(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) CH 698 351 B1

(51) Int. Cl.: G06Q 20/08 (2012.01)
G06Q 20/40 (2012.01)

Erfindungspatent für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) PATENTSCHRIFT

(21) Anmeldenummer: 00771/09

(22) Anmeldedatum: 16.11.2007

(43) Anmeldung veröffentlicht: 29.05.2009

(30) Priorität: 16.11.2006 ZA 2006/09533

(24) Patent erteilt: 15.06.2015

(45) Patentschrift veröffentlicht: 15.06.2015

(73) Inhaber:
NET1 UEPS TECHNOLOGIES INC, 4TH Floor, President's Place, Cnr Jan Smuts and Bolton Road, Rosebank
2196 Johannesburg (ZA)

(72) Erfinder:
Serge Christian Pierre Belamant, 2196 Sandton (ZA)

(74) Vertreter:
Vossius & Partner, Nadelberg 3
4051 Basel (CH)

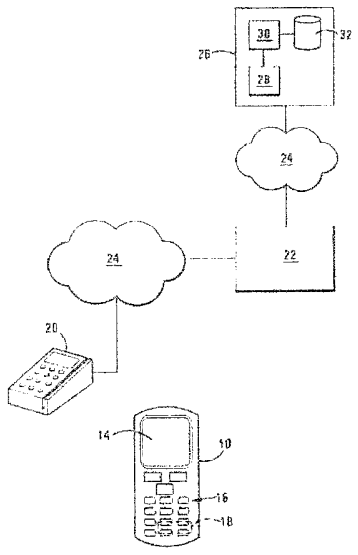
(86) Internationale Anmeldung:
PCT/IB 2007/054678

(87) Internationale Veröffentlichung:
WO 2008/059465

(54) Gesicherte finanzielle Transaktion.

(57) Die Erfindung betrifft einen Finanztransaktionsnummerngenerator (10) mit einer elektrischen Bearbeitungseinrichtung, welche ein Eingabegerät (16), eine Speichereinheit (18) und ein Display (14) enthält.

Der Generator (10) speichert eine Kontonummer eines Bezahlers und simuliert eine einmalige Transaktionsnummer mit einer darin enthaltenen simulierbaren primären Kontonummer einer Kredit- oder Debitkarte, aus welcher die Kontonummer des Bezahlers extrahierbar ist. Die einmalige Transaktionsnummer wird auf dem Display (14) angezeigt. Die Transaktionsnummer wird in ein POS-Gerät (20) eingegeben, von diesem geprüft und an die empfangende Bank des Händlers (22) über ein Netzwerk (24) übertragen. Die empfangende Bank (22) schickt diese Nummer an die ausgebende Bank (26), welche sie überprüft. Falls das Prüfergebnis positiv ausfällt, wird der in der Nummer verschlüsselte Betrag dem Konto des Bezahlers belastet und einem Konto des Händlers gutgeschrieben.



Beschreibung

[0001] Diese Erfindung bezieht sich auf elektronische finanzielle Transaktionen. Sie bezieht sich insbesondere auf einen Finanztransaktionsnummerngenerator.

[0002] Dieser ist im Allgemeinen so ausgestaltet, dass er eine primäre Kontonummer (pimary account number = PAN) eines normalen Kredit- oder Debitkontos bei einer Bank oder einem Finanzinstitut bildet oder simuliert, welche die richtige Kontonummer in verschlüsselter Form enthält. Die simulierte PAN kann auch einen Betrag enthalten, der von dem Konto abgezogen werden soll. Demgemäss wird eine Kontonummer zusammen mit einem Betrag verschlüsselt und in eine Ziffernfolge eingesetzt, die als eine gültige PAN erscheint. Damit wird die Kontonummer und der Transaktionsbetrag in die simulierte PAN eingebettet. Die simulierte PAN kann dann durch die bestehende Infrastruktur für Finanztransaktionen behandelt werden, wobei die ausstellende Bank weiss, dass dies keine PAN ist und die entsprechenden Ziffern entschlüsselt werden müssen, damit man die eingebettete Kontonummer und den eingebetteten Betrag sehen kann. In einer Anwendung generiert ein Bezahler (Transaktor), der eine Finanztransaktion vornehmen möchte, eine simulierte PAN und gibt sie einem Lieferanten von Waren oder Dienstleistungen, von welchem er diese Waren oder Dienstleistungen beziehen möchte. Der Lieferant gibt die simulierte PAN und den Transaktionsbetrag auf konventionelle Weise ein. Diese Daten werden dann einer empfangenden Bank übermittelt, welche diese zwecks Überprüfung an die ausstellende Bank weiterreicht. Die ausstellende Bank extrahiert dann die eingebettete Kontonummer und den eingebetteten Betrag, überprüft, ob der eingebettete Betrag und der angegebene Betrag gleich sind (und macht gleichzeitig die normalen, konventionellen Überprüfungen) und, wenn diese übereinstimmen, autorisiert die Transaktion.

[0003] Fachleute in diesem Gebiet werden anerkennen, dass in den meisten Fällen der Bezahler ein Verfalldatum und einen Kartenprüfwert (card verification value = CVV) angeben muss. Eine oder auch beide davon können ebenfalls simuliert und zum Verschlüsseln von Informationen eingesetzt werden. Weiterhin ist sich der Fachmann bewusst, dass eine «Bank Identification Number» (BIN) im ersten Teil einer PAN untergebracht ist, und das ändert sich auch nicht bei der simulierten PAN.

[0004] Es wird deshalb anerkannt werden, dass diese Erfindung die Sicherheit bei Transaktionen insbesondere über das Internet oder per Telefon verbessert.

[0005] Der Aspekt dieser Erfindung ist also ein Finanztransaktionsnummerngenerator zur Erstellung einer einmaligen Transaktionsnummer, wobei die Transaktionsnummer die primäre Kontonummer einer gewöhnlichen Kredit- oder Debitkarte simuliert und darin eine Kontonummer eines Bezahlers enthält.

[0006] Der Generator kann in die Transaktionsnummer auch einen Transaktionsbetrag einbauen.

[0007] Eine simulierte PAN kann erstellt werden, die eine Kontonummer und darin eingebettet zusammen, möglicherweise, einen Transaktionsbetrag enthält.

[0008] Dies umfasst ein Ausstellen einer solchen simulierten PAN an den Lieferanten für Waren oder Dienstleistungen und ein Erhalten einer solchen simulierten PAN durch einen Lieferanten von Waren oder Dienstleistungen.

[0009] Die simulierte PAN kann in einer Form erstellt werden, dass sie von Menschen erkannt werden kann. Um mit der bestehenden Finanzstruktur weiterarbeiten zu können, kann sie deshalb insbesondere aus einer Folge von numerischen Ziffern bestehen. Fachleute werden verstehen, dass eine solche Folge aus 16 bis 23 Ziffern bestehen kann.

[0010] Fachleute werden weiterhin anerkennen, dass die ersten 6 Ziffern der simulierten PAN die BIN angeben, die, wie bereits oben erwähnt, es möglich macht, dass die Transaktion an das korrekte Finanzinstitut weitergeleitet wird und es dem ausstellenden Finanzinstitut möglich macht, zu erkennen, dass sie eine simulierte PAN erhalten hat, die die eingebettete Transaktionsnummer und den Transaktionsbetrag enthält. Fachleute werden ähnlich auch anerkennen, dass die letzte Ziffer der simulierten PAN eine Prüfziffer sein kann.

[0011] Der PAN-Generator kann eine einmalige Sequenz von Ziffern erstellen, die die verschlüsselten Informationen enthält, wobei jedes Mal eine neue Sequenz bereitgestellt wird. Der Generator kann deshalb einen entsprechenden Verschlüsselungs-Algorithmus benützen, um jedes Mal eine einmalige verschlüsselte Sequenz zu liefern.

[0012] Wie bereits oben erwähnt, kann die verschlüsselte Sequenz auch einen Transaktionsbetrag enthalten.

[0013] Ausserdem kann, wie bereits erwähnt, der CVV und/oder das Verfalldatum simuliert und in die verschlüsselte Information eingebaut werden.

[0014] Der Generator kann eine elektronische Geldbörse enthalten, welche mit dem Transaktionsbetrag bei der Erstellung der simulierten PAN belastet wird.

[0015] Die simulierte PAN kann ebenfalls eingebettet eine Angabe über die Identität des beabsichtigten Zahlungsempfängers in verschlüsselter Form enthalten. Der Generator kann einen Benutzer so auffordern, den Namen oder die Kontonummer des beabsichtigten Zahlungsempfängers einzugeben, die dann auch in der simulierten PAN eingebettet und verschlüsselt werden.

[0016] Falls die simulierte PAN für die Benutzung durch einen Mittelsmann vorgesehen ist, kann sie in einer verschlüsselten Zwischenform erstellt werden, als eine alphanumerische Sequenz, die ein einmaliges Passwort für das Entschlüsseln

benötigt, und die eine benutzbare simulierte PAN liefert. Diese Zwischenform wird dann dem Mittelsmann auf einem Weg geliefert und das Passwort auf einem anderen Weg. Der Generator kann dann eine Einrichtung aufweisen, entweder die simulierte PAN oder die Zwischenform zusammen mit einem Passwort zur einmaligen Benutzung zu erstellen. Ausserdem kann der Generator eine Einrichtung aufweisen, um die Zwischenform mit seinem Passwort anzunehmen, die alphanumerische Sequenz zu entschlüsseln und eine benutzbare simulierte PAN zu liefern.

[0017] Weiterhin kann in der simulierten PAN ein zugelassenes Transaktionsmedium spezifiziert sein. Wenn die simulierte PAN nur ein POS-Gerät, eine ATM, eine telefonische Transaktion oder eine Internet-Transaktion oder auch alles erlauben soll, dann kann dies ebenfalls in die simulierte PAN eingebettet werden.

[0018] Der Generator beinhaltet ein elektronisches Bearbeitungsgerät, eine Speichereinheit, ein Eingabegerät zur Eingabe eines Antrags auf eine simulierte PAN und den Transaktionsbetrag sowie ein Display zur Anzeige der simulierten PAN. Es wird anerkannt werden, dass die relevante Kontonummer und der Verschlüsselungs-Algorithmus in der Speichereinheit gespeichert werden. Der Generator kann ein mobiles Gerät sein, insbesondere ein Mobiltelefon, in welchem Fall die Speichereinheit eine «subscriber identification module (SIM)» sein kann. Es wird anerkannt werden, dass, falls ein Benutzer eine Angabe zu dem Zahlungsempfänger einbauen möchte und/oder eine Zwischenform in einer alphanumerischen Sequenz mit dem entsprechenden Passwort benötigt, und/oder ein spezielles Transaktions-Medium angeben möchte, dies mit dem Eingabegerät und dem Display, welches entsprechende Aufforderungen und/oder Menüs anzeigt, gemacht werden kann.

[0019] Dementsprechend kann ein Speichermodul wie eine SIM-Karte vorgesehen sein, auf welcher eine geeignete BIN gespeichert ist, eine Kontonummer, ein Verschlüsselungs-Algorithmus zur Verschlüsselung der Kontonummer und eines zu übergebenden Transaktionsbetrages, woraus eine simulierte PAN erstellt wird, welche die BIN enthält, sowie eine verschlüsselte Sequenz von Ziffern, in welchen die Kontonummer und der Transaktionsbetrag eingebettet sind.

[0020] Es kann auch ein Carrier vorgesehen sein, der den Generator mit dem Vorschlüsselungs-Algorithmus versieht, welcher den Verschlüsselungs-Algorithmus, vorzugsweise zusammen mit der Kontonummer, darin oder darauf enthält.

[0021] Es kann eine Finanzinstitut-Bearbeitungseinrichtung zum Bearbeiten einer finanziellen Transaktionsnummer geben, welche die primäre Kontonummer einer konventionellen Kredit- oder Debitkarte simuliert und welche eine Kontonummer eines Bezahlers darin beinhaltet, die einen Extraktor zum Extrahieren der Kontonummer aus der simulierten primären Kontonummer einschliesst.

[0022] Es kann auch eine Vorrichtung für die Bearbeitung von finanziellen Transaktionen vorgesehen sein, die eine Finanzinstitut-Bearbeitungseinrichtung wie oben beschrieben einschliesst, zusammen mit einem Finanztransaktionsnummerngenerator wie ebenfalls oben beschrieben.

[0023] Weiterhin kann ein Verfahren zum Bearbeiten finanzieller Transaktionen bereitgestellt sein, das umfasst:
Erhalten einer offensichtlichen finanziellen Transaktionsnummer, welche die primäre Kontonummer einer konventionellen Kredit- oder Debitkarte simuliert und worin die Kontonummer eines Ausstellers aufgeführt ist, zusammen mit einem Antrag, die Zahlung zu autorisieren; und
Entnehmen der Kontonummer aus der primären Kontonummer.

[0024] Die simulierte PAN kann über ein konventionelles Finanzkommunikations-Netzwerk empfangen worden sein.

[0025] Wie bereits oben gezeigt, hat die PAN eine BIN eingearbeitet und die verbleibenden Zahlen der simulierten PAN sind verschlüsselt. Die Vorrichtung kann also Trennmittel aufweisen, um die verschlüsselten Zahlen von der BIN zu trennen. Wurde der Transaktionsbetrag ausserdem auch verschlüsselt, wird bei der Entschlüsselung auch der Transaktionsbetrag entschlüsselt.

[0026] Wenn, wie bereits oben besprochen, der CVV und/oder das Verfalldatum ebenfalls simuliert wurden und verschlüsselte Informationen enthalten, werden diese auch entschlüsselt.

[0027] Hat die simulierte PAN einen Transaktionsbetrag darin eingebettet, dann wird der eingebettete Betrag entschlüsselt und mittels Vergleichsmitteln mit dem Handelsbetrag verglichen, der auf die übliche Weise geliefert wurde. Falls sie unterschiedlich sind, wird die Transaktion verweigert.

[0028] Enthält die simulierte PAN eine Angabe über den beabsichtigten Zahlungsempfänger, dann wird das ebenfalls extrahiert und kann dann mit den Daten über den Empfänger verglichen werden, die zusammen mit der PAN auf konventionelle Weise geliefert werden; und sollte die simulierte PAN auch noch ein spezielles Transaktions-Medium enthalten, so wird auch dieses extrahiert und es wird geprüft, ob das benutzte Transaktions-Medium richtig war.

[0029] Die Vorrichtung kann einen Speicher zum Speichern der empfangenen, simulierten PANs enthalten, oder zumindest der verschlüsselte Teile davon, und Vergleichsmittel zum Vergleichen einer erhaltenen simulierten PAN (oder dem verschlüsselten Teil davon) mit gespeicherten PANs (oder den gespeicherten und verschlüsselten Teilen davon), um sicherzugehen, dass eine simulierte PAN nur einmal benutzt werden kann.

[0030] Wird eine Transaktion autorisiert, wird der anfragenden Bank oder dem Lieferanten von Waren oder Dienstleistungen eine Autorisation übermittelt und das entsprechende Konto des Bezahlers wird mit dem Transaktionsbetrag belastet.

[0031] Die Erfindung wird nunmehr anhand von nichteinschränkenden Beispielen beschrieben, die sich auf die beiliegenden Zeichnungen beziehen:

Abb. 1 zeigt eine erste Ausführung der Erfindung;

Abb. 2 zeigt eine zweite Ausführung der Erfindung; und

Abb. 3 zeigt eine dritte Ausführung der Erfindung.

[0032] In Abb. 1 wird eine erste Implementierung der Erfindung gezeigt. Ein Bezahler, der von einem Händler Waren kaufen möchte, hat einen Generator in der Form eines mobilen Telefons 10. Das Telefon 10 hat ein Display 14, eine Tastatur 16 und eine SIM-Karte 18. Die SIM-Karte 18 enthält ein Programm, das, wie oben besprochen, eine simulierte PAN liefern soll. Die SIM-Karte 18 hat also die Kontonummer des Bezahlers gespeichert, eine BIN, einen Verschlüsselungs-Algorithmus und eine PIN. Der Bezahler gibt mit der Tastatur 16 einen Antrag ein, das Programm zu aktivieren, zusammen mit seiner PIN, und gibt dann unter Benutzung der Tastatur 16 den Transaktionsbetrag ein, wenn er dazu auf dem Display aufgefordert wird. Das Programm generiert sodann die simulierte PAN, eine CVV und ein Verfalldatum, die auf dem Display 14 angezeigt werden. Es wird anerkannt werden, dass das Telefon 10 und die SIM-Karte 18 damit eine virtuelle Kredit- oder Debitkarte bereitstellen.

[0033] Der Bezahler liest einem Kassierer die PAN, den CVV und das Verfalldatum aus, der die relevanten Ziffern manuell in ein «Point of Sale»(POS)-Gerät 20 zusammen mit dem Handelsbetrag eingibt. Die simulierte PAN wird von dem POS-Gerät 20 geprüft, um sicherzugehen, dass die Prüfziffer korrekt ist. Die PAN, der CVV, das Verfalldatum und der Handelsbetrag werden auf konventionelle Weise an die empfangende Bank des Händlers 22 über ein konventionelles Finanznetzwerk 24 übersendet.

[0034] Die empfangende Bank 22 identifiziert die entsprechende ausgebende Bank 26 aus der BIN und schickt die simulierte PAN, den CVV, das Verfalldatum und den Handelsbetrag an die ausgebende Bank 26. Die ausgebende Bank 26 hat ein Kommunikations-Interface 28, einen Computer 30 und eine Speichereinheit 32. Die simulierte PAN, der CVV und das Verfalldatum sowie der Transaktionsbetrag werden dem Computer 30 zugeführt, der die verschlüsselten Teile von der simulierten PAN, dem CVV und dem Verfalldatum trennt. Dies wird dann mit einer Liste aller vorher erhaltenen numerischen Folgen, die in der Speichereinheit 32 gespeichert sind, verglichen. Ist die Folge einmalig und wurde sie vorher nicht benutzt, wird sie der gespeicherten Liste zugefügt. Ist sie vorher schon benutzt worden und wurde auf der Liste gespeichert, dann wird die Transaktion verweigert und eine entsprechende Nachricht wird an die empfangende Bank 22 und an den Lieferanten gesandt. Wenn die Serie vorher noch nicht benutzt worden ist, dann wird sie von dem Computer 30 mit einem entsprechenden Entschlüsselung-Algorithmus entschlüsselt, um die Kontonummer des Bezahlers und den eingebetteten Transaktionsbetrag zu extrahieren. Eine PIN oder eine andere Identifikation wird von der ausgebenden Bank nicht verlangt. Der eingebettete Transaktionsbetrag wird mit dem separat gelieferten Handelsbetrag verglichen und, wenn sich diese unterscheiden, so wird die Transaktion verweigert. Der Computer 30 prüft, ob das Guthaben des Bezahlers ausreicht, und wenn das so ist, wird das Konto des Bezahlers belastet und eine konventionelle Autorisation wird der empfangenden Bank 22 zugesandt, die den Betrag dem Konto des Händlers gutschreibt und den Händler informiert, dass die Transaktion vorgenommen worden ist.

[0035] Die SIM-Karte 18 kann auch wie eine elektronische Geldbörse funktionieren, in welchem Fall die Börse mit dem Transaktionsbetrag belastet wird, nachdem die simulierte PAN, der CVV und das Verfalldatum angegeben worden sind.

[0036] In Abb. 2 wird eine zweite Implementierung der Erfindung gezeigt, bei der eine finanzielle Transaktion über das Internet 40 vorgenommen wird. In dieser Anwendung ist der Generator 42 ein Laptop Computer, auf dem das Programm installiert wurde, damit eine simulierte PAN, wie oben besprochen, erstellt werden kann. Der Computer 42 hat ausserdem die Kontonummer des Bezahlers, die BIN, den Verschlüsselungs-Algorithmus und die PIN gespeichert.

[0037] Wenn der Käufer Waren oder Dienstleistungen kaufen möchte oder eine vorherige Genehmigung von einem Lieferanten über das Internet haben möchte, generiert er eine simulierte PAN, ein CVV und ein Verfalldatum, die dem Lieferanten über das Internet 40 an einen Server 44 des Lieferanten geliefert werden. Das wird dann an die empfangende Bank 22 des Lieferanten übertragen, die die Daten an die ausstellende Bank 26 weitergibt. Der Vorgang wird dann, wie bereits oben mit Bezug auf Abb. 1 besprochen, abgewickelt.

[0038] Auf ähnliche Weise kann eine gesicherte Transaktion telefonisch gemacht werden, wie in Abb. 3 gezeigt wird. Bei dieser Implementierung ist der Generator wieder ein Mobiltelefon 10, so wie in Abb. 1. Der Käufer liefert also die simulierte PAN, den CVV und ein Verfalldatum wie vom Telefon 10 abgelesen über ein Telefon-Netzwerk 50 an einen Angestellten in einem Callcenter 52. Von da wird es auf konventionelle Weise zusammen mit dem Transaktionsbetrag an die empfangende Bank 22 und die ausgebende Bank 26 weitergeleitet. Die ausgebende Bank bearbeitet die Transaktion, wie oben unter Abb. 1 gezeigt.

[0039] Ein Beispiel, wie die simulierte PAN generiert und bearbeitet wird, wird nun gezeigt:

BIN	PAN	CD	CVV	EXP DATE
6	9	1	3	4
XXXXXX	.....	X	(...)	MM/YY

1. Kunde USN = 3 Bytes

[0040] 1. Byte = FI, kann von der BIN bestimmt werden
USN = 9876 5432 (max. 8 Stellen)

2. Generieren eines Verfalldatums

[0041] – Benutze 5 Jahre als Verfalldatum der Karte – das sind 60 Monate
minus 12 Monate (zählt für das laufend Jahr –1)
– Es verbleiben 48 Monate
EXPDATE = TRXTYPE [2 BITS].AID[4 bits]
WHERE
AID[2 bits] = 00, 01, 10, 11
TRX TYPE[4 bits] = 0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011
MONAT = TRX TYPE + 1 (+1, so dass wir nicht mit einem Monat = 0 enden)
MM = Binary_To_ASCII(MONTH)
YEAR = (current year + 1) + AID (CCYY)
YY = Binary_To_ASCII(die letzten 2 Stellen des JAHRES)

[0042] HINWEIS:
– MM und YY sind (ASCII)-Zeichen, die angezeigt werden können. Diese 4 Zahlen werden als das gewünschte Verfalldatum am Terminal eingetippt
– MONAT [1] = binary gleichwertig mit MM (Ergebnis ist immer 1 Byte)
– YEAR[2] = binary vergleichbar mit YEAR einschl. Jahrhundert (Ergebnis sind immer 2 Bytes)
– AID ist das/die Konto/Börse, die belastet oder der etwas gutgeschrieben wird

3. Generieren des Verfalldatums Mapping Values (Expiry Date Mapping Values (EDMV)) (Hier haben wir Platz für mehr)

[0043] – Dies hier bringt etwas mehr Zufall in den generierten Monat und das Jahr und eine Prüfungsmethode, dass es am Terminal richtig eingegeben wurde.
EDMV = 1 DES((YEAR[2] + 00.MONTH[1])[2]). YEAR[2].MONTH[1].(YEAR[2] – 00.MONTH[1])[2].FF)

[0044] HINWEIS:
– Es wird ein statischer Schlüssel benutzt, um den verschlüsselten Block (EDMV-Taste) zu generieren
– (YEAR[2] + 00.MONTH[1]), das Ergebnis ist immer ein 2-Bytes-Wert
– (YEAR[2] – 00.MONTH[1]), das Ergebnis ist immer ein 2-Bytes-Wert
– EDMV1[2] = die letzten beiden Bytes des EDMV-Ergebnisses
– EDMV2[2] = die zweiten 2 Bytes des EDMV-Ergebnisses
– Wurde MM/YY am Terminal falsch eingegeben, dann fällt EDMV anders aus und deshalb wird der Verschlüsselungsblock nicht richtig eingerichtet und der CVV-Abgleich schlägt fehl.

4. Generieren einer CheckSum für die USN – (diversifizierter Schlüssel)

[0045] CVV = 3DES(USN[3].ULSN[2].ULP[1].EDMV1[2])

[0046] HINWEIS:
– Benutzen Sie dreifache DES, dreifacher Schlüssel, unter USN diversifiziert
– Diversifizierte Schlüssel (USN-basiert) werden benutzt, um den Verschlüsselungsblock zu generieren (Host-Schlüssel)
– Man verwandelt CVV zu darstellbaren (ASCII)-Zahlen
– CVV_1 = die letzten 3 Stellen des darstellbaren (ASCII)-Ergebnisses.
Dieser 3-stellige Wert wird als der erwünschte CVV in den Terminal eingegeben (endgültiger CVV)
– CVV_2 = binary gleichwertig mit CVV_1 (immer 2 Bytes)

5. Generieren einer PIN verschlüsselte CheckSum für USN

[0047] – Wenn der Benutzer eine PIN eingibt, wird sie Teil des Verschlüsselungs-Schlüssels.
– Wenn der Benutzer keine PIN eingibt, wird ein Voreinstellungs-PIN-Schlüssel benutzt.
CVV_PIN = 1DES(CVV[8])

[0048] HINWEIS:
– Wenn keine PIN benötigt wird, dann wird ein statischer (PIN-Schlüssel) benutzt, um den Verschlüsselungsblock zu generieren.
– Wenn eine PIN benötigt wird, dann kann der Benutzer eine generieren, die aus 4–8 Stellen (einschliesslich) bestehen kann.
Jede Stelle repräsentiert einen hex-ähnlichen Nibble, der den PIN-Schlüssel von dem unbedeutendsten Nibble bis hin zum bedeutendsten ersetzt.
– Verwandlung einer CVV_PIN zu darstellbaren (ASCII)-Zahlen
– CVV_PIN1 = die letzten 3 Stellen des darstellbaren (ASCII)-Ergebnisses. Dieser 3-stellige Wert wird als der gewünschte CVV in das Terminal eingetippt.
– Der CVV wird auf aufgrund der PIN verändert und deshalb generiert der HOST einen falschen CVV und der CVV-Vergleich fällt durch.

6. Generieren einer Unload Signature

[0049] AMT[2] = letzte 2 Bytes des 4-Byte-Betrages
CVV_PIN2[2] = binares Äquivalent von CVV_PIN1 (Ergebnis sind immer 2 Bytes)
CVV_TEMP = (AMT[2] XOR CVV_PIN2[2])
ZEICHEN = 3DES(AMT[4].CVV_TEMP[2].EDMV2[2])
ZEICHEN = 9999 9999 99

[0050] HINWEIS:
– Zum Generieren einer Unload Signature werden statische Schlüssel benutzt
– Die Unload Signature enthält normalerweise ein Unload LSN, in der CVV+TEMP ist das jedoch bereits enthalten.

7. SIGN = Erste 8 Stellen

[0051] PAN = USN + SIGN (Ergebnis sind maximal 9 Ziffern). Wahlweise – [(USN*YY +YY*MM) + SIGN]
PAN = 9876 5432 (USN) + 9999 9999 (SIGN)
PAN = 1987 6534 1

[0052] Kalkulation der Checksumme für PAN
– Bringe PAN in den PAN-Buffer
– An dieser Stelle wird der vollständige PAN, das Verfalldatum und der CVV generiert.

8. ON HOST:

[0053] 1. Wiederherstellung des Verfalldatum-Mapping-Wertes (EDMV1 und EDMV2)
(Schritt 3)
TRXTYPE und AID können vom MM und YY bestimmt werden
TRXTYPE[2 bits].AID[3 bits] = ((YY – (current year + 1))* 12) + MM
2. Wiederherstellung der Unload Signatare (SIGN), unter Benutzung des CVV, der am Terminal eingegeben wurde (Schritt 4, 5)
3. USN = PAN-SIGN
4. Jetzt kann der Host den HOST_SCHLÜSSEL, ULSN und ULP erhalten
5. Wiederherstellung von CVV unter Benutzung der kalkulierten USN
6. Vergleich des wiederhergestellten CVV (Schritt 4) mit dem CVV, der im Terminal eingegeben wurde.

[0054] Verifikationen
1. 3-stellige CVV passen
2. CVV wird nicht generiert, wenn SIGN falsch ist.
3. CVV wird nicht wiederhergestellt, wenn USN falsch ist.
4. CVV passt nicht richtig, wenn die EDMV falsch ist.

[0055] Zusammenfassung auf der Karte
1. Benutze die USN, ULSN, ULP, um CVV zu generieren.
2. Benutze die CVV, um das SIGN zu generieren.
3. Jetzt ist PAN = USN + SIGN

[0056] Zusammenfassung auf dem Host
1. Benutze die erhaltene CVV, um das SIGN zu generieren.
2. Benutze das SIGN, um das USN zu erhalten durch Benutzung von PAN (USN=PAN-SIGN)
3. Benutze USN, um den HOST SCHLÜSSEL, ULSN, ULP für das Generieren von CVV zu erhalten.
4. Vergleiche den generierten CVV mit dem CVV des Terminals.

[0057] Fachleute auf diesem Gebiet werden bestätigen, dass es ausserordentlich schwer, wenn nicht sogar unmöglich sein dürfte, eine betrügerische Transaktion durchzuführen, wenn die Transaktion gemäss dieser Erfindung durchgeführt wird.

Patentansprüche

1. Finanztransaktionsnummerngenerator zum Generieren einer einmaligen Transaktionsnummer, der eine elektronische Bearbeitungseinrichtung beinhaltet, wobei ein Eingabegerät, das zur Eingabe eines Antrags auf eine einmalige Transaktionsnummer und eines Transaktionsbetrags von einem Bezahler, der ein Konto mit einer Kontonummer besitzt, bedienbar ist, eine Speichereinheit, die zum Speichern der Kontonummer des Bezahlers ausgebildet ist, sowie ein Display zur Anzeige der einmaligen Transaktionsnummer beinhaltet sind, wobei
der Finanztransaktionsnummerngenerator mit der Speichereinheit, die zum Speichern der Kontonummer des Bezahlers ausgebildet ist, dazu ausgestaltet ist, dass als generierte einmalige Transaktionsnummer eine Zahl, mit der eine primäre Kontonummer einer Kredit- oder Debitkarte simulierbar und aus welcher die Kontonummer des Bezahlers von einer ausgewählten Finanzinstitut-Bearbeitungseinrichtung extrahierbar ist, generierbar und auf dem Display anzeigbar ist.
2. Finanztransaktionsnummerngenerator nach Anspruch 1, der dazu ausgestaltet ist, dass als generierte einmalige Transaktionsnummer eine den Transaktionsbetrag enthaltende Transaktionsnummer generierbar ist.
3. Finanztransaktionsnummerngenerator nach Anspruch 1 oder 2, der dazu ausgestaltet ist, dass als generierte einmalige Transaktionsnummer eine Ziffernfolge generierbar ist, die mit einem konventionellen Protokoll derart übereinstimmt, dass eine festgelegte Nummer davon die Bank-Identifikationsnummer jener bestimmten Finanz-Institution ist, von welcher die Transaktion zu genehmigen und der Transaktionsbetrag zu zahlen ist.
4. Finanztransaktionsnummerngenerator nach Anspruch 1, der dazu ausgestaltet ist, dass eine Ziffernfolge in Übereinstimmung mit einem konventionellen Protokoll als generierte einmalige Transaktionsnummer so generierbar ist, dass deren letzte Ziffer eine Prüfziffer ist.
5. Finanztransaktionsnummerngenerator nach Anspruch 1 oder 2, der dazu ausgestaltet ist, dass eine Ziffernfolge in Übereinstimmung mit einem konventionellen Protokoll als generierte einmalige Transaktionsnummer so generierbar ist, dass sie ein simuliertes Verfalldatum umfasst.
6. Finanztransaktionsnummerngenerator nach Anspruch 1 oder 2, der dazu ausgestaltet ist, dass eine Ziffernfolge in Übereinstimmung mit einem konventionellen Protokoll als generierte einmalige Transaktionsnummer so generierbar ist, dass sie eine simulierte Kartenverifikations-Wertnummer umfasst.
7. Finanztransaktionsnummerngenerator nach Anspruch 1 oder 2, der dazu ausgestaltet ist, dass die simulierte primäre Kontonummer verschlüsselbar ist und welcher einen Verschlüsselungsmechanismus enthält, mittels welchem eine verschlüsselte primäre Kontonummer gemäss einem vorher festgelegten Verschlüsselungs-Algorithmus erstellbar ist.
8. Finanztransaktionsnummerngenerator nach Anspruch 1, der dazu ausgestaltet ist, dass in die simulierte primäre Kontonummer ebenfalls eine Identifikation eines vereinbarten Zahlungsempfängers aufnehmbar ist.
9. Finanztransaktionsnummerngenerator nach Anspruch 1, der dazu ausgestaltet ist, dass in die simulierte primäre Kontonummer ebenfalls eine Identifikation eines bestimmten Transaktions-Mediums aufnehmbar ist.
10. Finanztransaktionsnummerngenerator nach Anspruch 2, dessen Speichereinheit als eine elektronische Geldbörse ausgestaltet ist, in welcher ein Kreditbetrag enthalten ist, wobei der Finanztransaktionsnummerngenerator so ausgestaltet ist, dass der in der Speichereinheit enthaltene Kreditbetrag um den Transaktionsbetrag auf das Simulieren der primären Kontonummer hin reduzierbar ist.
11. Finanztransaktionsnummerngenerator nach Anspruch 7, der dazu ausgestaltet ist, dass er ein Speichermodul enthält, in welchem neben der Kontonummer des Bezahlers auch der Verschlüsselungs-Algorithmus gespeichert ist.
12. Finanztransaktionsnummerngenerator nach Ansprach 2, der dazu ausgestaltet ist, dass eine Zwischennummer und ein Passwort generierbar sind, die die primäre Kontonummer liefern, wenn ein vorher festgelegter Entschlüsselungs-Algorithmus benutzt wird.
13. Finanztransaktionsnummerngenerator nach Anspruch 12, der einen Speicher mit dem vorher festgelegten Entschlüsselungs-Algorithmus enthält.

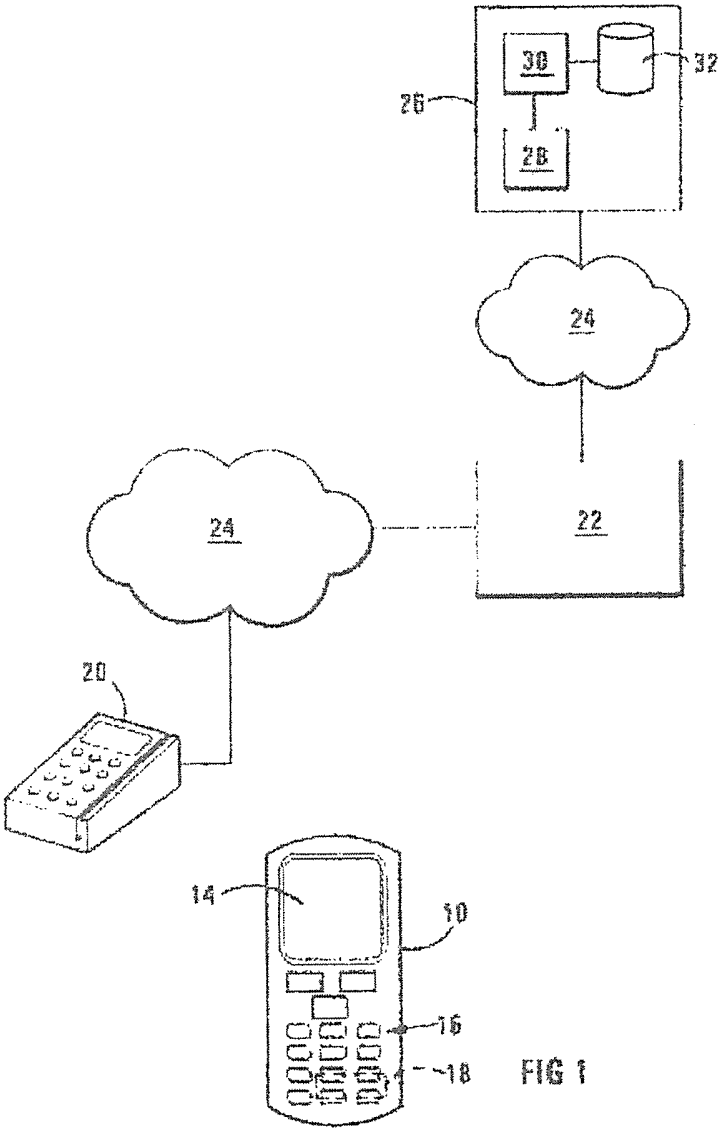


FIG 1

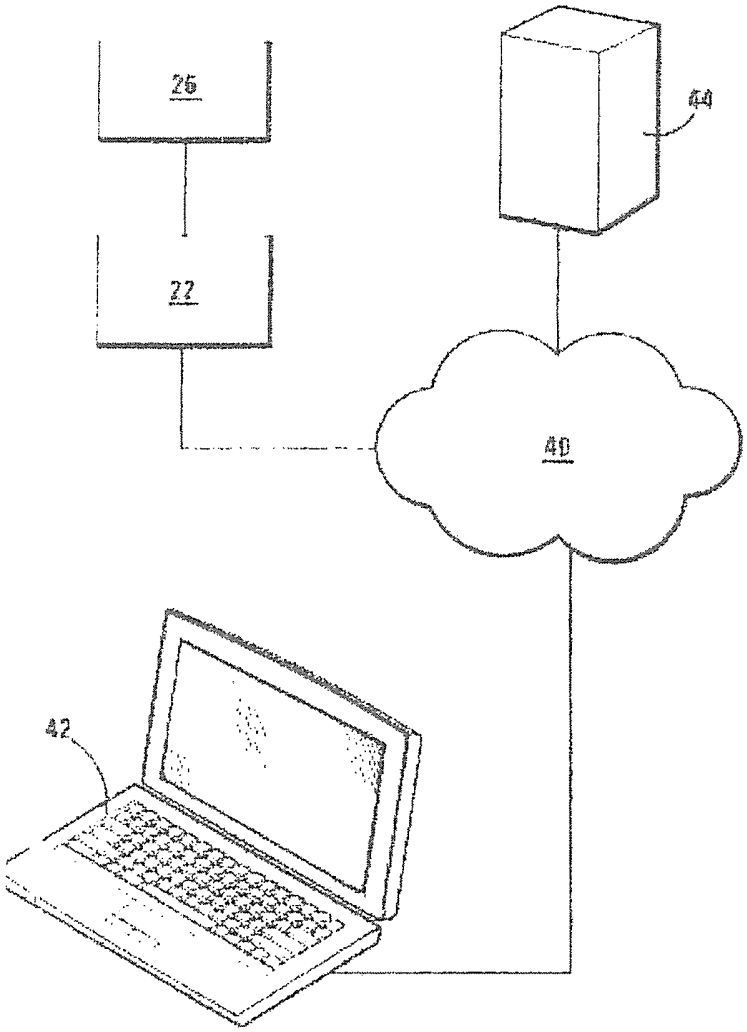


Abb. 2

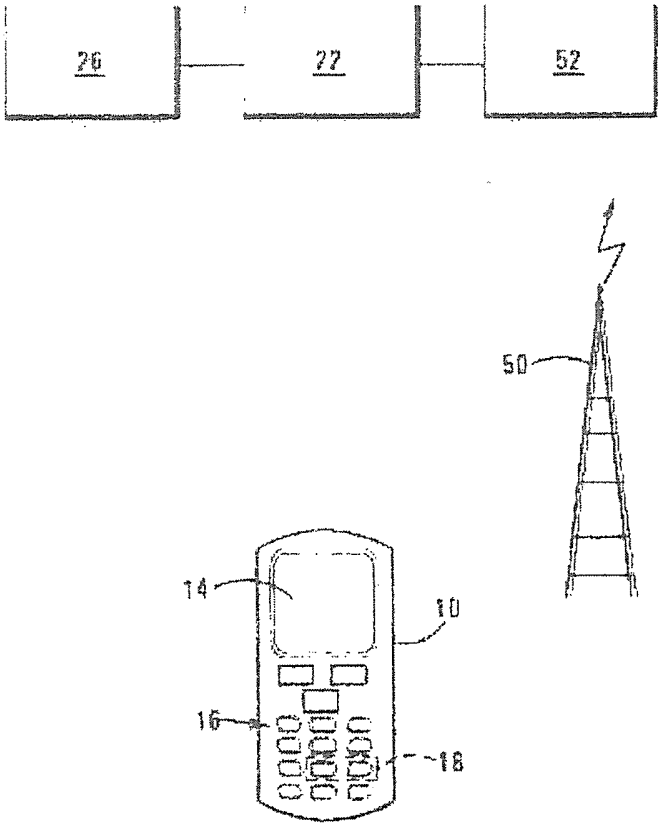


Abb. 3