República Federativa do Brasil
Ministério da Economia
Instituto Nacional da Propriedade Industrial

(11) PI 0919169-0 B1

(22) Data do Depósito: 16/09/2009

(45) Data de Concessão: 24/11/2020

(54) Título: MÉTODO PARA FAZER CUMPRIR AS REGRAS DE ACESSO POR INTERMÉDIO DE UM CENTRO DE GERENCIAMENTO PARA UM PRODUTO DE DIFUSÃO

(51) Int.Cl.: H04N 7/16; H04N 7/167; H04N 21/258; H04N 21/4623; H04N 21/6334.

(52) CPC: H04N 7/165; H04N 7/1675; H04N 21/25833; H04N 21/4623; H04N 21/63345.

(30) Prioridade Unionista: 19/09/2008 EP 081646747; 19/09/2008 US 61/136,623.

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

(72) Inventor(es): PASCAL JUNOD; ALEXANDRE KARLOV.

(86) Pedido PCT: PCT EP2009061986 de 16/09/2009

(87) Publicação PCT: WO 2010/031781 de 25/03/2010

(85) Data do Início da Fase Nacional: 17/03/2011

(57) Resumo: MÉTODO PARA FAZER CUMPRIR AS REGRAS DE ACESSO POR INTERMÉDIO DE UM CENTRO DE GERENCIAMENTO PARA UM PRODUTO DE DIFUSÃO. O propósito desta invenção é o de, por um lado, propor uma forma de se basear em uma amplitude menor no meio de segurança do módulo de segurança do receptor para fazer cumprir as condições de acesso definidas nas mensagens essenciais e, por outro lado,lidar com condições de acesso, complexas, com base na característica e propriedades do dispositivo de recepção ou do usuário de tal dispositivo. Portanto, é proposto um método para fazer cumprir por intermédio de um centro de gerenciamento as regras de acesso para um produto de transmissão recebido pelos receptores, o acesso ao produto sendo liberado por uma chave de acesso, o centro de gerenciamento gerenciando uma pluralidade de atributos Booleanos, positivos e negativos,nos receptores, o método compreendendo as etapas de associar um atributo Booleano positivo a um receptor com direito ao atributo e carregar o mesmo; associar um atributo Booleano negativo ao receptor que não tem direito ao atributo e carregar o mesmo; definir ao menos um segundo esquema de criptografia de difusão visando o conjunto dos atributos«Booleanos, negativos e associar a cada (...).

“MÉTODO PARA FAZER CUMPRIR AS REGRAS DE ACESSO, POR INTERMÉDIO DE UM CENTRO DE GERENCIAMENTO, A UM PRODUTO DE DIFUSÃO”

CAMPO DA INVENÇÃO

Esta invenção se refere ao campo de criptografia de difusão, particularmente a forma de gerenciar direitos de autorização em um sistema de transmissão tendo um centro de gerenciamento e vários dispositivos de recepção.

INTRODUÇÃO

No modelo de difusão de TV baseado em assinatura padrão, conhecido, conforme revelado no “EBU Functional Model of a Conditional Access System”, revisão técnica EBU, inverno de 1995, o produto de TV baseado em assinatura a ser transmitido é criptografado e as chaves para decriptografar o produto de TV baseado em assinatura pelo lado de recepção são colocadas nas Mensagens de Controle de Direitos (ECM) enviadas junto com o produto de TV baseado em assinatura, embaralhado. As ECMs são criptografadas com uma chave de transmissão, a qual é mudada frequentemente por razões de segurança.

Além das chaves de desembaralhamento, a ECM carrega informação sobre os direitos de acesso condicional do produto de TV baseado em assinatura na forma de condições de acesso a serem impostas ao lado de recepção.

Os direitos de acesso condicional, de assinante individual (por exemplo, um direito de subscrição de serviço por um mês) assim como as chaves de transmissão, são gerenciados e transmitidos de uma forma assíncrona na forma de Mensagens de Gerenciamento de Direitos (EMM). As EMMs são criptografadas com chaves secretas conhecidas apenas pelos receptores.

Para um dispositivo de recepção poder receber e decriptografar um produto, a primeira etapa, portanto, é a de receber e decriptografar as mensagens EMM carregando os direitos que correspondem aos produtos assim como as mensagens EMM carregando as chaves de transmissão necessárias para decriptografar as mensagens ECM. Para essa finalidade, o dispositivo de recepção compreende uma chave única e o EMM é criptografado pela chave única de combinação do dispositivo de recepção; e transmitida de modo que apenas esse dispositivo específico pode decriptografar a EMM. Com essa finalidade, chaves simétricas ou assimétricas podem ser usadas.

TÉCNICA ANTERIOR

Diferentes direitos podem ser carregados na memória do meio de segurança do dispositivo de recepção; esse meio de segurança geralmente estando na forma de um cartão inteligente; e são então impostos pelo meio de segurança.

Esses meios de segurança podem ter formas diferentes, tal como cartão inteligente, chip de segurança, peça de hardware de segurança USB ou software à prova de violação no dispositivo.

Consideramos esses meios de segurança como suficientemente seguros para armazenar ao menos a chave de transmissão, a chave única pertencendo a esse dispositivo de recepção e o direito (ou direitos) associado a esse dispositivo de recepção.

A função do meio de segurança é a de receber as mensagens ECM e EMM, decriptografar a ECM utilizando a chave de transmissão e extrair a chave (ou chaves) de acesso assim como as condições de acesso relacionadas a esse produto de TV baseado em assinatura. A verificação do meio de segurança se estiver presente o direito combinando com as condições de acesso contidas na ECM na memória de meio de segurança, e em caso positivo, a chave de acesso é retornada ao dispositivo de recepção para decriptografia do produto.

Uma ECM pode conter mais do que uma definição de condição de acesso. Nesse caso, de acordo com a política aplicada, o meio de segurança pode verificar a presença dos direitos em sua memória e retornar a chave de acesso se ao menos um dos direitos estiver presente (função OU, Booleana). De acordo com outra política, o meio de segurança pode retornar à chave de acesso apenas se todos os direitos combinando com o conjunto completo de condições de acesso estiverem presentes na memória de meio de segurança (função E, Booleana).

Consultas complexas sobre o conteúdo de memória podem ser executadas conforma revelado em WO2004052005. A chave de acesso é retornada ao dispositivo de recepção apenas se os vários testes proporcionarem um resultado positivo. Não apenas os direitos em si são considerados, mas também a data de expiração ou status de crédito podem ser usados na decisão sobre a validade dos direitos.

Os direitos assim como a chave de transmissão podem ser carregados através de mensagens EMM na memória de meio de segurança de acordo com várias formas:

- Na fase de iniciação do dispositivo de recepção, por intermédio de uma conexão local com dispositivo hospedeiro ou por intermédio da recepção de mensagens de inicialização enviadas no canal de difusão.

- A qualquer momento, por exemplo, quando os dados de assinante são modificados, subscrição ou cancelamento de serviços, renovação dos direitos, modificação da chave de serviço (incluindo a chave de transmissão).

Com a advertência do meio de segurança feita apenas por software, o risco desse software estar comprometido é superior do que com o meio de segurança de hardware, específico.

Primitivas de criptografia de difusão tais como aquelas reveladas em “Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys” por Dan Boneh, Craig Gentry e Brent Waters constituem uma forma eficiente para transmitir com segurança conteúdo digital por intermédio de um canal de transmissão com relação à largura de banda

de canal, capacidade de armazenamento do receptor e complexidade de criptografia/decriptografia. Elas consistem em três algoritmos. Algoritmo de configuração, que inicializa os parâmetros de sistema tal como material de chave de criptografia para os receptores (alvos) e a chave de criptografia para o centro de transmissão. O algoritmo de criptografia gera um criptograma para um subconjunto autorizado de receptores, de modo que outros receptores fora do subconjunto autorizado são incapazes de decriptografar o criptograma. O algoritmo de decriptografia decriptografa corretamente o criptograma desde que o receptor tenha a chave de decriptografia e esteja no subconjunto autorizado.

PROBLEMA A SER RESOLVIDO

Considere uma situação onde o centro deseja transmitir conteúdo especial para o conjunto autorizado de receptores que preenchem determinados critérios ou característica (ou ausência dos mesmos). Essa característica poderia ser, por exemplo, a subscrição para um pacote de serviços, a quantidade de dinheiro restante no cartão inteligente, o Código de Endereçamento Postal do receptor (ou outra informação geográfica), propriedades de chipset ou qualquer outra informação relacionada ao cliente ou ao dispositivo.

O benefício da presente invenção é o de eficientemente resolver esse problema mediante uso de pelo menos dois casos de material de chave, permitindo assim a execução das condições de transmissão.

Ao contrário do método revelado em WO2004052005 o qual tem uma funcionalidade comparativa, a presente invenção permite realizar execução de direitos no centro de transmissão (isto é, cabeça de rede). Isso tem uma vantagem em relação ao método anterior que impõe a execução dos direitos no módulo de segurança (SC) uma vez que a segurança no caso mencionado em primeiro lugar se baseia na dificuldade de planejamento reverso (quebra) de um módulo de segurança, enquanto que em nosso caso a segurança se baseia em um problema matemático difícil. Além disso, ao contrário da revelação em WO 2004052005 a presente invenção pode lidar com condições de acesso complexas e políticas sem qualquer impacto em relação à segurança do sistema.

BREVE DESCRIÇÃO DA INVENÇÃO

O propósito desta invenção é o de propor uma forma de se basear em uma amplitude menor no meio de segurança do módulo de segurança (SC) do receptor para fazer cumprir as condições de acesso definidas nas mensagens essenciais por um lado e lidar com condições de acesso, complexas, com base na característica e propriedades do dispositivo de recepção ou do usuário de tal dispositivo por outro lado.

Portanto, é proposto um método para obrigar a execução por intermédio de um centro de gerenciamento das regras de acesso para um produto de difusão recebido pelos receptores, o acesso ao produto sendo liberado por uma chave de produto, o centro de gerenciamento gerenciando uma pluralidade de pacotes de subscrição para os quais ao

menos um pacote de subscrição permite o acesso ao produto, o método compreendendo as etapas iniciais de:

- definir para cada pacote de subscrição ao menos um material de chave positiva e um material de chave negativa,

- para um receptor tendo subscrito para ao menos um pacote de subscrição, carregar o material de chave positiva do pacote de subscrição e o material de chave negativa dos pacotes de subscrição para os quais nenhuma subscrição foi feita.

No caso em que o produto é acessível por intermédio de ao menos um primeiro pacote de subscrição e não é acessível para ao menos um segundo pacote de subscrição:

- preparar uma mensagem de autorização para proporcionar acesso ao produto, a chave de produto ou os dados permitindo recuperar a chave de produto que é usada para produzir um criptograma, o criptograma sendo criptografado pela chave de acesso de material de chave positiva do primeiro pacote de subscrição e material de chave negativa do segundo pacote de subscrição de modo que o criptograma permitindo recuperar a chave de produto é acessível apenas quando estiver presente no receptor o material de chave positiva do primeiro pacote de subscrição e o material de chave negativa do segundo pacote de subscrição.

A particularidade do presente método é a de definir dois materiais essenciais para um pacote de subscrição. Um desses materiais essenciais (material de chave positiva) é carregado quando o receptor tem permissão para o pacote de subscrição e o outro (o material de chave negativa) é carregado em um receptor que não tem acesso ao pacote de subscrição. Esse conceito pode ser estendido para Código de Endereçamento Postal, por exemplo, o receptor recebendo o material de chave de uma primeira zona e o material de chave das outras zonas.

O centro de gerenciamento em primeiro lugar visa um atributo (por exemplo, conjunto de serviços ou pacote de subscrição) e relaciona os possíveis atributos e para cada atributo, material de chave é determinado. Por material de chave, se quer dizer ao menos uma chave associada a esse atributo e opcionalmente uma definição de direitos.

Esta invenção se baseia no fato de que para um dispositivo de recepção específico tendo direito a um primeiro pacote de subscrição e não a um segundo pacote de subscrição, o dispositivo de recepção recebe o material de chave positiva do primeiro pacote de subscrição e o material negativo do segundo pacote de subscrição.

Essa modalidade pode ser estendida a outras condições onde podemos definir um primeiro material de chave para preencher aquela condição e um segundo material de chave para não satisfazer àquela condição. Este é o caso para Código Postal, valor de crédito (por exemplo, alguns receptores tendo um crédito para comprar conteúdo e outros receptores não tendo tal crédito).

Graças a esse material de chave, as mensagens essenciais podem carregar consultas complexas tais como permitir acesso à chave de produto apenas se o dispositivo de recepção tiver direito à primeira condição e não tiver direito à segunda condição. A descrição abaixo considerará o exemplo de um primeiro pacote de subscrição e de pelo menos um segundo pacote de subscrição para definir as condições.

A chave de acesso ou chave de produto pode ser usada para acessar diretamente o produto ou acessar indiretamente o produto, isto é, mediante uso de chaves ou algoritmos adicionais no módulo de segurança. Essa chave de acesso pode ser combinada com outras chaves na mesma mensagem ou em outras mensagens de controle de direitos; tal como descrito em EP1252768, a chave de acesso desempenhando a função nesse caso de uma chave mestre.

Em uma modalidade alternativa, a chave de acesso é a assim chamada chave de transmissão que é usada para criptografar (ou decriptografar) as mensagens contendo as palavras de controle e as condições de acesso.

BREVE DESCRIÇÃO DO DESENHO

A invenção será explicada com ajuda da figura anexa na qual um esboço geral do ambiente de difusão é ilustrado.

DESCRIÇÃO DETALHADA DA INVENÇÃO

Durante a inicialização de um novo assinante, o módulo de segurança de seu receptor recebe mensagens contendo o material de chave dedicado a esse usuário.

Consideremos o exemplo em que o centro de gerenciamento gerencia quatro pacotes de subscrição, cada pacote contendo ao menos um serviço de áudio/vídeo e pode compreender uma pluralidade de serviço. No caso em que esse usuário subscreveu para um primeiro pacote de subscrição, o material de chave positiva do primeiro pacote de subscrição é enviado para o receptor para armazenamento em seu módulo de segurança. O centro de gerenciamento também enviará o material de chave negativa dos outros pacotes de subscrição, aos quais o assinante não tem acesso.

Graças a essa estrutura, agora é possível definir as condições de acesso para um produto de difusão específico utilizando o material de chave, positivo e negativo. De acordo com um exemplo, onde o produto é acessível ao assinante que subscreveu para o primeiro pacote e não para o segundo pacote, a chave de produto, isto é, a chave para decriptografar o produto, portanto, é criptografada pela chave positiva do primeiro pacote de subscrição e outra vez pela chave negativa do segundo pacote de subscrição. Uma mensagem é formada com essa chave de produto criptografada dupla e enviada aos assinantes. Nosso assinante específico que tem acesso ao primeiro pacote e não ao segundo pacote pode então decriptografar essa chave de produto criptografada dupla. No caso em que outro assinante tem acesso ao primeiro e ao segundo pacote, o assinante não possuirá a chave negativa do

segundo pacote de subscrição e será incapaz de decriptografar a chave de produto.

As condições de acesso ao produto, portanto, são impostas pelo centro de gerenciamento e não se baseiam na verificação feita pela unidade de assinante.

A ordem de criptografia, isto é, a chave positiva e então a chave negativa poderia ser invertida sem consequência. A chave negativa pode ser usada em primeiro lugar e a chave positiva pode ser usada subsequentemente.

No caso em que a condição de acesso deve impactar um terceiro pacote de subscrição, a chave de produto pode ser criptografada adicionalmente pela chave positiva ou negativa do terceiro pacote de subscrição, dependendo do fato de que a condição deve ter ou não acesso ao terceiro pacote de subscrição.

De acordo com uma modalidade da invenção, a chave de produto é inicialmente criptografada por uma chave de sessão. Isso permite uma forma mais flexível de lidar com as chaves positiva e negativa. No caso em que as chaves positiva e negativa são chaves assimétricas, o tamanho do material criptografado por uma chave assimétrica é definido pelo algoritmo assimétrico. Isso impactará apenas o tamanho da chave de sessão e deixa em aberto o tamanho da chave de produto. Uma chave de produto de 96 bits pode ser usada e criptografada por uma chave de sessão de 128 bits. A chave de sessão, posteriormente, é criptografada de acordo com a condição de acesso em vez da chave de produto conforme descrito acima. A mensagem enviada à unidade de assinante conterá a chave de produto criptografada pela chave de sessão, e a chave de sessão criptografada por chaves, positiva ou negativa, de acordo com as condições de acesso nos pacotes de subscrição.

Como um assinante pode mudar suas subscrições, de acordo com uma modalidade da invenção, os materiais essenciais, positivo e negativo, são renovados regularmente, por exemplo, todo mês. Desse modo para que um assinante não tenha interesse em manter a chave negativa de um determinado pacote de subscrição quando ele subscrever para esse pacote. O centro de gerenciamento enviará a esse assinante a nova chave positiva para o mês vindouro para os pacotes de subscrição aos quais ele está intitulado, e a nova chave positiva e a nova chave negativa para o mês vindouro para os pacotes de subscrição aos quais ele não está intitulado. Assim manter no meio de armazenamento da unidade de assinante os guardados do mês anterior não permite que ele ignore as condições de acesso com base em uma combinação de chaves, positivas e negativas.

EXPLANAÇÃO DA FIGURA

Na Figura 1, o centro de gerenciamento MC armazena em seu banco de dados DB uma cópia dos materiais essenciais enviados nos dispositivos de recepção RD1, RD2, RD3. De acordo com nosso exemplo, dois pacotes de subscrição D1, D2 foram definidos, o primeiro sendo relacionado ao material de chave positiva K1 e ao material de chave negativa K1', o segundo sendo relacionado ao material de chave positiva K2 e ao material

de chave negativa K2'.

O dispositivo de recepção RD1 tendo direito ao pacote de subscrição B1 recebeu o material de chave K1. Devido ao fato de que esse dispositivo de recepção RD1 não está intitulado ao pacote de subscrição B2, o material de chave K2' também foi enviado a ele.

O dispositivo de recepção RD2 tendo direito ao pacote de subscrição D1 e D2, recebeu ambos os materiais de chave, K1 e K2, enviados a esse dispositivo.

O dispositivo de recepção RD2 tendo direito ao pacote de subscrição B2, recebeu o material de chave K2 enviado a ele. Devido ao fato de que esse dispositivo de recepção RD3 não tem direito ao pacote de subscrição B1, o material de chave K1' foi enviado também a ele.

No caso em que o centro de gerenciamento MC precisa transmitir uma chave de acesso K apenas aos dispositivos de recepção que tem direito ao segundo pacote de subscrição B2 e não tem direito ao primeiro pacote de subscrição B1, o criptograma CY enviado aos dispositivos de recepção RD conterão a chave de acesso combinada com o material de chave negativa K1' e ao material de chave positiva K2.

Na mensagem de autorização contendo o criptograma, outro campo para a mensagem contém um descritor das chaves a serem usadas para a decriptografia. Isso pode estar na forma de dois mapas de bits, cada um dos bits ativos definindo um pacote de subscrição, e um mapa de bits para as chaves positivas e o outro para as chaves negativas. De acordo com a implementação da invenção, poderia ser decidido se as chaves positivas são usadas primeiramente para decriptografar o criptograma e então as chaves negativas.

A chave de produto pode liberar um único produto de transmissão, por exemplo, um filme ou pode liberar um serviço para um dia ou para um mês.

O pacote de subscrição pode se referir a uma pluralidade de serviços ou a um único serviço. A invenção assim permite que se defina a regra de acesso desse produto mediante combinação do acesso ao canal 3 (primeiro pacote de subscrição) e não ao canal 6 (segundo pacote de subscrição).

REIVINDICAÇÕES

1. Método para fazer cumprir as regras de acesso, por intermédio de um centro de gerenciamento, a um produto de difusão recebido por receptores, o acesso ao produto sendo liberado por uma chave de produto, o centro de gerenciamento gerenciando uma pluralidade de pacotes de subscrição para os quais pelo menos um pacote de subscrição permite o acesso ao produto, o método compreendendo as etapas iniciais de:

definir, para cada pacote de subscrição, pelo menos um material de chave positiva, o material de chave positiva tendo pelo menos uma chave positiva e sendo direcionado para receptores subscritos no pacote de subscrição,

para um receptor tendo acesso a pelo menos um pacote de subscrição, carregar o material de chave positiva do pacote de subscrição, **CARACTERIZADO** por ainda compreender as etapas de:

definir, para cada pacote de subscrição, pelo menos um material de chave negativa, o material de chave negativa tendo pelo menos uma chave negativa e sendo direcionado para receptores não subscritos no pacote de subscrição,

e carregar, para o receptor, o material de chave negativa dos pacotes de subscrição para os quais nenhuma subscrição foi feita,

no caso em que o produto é acessível por intermédio de pelo menos um primeiro pacote de subscrição e é inacessível para pelo menos um segundo pacote de subscrição:

preparar uma mensagem de autorização para proporcionar acesso ao produto, a chave de produto ou os dados permitindo recuperar a chave de produto que é usada para produzir um criptograma, o criptograma sendo criptografado pela chave positiva do primeiro pacote de subscrição e pela chave negativa do segundo pacote de subscrição, de modo que o criptograma permitindo recuperar a chave de produto é acessível apenas quando o material de chave positiva do primeiro pacote de subscrição e o material de chave negativa do segundo pacote de subscrição estiverem presente no receptor.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo criptograma ser a chave de produto.

3. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo criptograma ser uma chave de sessão, a chave de produto sendo criptografada pela chave de sessão, o método compreendendo a etapa de adicionar a chave de produto criptografada na mensagem de autorização.

4. Método, de acordo com qualquer uma das reivindicações 1 a 3, **CARACTERIZADO** pelo criptograma ser gerado mediante criptografia sequencial do criptograma por intermédio de pelo menos uma chave negativa e pelo menos uma chave positiva.

5. Método, de acordo com qualquer uma das reivindicações 1 a 4,

CARACTERIZADO pela mensagem de autorização compreender informação de identificação descrevendo os pacotes de subscrição usados para a criptografia.

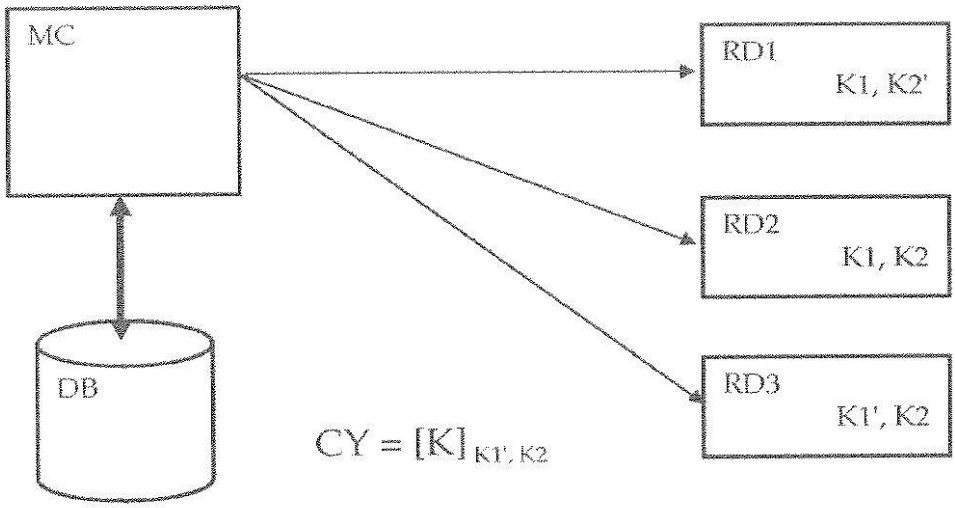

Fig. 1