(11) Número de Publicação: **PT 1547005 T**

(51) Classificação Internacional:
G06K 19/07 (2016.01)

(12) **FASCÍCULO DE PATENTE DE INVENÇÃO**

(22) Data de pedido: **2003.09.29**

(30) Prioridade(s): **2002.10.04 FR 0212340**

(43) Data de publicação do pedido: **2005.06.29**

(45) Data e BPI da concessão: **2016.05.04**
174/2016

(73) Titular(es):
OBERTHUR TECHNOLOGIES
420, RUE D'ESTIENNES D'ORVES 92700 COLOMBES **FR**

(72) Inventor(es):
STÉPHANE JAYET **FR**
JEAN-CLAUDE HUOT **FR**

(74) Mandatário:
FERNANDO ANTÓNIO FERREIRA MAGNO
AV. 5 DE OUTUBRO, Nº 146, 7º ANDAR 1050-061 LISBOA PT

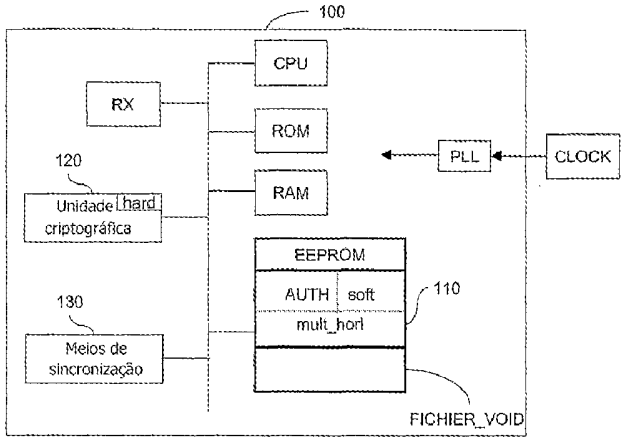
(54) Epígrafe: **CARTÃO DE MICROCIRCUITO CUJOS DESEMPENHOS PODEM SER MODIFICADOS APÓS A PERSONALIZAÇÃO**

(57) Resumo:
ESTE CARTÃO DE MICROCIRCUITO COMPREENDE MEIOS (RX) PARA RECEBER DE UM COMANDO E MEIOS DE MODIFICAÇÃO DE, PELO MENOS, UM DESEMPENHO DO CARTÃO QUE PODEM SER IMPLEMENTADOS APÓS UM PASSO DE PERSONALIZAÇÃO DO CARTÃO.

RESUMO

"Cartão de microcircuito cujos desempenhos podem ser modificados após a personalização"

Este cartão de microcircuito compreende meios (RX) para receber de um comando e meios de modificação de, pelo menos, um desempenho do cartão que podem ser implementados após um passo de personalização do cartão.



DESCRIÇÃO

"Cartão de microcircuito cujos desempenhos podem ser modificados após a personalização"

O presente invento refere-se a um cartão de microcircuito, cujos desempenhos podem ser modificados após um passo de personalização do cartão, e a um processo de configuração de um tal cartão.

No que se segue deste documento, o termo *"personalização"* (ou individualização) será entendido como sendo o mesmo utilizado correntemente pelo especialista da técnica na indústria dos cartões de microcircuito, ou tal como definido por W.Rankl e W.Effing no documento "Smart Card Handbook, Second Edition, Ed. John Wiley & Sons, Ltd" da maneira seguinte:

"O termo personalização, no seu sentido mais lato, significa que os dados específicos de um cartão ou de uma pessoa são inseridos no cartão. Estes dados podem ser, por exemplo, um nome, um endereço, mas também chaves associadas ao cartão. A única coisa que importa é que estes dados sejam específicos para este cartão."

Certas operações podem ser efetuadas nos cartões de microcircuito após o passo de personalização., por exemplo, a patente americana US 6,273,335 descreve um método e um sistema para bloquear ou desbloquear uma aplicação num cartão de microcircuito, que utiliza um mecanismo de autenticação automático com base na comparação de números de PIN e palavras passe.

O invento encontra uma aplicação privilegiada, mas não limitativa no domínio dos cartões de microcircuito das telecomunicações móveis, tais como os cartões SIM, de acordo com a norma GSM ou cartões de acordo com normas semelhantes, tais como as normas CDMA, TDMA e UMTS. Neste contexto, o invento permite a mudança dos desempenhos de um cartão de telecomunicações móveis personalizado e já atribuído a um utilizador subscritor de um serviço de telefonia móvel.

A modificação da frequência de relógio de um cartão de microcircuito é já conhecida do especialista da técnica, quando a mesma é efetuada antes do passo de personalização do cartão.

Um tal procedimento é, em particular, utilizado durante uma das fases de desenvolvimento de um cartão de microcircuito, as fases no decorrer das quais os cartões são testados com diferentes frequências de relógio, sendo a frequência de relógio a seguir fixa antes do fim da personalização.

Todavia, de acordo com a técnica anterior, ainda que as aplicações pudessem ser instaladas após a personalização do cartão, tal como descrito, por exemplo, no pedido de patente WO 00/25278, a modificação dos desempenhos do cartão não pode ser feita após a personalização do cartão.

Seria, portanto, desejável modificar os desempenhos de um cartão de microcircuito, após a personalização, nomeadamente, após a sua comercialização, ou mais geralmente, após o mesmo ter sido atribuído a um utilizador.

Para este efeito, o invento refere-se a um cartão de microcircuito, tal como definido na reivindicação 1.

Correlativamente, o invento visa, de acordo com um segundo aspeto, um processo de configuração de um cartão de microcircuito, tal como definido na reivindicação 11.

No contexto do presente invento, um desempenho de um cartão de microcircuito que pode ser modificado por um processo de configuração de acordo com o presente invento, deve ser entendido como sendo qualquer característica material ou suporte lógico pré-existente no cartão e não acessível após a personalização.

O invento permite assim melhorar ou degradar um desempenho de um cartão de microcircuito, pelo envio do comando citado anteriormente após a personalização, estando o cartão já atribuído a um utilizador. Sem o presente invento, em contrapartida, um utilizador que deseje utilizar um cartão com receção do comando, não pode beneficiar de todos 64 kilobytes da memória física sem ter que mudar de cartão.

Num modo preferido de realização, estes meios de autenticação incluem meios criptográficos que permitem verificar se o comando foi encriptado com uma chave de autenticação predeterminada.

Estes meios de verificação podem utilizar uma função endereçamento (hash) de acordo com um algoritmo do tipo MD4, MD5 ou SHA-1.

Assim, de acordo com esta característica vantajosa, as modificações de desempenho do cartão necessitam do conhecimento da chave de autenticação, podendo esta chave ser mantida secreta por um operador, pelo fabricante do cartão ou por qualquer terceiro, ao qual se reserva assim s possibilidade de modificar os desempenhos do cartão.

Numa variante de realização, a chave de autenticação citada anteriormente está associada à modificação de um desempenho predeterminado de um cartão predeterminado.

De acordo com uma outra característica, os meios de modificação estão adaptados para determinar qual desempenho do cartão é que deve ser modificado em função de uma ordem predeterminada recebida no comando.

Esta característica permite, de acordo com a ordem predeterminada recebida no comando, modificar uma ou diversas características do cartão.

De acordo com um modo de realização particularmente vantajoso, os meios de receção estão adaptados para receberem a ordem, de acordo com o protocolo SMS ou semelhante, tal como uma mensagem MMS (serviço multimédia).

Este modo de realização permite, assim, a modificação, pelo menos, de um desempenho do cartão através de uma rede de telecomunicações móveis.

Bem entendido, noutros modos de realização, o comando pode ser recebido pelos meios de receção através de uma rede com fios ou localmente.

De acordo com um modo preferido de realização do cartão, de acordo com o invento, os meios de modificação estão adaptados para modificarem o tamanho de uma zona utilizável de uma memória física do cartão.

Esta característica permite assim aumentar as capacidades de memorização do cartão, por exemplo, para permitir o telecarregamento de novas aplicações no cartão.

Numa variante preferida deste modo de realização, a modificação do tamanho da zona utilizável da memória física é efetuada através criando ou destruindo, pelo menos, um ficheiro específico compreendido na memória física, ou modificando o tamanho de, pelo menos, um ficheiro específico compreendido na memória física.

Este ficheiro pode ser um ficheiro especialmente criado para ocupar um espaço da memória física ou um ficheiro de dados, utilizado por uma aplicação do cartão de microcircuito.

Num outro modo preferido de realização, os meios de modificação de, pelo menos, um desempenho, estão adaptados para modificarem, de forma reversível ou não, uma frequência de relógio do cartão.

De acordo com esta característica particular, pode-se acelerar a velocidade de cálculo de um processador ou de um componente criptográfico do cartão, o que permite realizar tratamentos mais complexos nos dados digitais recebidos pelo cartão de microcircuito.

Num outro modo de realização, os meios de modificação de, pelo menos, um desempenho, estão adaptados para permitirem ou impedirem, de maneira reversível ou não, a utilização de, pelo menos, uma função de suporte lógico do cartão.

Esta característica particular permite assim validar aplicações de suportes lógicos previstas inicialmente no cartão, mas invalidadas antes do fim da sua personalização.

Uma tal função de suporte lógico pode, por exemplo, ser uma função criptográfica, tal como uma função de controlo de uma assinatura de dados digitais.

Da mesma maneira, num outro modo de realização, os meios de modificação do desempenho do cartão estão adaptados para permitirem ou impedirem, de maneira reversível ou não, a utilização de todo ou parte de um circuito eletrónico do cartão, podendo este circuito eletrónico, por exemplo, ser uma unidade criptográfica.

Os tratamentos criptográficos, que foram realizados por suporte lógico, podem assim ser vantajosamente acelerados pela utilização desta unidade criptográfica.

Num modo preferido de realização, o cartão de microcircuito, de acordo com o invento, compreende ainda meios de sincronização adaptados para verificarem a unicidade do comando.

Esta característica particular permite vantajosamente evitar a utilização desonesta do cartão de microcircuito, impedindo que um comando já recebido e copiado fraudulentamente não seja tido em conta uma segunda vez.

As vantagens e características particulares próprias do processo de configuração, de acordo com o invento, sendo semelhantes às expostas acima referentes ao cartão de microcircuito de acordo com o invento, que não serão aqui relembradas.

Outros aspetos e vantagens do presente invento aparecerão mais claramente com a leitura das descrições de um modo particular de realização, o qual vai seguir esta descrição, que é dado a título de exemplo não limitativo, é feita com referência aos desenhos juntos, nos quais:

a Figura 1 representa de maneira esquemática a arquitetura de um cartão de microcircuito de acordo com o invento;

a Figura 2 representa um comando de acordo com o presente invento, num modo preferido de realização; e

a Figura 3 representa, na forma de organigrama, os principais passos de um processo de configuração, de acordo com o invento, num modo preferido de realização.

A Figura 1 representa de maneira esquemática a arquitetura de um cartão de microcircuito 100, de acordo com o invento.

O cartão de microcircuito 100 inclui principalmente um processador CPU associado de maneira clássica a um certo número de memórias tipo RAM, ROM e EEPROM.

A memória ROM inclui, em particular, as instruções de um programa de informático, adaptadas para implementar um processo de configuração, de acordo com o presente invento, e cujos passos principais serão descritos ulteriormente com referência à Figura 3.

Da mesma maneira, a memória viva RAM inclui os registos necessários para a execução deste programa.

O cartão de microcircuito 100 inclui igualmente uma memória física, por exemplo, uma memória tipo EEPROM, cujo tamanho de uma zona utilizável 110 pode ser modificado após a personalização.

O cartão de microcircuito 100 inclui igualmente um circuito eletrónico 120, constituído, no modo de realização aqui descrito, por uma unidade criptográfica.

De uma maneira conhecida, o cartão de microcircuito 100 recebe igualmente um sinal de um relógio do relógio CLOCK externo ao cartão, sendo este sinal de relógio fornecido aos diferentes componentes do cartão.

No modo de realização particular aqui descrito, o cartão de microcircuito 100 inclui um componente PLL (Phase Lock Looping em inglês) conhecido pelo especialista da técnica e que permite derivar sinais com diferentes frequências de relógio a partir do sinal do relógio externo CLOCK.

Mais precisamente, no modo de realização aqui descrito, a zona utilizável 110 a memória EEPROM inclui um registo

mult_horl para memorizar um fator multiplicador aplicado à frequência do sinal de relógio externo CLOCK.

Com a colocação sob tensão do cartão de microcircuito, o processador CPU lê este registo mult_horl e programa o componente PLL com o valor contido neste registo, sendo o sinal de relógio na saída do componente PLL em seguida aplicado a certos componentes do cartão.

No modo de realização aqui descrito, o componente PLL permite assim modificar a velocidade de cálculo do processador CPU e da unidade criptográfica 120.

O cartão de microcircuito 100, de acordo com o invento, inclui meios de receção RX de um comando 200, o qual vai agora ser descrito, num modo preferido de realização, com referência à Figura 2.

O comando 200 inclui um campo 210, que inclui uma ordem predeterminada, cuja análise permite determinar quais são os desempenhos do cartão 100, que devem ser modificados.

No exemplo de realização aqui descrito, os desempenhos do cartão de microcircuito 100, que podem ser modificados após a personalização, são o tamanho da zona utilizável 110 da memória física EEPROM, a frequência do sinal de relógio, a função de suporte lógico f implementada pelo processador CPU e pelo circuito eletrónico 120.

No modo preferido de realização aqui descrito, a ordem 210 é constituída por um byte em que:

- o primeiro bit (bit1) e o segundo bit (bit2) são representativos de uma ordem de criação ou a destruição de uma zona utilizável 110, ou uma ordem de modificação do tamanho da zona utilizável 110 da memória física EEPROM do cartão de microcircuito 100;

- o terceiro bit (bit3) e o quarto bit (bit4) constituem um fator multiplicador da frequência do sinal de relógio fornecido pelo relógio externo CLOCK;

- o quinto bit (bit5) é representativo de uma ordem de utilização ou de não utilização de uma função de suporte lógico f do cartão;

- o sexto bit (bit6) é representativo de uma ordem de utilização ou de não utilização do circuito eletrónico 120; e

- o sétimo e o oitavo bits não são utilizados.

No modo preferido de realização aqui descrito, os meios de receção RX estão adaptados para receberem o comando 200 de acordo com o protocolo SMS, por exemplo, por meio do comando ENVELOPE deste protocolo, e para memorizar este comando 200 numa zona de memória viva RAM.

O cartão de microcircuito 100 inclui igualmente meios de autenticação de um emissor do comando 200.

Num modo preferido de realização, os meios de autenticação incluem meios criptográficos que permitem verificar se o comando 200 foi encriptado com uma chave de autenticação AUTH predeterminada, sendo a chave de autenticação AUTH memorizada numa parte AUTH da zona utilizável 110 da memória EEPROM no momento da personalização do cartão.

Estes meios criptográficos podem ser constituídos por um programa informático, executado pelo processador CPU, incluindo este programa informático instruções de implementação de um algoritmo de desencriptação da chave pública, tal como o algoritmo RSA conhecido do especialista da técnica.

No modo preferido de realização aqui descrito, o cartão de microcircuito 100 inclui ainda meios de sincronização 130, adaptados para verificarem a unicidade do comando 200, de maneira a evitar que um comando 200 já recebido e copiado fraudulentamente não seja tido em conta uma segunda vez de maneira não autorizada.

Os meios de sincronização 130 podem, em particular, serem constituídos por um circuito eletrónico que implementa o teste

E35 de verificação, descrito ulteriormente com referência à Figura 3.

De acordo com um modo preferido de realização, o processador CPU determina, a partir do comando 200, o ou os desempenhos do cartão de microcircuito 100, os quais devem ser modificados.

Em particular, se o par (bit1, bit2) constituído pelo primeiro bit, bit1, e pelo segundo bit, bit2, da ordem 210 for igual a (1,1), isto significa que o tamanho da zona utilizável 110 da memória física EEPROM deve, se possível, ser aumentada.

Na prática, e no modo preferido de realização aqui descrito, o cartão de microcircuito 100 inclui, antes da personalização, um ficheiro informático FICHIER_VOID na memória física EEPROM, de tal modo que, quando o par (bit1, bit2) é igual a (1, 1), o processador CPU destrói esse ficheiro FICHIER_VOID, libertando assim uma parte da memória física EEPROM.

Como variante, quando o par (bit1, bit2) é igual a (1,1), o tamanho da zona utilizável da memória física EEPROM é (se possível) aumentado, diminuindo o tamanho do ficheiro FICHIER_VOID de maneira predeterminada, por exemplo, de 16 kilobytes.

Igualmente, no modo preferido de realização aqui descrito, quando o par (bit1, bit2) for igual a (0,0), isto significa que o tamanho da zona utilizável 110 da memória física EEPROM deve, se possível, ser diminuído, sendo esta operação realizada aumentando (se possível) o tamanho do ficheiro FICHIER_VOID de maneira predeterminada, por exemplo, de 16 kilobytes.

Como variante, quando o par (bit1, bit2) é igual a (0,0), isto significa que o ficheiro FICHIER_VOID deve ser criado, se possível, num endereço e com um tamanho predeterminado na memória física EEPROM.

No modo de realização aqui descrito, a receção de um comando 200 cujo par (bit1, bit2) é igual a (1,0) ou (0,1) não tem efeito.

De acordo com a norma ISO7816, a modificação das características (criação, destruição, modificação de tamanho) de ficheiro FICHIER_VOID pode necessitar uma chave específica CLEF 220 recebida no comando 200, tal como representado na Figura 2.

Num outro modo preferido de realização, vários ficheiros do mesmo tipo podem ser previstos antes da personalização do cartão, o que permite aumentar, progressivamente, por destruição destes ficheiros, o tamanho da zona utilizável da memória física EEPROM.

Por outro lado, quando o cartão de microcircuito 100 recebe a ordem 210, o processador CPU obtém, pela leitura do terceiro, bit3, e do quarto bit, bit4, desta ordem 210, um multiplicador de relógio.

No modo preferido de realização aqui descrito, este fator multiplicador de relógio é igual, respetivamente, a 1, 2 e 3 para os valores de pares (bit3, bit4), respetivamente, igual a (0,1) (1,0) (1,1).

No modo realização particular aqui descrito, este multiplicador é memorizado no registro mult_horl da zona utilizável 110 da memória EEPROM, sendo este registo lido pelo processador CPU, com a colocação sob tensão, para parametrizar o componente PLL.

No modo de realização aqui descrito, o cartão de microcircuito compreende meios de modificação, adaptados para permitirem ou impedirem a utilização de uma função de suporte lógico f do cartão.

Na prática, a memória morta ROM inclui um programa informático que pode invocar esta função de suporte lógico f, quando um registo *soft* (lógico) da zona utilizável 110 da memória não volátil EEPROM contém o valor 1.

Na receção do comando 200, o processador CPU lê, escreve no registo *soft* o valor do quinto bit, bit5, da ordem predeterminada recebida no comando 200.

No exemplo aqui descrito, a função do suporte lógico é uma função criptográfica ou uma função de controlo de uma assinatura de dados digitais, recebidos pelos meios de receção RX.

O cartão de microcircuito 100 inclui também meios de modificação adaptados para permitirem ou impedirem a utilização de todo ou parte de um circuito eletrónico 120 do cartão.

No modo de realização aqui descrito, este circuito eletrónico 120 inclui uma unidade criptográfica.

Na prática, a utilização deste circuito eletrónico 120 é possível após a escrita do valor de 1 num registo *hard* (físico) deste componente, sendo o valor deste registo modificado pelo processador CPU com o conteúdo do sexto bit, bit6, da ordem predeterminada.

No exemplo aqui descrito, a modificação da frequência de relógio, a autorização ou o impedimento de utilizar a função de suporte lógico ou o componente eletrónico são operações reversíveis. Num outro modo de realização, pelo menos, uma destas operações pode não ser reversível.

Vão ser agora descritos, com referência à Figura 3, os principais passos de um processo de configuração de acordo com o invento num modo preferido de realização.

O processo de configuração inclui um primeiro passo E10 de personalização. Este passo é conhecido do especialista da técnica, e não será descrito aqui em pormenor.

De qualquer modo, este passo de personalização consiste em escrever numa memória do cartão, por exemplo, na EEPROM dados específicos deste cartão ou de um utilizador deste cartão.

No exemplo aqui descrito, este passo de personalização compreende, em particular, a escrita numa memória EEPROM do cartão de microcircuito 100, do valor da chave de autenticação AUTH.

Este passo de personalização compreende também a criação do ficheiro FICHIER_VOID e da sua chave 220 na memória EEPROM.

O passo E10 é seguido por um passo E20 de receção do comando 200 descrito anteriormente com referência à Figura 2.

O passo E20 é seguido por um passo E30 de verificação, no decurso do qual o processador CPU autentica um emissor do comando 200. Este passo de autenticação é efetuado, no modo de realização aqui descrito, verificando se o comando 200 foi encriptado com uma chave de autenticação AUTH predeterminada, sendo a chave de autenticação AUTH memorizada num registo da memória EEPROM no momento da personalização do cartão.

Se tal não for o caso, o resultado do teste E30 é negativo. Este teste é, então, seguido pelo passo E20 de receção de um comando já descrito.

Em contrapartida, se o emissor do comando 200 for autenticado como autorizado a emitir o comando 200, o resultado do teste E30 é positivo.

Este teste é então seguido por um teste E35, no decurso do qual é verificada a unicidade do comando 200. Este teste E35 de verificação permite evitar que um comando 200 já recebido e copiado fraudulentamente não seja tido em conta uma segunda vez de maneira não autorizada.

De maneira conhecida, este teste E35 de verificação pode ser implementado, incluindo um número de mensagem em cada comando 200, sendo este número incrementado por cada comando, e comparando este número recebido num comando 200 particular com o valor do número recebido no comando 200 anterior.

Se o comando 200 tiver sido já recebido, o resultado do teste de verificação E35 é negativo. Este teste é então seguido pelo passo E20 de receção de um comando 200 já descrito.

Em contrapartida, se o comando 200 for recebido pela primeira vez, o resultado do teste de verificação E35 é positivo.

Este teste é, então, seguido por um passo E40, no decurso do qual é modificado o tamanho da zona utilizável 110 da memória física EEPROM em função dos valores dos primeiro e segundo bits (bit1, bit2) da ordem predeterminada 210 recebida no comando 200.

De acordo com as diferentes variantes de realização descritas anteriormente com referência à Figura 1, este passo E40 é realizado criando, destruindo o ficheiro FICHIER_VOID na memória física EEPROM, modificando o tamanho deste ficheiro FICHIER_VOID.

O passo E40 de modificação do tamanho da zona utilizável 110 da memória física EEPROM é seguido por um passo E60, no decurso do qual é memorizado o fator multiplicador da frequência do relógio externo CLOCK no registo mult_horl da zona utilizável 110 da memória EEPROM, sendo este registo lido pelo processador CPU na colocação sob tensão, para parametrizar o componente PLL, que tem o por efeito modificar de maneira reversível a frequência de relógio do cartão.

Como descrito anteriormente, o fator multiplicador desta frequência de relógio é determinado pelo valor da ordem terceiro bit, bit3, e do quarto bit, bit4, da ordem 210 predeterminada.

O passo E60 de modificação a frequência de relógio é seguido por um passo E70, no decurso do qual o processador CPU escreve no registo *soft* da memória não volátil EEPROM, o valor do quinto bit, bit5, da ordem 210.

Como descrito anteriormente, quando este registo *soft* memoriza o valor 1, uma função de suporte lógico f, por exemplo, uma função criptográfica, tal como uma função de controlo de uma assinatura de dados digitais é tornada acessível, por a mesma poder ser invocada por um programa informático, memorizado na memória ROM ou na memória EEPROM.

O passo E70 é seguido por um passo E80, no decurso do qual o processador CPU memoriza no registo *hard* do circuito eletrónico 120 o valor do sexto bit, bit6, da ordem predeterminada.

Quando este registo *hard* memoriza o valor 1, é autorizada a utilização deste circuito eletrónico 120. No modo preferido de realização aqui descrito, o circuito eletrónico 120 é uma unidade criptográfica.

O passo E80 é seguido pelo passo E20 de receção de um comando já descrito.

Lisboa, 2016-09-02

REIVINDICAÇÕES

1 - Cartão de microcircuito (100) que inclui meios (RX) de receção de um comando (200) e meios de modificação de, pelo menos, um desempenho do referido cartão na receção do referido comando, podendo os meios de modificação serem implementados após um passo (E10) de personalização do referido cartão, e que inclui igualmente meios criptográficos para autenticar um emissor do referido comando, visando o referido, pelo menos, um desempenho, pelo menos, uma característica pré-existente no referido cartão, sendo os referidos meios de receção (RX) caracterizados por os mesmos estarem adaptados para receberem o referido comando (200) de acordo com um protocolo tipo SMS.

2 - Cartão de microcircuito de acordo com a reivindicação 1, caracterizado por os referidos meios criptográficos de autenticação compreendem uma chave de autenticação.

3 - Cartão de microcircuito de acordo com a reivindicação 1 ou 2, caracterizado por os meios de modificação estarem adaptados para determinarem o referido, pelo menos, um desempenho em função de uma ordem predeterminada (210) recebida no referido comando (200).

4 - Cartão de microcircuito de acordo com qualquer uma das reivindicações 1 a 3, caracterizado por os referidos meios de modificação de, pelo menos, um desempenho estarem adaptados para modificar o tamanho de uma zona utilizável (110) de uma memória física (EEPROM) do referido cartão.

5 - Cartão de microcircuito de acordo com a reivindicação 4, caracterizado por a referida modificação do tamanho de uma zona utilizável (110) de uma memória física (EEPROM) ser efetuada criando ou destruindo, pelo menos, um ficheiro específico (FICHIER_VOID) compreendido na referida memória física, ou modificando o tamanho de, pelo menos, um ficheiro específico (FICHIER_VOID) compreendido na referida memória física.

6 - Cartão de microcircuito de acordo com qualquer uma das reivindicações 1 a 5, caracterizado por os referidos meios de modificação de, pelo menos, um desempenho estarem adaptados

para modificar, de maneira reversível ou não, uma frequência de relógio do referido cartão.

7 - Cartão de microcircuito de acordo com qualquer uma das reivindicações 1 a 6, caracterizado por os referidos meios de modificação de, pelo menos, um desempenho estarem adaptados para permitirem ou impedirem, de forma reversível ou não, a utilização de, pelo menos, uma função de suporte lógico (f) do referido cartão.

8 - Cartão de microcircuito de acordo com qualquer uma das reivindicações 1 a 7, caracterizado por os referidos meios de modificação de, pelo menos, um desempenho estarem adaptados para permitirem ou impedirem, de maneira reversível ou não, a utilização de todo ou parte de um circuito eletrónico (120) do referido cartão.

9 - Cartão de microcircuito de acordo com a reivindicação 8, caracterizado por o referido circuito eletrónico (120) ser uma unidade criptográfica.

10 - Cartão de microcircuito de acordo com qualquer uma das reivindicações 1 a 9, caracterizado por compreender ainda meios de sincronização (130) adaptados para verificarem a unicidade do referido comando (200).

11 - Processo de configuração de um cartão de microcircuito (100) que inclui os passos sucessivos seguintes:

- de personalização (E10) do referido cartão;

- de receção (E20) de um comando (200);

- de autenticação (E30) por criptografia de um emissor do referido comando (200); e

- de modificação (E40, E60, E70, E80) de, pelo menos, um desempenho do cartão na receção do referido comando (200),

visando o referido, pelo menos, um desempenho, pelo menos, uma característica pré-existente no referido cartão, sendo o

processo caracterizado por o referido passo (E20) de receção de um comando (200) ser de acordo com um protocolo tipo SMS.

12 - Processo de configuração de acordo com a reivindicação 11, caracterizado por, no decurso do referido passo de modificação (E40, E60, E70, E80), ser determinado o referido, pelo menos, um desempenho em função de uma ordem predeterminada (210) recebida no referido comando (200).

13 - Processo de configuração de acordo com qualquer uma das reivindicações 11 a 12, caracterizado por, no decurso do referido passo (F40) de modificação de, pelo menos, um desempenho, ser modificado o tamanho de uma zona utilizável (110) de uma memória física (EEPROM) do referido cartão.

14 - Processo de configuração de acordo com a reivindicação 13, caracterizado por, no decurso da referida modificação do tamanho de uma zona utilizável (110) de uma memória física (EEPROM), ser criado ou ser destruído, pelo menos, um ficheiro específico (FICHIER_VOID) compreendido na referida memória física.

15 - Processo de configuração de acordo com qualquer uma das reivindicações 11 a 14, caracterizado por no decurso do referido passo (E60) de modificação de, pelo menos, um desempenho, ser modificada, de maneira reversível ou não, uma frequência de relógio do referido cartão.

16 - Processo de configuração de acordo com qualquer uma das reivindicações 11 a 15, caracterizado por no decurso do referido passo (E70) de modificação de, pelo menos, um desempenho, ser permitida ou ser impedida, de maneira reversível ou não, a utilização de, pelo menos, uma função de suporte lógico (f) do referido cartão.

17 - Processo de configuração de acordo com qualquer uma das reivindicações 11 a 16, caracterizado por no decurso do referido passo (E80) de modificação de, pelo menos, um desempenho, ser permitida ou ser impedida, de maneira reversível ou não, a utilização de todo ou parte de um circuito eletrónico (120) do referido cartão.

18 - Processo de configuração de acordo com a reivindicação 17, caracterizado por o referido componente eletrónico (120) ser uma unidade criptográfica.

19 - Processo de configuração de acordo com qualquer uma das reivindicações 11 a 18, caracterizado por compreender, anteriormente ao referido passo (E40) de modificação de, pelo menos, um desempenho, um passo (E35) de verificação da unicidade do referido comando (200).

Lisboa, 2016-09-02

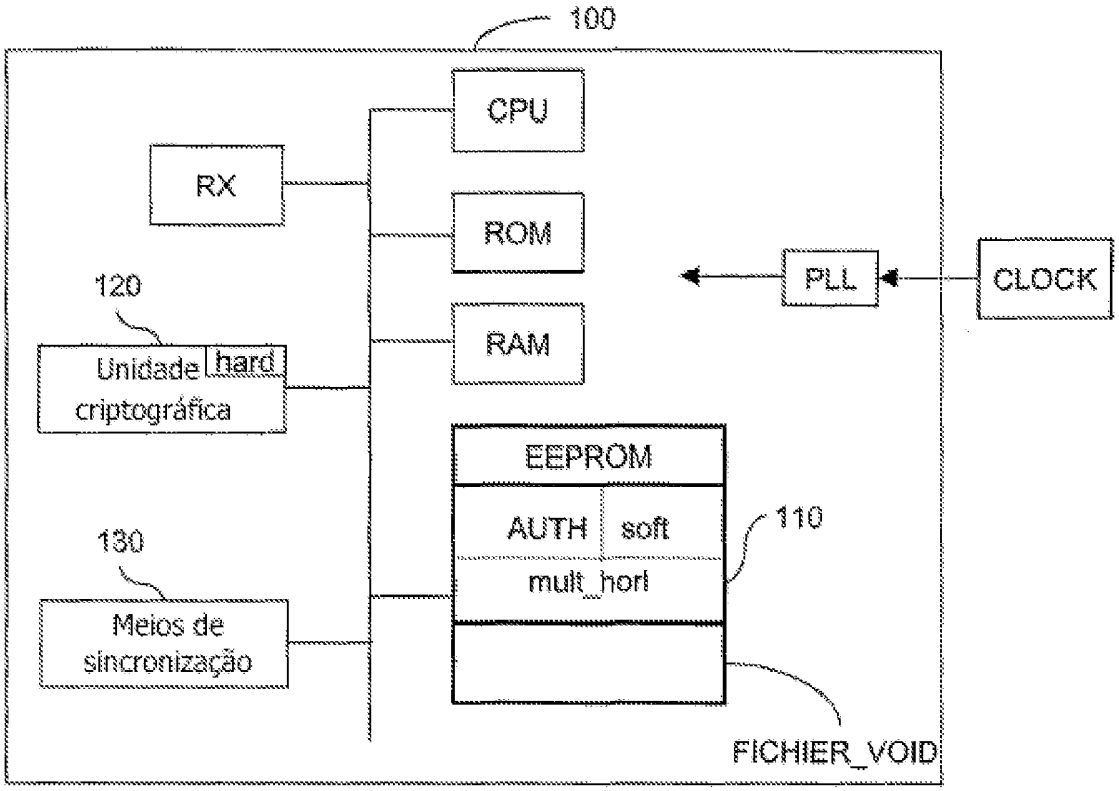


FIGURA 1

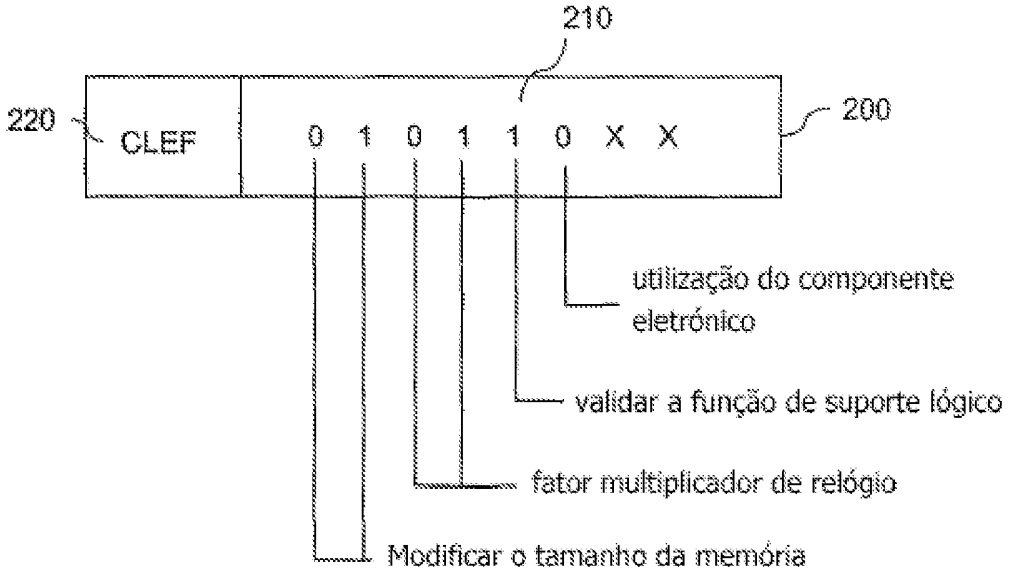


FIGURA 2

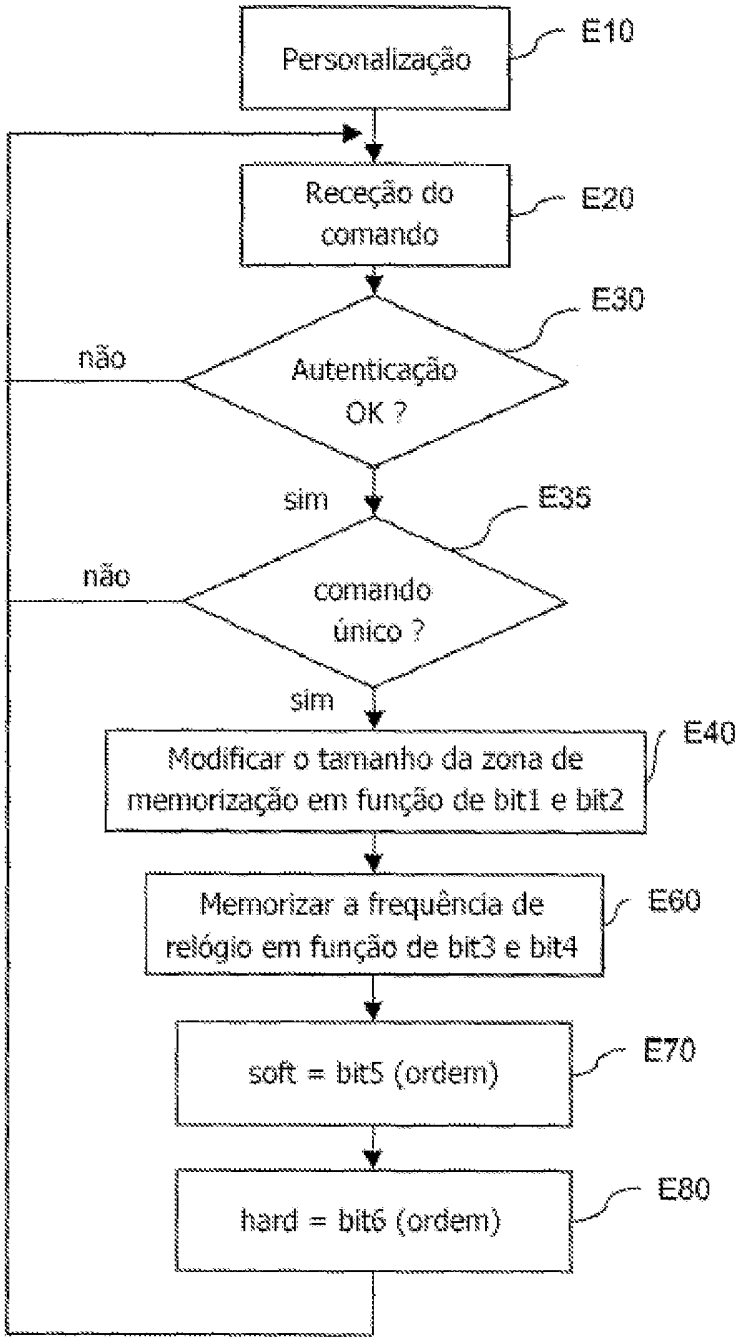

Personalização
E10
Receção do comando
E20
E30
não
Autenticação OK ?
sim
E35
não
comando único ?
sim
E40
Modificar o tamanho da zona de memorização em função de bit1 e bit2
Memorizar a frequência de relógio em função de bit3 e bit4
E60
soft = bit5 (ordem)
E70
hard = bit6 (ordem)
E80

FIGURA 3