(11) Número de Publicação: **PT 2115656 E**

(51) Classificação Internacional:
G06F 21/02 (2009.01) ***G06F 21/24*** (2009.01)

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

(22) Data de pedido: **2008.02.27**

(30) Prioridade(s): **2007.03.06 FR 0701625**

(43) Data de publicação do pedido: **2009.11.11**

(45) Data e BPI da concessão: **2011.01.05**
053/2011

(73) Titular(es):
THALES
45, RUE DE VILLIERS 92200 NEUILLY-SUR-SEINE **FR**

(72) Inventor(es):
THIERRY D'ATHIS **FR**
PHILIPPE DAILLY **FR**
DENIS RATIER **FR**

(74) Mandatário:
MANUEL ANTÓNIO DURÃES DA CONCEIÇÃO ROCHA
AV LIBERDADE, Nº. 69 1250-148 LISBOA **PT**

(54) Epígrafe: **PROCEDIMENTO DE MODIFICAÇÃO DE SEGREDOS CONTIDOS NUM MÓDULO CRIPTOGRÁFICO, PARTICULARMENTE EM MEIO NÃO PROTEGIDO**

(57) Resumo:
A INVENÇÃO REFERE-SE A UM PROCEDIMENTO DE MODIFICAÇÃO DE UM CONJUNTO DE SEGREDOS CONTIDOS NUM MÓDULO CRIPTOGRÁFICO. O MÓDULO CRIPTOGRÁFICO GARANTE QUE O CARREGAMENTO DE UM SEGREDO É OU CONCLUÍDO OU NULIFICADO. O MÓDULO PERMITE A LEITURA DE UM NÚMERO DE VERSÃO PARA CADA SEGREDO. O MÓDULO CONTÉM UMA INFORMAÇÃO QUE INDICA UM NÚMERO DE VERSÃO CORRESPONDENTE AO CONJUNTO DOS SEGREDOS. O PROCEDIMENTO DE ACORDO COM A INVENÇÃO INCLUI UM PRIMEIRO PASSO, DURANTE O QUAL, SE O NÚMERO DE VERSÃO DO CONJUNTO DOS SEGREDOS FOR IGUAL A UM NÚMERO DE VERSÃO QUE REQUEIRA O CARREGAMENTO DE UM CONJUNTO DE SEGREDOS NOVOS, O NÚMERO DE VERSÃO DO CONJUNTO DOS SEGREDOS DO MÓDULO CRIPTOGRÁFICO É IGUALADO A UM NÚMERO DISTINTIVO QUE PERMITE DETERMINAR QUE O MÓDULO CRIPTOGRÁFICO ESTÁ A SER RECARREGADO. O PROCEDIMENTO INCLUI UM SEGUNDO PASSO, DURANTE O QUAL, PARA CADA SEGREDO, SE O NÚMERO DE VERSÃO DO REFERIDO SEGREDO DIFERIR DO NÚMERO DE VERSÃO DO SEGREDO NOVO CORRESPONDENTE A CARREGAR, É CARREGADO O SEGREDO NOVO, ASSIM COMO O RESPECTIVO NÚMERO DE VERSÃO. O PROCEDIMENTO INCLUI UM TERCEIRO PASSO, DURANTE O QUAL O NÚMERO DE VERSÃO DO CONJUNTO DOS SEGREDOS DO MÓDULO CRIPTOGRÁFICO É IGUALADO AO NÚMERO DE VERSÃO DO CONJUNTO DOS SEGREDOS NOVOS. EM PARTICULAR, A INVENÇÃO É APLICÁVEL AO RECARREGAMENTO DE CHAVES DE ACESSO CONTIDAS NUM CONJUNTO DE CARTÕES COM CHIP EM MEIO NÃO PROTEGIDO.

RESUMO

«PROCEDIMENTO DE MODIFICAÇÃO DE SEGREDOS CONTIDOS NUM MÓDULO CRIPTOGRÁFICO, PARTICULARMENTE EM MEIO NÃO PROTEGIDO»

A invenção refere-se a um procedimento de modificação de um conjunto de segredos contidos num módulo criptográfico. O módulo criptográfico garante que o carregamento de um segredo é ou concluído ou nulificado. O módulo permite a leitura de um número de versão para cada segredo. O módulo contém uma informação que indica um número de versão correspondente ao conjunto dos segredos. O procedimento de acordo com a invenção inclui um primeiro passo, durante o qual, se o número de versão do conjunto dos segredos for igual a um número de versão que requeira o carregamento de um conjunto de segredos novos, o número de versão do conjunto dos segredos do módulo criptográfico é igualado a um número distintivo que permite determinar que o módulo criptográfico está a ser recarregado. O procedimento inclui um segundo passo, durante o qual, para cada segredo, se o número de versão do referido segredo diferir do número de versão do segredo novo correspondente a carregar, é carregado o segredo novo, assim como o respectivo número de versão. O procedimento inclui um terceiro passo, durante o qual o número de versão do conjunto dos segredos do módulo criptográfico é igualado ao número de versão do conjunto dos segredos novos. Em particular, a invenção é aplicável ao recarregamento de chaves de acesso contidas num conjunto de cartões com chip em meio não protegido.

DESCRIÇÃO

«PROCEDIMENTO DE MODIFICAÇÃO DE SEGREDOS CONTIDOS NUM MÓDULO CRIPTOGRÁFICO, PARTICULARMENTE EM MEIO NÃO PROTEGIDO»

A invenção refere-se a um procedimento de modificação de um conjunto de segredos contido num módulo criptográfico. A invenção aplica-se especificamente ao carregamento de chaves de acesso contidas num conjunto de cartões com chip em meio não protegido.

Num sistema que disponha de um conjunto de módulos criptográficos (por exemplo cartões com chip contendo segredos criptográficos), a gestão dos segredos nos referidos módulos é uma tarefa complexa. Em particular, a operação de actualização dos segredos deve responder a um certo número de exigências de segurança. Do mesmo modo, é habitual que os segredos sejam actualizados em meio protegido, ou seja, geralmente num local protegido, fora do contexto de exploração dos módulos criptográficos. Uma vez que o número de módulos criptográficos é importante, esta operação de manutenção é complexa e dispendiosa.

Por outro lado, a fim de garantir um nível de segurança correcto, os módulos criptográficos não permitem aceder aos segredos em modo de leitura e de escrita. Em caso de falha no processo de actualização dos segredos, por exemplo, após uma interrupção involuntária do processo, não é possível retomar e terminar o processo no mesmo local onde ocorreu a falha.

A invenção tem, nomeadamente, a finalidade de solucionar os inconvenientes atrás referidos. Para esse efeito, o objecto da invenção é um procedimento de modificação de segredos contidos num módulo criptográfico. O módulo criptográfico garante que o carregamento de um segredo é ou concluído ou nulificado. O módulo criptográfico permite a leitura de um número de versão para cada segredo. O módulo criptográfico contém uma informação que indica um número de versão correspondente ao conjunto dos segredos. O procedimento de acordo com a invenção é composto, nomeadamente, por um primeiro passo, durante o qual, se o número de versão do conjunto dos segredos for igual a um número de versão que requeira o carregamento de um conjunto de segredos novos, o número de versão do conjunto dos segredos do módulo criptográfico é igualado a um número distintivo que permite determinar que o módulo criptográfico está a ser recarregado. O procedimento de acordo com a invenção inclui um segundo passo, durante o qual, para cada segredo, se o número de versão do referido segredo diferir do número de versão do segredo novo correspondente a carregar, é carregado o segredo novo, assim como o respectivo número de versão. O procedimento de acordo com a invenção inclui um terceiro passo, durante o qual o número de versão do conjunto dos segredos do módulo criptográfico é igualado ao número de versão do conjunto dos segredos novos.

Numa forma de execução, o número de versão do conjunto dos segredos do módulo criptográfico no cartão é registado num ficheiro do módulo criptográfico do cartão através de

um segredo invariável.

Numa outra forma de execução, o número de versão do conjunto dos segredos do módulo criptográfico no cartão é registado sob a forma de segredo utilizado apenas para indicar a versão global dos segredos.

Numa outra forma de execução, o número de versão do conjunto dos segredos do módulo criptográfico no cartão é registado sob a forma do último dos segredos a recarregar no segundo passo.

Durante o segundo passo, a verificação do número de versão de cada segredo pode ser efectuada através de uma autenticação mútua dos diferentes segredos até encontrar o ponto de interrupção.

A invenção tem, nomeadamente, a vantagem de permitir a modificação de um conjunto de segredos num módulo criptográfico, de modo a garantir a respectiva coerência mesmo que a actualização apenas possa ser feita segredo a segredo. A invenção permite igualmente garantir que, após o recarregamento dos segredos no módulo criptográfico, os dados já existentes no módulo criptográfico permanecem acessíveis e não corrompidos. Para além disso, o procedimento de acordo com a invenção pode ser interrompido a qualquer momento sem que isso implique a corrupção dos segredos contidos no módulo criptográfico. Por outro lado, após uma ou várias interrupções, voluntárias ou acidentais, durante a aplicação dos passos do procedimento de acordo com a invenção, o procedimento pode continuar a ser

efectuado a partir da própria máquina ou de uma máquina diferente, preparada para dar continuidade à aplicação dos passos do procedimento.

Outras características e vantagens da invenção serão explicadas através da descrição que se segue, a qual se baseia nos desenhos anexados, que representam, na figura 1, uma sinopse dos passos do procedimento de acordo com a invenção para a modificação de segredos incluídos num módulo criptográfico.

O procedimento de acordo com a invenção permite, nomeadamente, retomar e concluir a modificação de um conjunto de segredos (dados sensíveis associados às respectivas chaves de acesso), sendo que os referidos segredos não podem ser relidos nem necessariamente reescritos.

Na forma de execução do procedimento de acordo com a invenção ilustrada na figura 1, o módulo criptográfico que contém os segredos, manipulado durante a aplicação dos passos do procedimento, tem as seguintes características:

- garantia de que o carregamento de um segredo é concluído ou nulificado (princípio anti-extracção, também referido em inglês como princípio «anti-tear»);
- actualização simultânea do segredo e da respectiva versão;
- possibilidade de leitura de um número de versão para cada segredo, ao qual não é possível aceder.

O módulo criptográfico contém igualmente uma informação que indica um número de versão correspondente ao conjunto dos segredos.

Este tipo de módulo criptográfico pode corresponder, por exemplo, a um cartão com chip, mais especificamente a um cartão «Mifare® DESFire».

O procedimento de acordo com a invenção recebe a entrada de segredos novos que serão carregados em vez dos segredos contidos no módulo criptográfico. Ao conjunto de segredos novos corresponde um número de versão correspondente ao conjunto dos segredos novos. Do mesmo modo, ao conjunto dos segredos contidos no módulo criptográfico corresponde um número de versão. A cada segredo contido no módulo criptográfico corresponde um número de versão. A cada segredo novo a carregar corresponde um número de versão. A cada segredo corresponde, assim, um número de versão. Se os números de versão forem idênticos, tal significa que os segredos são idênticos. O mesmo se aplica ao número de versão do conjunto dos segredos.

O procedimento de acordo com a invenção é composto por um primeiro passo 1, durante o qual o módulo criptográfico é assinalado como estando em processo de recarregamento de segredos. Assim, durante o primeiro passo 1, após assegurar, se necessário, que o recarregamento dos segredos foi solicitado, é lido o número de versão do conjunto dos segredos do módulo criptográfico.

De seguida, o número de versão do conjunto dos segredos do módulo criptográfico é comparado com o número de versão do conjunto dos segredos a carregar. Esta comparação determina se é necessário carregar os segredos novos (por exemplo, o número de versão do conjunto dos segredos a carregar é superior ao número de versão do conjunto dos segredos já carregados). Se for esse o caso:

- o número de versão do conjunto dos segredos do módulo criptográfico é igualado a um número distintivo que permita determinar que o módulo criptográfico se encontra em recarregamento;
- seguidamente, no decurso de um segundo passo 2 do procedimento de acordo com a invenção, para cada segredo, se o número de versão do referido segredo diferir do número de versão do segredo novo a carregar, é carregado o segredo novo correspondente, assim como o respectivo número de versão;
- depois, no decurso de um terceiro passo 3 do procedimento de acordo com a invenção, o número de versão do conjunto dos segredos do módulo criptográfico é igualado ao número de versão do conjunto dos segredos novos.

Durante o primeiro passo 1, se o número de versão do conjunto dos segredos do módulo criptográfico for igual ao número distintivo que permite determinar que o módulo criptográfico se encontra em recarregamento,

isso significa que a operação de actualização não pôde ser concluída antes. Nesse caso:

- durante o passo 2, para cada segredo, se o número de versão do referido segredo diferir do número de versão do segredo novo a carregar, é carregado o segredo novo correspondente, assim como o respectivo número de versão;
- seguidamente, durante o passo 3, o número de versão do conjunto dos segredos do módulo criptográfico é igualado ao número de versão do conjunto dos segredos novos.

Qualquer interrupção durante estes passos pode ser retomada de modo a prosseguir o recarregamento no ponto de paragem, quer na própria máquina, quer noutra máquina.

O número de versão do conjunto dos segredos do módulo criptográfico no cartão pode ser guardado:

- quer num ficheiro do cartão acessível através de um segredo invariável;
- quer sob a forma da versão de um segredo específico, ou seja:
    - um segredo destinado apenas a indicar a versão geral dos segredos; ou
    - o último dos segredos a recarregar no passo onde os segredos são carregados por uma ordem invariável predefinida.

Em particular, o procedimento de acordo com a invenção pode aplicar-se a vários cartões com chip que podem ter números de versão de segredos diferentes. É nomeadamente esse o caso quando o conjunto de cartões com chip corresponde a um lote e quando os segredos consistem em chaves de acesso aos dados. O procedimento pode ser aplicado a um conjunto de terminais sensíveis cujos segredos de comunicação devem ser alterados no terreno. O procedimento de acordo com a invenção pode ainda ser aplicado a bases de dados cuja administração não permite a modificação dos direitos de acesso numa única transacção.

Numa forma de execução, a verificação do número de versão de cada segredo (sobretudo quando esta não está disponível ou não é legível) pode ser efectuada através de uma autenticação mútua dos diferentes segredos até encontrar o ponto de interrupção.

Reivindicações

1. Procedimento de modificação de segredos contidos num módulo criptográfico, sendo que o módulo criptográfico:

- garante que o carregamento de um segredo é ou concluído ou nulificado;
- permite a leitura de um número de versão para cada segredo;
- contém uma informação que indica um número de versão correspondente ao conjunto dos segredos;

sendo o procedimento é composto por:

- um primeiro passo (1), durante o qual, se o número de versão do conjunto dos segredos for igual a um número de versão que requeira o carregamento de um conjunto de segredos novos, o número de versão do conjunto dos segredos do módulo criptográfico é igualado a um número distintivo que permite determinar que o módulo criptográfico está a ser recarregado;
- um segundo passo (2), durante o qual, para cada segredo, se o número de versão do referido segredo diferir do número de versão do segredo novo correspondente a carregar, é carregado o segredo novo, assim como o respectivo número de versão;
- um terceiro passo (3), durante o qual o número de versão do conjunto dos segredos do módulo criptográfico é igualado ao número de versão do

conjunto dos segredos novos.

2. Procedimento de acordo com a reivindicação n.º 1, **caracterizado pelo facto de**, sendo o módulo criptográfico um cartão com chip, o número de versão do conjunto dos segredos do módulo criptográfico no cartão ser registado num ficheiro do módulo criptográfico do cartão acessível através de um segredo invariável.

3. Procedimento de acordo com a reivindicação n.º 1, **caracterizado pelo facto de**, sendo o módulo criptográfico um cartão com chip, o número de versão do conjunto dos segredos do módulo criptográfico no cartão ser registado sob a forma de um segredo utilizado apenas para indicar a versão global dos segredos.

4. Procedimento de acordo com a reivindicação n.º 1, **caracterizado pelo facto de**, sendo o módulo criptográfico um cartão com chip, o número de versão do conjunto dos segredos do módulo criptográfico no cartão ser registado sob a forma do último dos segredos a recarregar no segundo passo (2).

5. Procedimento de acordo com qualquer uma das reivindicações anteriores, **caracterizado pelo facto de**, durante o segundo passo (2), a verificação do número de versão de cada segredo ser efectuada através de uma autenticação mútua dos diferentes segredos até encontrar o ponto de interrupção.

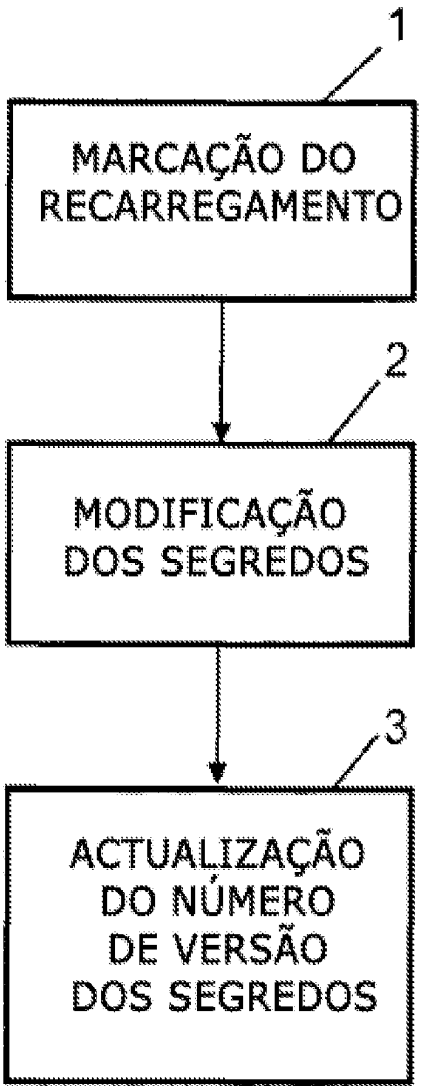
1
MARCAÇÃO DO RECARREGAMENTO
2
MODIFICAÇÃO DOS SEGREDOS
3
ACTUALIZAÇÃO DO NÚMERO DE VERSÃO DOS SEGREDOS

FIG.1