(19) Bureau voor de Industriële Eigendom Nederland

(11) **1001863**

(12) C **OCTROOI**[20]

(21) Aanvrage om octrooi: **1001863**

(22) Ingediend: **08.12.95**

(51) Int.Cl.[6]
G07F7/02, G07F7/08, G07F19/00

(41) Ingeschreven:
10.06.97

(47) Dagtekening:
10.06.97

(45) Uitgegeven:
01.08.97 I.E. 97/08

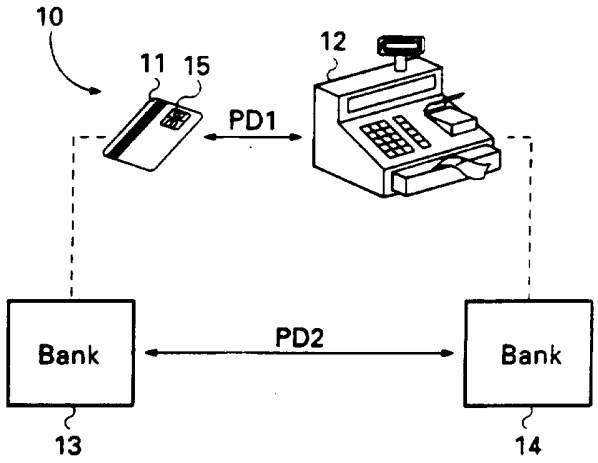
(73) Octrooihouder(s):
Koninklijke PTT Nederland N.V. te Den Haag.

(72) Uitvinder(s):
Jelle Wissenburgh te Den Haag
Frank Muller te Delft
Martin Klaas de Lange te Voorburg
Albertus Feiken te Amstelveen
Johannes Brehler te Leidschendam
Hendricus Johannes Wilhemes Maria van de Pavert te Veenendaal

(74) Gemachtigde:
Ir. G.R. Beltsma te 2509 CH Den Haag.

(54) **Werkwijze voor het beveiligd afwaarderen van een elektronisch betaalmiddel, alsmede betaalmiddel voor het ten uitvoer leggen van de werkwijze.**

(57) De uitvinding een werkwijze voor het beveiligd afwaarden van een elektronisch betaalmiddel, zoals een zogenaamde "smart card" of "chip card", tijdens een transactie met een betaalstation, zoals een kassa. Teneinde te voorkomen dat het betaalmiddel tegelijkertijd transacties met meerdere betaalstations uitvoert, wordt volgens de uitvinding in de gegevens, die tussen betaalmiddel en betaalstation worden uitgewisseld, een authenticatiewaarde gebruikt die voor de betreffende transactie uniek is.



NL C 1001863

KONINKLIJKE PTT NEDERLAND N.V.
GRONINGEN

Werkwijze voor het beveiligd afwaarderen van een elektronisch betaalmiddel, alsmede betaalmiddel voor het ten uitvoer leggen van de werkwijze.

A. ACHTERGROND VAN DE UITVINDING

De uitvinding heeft betrekking op een werkwijze voor het afwaarderen van een elektronisch betaalmiddel, zoals een elektronische betaalkaart voorzien van een geïntegreerde schakeling ("chip card"). In het bijzonder, maar niet uitsluitend, heeft de uitvinding betrekking op een werkwijze voor het beveiligd afwaarderen van vooruitbetaalde elektronische betaalkaarten ("pre-paid cards"), zoals deze bijvoorbeeld voor telefooncellen worden toegepast. In deze tekst zal het woord betaalmiddel worden gebruikt, onafhankelijk van de vorm of de soort van het specifieke betaalmiddel. Een betaalmiddel kan derhalve bijvoorbeeld door een oplaadbare betaalkaart of een niet-kaartvormig elektronisch betaalmiddel worden gevormd.

Elektronische betaalmiddelen worden de laatste jaren steeds vaker toegepast, niet alleen voor het betalen voor het gebruik van openbare telefoontoestellen, maar ook voor vele andere betalingsdoeleinden. Aangezien een dergelijk betaalmiddel in het algemeen een (batig) saldo omvat dat een geldwaarde vertegenwoordigt, is het noodzakelijk om de uitwisseling van gegevens tussen een dergelijk betaalmiddel en een betaalstation (zoals een voor elektronisch betalen ingericht telefoontoestel of een elektronische kassa) volgens een beveiligde werkwijze (betalingsprotocol) te laten verlopen. Daarbij dient bijvoorbeeld te worden verzekerd dat een van het betaalmiddel afgewaardeerde hoeveelheid (geldwaarde of aantal rekeneenheden) overeenkomt met een elders opgewaardeerde hoeveelheid (geldwaarde of rekeneenheden): het door een klant betaalde bedrag dient te corresponderen met het door een leverancier te ontvangen bedrag. De opgewaardeerde hoeveelheid kan bijvoorbeeld worden opgeslagen in een, in het betaalstation aanwezige, beveiligde module.

Bekende betalingswerkwijzen omvatten een eerste stap, waarin het saldo van het betaalmiddel door het betaalstation wordt opgevraagd,

een tweede stap, waarin het saldo van het betaalmiddel wordt verlaagd (afwaarderen van het betaalmiddel) en een derde stap, waarin opnieuw het saldo van het betaalmiddel wordt opgevraagd. Uit het verschil tussen het saldo van de eerste en derde stap kan de afgewaardeerde hoeveelheid en daarmee de in het betaalstation op te waarderen hoeveelheid worden bepaald. De tweede stap kan een aantal malen worden herhaald, eventueel in combinatie met de derde stap.

Ter voorkoming van fraude wordt bij een dergelijke werkwijze in de eerste stap gebruik gemaakt van een toevalsgetal ("random number"), dat door het betaalstation wordt gegenereerd en naar het betaalmiddel wordt overgedragen, bijvoorbeeld als deel van een code waarmee het saldo wordt opgevraagd. Aan de hand van dit toevalsgetal genereert het betaalmiddel als eerste respons een authenticatiecode, die een (bijvoorbeeld cryptografische) bewerking van onder meer het toevalsgetal en het saldo kan omvatten. Door voor elke transactie een ander toevalsgetal te gebruiken wordt voorkomen dat door naspelen ("replay") een transactie kan worden nagebootst. Tevens wordt in de derde stap gebruik gemaakt van een tweede toevalsgetal ("random number"), dat eveneens door het betaalstation wordt gegenereerd en naar het betaalmiddel wordt overgedragen. Aan de hand van het tweede toevalsgetal genereert het betaalmiddel als tweede respons een tweede, nieuwe authenticatiecode, die een bewerking van onder meer het tweede toevalsgetal en het nieuwe saldo kan omvatten. Op basis van het verschil van de twee overgedragen saldo's kan het betaalstation (dan wel een beveiligde module van het betaalstation) bepalen met welke hoeveelheid het saldo van het betaalstation dient te worden opgewaardeerd.

Deze bekende werkwijze is in principe zeer fraudebestendig zolang een betaalmiddel met één betaalstation (resp. beveiligde module) communiceert. Het nadeel van de bekende werkwijze is echter gelegen in het feit dat de eerste en tweede authenticatiecodes onafhankelijk zijn. Indien een tweede of derde betaalstation (resp. beveiligde module) met het betaalmiddel communiceert, is het door deze onafhankelijkheid mogelijk de eerste stap van de tweede en derde stap te scheiden. Hierdoor kan een ogenschijnlijk complete transactie worden bereikt zonder dat het betreffende betaalmiddel met hetzelfde bedrag wordt afgewaardeerd als de betaalstations (resp. beveiligde modules) in totaal worden opgewaardeerd. Het zal duidelijk zijn dat

dit ongewenst is.

B. SAMENVATTING VAN DE UITVINDING

De uitvinding beoogt bovengenoemde en andere nadelen van de stand van de techniek op te heffen en een werkwijze te verschaffen, die een nog grotere mate van beveiliging van afwaardeertransacties biedt. In het bijzonder beoogt de uitvinding een werkwijze te verschaffen, die verzekert dat tijdens een transactie slechts communicatie tussen het betaalmiddel en één betaalstation respectievelijk beveiligde module plaatsvindt. Meer in het bijzonder beoogt de uitvinding een werkwijze te verschaffen, die verzekert dat het bedrag, waarmee het saldo van een betaalmiddel tijdens een transactie wordt verlaagd, overeenstemt met het bedrag waarmee het saldo van slechts één betaalstation respectievelijk beveiligde module wordt verhoogd.

Een werkwijze voor het met behulp van een betaalstation beveiligd afwaarderen van een elektronisch betaalmiddel, omvattende:

- een eerste stap, waarin:
  - het betaalstation een eerste toevalsgetal naar het betaalmiddel overdraagt,
  - het betaalmiddel, in respons op dit eerste toevalsgetal, een eerste authenticatiecode naar het betaalstation overdraagt, welke eerste authenticatiecode op basis van tenminste het eerste toevalsgetal en een saldo van het betaalmiddel wordt bepaald, en
  - het betaalstation de eerste authenticatiecode controleert;
- een tweede stap, waarin:
  - het betaalstation een afwaardeercommando naar het betaalmiddel overdraagt en het saldo van het betaalmiddel aan de hand van het afwaardeercommando wordt verlaagd; en
- een derde stap, waarin:
  - het betaalmiddel een tweede toevalsgetal naar het betaalmiddel overdraagt,
  - het betaalmiddel, in respons op dit tweede toevalsgetal, een tweede authenticatiecode naar het betaalstation overdraagt, waarbij tweede authenticatiecode op basis van tenminste het tweede toevalsgetal en het actuele saldo van het betaalmiddel wordt bepaald, en
  - het betaalstation de eerste authenticatiecode controleert;

heeft hiertoe volgens de uitvinding het kenmerk, dat de eerste authenticatiecode mede op basis van een eerste authenticatiewaarde en de tweede authenticatiecode mede op basis van een tweede authenticatiewaarde wordt bepaald, waarbij de eerste en tweede authenticatiewaarden gerelateerd zijn, en dat het betaalmiddel in respons op het ontvangen van een toevalsgetal een nieuwe authenticatiewaarde genereert.

Door de authenticatiecodes te vormen op basis van onder meer authenticatiewaarden, die binnen een transactie gerelateerd zijn, wordt een mogelijkheid geboden te controleren of de tweede authenticatiecode (in de derde stap) gerelateerd is aan de eerste authenticatiecode (in de eerste stap). Door nu een nieuwe authenticatiewaarde te genereren, steeds wanneer een authenticatiecode moet worden bepaald, wordt de mogelijkheid geboden opeenvolgende authenticatiecodes, en daarmee opeenvolgende transacties, te onderscheiden. Indien elke keer dat de eerste of derde stap wordt uitgevoerd een (zoveel mogelijk) unieke authenticatiewaarde wordt gegenereerd, kan eenduidig worden vastgesteld welke tweede authenticatiecode met welke eerste gerelateerd is. Daarmee kan ook worden vastgesteld, of binnen een transactie al een tweede authenticatiecode is afgegeven.

De authenticatiewaarden worden in principe autonoom door het betaalmiddel gegenereerd. Bij voorkeur is geen beïnvloeding van buitenaf mogelijk, dit teneinde fraude te vermijden. De authenticatiewaarden kunnen op verschillende wijzen worden gegenereerd, bijvoorbeeld door een toevalsgenerator of door een teller.

De eerste en tweede authenticatiewaarden van een transactie kunnen gerelateerd zijn doordat zij bijvoorbeeld dezelfde waarde hebben, of doordat ze onderling afhankelijke waarden hebben, zoals opeenvolgende waarden van een teller. Ook kan de eerste authenticatiewaarde een toevalsgetal zijn, en kan de tweede authenticatiewaarde uit de eerste worden gevormd door het daarbij optellen van een bepaald getal. In principe dient elk paar authenticatiewaarden zodanig gerelateerd te zijn, dat dit eenduidig controleerbaar is.

De uitvinding beoogt verder een elektronisch betaalmiddel en een betaalstation te verschaffen waarin de werkwijze wordt toegepast.

C. REFERENTIES

[1] EP-A-0.637.004

[2] EP-A-0.223.213

D. UITVOERINGSVOORBEELDEN

De uitvinding zal in het onderstaande aan de hand van de figuren nader worden toegelicht.

Figuur 1 toont schematisch een betaalsysteem waarin de uitvinding kan worden toegepast.

Figuur 2 toont schematisch een werkwijze waarin de uitvinding wordt toegepast.

Figuur 3 toont schematisch de geïntegreerde schakeling van een betaalmiddel waarbij de uitvinding kan worden toegepast.

Het in figuur 1 bij wijze van voorbeeld schematisch weergegeven systeem 10 voor elektronisch betalen omvat een elektronisch betaalmiddel, zoals een zogenaamde "chip card" of "smart card" 11, een betaalstation 12, een eerste betalingsinstelling 13, en een tweede betalingsinstelling 14. Het betaalstation (terminal) 12 is in figuur 1 weergegeven als een kassa, maar kan bijvoorbeeld ook een (openbaar) telefoontoestel omvatten. De betalingsinstellingen 13 en 14, in figuur 1 beide aangeduid als bank, kunnen niet alleen banken maar ook nadere instellingen zijn die beschikken over middelen (computers) voor het verrekenen van betalingen. In de praktijk kunnen de betalingsinstellingen 13 en 14 één betalingsinstelling vormen. Het betaalmiddel 11 omvat in het weergegeven voorbeeld een substraat en een geïntegreerde schakeling met contacten 15, welke schakeling is ingericht voor het afhandelen van (betalings)transacties. Het betaalmiddel kan ook een elektronische beurs ("wallet") omvatten.

Tussen het betaalmiddel 11 en het betaalstation 12 vindt, tijdens een transactie, een uitwisseling van betalingsgegevens PD1 plaats. Het betaalmiddel 11 is geassocieerd met de betalingsinstelling 13, terwijl het betaalstation 12 is geassocieerd met de betalingsinstelling 14. Tussen de betalingsinstellingen 13 en 14 vindt na een transactie een verrekening plaats door het uitwisselen van betalingsgegevens PD2, die van de betalingsgegevens PD1 zijn afgeleid. Tijdens een transactie vindt in principe geen communicatie tussen het betaalstation 12 en de betreffende betalingsinstelling 14 plaats (zogenaamd "off-line" systeem). Derhalve moeten transacties onder

gecontroleerde omstandingheden verlopen om te verzekeren dat geen misbruik van het systeem kan plaatsvinden. Een dergelijk misbruik kan bijvoorbeeld zijn het verhogen van een saldo van het betaalmiddel 11 waar geen saldowijziging van een tegenrekening bij de betalingsinstelling 13 tegenover staat.

Het schema van figuur 2 geeft de uitwisseling van gegevens tussen (de geïntegreerde schakeling van) een betaalmiddel C (11 in figuur 1) en (de beveiligde module van) een betaalstation T (12 in figuur 1) weer, waarbij opeenvolgende gebeurtenissen onder elkaar zijn weergegeven.

In de eerste stap, aangeduid met I, produceert het betaalstation T een eerste toevalsgetal R1 en draagt dit aan het betaalmiddel C over (deelstap Ia). In de praktijk kan het toevalsgetal R1 onderdeel uitmaken van een code voor het opvragen van een authenticatiecode. In respons op het ontvangen van het toevalsgetal R1 (resp. een betreffende code) genereert het betaalmiddel C overeenkomstig de uitvinding een eerste authenticatiewaarde AV1, bijvoorbeeld door een teller te verhogen, een toevalsgenerator te activeren, of beide (deelstap Ib). Aan de hand van het toevalsgetal R1, de eerste authenticatiewaarde AV1 en andere gegevens, waaronder het saldo SC1 van het betaalmiddel, produceert het betaalmiddel C een authenticatiecode AC1 die aan het betaalstation T wordt overgedragen (deelstap Ic): AC1 = F(R1, AV1, SC1, ...), waarbij F een op zich bekende cryptografische functie kan zijn. Het betaalstation T controleert de authenticatiecode aan de hand van onder meer R1 en registreert, bij een positief controleresultaat, het saldo SC1 en de eerste authenticatiewaarde AV1, die in de authenticatiecode AC1 zijn bevat.

In de tweede stap, aangeduid met II, produceert het betaalstation T een afwaardeercommando D, dat de van het betaalmiddel af te waarderen waarde (hoeveelheid) omvat. Het afwaardeercommando D wordt naar het betaalmiddel C overgedragen, waarna het saldo SC1 van het betaalmiddel met de af te waarderen hoeveelheid wordt verlaagd tot SC2. Eventueel kan de tweede stap enkele malen worden herhaald.

In de derde stap, aangeduid met III, produceert het betaalstation T een tweede toevalsgetal R2 en draagt dit aan het betaalmiddel C over (deelstap IIIa). Hierop genereert het betaalmiddel C een tweede authenticatiewaarde AV2 (deelstap IIIb). Aan de hand van het tweede toevalsgetal R2, de tweede authenticatiewaarde AV2 en

andere gegevens, waaronder het nieuwe saldo SC2 van het betaalmiddel, produceert het betaalmiddel C een authenticatiecode AC2 die aan het betaalstation T wordt overgedragen (deelstap IIIc): AC2 = F(R2, SC2, ...), waarbij F een op zich bekende cryptografische functie kan zijn. De derde stap kan dus voor het betaalmiddel C geheel analoog aan de eerste stap verlopen.

Het betaalstation T controleert de ontvangen tweede authenticatiecode AC2, bijvoorbeeld door ontcijferen van de authenticatiecode en vergelijken van het toevalsgetal R2. Ook controleert het betaalstation T of de uit de tweede authenticatiecode AC2 verkregen tweede authenticatiewaarde AV2 op de juiste wijze gerelateerd is aan de in de eerste stap geregistreerde eerste authenticatiewaarde AV1. Indien het paar authenticatiewaarden AV1 en AV2 niet (juist) gerelateerd zijn, wordt de transactie beëindigd en wordt het saldo van het betaalstation T dus niet gewijzigd.

Indien de controle van de authenticatiecode AC2 een positief resultaat heeft, registreert het betaalstation T het saldo SC2 dat in de authenticatiecode AC2 is bevat. Het genoemde ontcijferen kan bijvoorbeeld plaatsvinden door het uitvoeren van de inverse van de functie F.

In een vierde stap, aangeduid met IV, kan in het betaalstation T het verschil van de saldo's SC1 en SC2 worden bepaald en in het betaalstation worden geregisteerd. Daarbij kan dit verschil ofwel afzonderlijk worden opgeslagen, ofwel bij een bestaande waarde (saldo van het betaalstation) worden opgeteld, om later te worden verrekend. Deze vierde stap is evenals mogelijke volgende stappen niet wezenlijk voor de uitvinding. Aan de in figuur 2 weergegeven stappen kan een authenticatie- of verificatiestap voorafgaan; deze is echter eveneens niet wezenlijk voor de onderhavige uitvinding.

In het schema, dat in het bovenstaande is besproken, zijn de toevalsgetallen R1 en R2 verschillend. De toevalsgetallen R1 en R2 kunnen echter identiek zijn (R1 = R2 = R), zodat in stap III tevens gecontroleerd kan worden of in de authenticatiecode AC2 nog steeds van hetzelfde toevalsgetal R (= R1) gebruik wordt gemaakt.

Opgemerkt wordt dat het getal R1, evenals het getal R2, strikt genomen geen toevalsgetal hoeft te zijn: het dient voor de eenduidige identificatie van de authenticatiecode AC1 als antwoord ("response") op R1 ("challenge"). Essentieel is slechts dat R1 voor het

betaalmiddel C niet kenbaar is.

Volgens de stand van de techniek zijn de authenticatiecodes AC1 en AC2 in principe onafhankelijk. Dat wil zeggen, indien de toevalsgetallen R1 en R2 verschillen is er geen direct of indirect verband tussen de codes AC1 en AC2. Door deze onafhankelijkheid is er in principe geen garantie dat de stappen I en III tussen hetzelfde betaalmiddel-betaalstation-paar worden uitgevoerd.

Volgens de uitvinding wordt bij het bepalen van de tweede authenticatiecode echter uitgegaan van een authenticatiewaarde, die gerelateerd is aan de authenticatiewaarde die bij het bepalen van de eerste authenticatiecode werd gebruikt. Hierdoor is er een verband gelegd tussen de twee authenticatiecodes van de betreffende transactie.

Indien bijvoorbeeld het betaalmiddel C van een tweede betaalstation T' een (eerste) toevalsgetal R1' ontvangt, nadat het betaalmiddel C aan een eerste betaalstation T een eerste authenticatiecode AC1 heeft afgegeven, zal het betaalmiddel C een authenticatiecode AC2 afgeven. Indien daarop het eerste betaalstation T, na het afgeven van een afwaardeercommando, opnieuw een authenticatiecode opvraagt, geeft het betaalmiddel C een verdere authenticatiecode AC3 af, die onder meer is gebaseerd op de verdere authenticatiewaarde AV3. Het betaalstation T zal constateren dat de authenticatiecodes AC1 en AC3 niet gerelateerd zijn en zal de saldowaarde SC3, die in de authenticatiecode AC3 was opgenomen, niet kunnen gebruiken. Evenzo levert een authenticatie AC4, die door het tweede betaalstation T' wordt opgevraagd, geen geldige authenticatie en dus geen geldige saldowaarde op. Het overdragen van gewijzigde saldowaarden naar meerdere betaalstations wordt op deze wijze effectief voorkomen.

De authenticatiewaarden worden bij voorkeur gevormd door opeenvolgende getallen, bijvoorbeeld tellerstanden. Het is echter ook mogelijk een teller te gebruiken die elke tweede keer (tweede keer genereren van een authenticatiewaarde) verhoogd wordt, zodat steeds twee opeenvolgende authenticatiewaarden gelijk zullen zijn. Opgemerkt wordt dat het betaalmiddel verschil kan maken tussen de eerste en de derde stap, maar dit niet hoeft te doen.

De genoemde afhankelijkheid van de authenticatiewaarden overeenkomstig de uitvinding verzekert dat alle stappen van de

transactie, waarin de werkwijze volgens de uitvinding wordt toegepast, tussen hetzelfde betaalmiddel en hetzelfde betaalstation plaatsvinden.

Aan de hand van figuur 3 zal nader worden uiteengezet hoe de werkwijze volgens de uitvinding bij betaalkaarten kan worden toegepast.

Het schema van figuur 3 toont een schakeling 100 met een besturingseenheid 101, een geheugen 102, en een invoer-uitvoer-eenheid 103, die onderling zijn gekoppeld. De besturingseenheid kan bijvoorbeeld worden gevormd door een microprocessor of een microcontroller. Het geheugen 102 kan een RAM- en/of ROM-geheugen omvatten. Bij voorkeur omvat het geheugen 102 een herschrijfbaar ROM-geheugen (EEPROM).

Volgens de uitvinding omvat de schakeling 100 tevens een aanvullend geheugen 105 voor het opslaan van authenticatiewaarden. Dit geheugen 105 kan, zoals in figuur 3 is getoond, een aparte eenheid vormen, maar kan ook deel uitmaken van het geheugen 102 en bijvoorbeeld door enkele geheugenplaatsen van het geheugen 102 worden gevormd. Bij voorkeur wordt het geheugen 105 gevormd door een tellerschakeling.

In een voorkeursuitvoeringsvorm worden opeenvolgende authenticatiewaarden gevormd door opeenvolgende tellerstanden. Een eerste authenticatiewaarde AV1, die gebruikt wordt om de authenticatiécode AC1 te vormen, komt overeen met een (in principe willekeurige) stand van de teller, zoals deze in het geheugen 105 is opgeslagen. Na de tweede stap (zie ook figuur 2) wordt de tellerstand met één verhoogd.

Het genereren van authenticatiewaarden gebeurt autonoom, dat wil zeggen zonder (mogelijke) beïnvloeding van buitenaf, zoals van een betaalstation. Hierdoor wordt de fraudebestendigheid verder verhoogd.

Het zal duidelijk zijn dat in plaats van het telkens met één verhogen van de tellerstand deze telkens met één kan worden verlaagd. Evenzo kan de tellerstand telkens met meer dan één, bijvoorbeeld met twee of vier, worden verhoogd of verlaagd. Ook is het mogelijk de schakeling 100 zodanig uit te voeren, dat de authenticatiewaarde(n) niet binnen een transactie maar alleen tussen transacties worden gewijzigd. Het betaalstation is in een dergelijk geval uiteraard overeenkomstig ingericht.

Een betaalstation voor toepassing van de uitvinding omvat

middelen (zoals een kaartlezer) voor het communiceren met een betaalmiddel, middelen voor het uitvoeren van authenticaties (zoals een processor) en middelen voor het registreren van saldowaarden (zoals een halfgeleidergeheugen). Het betaalstation is zodanig uitgevoerd, dat een mislukte authenticatie het onmogelijk maakt dat een nieuwe saldowaarde wordt geregisteerd. De authenticatie omvat overeenkomstig de uitvinding ook de authenticatiewaarden. De stappen van de werkwijze volgens de uitvinding kunnen zowel in apparatuur (specifieke schakeling, zoals een ASIC) als in programmatuur (geschikt programma voor een processor) zijn vastgelegd.

Het zal deskundigen duidelijk zijn dat de uitvinding niet beperkt is tot de weergegeven uitvoeringsvormen en dat vele wijzigingen en aanvullingen mogelijk zijn zonder buiten het kader van de uitvinding te treden. Zo is het principe van de uitvinding in het bovenstaande beschreven aan de hand van het afwaarderen van een betaalmiddel, maar dit principe kan ook voor het opwaarderen van betaalmiddelen worden toegepast.

E. CONCLUSIES

1. Werkwijze voor het met behulp van een betaalstation beveiligd afwaarderen van een elektronisch betaalmiddel, omvattende:
- een eerste stap, waarin:
  - het betaalstation een eerste toevalsgetal naar het betaalmiddel overdraagt,
  - het betaalmiddel, in respons op dit eerste toevalsgetal, een eerste authenticatiecode naar het betaalstation overdraagt, welke eerste authenticatiecode op basis van tenminste het eerste toevalsgetal en een saldo van het betaalmiddel wordt bepaald, en
  - het betaalstation de eerste authenticatiecode controleert;
- een tweede stap, waarin:
  - het betaalstation een afwaardeercommando naar het betaalmiddel overdraagt en het saldo van het betaalmiddel aan de hand van het afwaardeercommando wordt verlaagd; en
- een derde stap, waarin:
  - het betaalmiddel een tweede toevalsgetal naar het betaalmiddel overdraagt,
  - het betaalmiddel, in respons op dit tweede toevalsgetal, een tweede authenticatiecode naar het betaalstation overdraagt, waarbij tweede authenticatiecode op basis van tenminste het tweede toevalsgetal en het actuele saldo van het betaalmiddel wordt bepaald, en
  - het betaalstation de eerste authenticatiecode controleert;

met het kenmerk, dat de eerste authenticatiecode mede op basis van een eerste authenticatiewaarde en de tweede authenticatiecode mede op basis van een tweede authenticatiewaarde wordt bepaald, waarbij de eerste en tweede authenticatiewaarden gerelateerd zijn, en dat het betaalmiddel in respons op het ontvangen van een toevalsgetal een nieuwe authenticatiewaarde genereert.

2. Werkwijze volgens conclusie 1, waarin de eerste en tweede authenticatiewaarden identiek zijn.

3. Werkwijze volgens conclusie 1, waarin de eerste en tweede authenticatiewaarden opeenvolgende tellerwaarden omvatten.

4. Werkwijze volgens conclusie 1, waarin de eerste authenticatiewaarde telkens op basis van een toevalsgetal wordt gevormd.

5. Werkwijze volgens een van de voorgaande conclusies, waarin een

authenticatiecode tevens op basis van een sleutel en een identificatiecode wordt bepaald.

6. Werkwijze volgens een van de voorgaande conclusies, waarin een authenticatiecode met behulp van een cryptografische functie wordt bepaald.

7. Werkwijze volgens een van de voorgaande conclusies, verder omvattende een vierde stap waarin het verschil tussen de saldi van de eerste en derde stap in het betaalstation wordt geregistreerd.

8. Werkwijze volgens een van de voorgaande conclusies, waarin de eerste en tweede toevalsgetallen identiek zijn.

9. Werkwijze volgens een van de voorgaande conclusies, waarin het betaalstation een module voor het beveiligd registreren van gegevens omvat.

10. Financiële transactie, uitgevoerd met toepassing van de werkwijze volgens een van de voorgaande conclusies.

11. Elektronisch betaalmiddel, omvattende een geïntegreerde schakeling met een processor, een geheugen en een invoer-uitvoer-schakeling, ingericht voor het ten uitvoer leggen van de werkwijze volgens een van de conclusies 1 tot en met 10.

12. Betaalstation, ingericht voor toepassing van de werkwijze volgens een van de conclusies 1 tot en met 10.

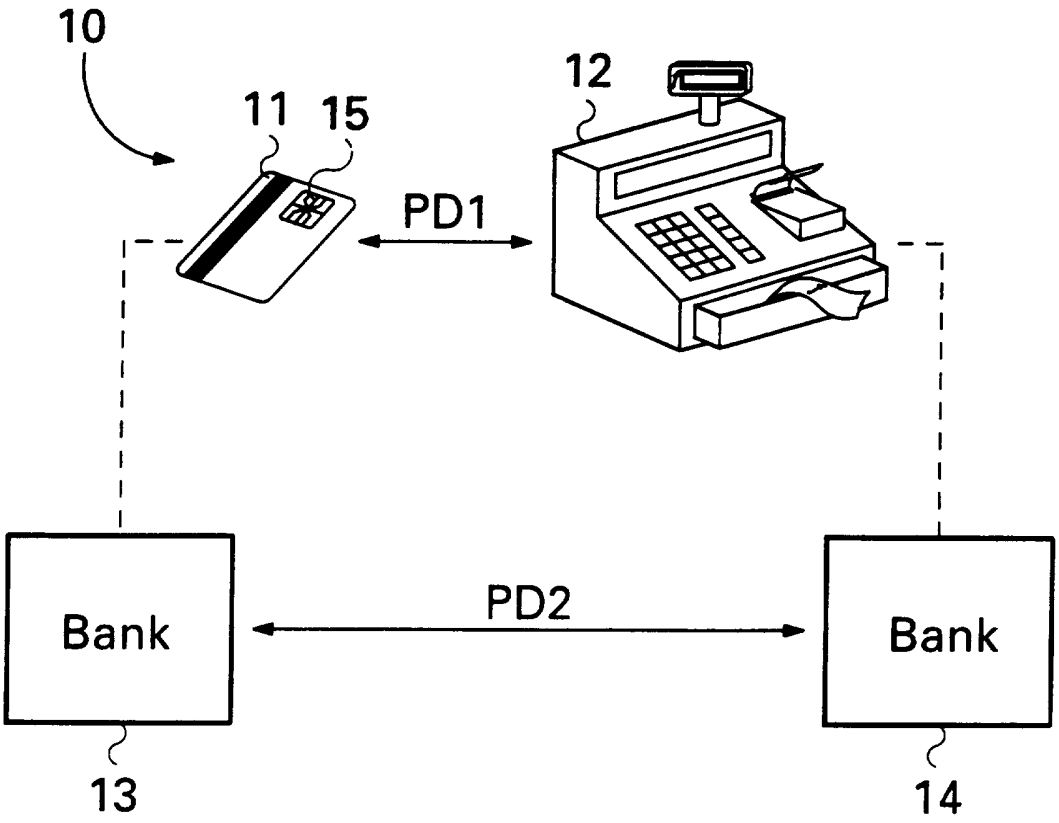


Fig. 1

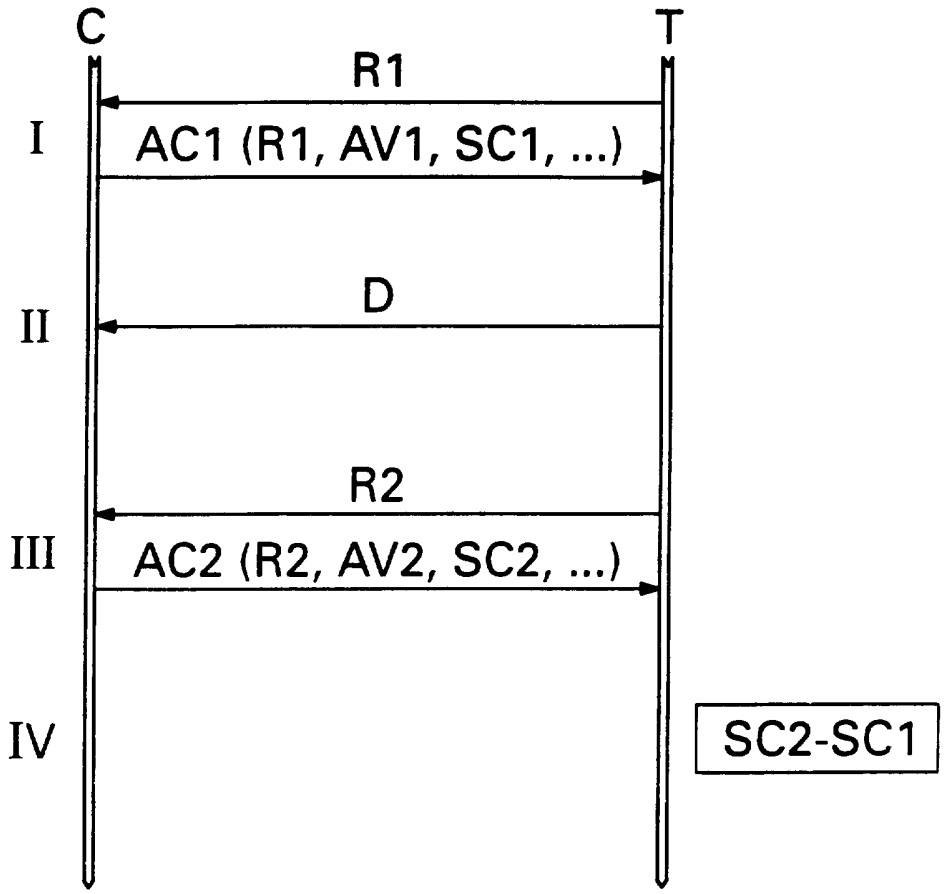


Fig. 2

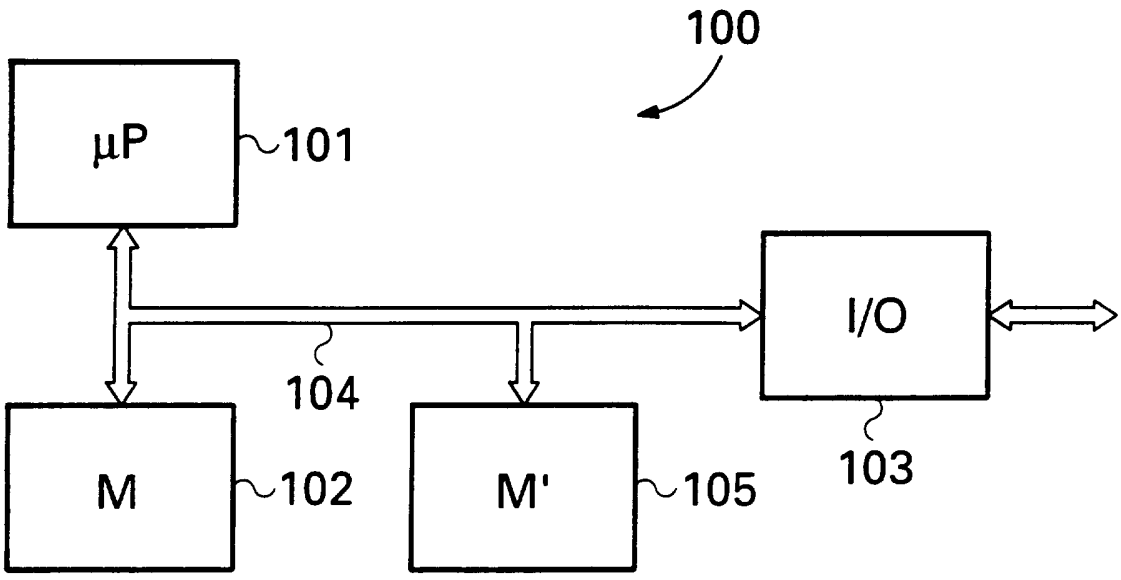


Fig. 3

RAPPORT BETREFFENDE
NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

IDENTIFIKATIE VAN DE NATIONALE AANVRAGE	Kenmerk van de aanvrager of van de gemachtigde
	402192NE
Nederlandse aanvrage nr.	**Indieningsdatum**
1001863	8 december 1995
	Ingeroepen voorrangsdatum

Aanvrager (Naam)

KONINKLIJKE PTT NEDERLAND N.V.

Datum van het verzoek voor een onderzoek van internationaal type	Door de Instantie voor Internationaal Onderzoek (ISA) aan het verzoek voor een onderzoek van internationaal type toegekend nr.
--	SN 26805 NL

I. CLASSIFICATIE VAN HET ONDERWERP (bij toepassing van verschillende classificaties, alle classificatiesymbolen opgeven)

Volgens de Internationale classificatie (IPC)

Int.Cl.6: G 07 F 7/10

II. ONDERZOCHTE GEBIEDEN VAN DE TECHNIEK

Onderzochte minimum documentatie

Classificatiesysteem	Classificatiesymbolen
Int.Cl.6:	G 07 F

Onderzochte andere documentatie dan de minimum documentatie voor zover dergelijke documenten in de onderzochte gebieden zijn opgenomen

III. ☐ GEEN ONDERZOEK MOGELIJK VOOR BEPAALDE CONCLUSIES (opmerkingen op aanvullingsblad)

IV. ☐ GEBREK AAN EENHEID VAN UITVINDING (opmerkingen op aanvullingsblad)

VERSLAG VAN HET NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

Nummer van het verzoek om een nieuwheidsonderzoek
NL 1001863

A. CLASSIFICATIE VAN HET ONDERWERP
IPC 6 G07F7/10

Volgens de Internationale Classificatie van octrooien (IPC) of zowel volgens de nationale classificatie als volgens de IPC.

B. ONDERZOCHTE GEBIEDEN VAN DE TECHNIEK

Onderzochte minimum documentatie (classificatie gevolgd door classificatiesymbolen)
IPC 6 G07F

Onderzochte andere documentatie dan de minimum documentatie, voor dergelijke documenten, voor zover dergelijke documenten in de onderzochte gebieden zijn opgenomen

Tijdens het internationaal nieuwheidsonderzoek geraadpleegde elektronische gegevensbestanden (naam van de gegevensbestanden en, waar uitvoerbaar, gebruikte trefwoorden)

C. VAN BELANG GEACHTE DOCUMENTEN

Categorie *	Geciteerde documenten, eventueel met aanduiding van speciaal van belang zijnde passages	Van belang voor conclusie nr.
Y A	EP,A,0 621 570 (FRANCE TELECOM) 26 Oktober 1994 zie het gehele document	1,3,5-7, 10-12 9
Y	EP,A,0 570 924 (SIEMENS) 24 November 1993 zie samenvatting; conclusies; figuur	1,3,5-7, 10-12
A	EP,A,0 409 701 (ÉTAT FRANCAIS) 23 Januari 1991	

☐ Verdere documenten worden vermeld in het vervolg van vak C.

☒ Leden van dezelfde octrooifamilie zijn vermeld in een bijlage

* Speciale categorieën van aangehaalde documenten

"A" document dat de algemene stand van de techniek weergeeft, maar niet beschouwd wordt als zijnde van bijzonder belang
"E" eerder document, maar gepubliceerd op de datum van indiening of daarna
"L" document dat het beroep op een recht van voorrang aan twijfel onderhevig maakt of dat aangehaald wordt om de publikatiedatum van een andere aanhaling vast te stellen of om een andere reden zoals aangegeven
"O" document dat betrekking heeft op een mondelinge uiteenzetting, een gebruik, een tentoonstelling of een ander middel
"P" document gepubliceerd voor de datum van indiening maar na de ingeroepen datum van voorrang
"T" later document, gepubliceerd na de datum van indiening of datum van voorrang en niet in strijd met de aanvrage, maar aangehaald ter verduidelijking van het principe of de theorie die aan de uitvinding ten grondslag ligt
"X" document van bijzonder belang; de uitvinding waarvoor uitsluitende rechten worden aangevraagd kan niet als nieuw worden beschouwd of kan niet worden beschouwd op inventiviteit te berusten
"Y" document van bijzonder belang; de uitvinding waarvoor uitsluitende rechten worden aangevraagd kan niet worden beschouwd als inventief wanneer het document beschouwd wordt in combinatie met één of meerdere soortgelijke documenten, en deze combinatie voor een deskundige voor de hand ligt
"&" document dat deel uitmaakt van dezelfde octrooifamilie

1

Datum waarop het nieuwheidsonderzoek van internationaal type werd voltooid	Verzenddatum van het rapport van het nieuwheidsonderzoek van internationaal type
3 September 1996	

Naam en adres van de instantie	De bevoegde ambtenaar
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	David, J

VERSLAG VAN HET NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

Informatie over leden van dezelfde octrooifamilie

Nummer van het verzoek om een nieuwheidsonderzoek
NL 1001863

In het rapport genoemd octrooigeschrift	Datum van publicatie	Overeenkomend(e) geschrift(en)		Datum van publicatie
EP-A-0621570	26-10-94	FR-A-	2704081	21-10-94
		JP-A-	7110876	25-04-95
		US-A-	5495098	27-02-96
EP-A-0570924	24-11-93	EP-A-	0570828	24-11-93
EP-A-0409701	23-01-91	FR-A-	2650097	25-01-91
		DE-D-	69012692	27-10-94
		DE-T-	69012692	19-01-95
		JP-A-	3141487	17-06-91
		US-A-	5128997	07-07-92