República Federativa do Brasil
Ministério do Desenvolvimento, Indústria
e do Comércio Exterior
Instituto Nacional da Propriedade Industrial

(21) BR 102014004427-2 A2

(22) Data do Depósito: 25/02/2014

(43) Data da Publicação: 17/11/2015
(RPI 2341)

(54) Título: DISPOSITIVO PARA GERAR UMA CHAVE CRIPTOGRAFADA E MÉTODO PARA FORNECER UMA CHAVE CRIPTOGRAFADA PARA UM RECEPTOR

(51) Int. Cl.: H04L 9/00; H04L 9/08

(52) CPC: H04L 9/006; H04L 9/08

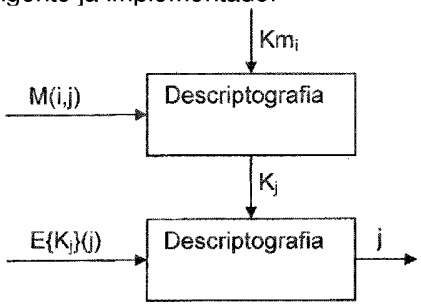
(30) Prioridade Unionista: 04/03/2013 EP 13305245.6

(73) Titular(es): THOMPSON LICENSING

(72) Inventor(es): ERIC DESMICHT, OLIVIER COURTAY, RENAUD RIGAL

(74) Procurador(es): NELLIE D SHORES

(57) Resumo: DISPOSITIVO PARA GERAR UMA CHAVE CRIPTOGRAFADA E MÉTODO PARA FORNECER UMA CHAVE CRIPTOGRAFADA PARA UM RECEPTOR. Um dispositivo (100) para gerar uma chave mestra criptografada. O dispositivo (100) compreende pelo menos uma interface de entrada configurada para receber um identificador de receptor (STBi), um identificador de provedor de serviços (Id(k)) e uma chave mestra (Kmj,k) para o provedor de serviços; uma memória configurada para armazenar um segredo do dispositivo; um processador configurado para: processar o identificador de receptor usando o segredo para obter uma chave raiz (Kri), processar o identificador de provedor de serviços usando a chave raiz para obter uma chave superior (Kti,k) e processar a chave mestra usando a chave superior para obter uma chave mestra criptografada (W(i,k)); e uma interface de saída configurada para enviar a chave mestra criptografada. Também é fornecido um método para fornecer uma chave mestra criptografada para um receptor. Uma vantagem é que o dispositivo pode capacitar um novo provedor de serviços para fornecer serviços para um receptor usando um cartão inteligente já implementado.



"DISPOSITIVO PARA GERAR UMA CHAVE CRIPTOGRAFADA E MÉTODO PARA FORNECER UMA CHAVE CRIPTOGRAFADA PARA UM RECEPTOR"

CAMPO TÉCNICO

[001]A presente invenção diz respeito de uma maneira geral a sistemas criptográficos e em particular à capacitação de uma implementação de serviço necessitando de chaves criptográficas fornecidas por novos provedores de serviços de uma maneira segura.

ANTECEDENTES

[002]Esta seção é pretendida para apresentar ao leitor vários aspectos da técnica, os quais podem estar relacionados com vários aspectos da presente invenção que serão descritos e/ou reivindicados a seguir. Acredita-se que esta discussão seja útil ao prover o leitor com informação anterior para facilitar um melhor entendimento dos vários aspectos da presente invenção. Desta maneira, deve ser entendido que estas declarações são para ser lidas com esta finalidade, e não como admissões de técnica anterior.

[003]Sistemas de acesso condicional (os quais serão usados como um exemplo não limitativo) para televisão (e outras mídias) têm sido usados por toda parte desde muito tempo para proteger diferentes tipos de conteúdo. Falando de forma resumida, em um sistema como este, um provedor de serviços obtém conteúdo de um provedor de conteúdo e usa o sistema de acesso condicional (CAS) para proteger o conteúdo, notavelmente usando criptografia, antes da entrega para um cliente. O cliente de uma maneira geral tem algum tipo de decodificador que implementa parte do sistema de acesso condicional e assim verifica se o usuário tem os direitos para acessar o conteúdo e, se assim, descriptografa e renderiza o conteúdo.

[004]Tal como é bem conhecido, no usuário final, a parte do CAS frequentemente é implementada em um cartão inteligente (o qual será usado neste documento como

um exemplo não limitativo de um módulo de segurança) que é inserido de modo removível no decodificador. O cartão inteligente é fornecido, pelo menos indiretamente, pelo provedor CAS que garante a segurança do sistema: não deve ser possível extrair do cartão inteligente nem a chave mestra decodificadora Km_i nem as chaves que são obtidas por meio de seu uso.

[005]A figura 1 ilustra um primeiro esquema de técnica anterior para acessar um serviço. Para permitir a um decodificador equipado com um cartão inteligente com identificador STBi acesso a um serviço j, criptografado usando uma chave de serviço K_j (vantajosamente comum para todos os decodificadores no sistema), o provedor de serviços criptografa o serviço j usando um algoritmo de criptografia simétrica (tal como, por exemplo, o Padrão de Criptografia Avançado, AES) e a chave de serviço K_j antes da transmissão. O provedor de serviços também criptografa a chave de serviço K_j, a qual pode ser comum para todos os decodificadores, usando uma chave que corresponde à chave mestra Km_i e, preferivelmente, ao algoritmo de criptografia simétrica e transmite o serviço criptografado $E\{K_j\}(j)$ e uma mensagem M(i,j) com a chave de serviço criptografada para o decodificador.

[006]O decodificador primeiro descriptografa a mensagem M(i,j) usando o algoritmo de criptografia simétrica e sua chave mestra Km_i para obter a chave de serviço K_j que é usada com o algoritmo de criptografia simétrica para descriptografia do serviço criptografado $E\{K_j\}(j)$ para obter o serviço j. Uma vez que a chave mestra Km_i é específica para o decodificador, ele é o único decodificador que pode descriptografar o serviço usando a mensagem M(i,j).

[007]A figura 2 ilustra um segundo esquema de técnica anterior para acesso a um serviço. A fim de capacitar mais flexibilidade e mais segurança no sistema, frequentemente é preferível usar uma chave de sessão $Ks_{j,t}$ para o serviço j e, tipicamente, um período de tempo t. Neste caso o provedor de serviços criptografa o serviço j usando a chave de sessão $Ks_{j,t}$ para obter um serviço criptografado $E\{Ks_{j,t}\}(j)$, cripto-

grafa a chave de sessão Ks(j,t) usando a chave de serviço K_j para obter uma primeira mensagem T(j,t), e criptografa a chave de serviço K_j usando a chave mestra decodificadora Km_i para obter uma segunda mensagem M(i,j). O serviço criptografado $E\{K_{j,t}\}(j)$, a primeira mensagem T(j,t) e a segunda mensagem M(i,j) são enviados, não necessariamente ao mesmo tempo, para o decodificador.

[008]Tal como na figura 1, o decodificador reverte as operações. Ele descriptografa a segunda mensagem M(i,j) usando a chave mestra decodificadora Km_i para obter a chave de serviço K_j, e descriptografa a primeira mensagem T(j,t) usando a chave de serviço K_j para obter a chave de sessão que é usada para descriptografar o serviço criptografado $E\{Ks_{j,t}\}(j)$ para obter o serviço j.

[009]Os esquemas ilustrados nas figuras 1 e 2 trabalham bem em sistemas com um único provedor de serviços. Entretanto, recentemente os decodificadores começaram a evoluir a partir de 'meramente' fornecer descriptografia de conteúdo para incluir novas aplicações. Exemplos de tais novas aplicações compreendem:

•Transmissão de serviços de valores agregados, em um formato compactado, destinados para outros dispositivos na rede doméstica do usuário, por exemplo, um segundo decodificador, um telefone inteligente ou um computador tabular.

•Transferência e execução de aplicações tais como jogos de um armazenamento de aplicações (por exemplo, Apple Store, Freebox Revolution).

•O provedor de conteúdo pode fornecer serviços de valores agregados via decodificador para o usuário, em que os serviços de valores agregados não estão sob o controle do provedor de serviços ou do provedor CAS.

[010]Isto significa que as responsabilidades do CAS estão evoluindo. Anteriormente fiadores para a segurança do sistema total, eles se tornaram responsáveis pela segurança dos serviços de valores agregados do provedor de serviços enquanto que eles ao mesmo tempo 'compartilham' o decodificador com outros provedores de serviços 'secundários'.

[011]É provável que os provedores de serviços secundários demandem sua própria funcionalidade de segurança para proteger seus serviços no decodificador e que esta funcionalidade forneça um nível de segurança pelo menos igual àquele do CAS.

[012]É possível adicionar mais provedores de serviços, por exemplo, ao adicionar um andar em cima dos elementos ilustrados nas figuras 1 e 2. Um esquema como este está ilustrado na figura 3 que estende o esquema ilustrado na figura 1.

[013]Os provedores de serviços adicionais têm suas chaves mestras $Km_{i,k}$, criptografadas usando uma chave raiz para STBi Kr_i para obter uma chave mestra criptografada W(i,k), onde i é o índice de STBi e k é o índice do provedor de serviços. Esta chave mestra criptografada W(i,k) pode ser obtida usando o cartão inteligente ao fornecer a chave mestra $Km_{i,k}$ para o cartão inteligente que, desde que um fusível específico não tem sido estourado, criptografa a chave mestra $Km_{i,k}$ usando a chave raiz Kr_i e produz a chave mestra criptografada W(i,k). A chave mestra criptografada W(i,k) pode então ser armazenada fora do cartão inteligente, por exemplo, em uma memória flash. Entretanto, uma vez que o fusível é estourado, o cartão inteligente não criptografa chaves, e ele somente descriptografa chaves criptografadas.

[014]É para ser notado que não é necessário conhecer a chave raiz, mas é impossível adicionar provedores de serviços durante a vida útil do cartão inteligente, uma vez que o fusível por razões de segurança é estourado antes da entrega para o usuário final. Embora criptografia seja igual à descriptografia em criptografia simétrica, não é possível fornecer uma chave para 'descriptografia' e esperar para obter a chave 'descriptografada', sendo a mesma tal como criptografada, uma vez que somente o serviço descriptografado é produzido pelo cartão inteligente; as chaves intermediárias ficam retidas no interior.

[015]O decodificador i recebe a chave mestra criptografada W(i,k) e a descriptografa usando a chave raiz Kr_i e produz a chave mestra $Km_{i,k}$, a qual é usada para descriptografar uma segunda mensagem (M,i,j,k) para obter uma chave de serviço

$K_{j,k}$ para o provedor de serviços k. A chave de serviço $K_{j,k}$ é então usada para descriptografar o serviço criptografado $E\{Ks_{j,k}\}(j,k)$ para obter o serviço j,k livre de suspeita.

[016]Tal como pode ser visto, existem diversos autores envolvidos: um fabricante de cartão inteligente, um integrador que fabrica o decodificador, um ou mais provedores de serviços e cliente que fornece o decodificador para os usuários finais. Embora as soluções de técnica anterior permitam personalizar o cartão inteligente para trabalhar com diversos provedores de serviços ao adicionar suas chaves, o número está limitado ao número de fusíveis em uma memória flash Programável Uma Única Vez no cartão inteligente (um fusível é estourado por chave adicionada). Além do mais, uma vez que as chaves devem ser adicionadas na fábrica usando uma máquina especial, estes provedores de serviços devem ser conhecidos antes de o cartão inteligente personalizado ser entregue.

[017]Será assim percebido que existe uma necessidade de um sistema que permita a um usuário final acessar provedores de serviços não considerados inicialmente. Por razões de segurança, o fabricante de decodificador deve controlar a adição de provedores de serviços, e as chaves secretas dos provedores de serviços não devem ser tornadas conhecidas para outros autores, em particular para outros provedores de serviços.

[018]A presente invenção fornece uma possibilidade como esta.

SUMÁRIO DA INVENÇÃO

[019]Em um primeiro aspecto, a invenção diz respeito a um dispositivo para gerar uma chave mestra criptografada. O dispositivo compreende pelo menos uma interface de entrada configurada para receber um identificador de receptor, um identificador de provedor de serviços e uma chave mestra para o provedor de serviços; uma memória configurada para armazenar um segredo do dispositivo; um processador configurado para: processar o identificador de receptor usando o segredo para obter

uma chave raiz, processar o identificador de provedor de serviços usando a chave raiz para obter uma chave superior, e processar a chave mestra usando a chave superior para obter uma chave mestra criptografada; e uma interface de saída configurada para enviar a chave mestra criptografada.

[020]Em uma primeira modalidade o dispositivo é implementado em um Módulo Seguro de Hardware.

[021]Em uma segunda modalidade, o dispositivo é implementado em um cartão inteligente.

[022]Em uma terceira modalidade, o processador é configurado para descriptografar o identificador de receptor usando o segredo como chave de descriptografia.

[023]Em uma quarta modalidade, o processador é configurado para criptografar o identificador de provedor de serviços usando a chave raiz como chave de criptografia.

[024]Em uma quinta modalidade, o processador é configurado para criptografar a chave mestra usando a chave superior como chave de criptografia.

[025]Em um segundo aspecto, a invenção diz respeito a um método de fornecer uma chave mestra criptografada para um receptor. Um dispositivo para gerar uma chave mestra criptografada de acordo com o primeiro aspecto recebe um identificador de receptor (STB_i), um identificador de provedor de serviços (Id(k)) e uma chave mestra ($Km_{j,k}$) para o provedor de serviços gerar a chave mestra criptografada de um primeiro dispositivo; gera a chave mestra criptografada; e produz a chave mestra criptografada gerada que é enviada, por meio de um terceiro dispositivo, para o receptor.

DESCRIÇÃO RESUMIDA DOS DESENHOS

[026]Recursos preferidos da presente invenção serão descritos agora, por meio de exemplo não limitativo, com referência aos desenhos anexos, nos quais:

[027]A figura 1 ilustra um primeiro esquema de técnica anterior para acesso a um

serviço;

[028]A figura 2 ilustra um segundo esquema de técnica anterior para acesso a um serviço;

[029]A figura 3 ilustra um terceiro esquema de técnica anterior para acesso a um serviço;

[030]A figura 4 ilustra acessar um serviço de acordo com uma modalidade preferida da presente invenção; e

[031]A figura 5 ilustra um Módulo de Segurança de Hardware de acordo com uma modalidade preferida da presente invenção.

DESCRIÇÃO DE MODALIDADES

[032]As soluções de técnica anterior exigem que o fabricante de decodificador conheça os provedores de serviços antes de os decodificadores serem fabricados.

[033]Adicionar um andar de chave extra torna possível contornar este problema. Adicionalmente, cada provedor de serviços tem um identificador único Id(k) que não tem que ser secreto e um dispositivo que gera chaves mestras criptografadas, tal como será descrito adicionalmente em seguida.

[034]A figura 4 ilustra acessar um serviço de acordo com uma modalidade preferida da presente invenção, a qual é uma extensão do esquema ilustrado na figura 3. Um processador tal como um cartão inteligente ou um criptoprocessador em um Sistema em Um chip do decodificador i tem acesso à sua chave raiz Kr_i em um de pelo menos dois modos: a chave raiz pode estar gravada na sua memória ou ela pode ser gerada ao usar um segredo do processador para descriptografar uma chave raiz criptografada – a última opção está ilustrada na caixa tracejada. O processador recebe o identificador Id(k) do provedor de serviços k e o descriptografa usando sua chave raiz Kr_i para obter uma chave superior $Kt_{i,k}$ para o processador e o provedor de serviços. A chave mestra criptografada W(i,k) é descriptografada usando a chave superior $Kt_{i,k}$ para obter a chave mestra $Km_{i,k}$, a qual é usada para descriptografar

uma segunda mensagem (M,i,j,k) para obter uma chave de serviço $K_{j,k}$ para o provedor de serviços k. A chave de serviço $K_{j,k}$ é então usada para descriptografar o serviço criptografado $E\{Ks_{j,k}\}(j,k)$ para obter o serviço j,k livre de suspeita.

[035]O provedor de serviços k obtém a chave mestra criptografada W(i,k) para o usuário i de uma maneira segura usando um assim chamado de Módulo de Segurança de Hardware (HSM) 100 fornecido pelo fabricante de decodificador, tal como ilustrado na figura 5. O HSM 100 é implementado para manter sua informação secreta ocultada para o exterior. O HSM 100 compreende pelo menos um processador 110 e outros recursos necessários, mas não ilustrados para efeito de clareza, tais como interfaces de entrada e saída, memória, conexões internas e uma fonte de energia (cuja energia pode ser fornecida pelo exterior).

[036]O HSM 100 recebe, de um dispositivo, o identificador STBi de um receptor, o identificador de provedor de serviços Id(k) e a chave mestra $Km_{i,k}$ para o provedor de serviços e o receptor. O processador 110 obtém, de uma memória interna, o segredo do HSM e o usa para descriptografar o identificador STBi para obter uma chave raiz Kr_i. O processador usa então a chave raiz Kr_i para criptografar o identificador de provedor de serviços Id(k) para obter a chave superior $Kt_{i,k}$ que é então usada para criptografar a chave mestra $Km_{i,k}$ para obter a chave mestra criptografada W(i,k) que é então produzida pelo HSM 100 e enviada para o decodificador i onde ela pode ser usada para acessar o serviço. Uma vez que a chave mestra criptografada W(i,k) já está criptografada, não existe necessidade de criptografá-la adicionalmente para a transmissão (usando qualquer dispositivo e método de transmissão adequados tais como mensagem de correio eletrônico ou transmissão na mesma banda) para o decodificador. Deve ser notado que em criptografia simétrica, criptografia e descriptografia são essencialmente idênticas.

[037]Será percebido que, uma vez que a chave superior $Kt_{i,k}$ não é produzida pelo HSM 100, ela não pode ser mudada pelo provedor de serviços, o que significa que

os provedores de serviços ficam isolados uns dos outros a partir de um ponto de vista de segurança.

[038]Os versados na técnica compreenderão que a presente invenção pode fornecer uma solução que permite a um cartão inteligente acessar novos provedores de serviços de uma maneira segura.

[039]Cada recurso revelado na descrição e (onde apropriado) nas reivindicações e desenhos pode ser fornecido independentemente ou em qualquer combinação apropriada. Recursos descritos como sendo implementados em hardware também podem ser implementados em software, e vice-versa. Os números de referência que aparecem nas reivindicações são somente a título de ilustração e não devem ter efeito limitativo sobre o escopo das reivindicações.

REIVINDICAÇÕES

1. Dispositivo (100) para gerar uma chave mestra criptografada, o dispositivo (100) **CARACTERIZADO** pelo fato de que compreende:

- pelo menos uma interface de entrada configurada para receber um identificador de receptor (STB_i), um identificador de provedor de serviços (Id(k)) e uma chave mestra ($Km_{j,k}$) para o provedor de serviços;

- uma memória configurada para armazenar um segredo do dispositivo;

- um processador configurado para:

- processar o identificador de receptor usando o segredo para obter uma chave raiz (Kr_i);

- processar o identificador de provedor de serviços usando a chave raiz para obter uma chave superior ($Kt_{i,k}$); e

- processar a chave mestra usando a chave superior para obter uma chave mestra criptografada (W(i,k)); e

- uma interface de saída configurada para enviar a chave mestra criptografada.

2. Dispositivo, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o dispositivo é implementado em um Módulo Seguro de Hardware.

3. Dispositivo, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o dispositivo é implementado em um cartão inteligente.

4. Dispositivo, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o processador é configurado para descriptografar o identificador de receptor usando o segredo como chave de descriptografia.

5. Dispositivo, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o processador é configurado para criptografar o identificador de provedor de serviços usando a chave raiz como chave de criptografia.

6. Dispositivo, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fa-

to de que o processador é configurado para criptografar a chave mestra usando a chave superior como chave de criptografia.

7. Método de fornecer uma chave mestra criptografada para um receptor, o método **CARACTERIZADO** pelo fato de que compreende as etapas de:

- receber, por meio de um dispositivo para gerar uma chave mestra criptografada de acordo com a reivindicação 1, um identificador de receptor (STB_i), um identificador de provedor de serviços (Id(k)) e uma chave mestra ($Km_{j,k}$) para o provedor de serviços gerar a chave mestra criptografada de um primeiro dispositivo;

- gerar, pelo dispositivo para gerar uma chave mestra criptografada, a chave mestra criptografada;

- produzir, pelo dispositivo para gerar uma chave mestra criptografada, a chave mestra criptografada gerada; e

- enviar, por meio de um terceiro dispositivo, a chave mestra criptografada para o receptor.

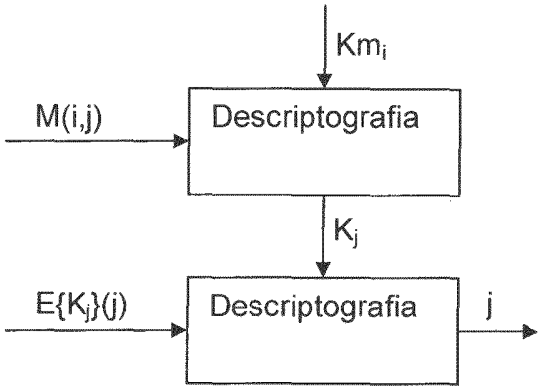

Km$_i$
M(i,j)
Descriptografia
K$_j$
E{K$_j$}(j)
Descriptografia
j

Fig.1

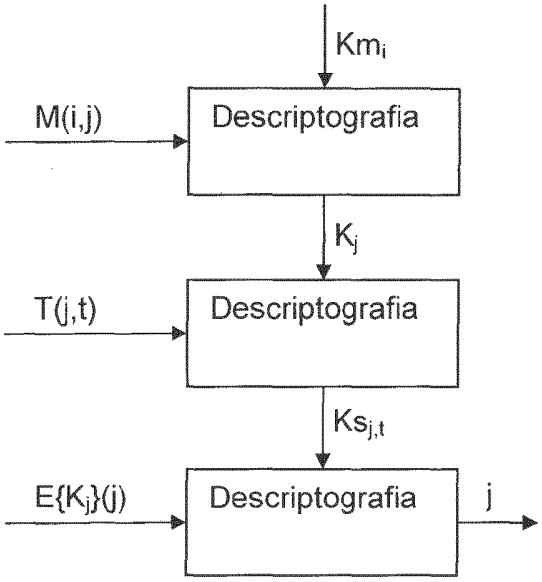

Km$_i$
M(i,j)
Descriptografia
K$_j$
T(j,t)
Descriptografia
Ks$_{j,t}$
E{K$_j$}(j)
Descriptografia
j

Fig.2

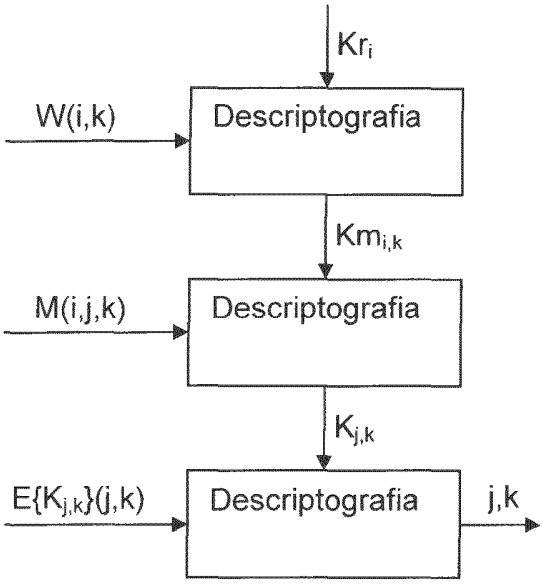

Kr$_i$
W(i,k)
Descriptografia
Km$_{i,k}$
M(i,j,k)
Descriptografia
K$_{j,k}$
E{K$_{j,k}$}(j,k)
Descriptografia
j,k

Fig.3

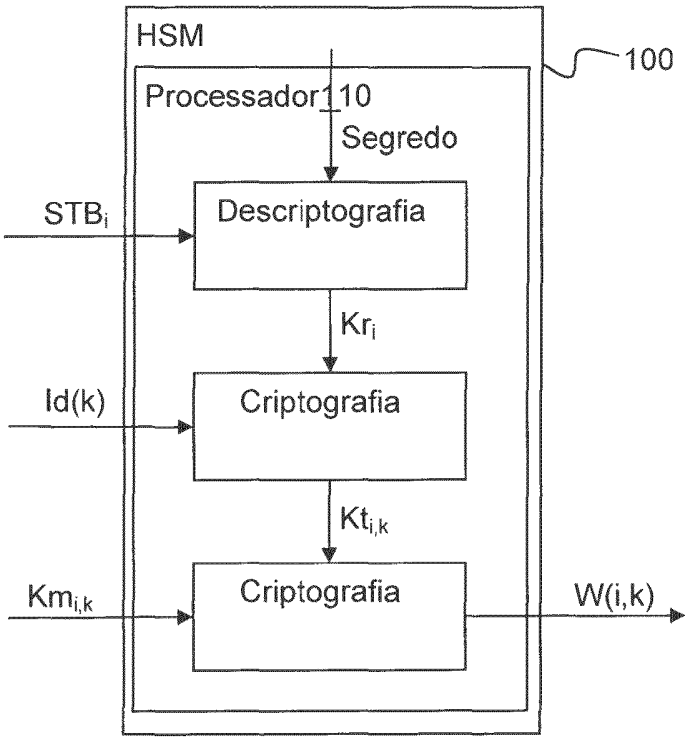

HSM
100
Processador 110
Segredo
STB$_i$
Descriptografia
Kr$_i$
Id(k)
Criptografia
Kt$_{i,k}$
Km$_{i,k}$
Criptografia
W(i,k)

Fig.5

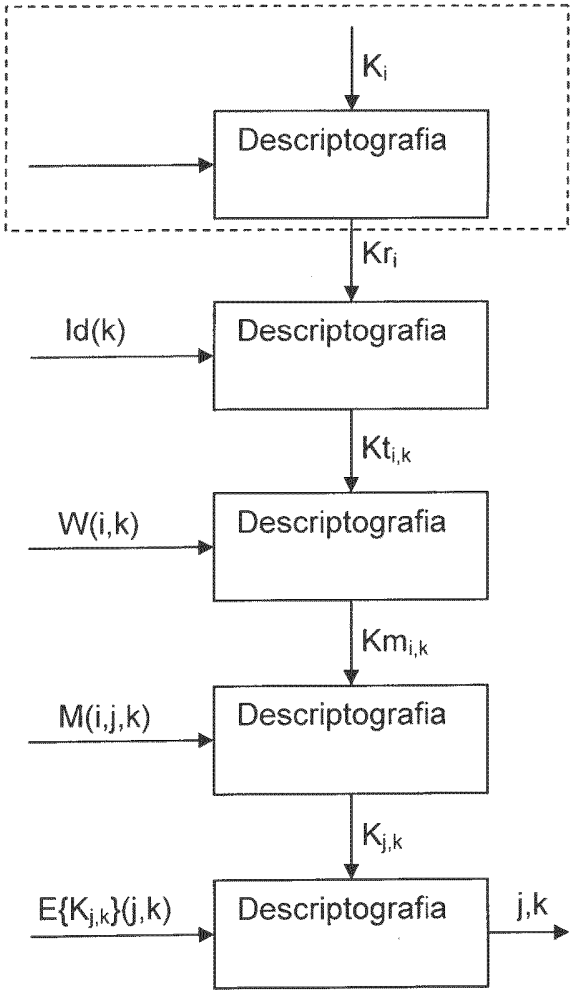

K_i
Descriptografia
Kr_i
Id(k)
Descriptografia
$Kt_{i,k}$
W(i,k)
Descriptografia
$Km_{i,k}$
M(i,j,k)
Descriptografia
$K_{j,k}$
$E\{K_{j,k}\}(j,k)$
Descriptografia
j,k

Fig.4

RESUMO

"DISPOSITIVO PARA GERAR UMA CHAVE CRIPTOGRAFADA E MÉTODO PARA FORNECER UMA CHAVE CRIPTOGRAFADA PARA UM RECEPTOR"

Um dispositivo (100) para gerar uma chave mestra criptografada. O dispositivo (100) compreende pelo menos uma interface de entrada configurada para receber um identificador de receptor (STBi), um identificador de provedor de serviços (Id(k)) e uma chave mestra ($Km_{j,k}$) para o provedor de serviços; uma memória configurada para armazenar um segredo do dispositivo; um processador configurado para: processar o identificador de receptor usando o segredo para obter uma chave raiz (Kr_i), processar o identificador de provedor de serviços usando a chave raiz para obter uma chave superior ($Kt_{i,k}$) e processar a chave mestra usando a chave superior para obter uma chave mestra criptografada (W(i,k)); e uma interface de saída configurada para enviar a chave mestra criptografada. Também é fornecido um método para fornecer uma chave mestra criptografada para um receptor. Uma vantagem é que o dispositivo pode capacitar um novo provedor de serviços para fornecer serviços para um receptor usando um cartão inteligente já implementado.