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

(21) **PI 1102918-8 A2**

BRPI1102918A2

(22) Data de Depósito: 03/06/2011
(43) Data da Publicação: 19/03/2013
(RPI 2202)

(51) Int.Cl.:
G06F 13/12
H04L 9/06

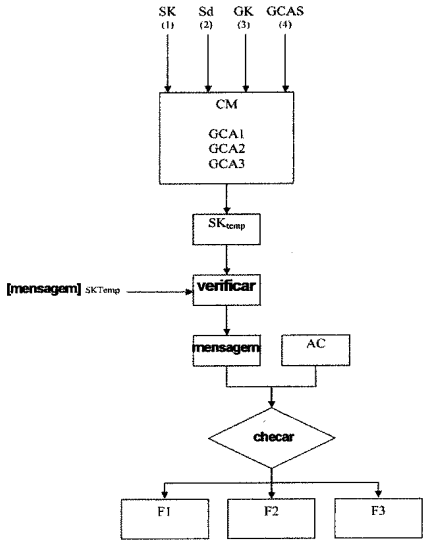
(54) Título: MÉTODO PARA ATIVAR PELO MENOS UMA FUNÇÃO EM UM CHIPSET E CHIPSET PARA A IMPLEMENTAÇÃO DO MÉTODO

(30) Prioridade Unionista: 04/06/2010 EP 10165003.4

(73) Titular(es): Nagravision S.A.

(72) Inventor(es): Didier Hunacek, Patrick Servet

(57) Resumo: MÉTODO ATIVAR PELO MENOS UMA FUNÇÃO EM UM CHIPSET E CHIPSET PARA A IMPLEMENTAÇÃO DO MÉTODO. A presente invenção refere-se a um método para ativar uma função de um chipset compreendendo pelo menos uma memória e um módulo de cálculo encarregado de operações criptográficas, a memória contendo pelo menos uma semente e o módulo de cálculo contendo pelo menos um algoritmo critográfico, esse método compreendendo as etapas de: receber pelo menos uma de segmentação, uma chave global e um seletor de algoritmo criptográfico global; trasmitir pelo menos dois de : a semente, a chave de segmentação recebida, a chave global e o setor de algoritmo criptográfico global para o módulo de cálculo, a semente, a chave de segmentação recebida, a chave global e o seletor de algoritmo criptográfico global sendo fornecidos por pelo menos duas entidades diferentes; gerar no módulo de cálculo, uma chave temporária utilizando um de pelo menos um algoritmo criptográfico do módulo de cálculo e pelo menos dois elementos entre a semente, a chave de segmentação, a chave global e o seletor de algoritmo criptográfico global; receber uma mensagem de ativação pelo módulo de cálculo; receber um código de autenticação da mensagem pelo módulo de cálculo, o código de autenticação de mensagem sendo computado utilizando a chave temporária; verificar a autenticação de mensagem e a chabe temporária; se a mensagem recebida for autêntica, ativar uma função correspondente do chipset; se a mensagem recebida não for autência, negar a ativação da função correspondente do chipset.



"MÉTODO PARA ATIVAR PELO MENOS UMA FUNÇÃO EM UM CHIPSET E CHIPSET PARA A IMPLEMENTAÇÃO DO MÉTODO"

CAMPO TÉCNICO

A presente invenção refere-se a um método para ativar pelo menos uma função de um chipset que compreende pelo menos uma memória e um módulo de cálculo encarregado de operações criptográficas. Refere-se ainda a um chipset seguro que implementa o método da invenção.

Esse chipset pode, por exemplo, ser utilizado em unidades de usuário destinadas a permitir acesso a dados de acesso condicional como conteúdo de TV paga. Pode ser utilizado essencialmente em qualquer dispositivo em que a segurança do chipset seja uma questão importante.

TÉCNICA ANTECEDENTE

Um chipset como utilizado na presente invenção é um conjunto de circuitos eletrônicos que permite que um processador gerencie trocas de dados entre componentes diferentes de um dispositivo ou uma unidade de usuário. A execução de operações no nível de chipset tem como objetivo evitar todo ataque de material que consiste em analisar os sinais permutados para descobrir as chaves específicas para o dispositivo ou unidade de usuário. Desse modo, a chave de chipset não é acessível do exterior do chipset.

Em alguns dos chipsets seguros existentes, uma chave exclusiva é introduzida no chipset na fabricação. A chave de chipset pode ser armazenada em uma memória de chipset e pode ser hard coded de modo que não seja possível modificar essa chave de modo fraudulento. Chaves adicionais também podem ser calculadas de tal chave de chipset de modo que, por um lado, a chave de chipset hard coded não possa ser modificada e por outro lado, chaves diferentes poderiam ser obtidas por modificar o cálculo da chave. O cálculo da chave poderia ser feito por uma concatenação, uma criptografia ou qualquer outra combinação da chave de chipset e um número que pode ser aleatório ou não.

Todas as chaves que são introduzidas posteriormente no chipset ou no dispositivo dependem de um modo ou de outro dessa chave de chipset inicial. Como exemplo no campo de TV de acesso condicional, os direitos que são utilizados para controlar o acesso a um conteúdo criptografado são criptografados por uma chave de decodificador pertinente a esse decodificador. Essa chave de decodificador é enviada para o decodificador em questão criptografada pela chave de chipset inicial. Desse modo, se a chave de chipset inicial estiver comprometida, a chave de decodificador também está comprometida, bem como o próprio conteúdo.

Essa chave inicial não pode ser alterada durante o tempo de vida do chipset. Isso é importante no caso da chave de chipset ser introduzida em um ambiente perfeitamente seguro. Se essa chave de chipset não for introduzida em condições de segurança estrita, a

segurança do chipset e da unidade de usuário não podem ser garantidas. Como a chave de chipset não pode ser trocada, se a chave inicial não for perfeitamente segura, não é possível aumentar a segurança posteriormente.

A chave inicial é sempre introduzida na fabricação do chipset. Entretanto, essa chave deve ser ativada se condições específicas forem atendidas em particular com relação à configuração do chipset. Na prática, imediatamente após a fabricação do chipset ou durante sua fabricação, testes de configuração devem ser passados pelo chipset para verificar se a configuração corresponde a exigências específicas, em particular exigências relacionadas a questões de segurança. Esses testes de configuração são realizados pelo fabricante que é o único que pode controlar os mesmos. Desse modo, é possível que a chave inicial seja ativada embora nem todos os testes de configuração tenham tido sucesso. A falha em cumprir com todas as exigências pode ser feita de forma fraudulenta ou por erro e pode levar a violações de segurança. Em qualquer caso, não há solução para evitar tal ativação incorreta da chave se todos os testes não forem aprovados. Em tal caso, a segurança da unidade de usuário não pode ser garantida.

Nos chipsets seguros da técnica anterior, como os testes de configuração podem ser realizados somente pelo fabricante, os testes são aprovados e funções específicas são ativadas ou os testes não são aprovados e as funções correspondentes não são ativadas. Não é possível acrescentar novas características após conclusão do processo de fabricação.

A patente número US 5.883.956 descreve uma unidade de processamento seguro (SPU) na qual funções podem ser dinamicamente configuradas após o chipset ter sido instalado em um dispositivo, o dispositivo estando nas dependências de um usuário. Uma autoridade confiável reconfigura a unidade de processamento seguro, utilizando uma tabela de capacidade e uma assinatura digital. A tabela de capacidade é formada em um headend e é hashed para obter uma compilação de mensagem. A compilação de mensagem é criptografada com a chave particular da unidade de processamento seguro para obter uma assinatura. A tabela de capacidade e a assinatura digital são enviadas para a unidade de processamento seguro. Na SPU, a compilação de mensagem é decriptografada com a chave pública de autoridade confiável.

Nesse dispositivo seguro, uma chave particular é exigida para permutar dados entre a headend e a unidade de processamento seguro. Essa chave particular é introduzida na SPU durante a fabricação ou derivada de uma chave que é introduzida durante a fabricação. Portanto, se essa chave estiver comprometida, os direitos também podem estar comprometidos.

Desse modo, a solução descrita em US 5.883.956 provê meio para adicionar ou retirar direitos ou funções em um chipset, porém a segurança das operações no chipset de-

pende da segurança da chave inicial. Essa chave inicial é definida por uma entidade, normalmente o fabricante do chipset, que pode definir a chave mesmo se todas as exigências não forem atendidas. Como somente uma entidade define a chave a partir da qual todas as outras chaves derivam, nenhuma outra entidade pode verificar e confirmar que todas as exigências são atendidas.

A publicação WO 2006/091304 se refere a um sistema e a um método para preparar e transmitir para pelo menos um chipset, chaves ou direitos dependendo tanto de uma região geográfica como de um fuso horário. O método é utilizado para fornecer funções blackout. Essas chaves ou direitos dependem de uma chave inicial contida no chipset em questão. Desse modo, se a chave inicial for comprometida, a segurança do chipset inteiro também está comprometida.

REVELAÇÃO DA INVENÇÃO

Um objetivo da invenção é fornecer um chipset seguro no qual seja possível garantir que todas as exigências são atendidas antes de ativar o chipset.

Outro objetivo da invenção é ativar funções adicionais após as etapas de fabricação do chipset. Essas funções adicionais são, entretanto, ativadas somente quando condições específicas são atendidas.

Ainda outro objetivo da invenção é fornecer uma possibilidade de alterar uma chave de chipset se parecer que essa chave de chipset está comprometida.

Os objetivos da presente invenção são obtidos por um método para ativar uma função de um chipset que compreende pelo menos uma memória e um módulo de cálculo encarregado de operações criptográficas, a memória contendo pelo menos uma semente e o módulo de cálculo contendo pelo menos um algoritmo criptográfico, esse método compreendendo as etapas de:

- receber pelo menos uma de uma chave de segmentação (SK), uma chave global (GK) e um seletor de algoritmo criptográfico global (GCAS);

- transmitir pelo menos dois de: a semente, a chave de segmentação recebida (SKI), a chave global (GK) e o seletor de algoritmo criptográfico global (GCAS) para o módulo de cálculo, a semente, a chave de segmentação recebida, a chave global e o seletor de algoritmo criptográfico global sendo fornecidos por pelo menos duas entidades diferentes;

- gerar no módulo de cálculo, uma chave temporária (SK_{temp}) utilizando um de pelo menos um algoritmo criptográfico do módulo de cálculo e pelo menos dois elementos entre a semente (Sd), a chave de segmentação (SK), a chave global (GK) e o seletor de algoritmo criptográfico global (GCAS);

- receber uma mensagem de ativação pelo módulo de cálculo;

- receber um código de autenticação da mensagem pelo módulo de cálculo (CM), o código de autenticação de mensagem (MAC) sendo computado utilizando a chave temporá-

ria (SK_{temp});

- verificar a autenticidade da mensagem recebida utilizando o código de autenticação de mensagem (MAC) e a chave temporária (SK_{temp});

- se a mensagem recebida for autêntica, ativar uma função correspondente (F1, F2, F3) do chipset;

- se a mensagem recebida não for autêntica, negar a ativação da função correspondente do chipset.

Os objetivos da invenção são também obtidos por um chipset que compreende pelo menos uma memória e um módulo de cálculo encarregado de operações criptográficas, a memória contendo pelo menos uma semente e o módulo de cálculo contendo pelo menos um algoritmo criptográfico, esse chipset compreendendo ainda:

- meio para receber pelo menos uma de uma chave de segmentação (SK), uma chave global (GK) e um seletor de algoritmo criptográfico global (GCAS);

- meio para transmitir pelo menos dois de: a semente, a chave de segmentação recebida (SKI), a chave global (GK) e o seletor de algoritmo criptográfico global (GCAS) para o módulo de cálculo, a semente, a chave de segmentação recebida, a chave global e o seletor de algoritmo criptográfico global sendo fornecidos por pelo menos duas entidades diferentes;

- meio para gerar no módulo de cálculo, uma chave temporária (SK_{temp}) utilizando um de pelo menos um algoritmo criptográfico do módulo de cálculo e pelo menos dois elementos entre a semente (Sd), a chave de segmentação (SK), a chave global (GK) e o seletor de algoritmo criptográfico global (GCAS);

- meio para receber uma mensagem de ativação pelo módulo de cálculo;

- meio para receber um código de autenticação da mensagem pelo módulo de cálculo (CM), o código de autenticação de mensagem (MAC) sendo computado utilizando a chave temporária (SK_{temp});

- meio para verificar a autenticidade da mensagem recebida utilizando o código de autenticação de mensagem (MAC) e a chave temporária (SK_{temp});

- meio para ativar uma função correspondente (F1, F2, F3) do chipset, se a mensagem recebida for autêntica; e

- meio para negar a ativação da função correspondente do chipset se a mensagem recebida não for autêntica.

Graças ao método e ao dispositivo da invenção, uma entidade, em particular, o fabricante não é capaz de ativar uma característica obrigatória do chipset sozinho. Isso significa que a segurança do chipset não pode ser comprometida por comportamento fraudulento no lado do fabricante ou por erros durante os testes finais.

O método da invenção permite ainda a substituição da chave de chipset caso a

chave esteja comprometida. Isso oferece grande flexibilidade para o uso desses chipsets.

É adicionalmente possível fornecer um chipset que tenha uma característica obrigatória inativa que pode ser ativada não no estágio de fabricação como na técnica anterior, porém posteriormente, em um estágio de personalização. Isso permite verificação dupla das exigências de ativação, uma verificação sendo feita na fabricação e a outra na ativação.

O chipset pode ter ainda somente algumas funções ou somente uma função ativada após a personalização. Funções adicionais podem ser ativadas posteriormente, enquanto o chipset já está instalado em um dispositivo e em uso.

BREVE DESCRIÇÃO DOS DESENHOS

A presente invenção e suas vantagens serão entendidas de forma melhor com referência aos desenhos em anexo e a uma descrição detalhada de uma modalidade específica, onde:

A figura 1 é uma vista esquemática do método da invenção.

MELHOR MODO PARA REALIZAR A INVENÇÃO

De acordo com a presente invenção, o chipset contém pelo menos uma memória e um módulo de cálculo CM. Durante a fabricação do chipset, a memória recebe um número de identificação exclusivo (Sd). Esse número de identificação pode ser secreto ou não.

O módulo de cálculo CM do chipset contém pelo menos um algoritmo criptográfico. De acordo com uma modalidade preferida, o algoritmo é de propriedade. Entretanto, algoritmos criptográficos bem conhecidos como, por exemplo, 3DES, AES, RSA poderiam ser também utilizados. Na figura 1, o módulo de cálculo é ilustrado com três algoritmos GCA1, GCA2 e GCA3.

Após a fabricação do chipset, o mesmo é personalizado, genericamente por outra entidade diferente do fabricante. Durante a personalização, o chipset recebe uma chave de segmentação SK. Pode receber ainda pelo menos uma de uma chave global GK ou um seletor de algoritmo criptográfico global GCAS. Desse modo, o chipset compreende pelo menos um número de identificação exclusivo que pode ser utilizado como uma semente e pelo menos um elemento entre uma chave de segmentação, uma chave global e um seletor de algoritmo criptográfico global.

Pelo menos dois elementos entre o número de identificação exclusiva, a chave de segmentação, a chave global e o seletor de algoritmo criptográfico global são enviados para o módulo criptográfico CM. No caso do seletor de algoritmo criptográfico global não ser enviado para o módulo criptográfico, um algoritmo default é utilizado. O número de identificação exclusivo pode ser utilizado como uma semente com um dos outros elementos enviados para o módulo de cálculo. O algoritmo contido no módulo criptográfico é adicionalmente utilizado para gerar uma chave temporária SK_{temp}.

Normalmente, a semente ou número de identificação exclusivo é conhecido do fa-

bricante do chipset. A chave de segmentação é conhecida do fabricante de STB e o(s) algoritmo(s) criptográfico(s) contido(s) no módulo de cálculo é (são) conhecido(s) do fornecedor de segurança. Desse modo, nem o fabricante nem a entidade de personalização sabem todos os segredos.

Como pode ser visto a partir de cima, vários trechos de informações são necessárias para formar a chave temporária. Esses trechos de informações são espalhados através de várias entidades, a saber, o fabricante, a entidade encarregada da personalização e o fornecedor de segurança. Os mesmos podem ser unidos com grande dificuldade por pessoas mal intencionadas. Isso assegura grande segurança do dispositivo contra comportamento fraudulento bem como contra erros.

De acordo com uma modalidade específica, uma característica obrigatória do chipset é inativa desde que não tenha recebido uma mensagem de ativação. O processamento da mensagem de ativação requer o uso da chave temporária SK_{temp} que foi formado como descrito acima. Uma mensagem de ativação é formada em um centro de gerenciamento, por exemplo, e é destinada a um chipset específico. A mensagem pode ser criptografada ou não. Essa mensagem de ativação é associada a um código de autenticação de mensagem, o código sendo computado utilizando a chave temporária que é sabida pelo centro de gerenciamento. A computação do código de autenticação de mensagem com a chave temporária pode ser uma criptografia ou qualquer outra operação apropriada utilizando o código de autenticação de mensagem e a chave temporária. Quando a mensagem é recebida pelo chipset, é processada para decriptografar a mesma, se necessário, e recuperar o código de autenticação de mensagem. A mensagem pode conter pelo menos duas partes. Uma parte se refere à operação que deve ser realizada se algumas condições forem atendidas. Outra parte pode conter as condições AC que devem ser atendidas antes da execução das operações. A mensagem pode conter ainda outras partes opcionais. Um exemplo de uma condição de ativação afirma que é verificado se a chave temporária SK_{temp} já está presente no chipset. A chave de segmentação SK não é armazenada se a chave temporária já estiver presente no chipset.

O código de autenticação de mensagem é computado com a chave temporária SK_{temp}. Esse código de autenticação de mensagem é processado no módulo de cálculo para obter o código de autenticação de mensagem em uma forma usável e a autenticação da mensagem é verificada. Se a mensagem for autêntica, o chipset verifica se as condições AC contidas na mensagem são atendidas. Se esse for o caso, a operação contida na mensagem e associada à lista de condições é realizada. De acordo com uma modalidade específica, a primeira função é ativar uma função obrigatória do chipset e tornar usável. A chave temporária SK_{temp} pode ser deletada após ser utilizada uma vez.

É possível que a mensagem não contenha condição. Nesse caso, somente o resul-

tado da autenticação da mensagem decide se a função é ativada ou não. Se a autenticação falhar ou as condições não forem atendidas, a função correspondente não é ativada. Outras conseqüências podem originar dependendo da implementação específica.

Durante o uso do chipset, é possível dotar esse chipset de funções adicionais F1, F2, F3. Como anteriormente, uma mensagem é enviada para o chipset, com um código de autenticação de mensagem com a chave temporária SK_{temp}. essa mensagem também contém pelo menos uma operação e uma lista de condições AC. O código de autenticação de mensagem é utilizado para verificar a autenticidade da mensagem. As condições são também verificadas e, se atendidas, a operação é realizada. A operação pode ser, por exemplo, a ativação de uma nova função do chipset.

Se as condições não forem atendidas, pelo menos a ativação da nova função não é habilitada. Outras conseqüências também podem ser implementadas. Por exemplo, se algumas condições não forem atendidas, todas ou uma parte das funções do chipset podem ser desativadas.

É possível enviar uma mensagem para cada função nova a ser ativada, com um conjunto de condições. Conjuntos diferentes de condições também podem estar contidos em uma única mensagem e possivelmente associados à mesma operação ou a operações diferentes.

De acordo com a presente invenção, é possível introduzir em um modo seguro, uma chave não somente quando o chipset é fabricado, como também posteriormente, durante um processo de customização. Isso oferece maior flexibilidade e maior segurança visto que os testes podem ser realizados duas vezes e por entidades diferentes.

No chipset da invenção, é possível alterar a chave de chipset. Desse modo, se a chave estiver comprometida, o chipset pode ser ainda utilizado, após ter trocado a chave.

De acordo com o método da invenção, o fornecer de segurança pode controlar totalmente o processo e pode em particular determinar que a configuração do chipset corresponda às características exigidas. Isso oferece maior segurança contra erros bem como contra manipulações fraudulentas.

É possível fornecer um chipset no qual uma função obrigatória seja inativa desde que não tenha recebido uma mensagem de ativação autêntica. Tal mensagem autêntica é feita e enviada por um centro de gerenciamento que é ligado ao fornecedor de segurança. Desse modo, o chipset deve corresponder às exigências no estágio de fabricação bem como no estágio de ativação. Como a fabricação e a ativação são normalmente realizadas por entidades diferentes, a segurança é aumentada.

REIVINDICAÇÕES

1. Método para ativar uma função de um chipset compreendendo pelo menos uma memória e um módulo de cálculo encarregado de operações criptográficas, a memória contendo pelo menos uma semente e o módulo de cálculo contendo pelo menos um algoritmo criptográfico, esse método sendo **CARACTERIZADO** pelo fato de que compreende as etapas de:

- receber pelo menos uma de uma chave de segmentação (SK), uma chave global (GK) e um seletor de algoritmo criptográfico global (GCAS);

- transmitir pelo menos dois de: a semente, a chave de segmentação recebida (SKI), a chave global (GK) e o seletor de algoritmo criptográfico global (GCAS) para o módulo de cálculo, a semente, a chave de segmentação recebida, a chave global e o seletor de algoritmo criptográfico global sendo fornecidos por pelo menos duas entidades diferentes;

- gerar no módulo de cálculo, uma chave temporária (SK_{temp}) utilizando um de pelo menos um algoritmo criptográfico do módulo de cálculo e pelo menos dois elementos entre a semente (Sd), a chave de segmentação (SK), a chave global (GK) e o seletor de algoritmo criptográfico global (GCAS);

- receber uma mensagem de ativação pelo módulo de cálculo;

- receber um código de autenticação da mensagem pelo módulo de cálculo (CM), o código de autenticação de mensagem (MAC) sendo computado utilizando a chave temporária (SK_{temp});

- verificar a autenticidade da mensagem recebida utilizando o código de autenticação de mensagem (MAC) e a chave temporária (SK_{temp});

- se a mensagem recebida for autêntica, ativar uma função correspondente (F1, F2, F3) do chipset;

- se a mensagem recebida não for autêntica, negar a ativação da função correspondente do chipset.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a mensagem de ativação compreende ainda pelo menos uma condição de ativação (AC) e em que o método compreende a etapa de:

- verificar se pelo menos uma condição de ativação contida na mensagem é atendida;

- Se pelo menos uma condição de ativação for atendida, ativar a função correspondente (F1, F2, F3) do chipset;

- se pelo menos uma das condições de ativação não for atendida, negar a ativação da função correspondente do chipset.

3. Método, de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que uma condição de ativação (AC) compreende verificar se a chave temporária (SK_{temp}) já está

presente no chipset e em que a chave de segmentação (SK) não é armazenada se a chave temporária já estiver presente no chipset.

4. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a semente (Sd) é introduzida quando o chipset é fabricado.

5. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a chave de segmentação (SK) é introduzida durante uma etapa de personalização do chipset.

6. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que pelo menos um do algoritmo criptográfico contido no módulo de cálculo é um algoritmo de propriedade.

7. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o módulo de cálculo (CM) compreende vários algoritmos e em que o chipset recebe instrução indicando qual algoritmo será utilizado para gerar a chave temporária (SK_{temp}).

8. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que pelo menos uma função do chipset é inativa até que uma mensagem de ativação seja recebida e processada.

9. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a chave temporária (SK_{temp}) é deletada após ser utilizada uma vez.

10. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a mensagem de ativação é criptografada.

11. Chipset compreendendo pelo menos uma memória e um módulo de cálculo encarregado de operações criptográficas, a memória contendo pelo menos uma semente e o módulo de cálculo contendo pelo menos um algoritmo criptográfico, esse chipset sendo **CARACTERIZADO** ainda pelo fato de que compreende:

- meio para receber pelo menos uma de uma chave de segmentação (SK), uma chave global (GK) e um seletor de algoritmo criptográfico global (GCAS);

- meio para transmitir pelo menos dois de: a semente, a chave de segmentação recebida (SKI), a chave global (GK) e o seletor de algoritmo criptográfico global (GCAS) para o módulo de cálculo, a semente, a chave de segmentação recebida, a chave global e o seletor de algoritmo criptográfico global sendo fornecidos por pelo menos duas entidades diferentes;

- meio para gerar no módulo de cálculo, uma chave temporária (SK_{temp}) utilizando um de pelo menos um algoritmo criptográfico do módulo de cálculo e pelo menos dois elementos entre a semente (Sd), a chave de segmentação (SK), a chave global (GK) e o seletor de algoritmo criptográfico global (GCAS);

- meio para receber uma mensagem de ativação pelo módulo de cálculo;

- meio para receber um código de autenticação da mensagem pelo módulo de cálculo (CM), o código de autenticação de mensagem (MAC) sendo computado utilizando a

chave temporária (SK_{temp});

- meio para verificar a autenticidade da mensagem recebida utilizando o código de autenticação de mensagem (MAC) e a chave temporária (SK_{temp});

- meio para ativar uma função correspondente (F1, F2, F3) do chipset, se a mensagem recebida for autêntica; e

- meio para negar a ativação da função correspondente do chipset se a mensagem recebida não for autêntica.

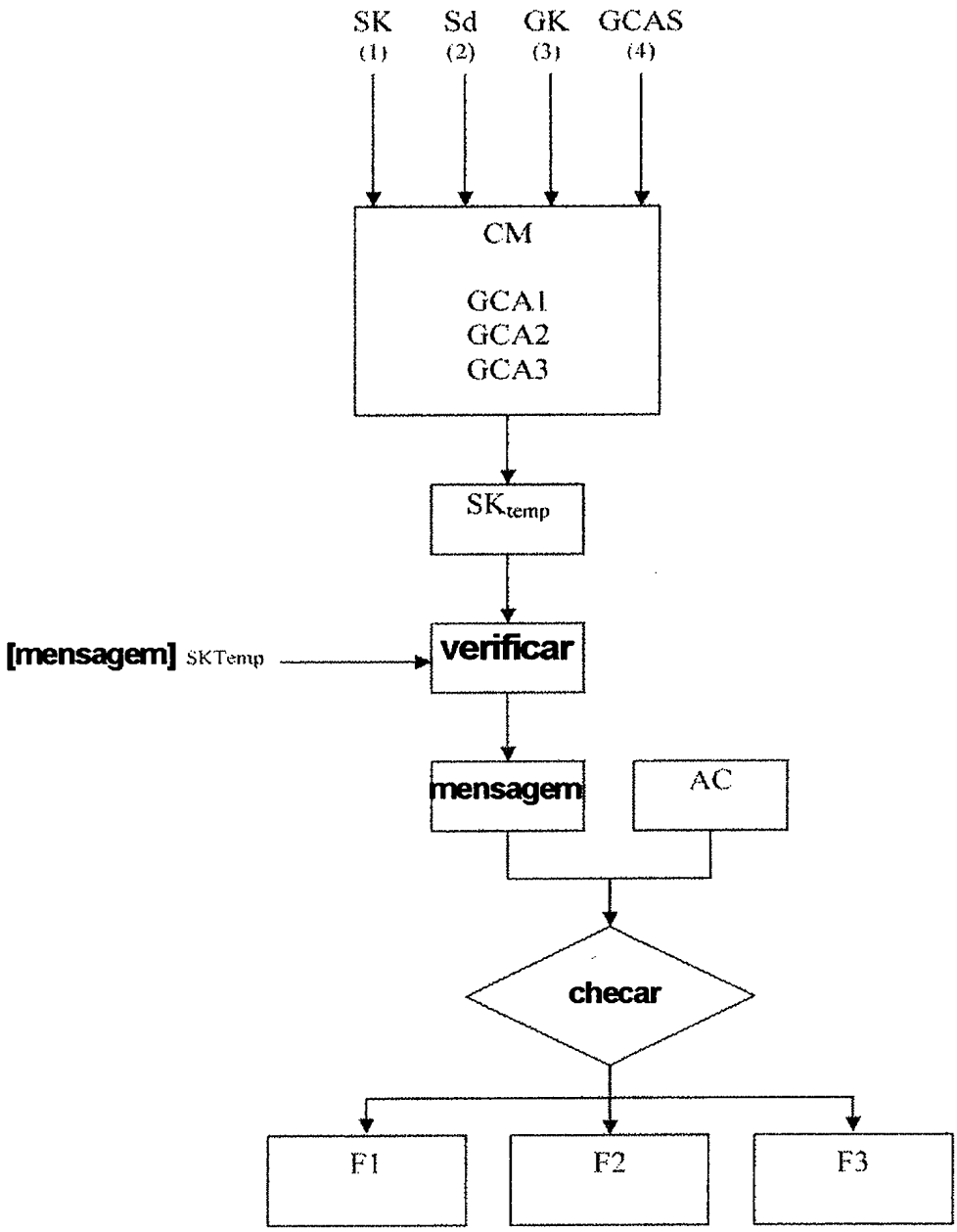

SK
(1)
Sd
(2)
GK
(3)
GCAS
(4)
CM
GCA1
GCA2
GCA3
SKtemp
[mensagem] SKTemp
verificar
mensagem
AC
checar
F1
F2
F3

Fig. 1

RESUMO

"MÉTODO PARA ATIVAR PELO MENOS UMA FUNÇÃO EM UM CHIPSET E CHIPSET PARA A IMPLEMENTAÇÃO DO MÉTODO"

A presente invenção refere-se a um método para ativar uma função de um chipset compreendendo pelo menos uma memória e um módulo de cálculo encarregado de operações criptográficas, a memória contendo pelo menos uma semente e o módulo de cálculo contendo pelo menos um algoritmo criptográfico, esse método compreendendo as etapas de:

- receber pelo menos uma de uma chave de segmentação, uma chave global e um seletor de algoritmo criptográfico global;

- transmitir pelo menos dois de: a semente, a chave de segmentação recebida, a chave global e o seletor de algoritmo criptográfico global para o módulo de cálculo, a semente, a chave de segmentação recebida, a chave global e o seletor de algoritmo criptográfico global sendo fornecidos por pelo menos duas entidades diferentes;

- gerar no módulo de cálculo, uma chave temporária utilizando um de pelo menos um algoritmo criptográfico do módulo de cálculo e pelo menos dois elementos entre a semente, a chave de segmentação, a chave global e o seletor de algoritmo criptográfico global;

- receber uma mensagem de ativação pelo módulo de cálculo;

- receber um código de autenticação da mensagem pelo módulo de cálculo, o código de autenticação de mensagem sendo computado utilizando a chave temporária;

- verificar a autenticidade da mensagem recebida utilizando o código de autenticação de mensagem e a chave temporária;

- se a mensagem recebida for autêntica, ativar uma função correspondente do chipset;

- se a mensagem recebida não for autêntica, negar a ativação da função correspondente do chipset.