

(11) *Número de Publicação:* PT 786746 E

(51) *Classificação Internacional:* (Ed. 6)
G07F007/02 A G06F017/60 B
G07G001/00 B

(12) *FASCÍCULO DE PATENTE DE INVENÇÃO*

<p>(22) <i>Data de depósito:</i> 1997.01.21</p>	<p>(73) <i>Titular(es):</i> WELCOME REAL TIME PARC CLUB DU GOLF, BÂT. 2 350, AVENUE DE LA LAUZIÈRE 13856 AIX EN PROVENCE CEDEX 3 FR</p>
<p>(30) <i>Prioridade:</i> 1996.01.22 FR 9600678</p>	
<p>(43) <i>Data de publicação do pedido:</i> 1997.07.30</p>	<p>(72) <i>Inventor(es):</i> BERNARD CHEVALLIER FR ANEACE HADDAD FR</p>
<p>(45) <i>Data e BPI da concessão:</i> 2000.03.15</p>	<p>(74) <i>Mandatário(s):</i> JOSÉ LUÍS FAZENDA ARNAUT DUARTE RUA DO PATROCÍNIO, 94 1350 LISBOA PT</p>

(54) *Epigrafe:* PROCESSO E DISPOSITIVO PARA TRATAMENTO DE INFORMAÇÕES CODIFICADAS DE UM CARTÃO COM CIRCUITOS INTEGRADOS (CHIP)

(57) *Resumo:*



786746
[Handwritten Signature]

DESCRIÇÃO

**"PROCESSO E DISPOSITIVO PARA TRATAMENTO DE INFORMAÇÕES
CODIFICADAS DE UM CARTÃO COM CIRCUITOS INTEGRADOS (CHIP)"**

(0001) A invenção refere-se a um processo de tratamento de informações codificadas, quando de uma operação de compra ou de pagamento numa loja por um cliente titular de um cartão com chip, no qual se lê o conteúdo da memória do cartão com chip e se imprime ou não um talão a partir das informações recolhidas a partir do conteúdo da referida memória.

(0002) A invenção refere-se também a um dispositivo que permite executar um tal método.

(0003) A invenção encontra uma aplicação particularmente importante, embora não exclusiva, no domínio do tratamento de cartões de fidelidade, apresentados no momento do pagamento pelos clientes numa loja, por exemplo num armazém de retalho, do tipo hipermercado ou supermercado, numa estação de serviço, ou num concessionário vendedor de automóveis.

(0004) Assim, com esta invenção, é possível modular uma oferta comercial em função do comportamento à posteriori do titular do cartão, o que permite conceder-lhe vantagens específicas, de forma personalizada e imediata, que podem além disso ser registadas no cartão.

(0005) Conhece-se já um processo, que permite conceder vantagens específicas em função da atitude comportamental dos clientes e que consiste essencialmente em enviar pelo correio



talões de desconto algum tempo depois da operação desencadeadora da compra ou do pagamento pelo titular.

(0006) Um tal processo apresenta inconvenientes. Dá origem, com efeito, a demoras importantes e apresenta uma fiabilidade limitada (perda de talões, mudanças de endereço).

(0007) Um dos problemas técnicos resolvidos pela invenção consiste na eliminação destas demoras importantes, atribuindo uma vantagem ao cliente no momento exacto do pagamento por este último ou, de uma maneira mais geral, da operação que desencadeia a vantagem.

(0008) O documento «Banking Technology», de Fevereiro de 1995, descreve no artigo «Smart times head», nas páginas 2, 3, cartões electrónicos que podem fornecer ao vendedor informações sobre os hábitos de compra dos clientes. Um tipo destes cartões pode também guardar em memória pontos de fidelidade.

(0009) O comerciante vai assim poder reconhecer um cliente em função da frequência das suas passagens pela loja e do volume dos seus gastos. Poderá então conceder-lhe automaticamente uma vantagem específica determinada e isto de maneira instantânea.

(0010) Com este objectivo, a invenção propõe, nomeadamente, um processo de tratamento de informações codificadas, quando de uma operação de compra ou de pagamento por um cliente titular de um cartão com chip numa loja, na qual se lê o conteúdo da memória do referido cartão e se imprime ou não um talão a partir das informações retiradas da referida memória, caracterizado por a memória do cartão com chip possuir um primeiro ficheiro de identificação, designado ficheiro Membro, que identifica o cliente portador do cartão, um segundo



ficheiro de contabilização, designado ficheiro Pontos, e um terceiro ficheiro designado ficheiro comportamento, que se refere ao comportamento do titular do cartão com o ou os comerciantes utilizadores, se efectuar um tratamento por algoritmo determinado em função, por um lado da data de operação, e por outro, das informações contidas no referido ficheiro, incluindo o ficheiro Comportamento, depois se escreverem dados no ficheiro Pontos, se escreverem novas informações no ficheiro Comportamento e se imprimir ou não o referido talão a partir do resultado do referido tratamento por algoritmo.

(0011) Em formas de realização vantajosas, recorre-se também a uma e/ou a outra das disposições seguintes:

- tratamento algorítmico, que inclui uma etapa de aumento ou diminuição de um número pré-determinado de pontos no ficheiro Pontos;

- impressão do talão, apenas se o número de pontos existente no ficheiro Pontos for superior a um valor determinado;

- impressão do talão e/ou aumento ou deminuição no ficheiro Pontos, apenas se o ficheiro Membro corresponder a critérios determinados;

- maior ou menor aumento no ficheiro Pontos em função do montante da operação de compra ou de pagamento;

- maior ou menor aumento no ficheiro Pontos em função da frequência e/ou do carácter de primeira visita, segunda visita ou visita de ordem x do titular do cartão referentes a um período de tempo de duração determinada;

- introdução de informações correspondentes à operação na memória de um terminal de pagamento situado na loja do referido comerciante, comparam-se as referidas informações introduzidas com as informações existentes nos ficheiros e respeitantes a séries de operações pré-determinadas, e tratam-se os resultados



destas comparações para imprimir um talão e/ou os registar num ficheiro Pontos.

(0012) É assim possível concretizar operações promocionais limitadas no tempo e relativas a um conjunto de comerciantes pertencentes a uma mesma cadeia,

- cifra-se o acesso aos ficheiros por um processo de encriptação chamado de triplo DES (Data Encryption Standard).

(0013) A invenção propõe igualmente um dispositivo de tratamento de informações codificadas, quando de uma operação de compra ou de pagamento por um utilizador titular de um cartão com chip, que compreende meios de leitura de dados codificados da memória do cartão com chip, meios de cálculo e meios de impressão de um talão, caracterizado por a memória do referido cartão possuir um primeiro ficheiro de identificação, designado ficheiro Membro, que identifica o cliente titular do cartão, um segundo ficheiro de contabilização, designado ficheiro Pontos, e um terceiro ficheiro, designado ficheiro Comportamento, que se refere ao comportamento do titular do cartão com o ou os comerciantes utilizadores, meios de cálculo possuindo meios de tratamento algorítmico de dados em função, por um lado, da data de operação e, por outro, das informações contidas nos referidos ficheiros, incluindo o ficheiro Comportamento e em que o dispositivo possuem meios de registo de novas informações no ficheiro Pontos e no ficheiro Comportamento a partir do referido tratamento algorítmico, estando os meios de impressão de um talão preparados para imprimir ou não o referido talão a partir das informações recebidas do conteúdo dos referidos ficheiros e do referido tratamento algorítmico.



(0014) Com vantagem, o dispositivo inclui também:

- meios para introdução de dados, que correspondem à referida operação numa memória intermédia e de apresentação de dados;

- meios para armazenar informação codificada referente a uma ou várias operações;

- meios para comparação entre dados introduzidos na referida memória intermédia e as informações armazenadas nos referidos meios de armazenagem de informações;

- meios para tratamento dos resultados destas comparações;

- meios preparados para imprimir ou não automaticamente o talão a partir das informações obtidas do conteúdo da memória do cartão com chip, comandados pelos referidos meios de tratamento dos referidos resultados.

(0015) A invenção será melhor compreendida com a leitura da descrição que se segue de uma forma de realização específica, dada a título de exemplo não limitativo.

(0016) A descrição refere-se aos desenhos anexos, nos quais:

- a figura 1 mostra um esquema geral de uma forma de realização de acordo com a invenção;

- a figura 2 é um diagrama de blocos parcial de uma forma de realização da memória do cartão com chip do dispositivo de acordo com a invenção;

- a figura 3 é um diagrama de blocos esquemático do processo de tratamento das informações de acordo com a forma de realização da invenção, mais particularmente aqui descrita.

(0017) A figura 1 representa um dispositivo 1, que compreende um terminal 2 de pagamento munido de um leitor 3 de cartões 4 com chip 5.



(0018) O terminal de pagamento é, por exemplo, do tipo comercializado sob a referência Delta 15 da sociedade francesa Schlumberger.

(0019) Os cartões com chip utilizáveis na invenção são, por exemplo, os cartões vendidos sob as referências MP-COS da sociedade francesa Gemplus ou ME 2000 da sociedade francesa Schlumberger.

(0020) Os cartões podem ser bancários, cartões privativos de crédito ou cartões de fidelidade.

(0021) O terminal 2 inclui um teclado 6, um monitor 7 e uma calculadora 8 programável em função de algoritmos determinados de maneira bem conhecida.

(0022) A calculadora 8 está ligada ao leitor 3 através de um circuito de leitura/registo e a um microcomputador 9, ele próprio ligado a uma memória de massa 10.

(0023) O dispositivo 1 compreende igualmente meios de inserção 11 de um talão 12, ligados à calculadora 8 e a uma caixa 13 registadora e impressora de facturas, por exemplo através de um computador 9.

(0024) A calculadora 8 está ligada eventualmente através do computador 9, a meios (não representados) distantes do local onde está implantado o dispositivo 1 e preparados para assegurar a coerência dos tratamentos e/ou das informações tratadas e recolhidas por diferentes dispositivos em diferentes lugares.

(0025) Representou-se na figura 2 a organização de uma forma de realização da memória 14 do chip 5 do cartão 4.

(0026) O cartão inclui várias aplicações, compreendendo a memória 14 um directório principal ou raiz 15.

(0027) A memória está organizada em directórios 16,17, etc.

(0028) As informações referentes ao titular ou portador do cartão estão contidas no ficheiro 18, designado ficheiro Membro no directório principal 15.

(0029) Está previsto um directório Sistema 16, que compreende, por exemplo, um ficheiro 19 que se refere ao próprio cartão e outros tipos de ficheiro 20 bem conhecidos.

(0030) De acordo com a forma de realização da invenção mais particularmente aqui descrita, a memória 14 compreende um directório 17 referido como «Directório de Cupões», que inclui o ficheiro Comportamento 21 e o ficheiro Pontos 22.

(0031) Formas de realização do ficheiro Membro 18, do ficheiro Comportamento 21 e do ficheiro Pontos 22 de acordo com a invenção são descritos a seguir a título de exemplo.

Ficheiro Membro 18

(0032) Código de leitura: Livre

Código de actualização: RCódigo01

Campo	Formato	Largura
Número de cartões	999999999	9
Tipo	Alfa	2
Versão	99	2
Aplicações presentes	O/N	9
Mês/ano da personalização (fabrico)	aamm	4
Mês/ano da primeira utilização	Aamm	4
Mês/ano de prescrição	Aamm	4
Reservado	Alfa	46

Ficheiro Comportamento 21

(0033) Código de Leitura: Livre

Código de actualização: R código 12

Campo	Formato	Largura
Número máximo de comerciantes	99	2
Número de comerciantes registados	99	2
Reservados	Alfa	16
Comerciantes (até ao nb de comerciantes registados)		
Código de comerciante	99999	5
Código de actividade	Alfa	1

Data da primeira visita	aammjj	6
Data da última visita	aammjj	6
Número de visitas neste mês	99	2
Valor de compras neste mês	99999	5
Número de visitas este ano	999	3
Valor de compras este ano	999999	6
Número total de visitas	999	3
Gastos totais	999999	6

Ficheiro Pontos 22 (Contagem de pontos)

(0034)

Chave de leitura de saldos	Livre
Chave de débito	Rkdeb 1
Chave de crédito	Rkcred 1
PIN (para acesso aos débitos)	R código 13



(0035) Numa forma de realização vantajosa, está prevista uma gestão da segurança das informações do cartão por tratamento criptográfico dos códigos em função do número de cartões.

(0036) A aplicação compreende, por exemplo, dois códigos de acesso aos ficheiros e duas chaves de acesso ao ficheiro Pontos. Os códigos mãe ou as chaves mãe estão integrados no terminal 2.

(0037) São utilizados para calcular códigos e chaves diversificados, que serão em seguida comparados com os códigos e chaves inscritos no cartão. Cada cartão compreende o seu próprio e único conjunto de códigos e chaves.

(0038) Esta diversificação faz-se pelo processo do triplo DES (Data Encryption Standard) aplicada tanto aos códigos mãe (ou às chaves mãe) como ao número do cartão.

(0039) Os códigos mãe e as chaves mãe integrados no terminal são, por exemplo:

Código01 Código mãe de actualização do ficheiro Membro

Código12 Código mãe de actualização do ficheiro
Comportamento

Kaut1 Chave mãe de autenticação do ficheiro Pontos

Kcred1 Chave mãe de crédito do ficheiro Pontos

(0040) Os códigos mãe ou as chaves mãe são, aliás e por exemplo, diversificados da maneira seguinte:

1. Os códigos mãe ou as chaves mãe (16 octetos) são repartidos em duas partes iguais de 8 octetos KL (parte esquerda) e KR (parte direita)

2. N (os oito primeiros octetos do n° do cartão) é cifrado por KL: $R1 = DES(KL, N)$



3. R1 em oito octetos é desifrado por KR: $R2 = \text{DES}^{-1}(KR, R1)$
4. R2 em oito octetos é cifrado por KL: $R = \text{DES}(KL, R2)$

(0041) R é o resultado em oito octetos da diversificação por triplo DES de um código ou de uma chave mãe e representa, portanto, o valor inscrito no cartão.

(0042) Vai-se em seguida descrever um exemplo de funcionamento do dispositivo da figura 1, com referência à figura 3.

(0043) O utilizador cliente, titular do cartão, introduz o cartão 4 no leitor 3 (etapa 30) e os ficheiros Membro, Comportamento e Pontos são então lidos (etapa 32).

(0044) Uma etapa de verificação 34 de ligação do cartão (data de prescrição) é então efectuada por comparação com a data do dia.

(0045) Depois, o montante da compra é introduzido (etapa 36), quer através da caixa 13 e do microcomputador 9, quer através do teclado 6.

(0046) Se a soma é superior a um valor determinado (verificação 38), efectua-se então um tratamento algorítmico 40 em função das informações contidas no ficheiro Membro, no ficheiro Comportamento e no ficheiro Pontos.

(0047) A operação continua numa etapa 42 de aumento no ficheiro Pontos de um número determinado de pontos, por exemplo em função do número de operações efectuadas pelo titular do cartão durante o mês.



(0048) Se não (etapa 44), o visor 7 mostra, por exemplo, uma mensagem «sem desconto».

(0049) Uma etapa de verificação 46 está em seguida prevista para comparar o número de pontos do ficheiro Pontos com um volume inicial determinado.

(0050) Se o número de pontos é inferior a esse valor, é emitida uma mensagem como em 48. Se é superior, imprime-se (etapa 50) um cupão de desconto de um montante determinado.

(0051) A invenção permite assim ao titular do cartão obter dois tipos de vantagens separada ou simultaneamente:

- um crédito de pontos no contador de pontos electrónico no chip do cartão,
- um cupão de desconto impresso no momento da compra, válido para a referida compra ou para uma compra seguinte.

(0052) Dão-se a seguir vários exemplos de funcionamento.

(0053) O comerciante pode escolher, por exemplo, dar 2 pontos ao cliente na primeira visita do mês, 4 pontos na segunda visita e 6 pontos na terceira visita de cada mês.

(0054) Um outro comerciante pode escolher ligar o crédito de pontos a um valor de transação. Assim, na sua primeira visita, o cliente receberá, por exemplo, um número de pontos igual a 10% da compra. Para qualquer visita seguinte o crédito de pontos será de 5%.

(0055) Um outro comerciante escolherá oferecer um talão de desconto válido para uma compra na sua loja. Por exemplo, o comerciante pode atribuir 25% de desconto aos seus clientes que venham pela primeira vez, e 10% aos outros.



(0056) O cupão de desconto pode ter um valor em pontos. Neste caso, o desconto é dado ao cliente contra um débito de pontos. Por exemplo, o comerciante propõe uma redução de 25% contra um montante de 10 pontos - o desconto só será impresso se o cartão dispuser de um mínimo de dez pontos.

(0057) A invenção permite igualmente atingir determinados cartões. O comerciante identifica previamente os números de cartões no ficheiro Membro, que receberão vantagens quando das suas próximas visitas.

(0058) Esta lista de cartões pode igualmente ser telecarregada por um sistema central através da ligação exterior descrita com referência à figura 1.

(0059) Uma vantagem da invenção é poder formular ofertas em função do comportamento do cliente em lojas de outros comerciantes, pertencendo cada comerciante a um «grupo de actividade» identificado por um campo existente no ficheiro Comportamento, descrito a seguir.

(0060) Este aspecto da invenção pode assim ser utilizado para identificar clientes que gastam pouco na loja do comerciante, mas muito num sector de actividade próximo do do comerciante. Aos clientes assim identificados podem ser-lhes propostas melhores vantagens.

(0061) É dado a seguir um exemplo de parâmetros do algoritmo de emissão de vantagens de acordo com a invenção.

Parâmetros do algoritmo

(0062)

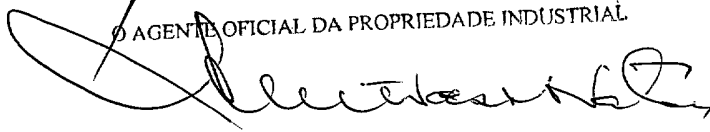
Categoria	Parâmetros	Natureza	Descrição
Parâmetros gerais	Compra mínima	Valor em centavos	Patamar abaixo do qual a operação é muito pequeno para ser causa elevada
	Uma visita por dia?	Sim	Apenas a primeira operação num mesmo dia será considerada visita
		Não	N.º de operações num mesmo dia = N.º visitas
	Função multi-visita	Não activada	Aplicar os parâmetros de "visita 1" para todas as visitas. Não actualizar o ficheiro Comportamento no cartão
		Mesmo mês	Distinguir entre 1ª, 2ª e 3ª visita num mesmo mês
		Mesmo ano	Num mesmo ano
		Após a criação do cartão	Após a criação do cartão
	Bónus linearm	Montante	Linearm para a emissão de pontos bónus
	Bónus pontos	999	Montante dos pontos bónus

Categoria	Parâmetro	Natureza	Designação
Parâmetros da visita 1	Cálculo de pontos	Não activada	Nem crédito nem débito de pontos na primeira visita
		Crédito	
		Débito	
	Cálculo de pontos	Fixo	O campo "Valor Pontos" é uma soma fixa de pontos
		Percentagem	O campo "Valor Pontos" é uma percentagem do montante da operação
		999	Valor Pontos 999 em pontos (até 999) ou percentagem até 99,9%
	Texto de cupões	Não activado	Nenhuma mensagem suplementar no talão
ASCII 2 x 20		Imprimir 2 linhas de 20 caracteres, além de infos sobre o saldo antigo, ou pontos a mais e o novo saldo	
Parâmetros da visita 2	Função pontos	Cf visita 1	
	Cálculo de pontos		
	Valor de pontos		
	Texto do cupão		
Parâmetros da visita 3	Função pontos	Cf visita 1	
	Cálculo de pontos		
	Valor de pontos		
	Texto do cupão		
Parâmetros da visita 4 e seguintes	Função pontos	Cf visita 1	
	Cálculo de pontos		
	Valor dos pontos		
	Texto do cupão		

(0063) Como é evidente e como resulta do que atrás foi descrito, a invenção não se limita à forma de realização mais particularmente aqui descrita. Como variante, o tratamento algorítmico pode ser programável à distância.

Lisboa, 14 de Junho de 2000

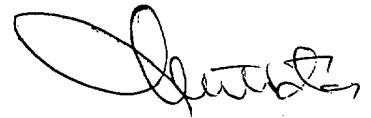
O AGENTE OFICIAL DA PROPRIEDADE INDUSTRIAL





REIVINDICAÇÕES

1. Processo de tratamento de informações codificadas quando de uma operação de compra ou de pagamento por um cliente titular de um cartão (4) com chip (5) (cartão inteligente) na loja de um comerciante, no qual se lê o conteúdo da memória de um cartão com chip e se imprime ou não um talão (12) através das informações obtidas a partir do conteúdo da referida memória, caracterizado por a memória do cartão com chip, que possui um primeiro ficheiro de identificação (18), designado ficheiro Membro, que identifica o cliente titular do cartão, um segundo ficheiro de contabilização (22), designado por ficheiro Pontos, e um terceiro ficheiro (21), designado ficheiro Comportamento, respeitante ao comportamento do titular do cartão relativamente ao ou aos comerciantes utilizadores;
por se efectuar um tratamento algorítmico determinado em função, por um lado, da data da operação e, por outro, das informações contidas nos referidos ficheiros, incluindo o ficheiro Comportamento;
por o tratamento algorítmico incluir uma etapa de aumento ou diminuição no ficheiro Pontos de um número de pontos pré-determinado em função da frequência e/ou do carácter de primeira visita, segunda visita ou visita de ordem x do titular do cartão num período de tempo com duração determinada;
por se imprimir o talão apenas se o número de pontos incluído no ficheiro Pontos for superior a um valor determinado,
por se registarem dados no ficheiro Pontos,
por se registarem novas informações no ficheiro Comportamento,



e por se imprimir ou não o referido talão a partir do resultado do referido tratamento algorítmico.

2. Processo de acordo com a reivindicação 1, caracterizado por só se imprimir o talão e/ou se aumentar ou diminuir o ficheiro Pontos se o ficheiro Membro corresponder a critérios determinados.
3. Processo de acordo com qualquer das reivindicações 1 e 2, caracterizado por o ficheiro Pontos ser aumentado mais ou menos de acordo com o valor da operação de compra ou de pagamento.
4. Processo de acordo com qualquer das reivindicações anteriores, caracterizado por se introduzirem informações correspondentes à operação numa memória de um terminal de pagamento (2) situado na loja do comerciante, se compararem as referidas informações introduzidas com as informações gravadas em meios para armazenar informação (9) e referentes a séries de operações determinadas, e se tratarem os resultados das referidas comparações para imprimir um talão (12) e/ou registar no ficheiro Pontos (22).
5. Processo de acordo com qualquer das reivindicações anteriores, caracterizado por se codificar o acesso aos ficheiros por um método de encriptação referido como de triplo DES (Data Encryption Standard).
6. Dispositivo (1) de tratamento de informações codificadas quando de uma operação de compra ou de pagamento por um utilizador titular de um cartão (4) com chip (5), que compreende meios (3) de leitura de dados codificados na



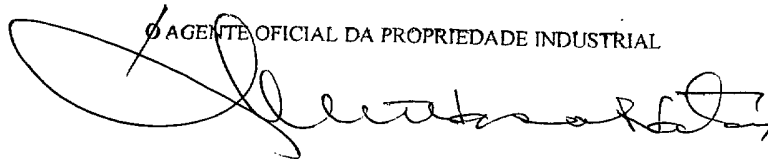
memória do cartão com chip, meios (8, 9) de cálculo e meios (11) de impressão de um talão (12), caracterizado por a memória (14) do cartão com chip, que possui um primeiro ficheiro de identificação (18), designado ficheiro Membro, que identifica o cliente titular do cartão, um segundo ficheiro de contabilização (22), designado ficheiro Pontos, e um terceiro ficheiro (21), designado ficheiro Comportamento, referente ao comportamento do titular do cartão relativamente ao ou aos comerciantes utilizadores, por os meios de cálculo (8) incluírem meios de tratamento algorítmico determinados em função, por um lado, da data da operação, e por outro, das informações contidas nos referidos ficheiros, por exemplo o ficheiro Comportamento, e por o dispositivo possuir meios (11) para registar informações no ficheiro Pontos e no ficheiro Comportamento a partir do referido tratamento algorítmico determinado, e por os meios de impressão de um talão estarem preparados para imprimir ou não o referido talão através das informações obtidas a partir do conteúdo dos referidos ficheiros e do referido tratamento algorítmico.

7. Dispositivo de acordo com a reivindicação 6, caracterizado por incluir
 - meios para introdução de dados correspondentes à referida operação numa memória de armazenamento intermédio e de apresentação (7) de dados,
 - meios (9) para armazenar informações codificadas referentes a uma ou várias operações,
 - meios para comparação entre os dados introduzidos na referida memória intermédia e as informações armazenadas nos referidos meios para armazenar informação,
 - meios para tratamento dos resultados dessas comparações,

meios (11) preparados para imprimir automaticamente um talão, comandados pelos referidos meios de tratamento dos referidos resultados e a partir das informações recolhidas do conteúdo da memória do referido cartão com chip.

Lisboa, 14 de Junho de 2000

~~O~~ AGENTE OFICIAL DA PROPRIEDADE INDUSTRIAL

A handwritten signature in black ink, written over the text 'O AGENTE OFICIAL DA PROPRIEDADE INDUSTRIAL'. The signature is highly stylized and cursive, starting with a large loop on the left and ending with a horizontal stroke on the right.

Handwritten signature

FIG. 1

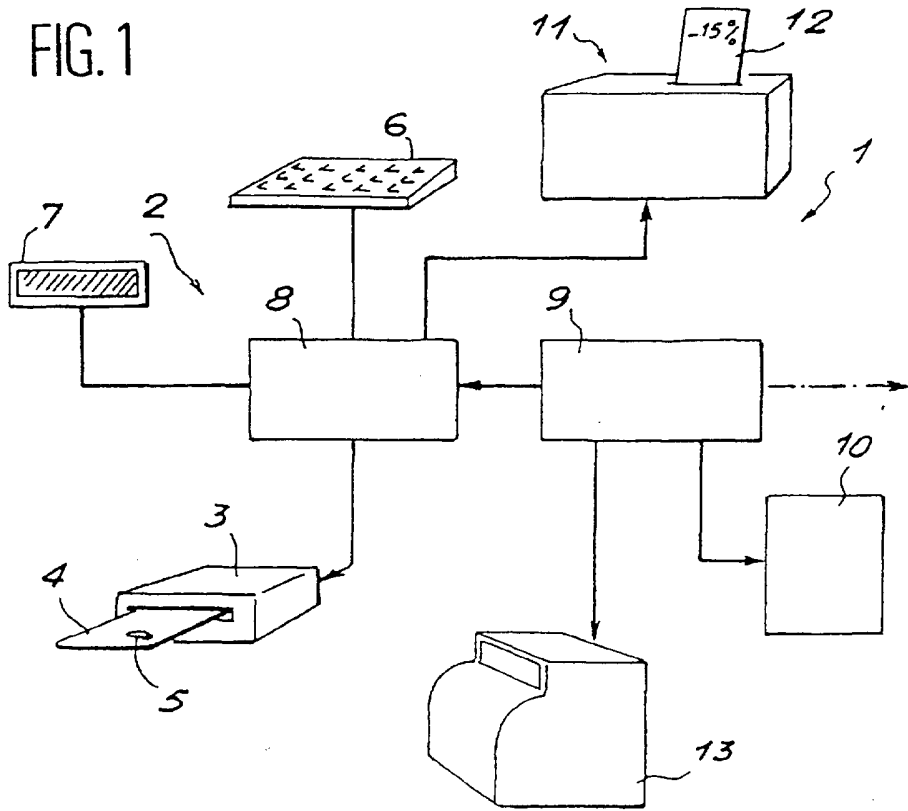
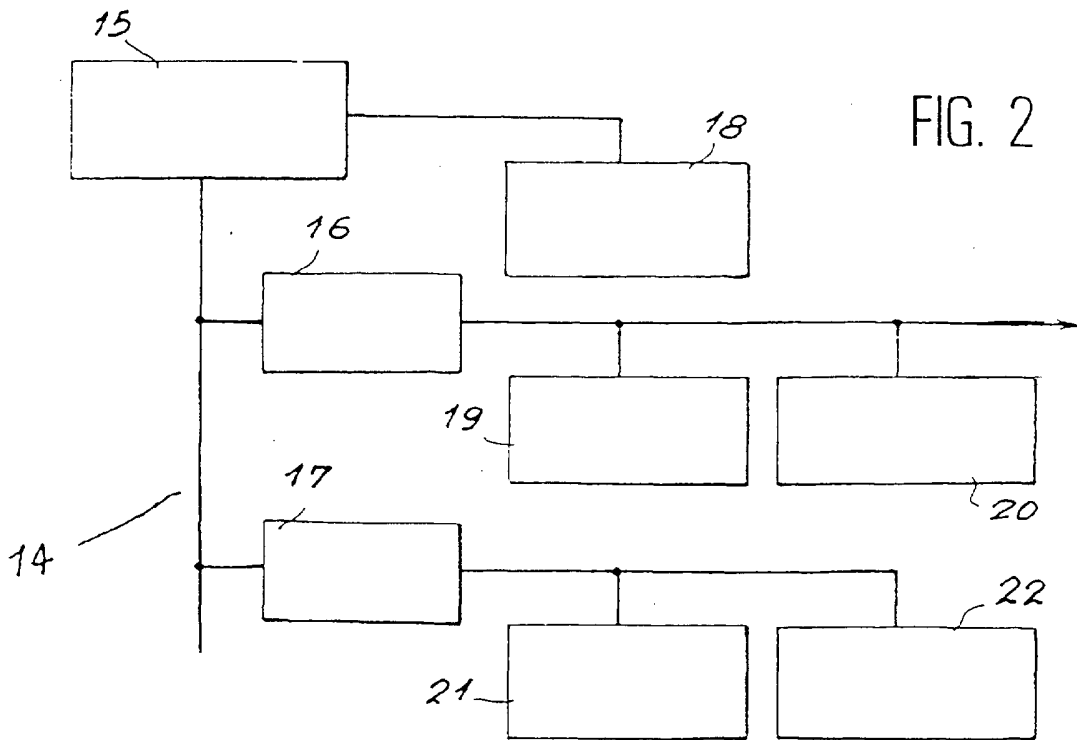


FIG. 2



Alvares

FIG. 3

