed within a time period not exceeding one (1) second.

44. A computer readable medium comprising instructions which, when executed by a computer, performs the method of Claim 33.