(11) Número de Publicação: **PT 1377035 E**

(51) Classificação Internacional:
H04N 5/00 (2007.10) ***H04N 7/16*** (2007.10)
H04N 7/167 (2007.10)

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

(22) Data de pedido: **2003.06.16**

(30) Prioridade(s): **2002.06.28 CH 11262002**

(43) Data de publicação do pedido: **2004.01.02**

(45) Data e BPI da concessão: **2010.02.25**
072/2010

(73) Titular(es):
NAGRAVISION S.A.
ROUTE DE GENÈVE 22-24 1033 CHESEAUX-SUR-LEUSANNE **CH**

(72) Inventor(es):
OLIVIER BRIQUE **CH**
CHRISTOPHE GOGNIAT **CH**
HENRI KUDELSKI **CH**

(74) Mandatário:
ÁLVARO ALBANO DUARTE CATANA
AVENIDA MARQUÊS DE TOMAR, Nº 44, 6º 1069-229 LISBOA **PT**

(54) Epígrafe: **MÉTODO PARA A ACTUALIZAÇÃO DE CHAVES DE SEGURANÇA NUM DESCODIFICADOR DE TELEVISÃO**

(57) Resumo:

Descrição

Método para a actualização de chaves de segurança num descodificador de televisão

Campo da invenção

[0001] A presente invenção diz respeito ao domínio dos receptores de televisão paga, em especial à segurança das ligações entre um receptor e o seu módulo de segurança.

Fundo da invenção

[0002] Num sistema de televisão paga, o fluxo numérico transmitido para estes receptores é codificado a fim de se poder controlar a utilização e de se definir condições para tal utilização. Esta codificação é realizada graças a palavras de controlo (Control Words) que são alteradas em intervalos regulares (tipicamente entre 5 e 30 segundos) de modo a dissuadir qualquer ataque que visa reencontrar uma tal palavra de controlo.

[0003] Para que o receptor possa decifrar o fluxo codificado por estas palavras de controlo, estas últimas são-lhe enviados independentemente do fluxo nas mensagens de controlo (ECM) codificadas por uma chave adequada ao sistema de transmissão entre o centro de gestão (CAS) e o módulo de segurança da unidade do utilizador. Com efeito, as operações de segurança são efectuadas numa unidade de segurança (SC) que está geralmente sob a forma de um cartão inteligente, conhecido por ser inviolável. Esta unidade pode ser quer de tipo amovível ou directamente integrada no receptor.

[0004] As palavras de controlo são devolvidas seguidamente ao descodificador a fim de se poder descodificar o fluxo codificado.

[0005] Para impedir que estas palavras de controlo sejam interceptadas aquando das suas transmissões para o

descodificador, esta ligação foi protegida quer seja por chaves de sessão tal como descrito no documento WO97/38530 quer seja por uma chave de emparelhamento tal como descrito no documento WO99/57901.

[0006] No segundo documento citado, uma chave secreta está contida no receptor que é emparelhado ao módulo de segurança que lhe é ligado no momento da fase de iniciação. Esta chave pode ser de tipo simétrico ou assimétrico. Os dois dispositivos são por conseguinte inseparáveis do ponto de vista operacional.

[0007] No entanto, pode-se provar útil provocar uma evolução desta segurança, por exemplo para substituir uma chave de uma certa tecnologia (comprimento de chave por exemplo) por uma outra tecnologia.

[0008] Esta operação reveste-se ela própria de um risco importante de fraude porque encarrega-se de instalar à distância novos meios de segurança. Sabe-se que os receptores estão nas mãos de pessoas atentamente à de todas as informações que lhes permita quebrar a segurança instalada.

Descrição da invenção

[0009] É por isto que, a invenção actual se propõe a provocar uma evolução da primeira segurança baseada numa primeira chave para uma segunda segurança baseada numa segunda chave, esta operação efectuada num meio não protegido por uma transmissão dita aberta, garantindo o mesmo nível de segurança se esta operação fosse efectuada localmente, num lugar adequado ao gestor do sistema.

[0010] Este objectivo é atingido por um método tal como foi definido na reivindicação 1.

[0011] Desta maneira, uma mensagem interceptada e descodificada pela chave pública comum, transmitida previamente não permite encontrar a nova chave pública

porque só a primeira chave pessoal do descodificador é a mesma do descodificador da mensagem.

[0012] Assim, este método garante que esta nova chave será instalada onde a primeira chave é armazenada. Se um descodificador não possui esta chave, nenhuma nova chave será instalada.

[0013] De acordo com o modo de funcionamento, esta primeira chave é a chave que serve ao emparelhamento com a unidade de segurança. Como indicado mais acima, pode ser de tipo simétrico ou do tipo assimétrico. No segundo caso, colocar-se-á a chave privada na unidade de segurança e a chave pública no descodificador.

[0014] Da mesma maneira, aquando da preparação da mensagem codificada, a nova chave assimétrica será codificada pela chave privada que corresponde à primeira chave pública do dito descodificador.

[0015] Uma verificação suplementar é aplicada pelo programa de actualização, a verificação é baseada no número único do descodificador. A mensagem contem igualmente o número único UA do descodificador. Este número é decifrado pela chave pública comum. Assim, antes de utilizar a primeira chave do descodificador, o programa verifica se o número único está de acordo com o que estava previsto.

[0016] O descodificador encontra-se por conseguinte com duas chaves pessoais, sejam a primeira chave e a nova chave pública. Estas duas chaves vão ser utilizadas no mecanismo de emparelhamento com a unidade de segurança.

[0017] A fim de garantir o bom funcionamento do conjunto, a unidade de segurança deverá igualmente receber uma nova chave privada que corresponda à nova chave pública recebida pelo descodificador. Para isso, dispõe de meios de segurança para a transmissão protegida desta chave, que é carregada seguidamente na memória não volátil desta unidade. Pode-se acrescentar um nível de segurança

suplementar à codificação por uma chave de sistema, codificando esta chave privada pela primeira chave. Assim, cada mensagem torna-se única e vinculada à condição de conhecer a primeira chave.

[0018] Esta estrutura permite provocar a evolução da segurança que utiliza uma chave de segurança, numa segurança que utiliza duas chaves (ou mais), sem ruptura do mecanismo de actualização.

[0019] Quando este processo vai decorrer, é recomendado verificar se a chave recebida é a correcta e isto porque, é acrescentado à nova chave assimétrica, um identificador constante, conhecido do programa de actualização. Assim, este programa vai verificar que a chave é mesmo válida antes de a introduzir na sua memória.

[0020] Na prática, é esta unidade de segurança do descodificador que vai receber a mensagem codificada e que a vai transmitir ao descodificador. Quando esta unidade é emparelhada com o descodificador, a mensagem assim transmitida é codificada pela primeira chave que é a chave de emparelhamento.

Reivindicações

1. Um método para a actualização da segurança aplicada à ligação entre um descodificador e a sua unidade de segurança que é constituído por uma primeira chave emparelhada, o referido descodificador que é composto por um número único e está ligado a um centro de gestão, este método que é constituído pelas etapas seguintes:

- transmissão do centro de gestão para os descodificadores em causa, de uma chave pública comum e de um programa de actualização,
- preparação no centro de gestão e para cada descodificador, de uma mensagem codificada, esta mensagem que contem o número único do descodificador assim como uma nova chave assimétrica pública codificada pela primeira chave do dito descodificador e pela chave privada comum,
- execução no descodificador do programa de actualização e verificação do número único do descodificador, com aquele recebido na mensagem e extracção da nova chave assimétrica pública da mensagem, graças à chave pública comum e sua primeira chave,
- armazenamento desta nova chave assimétrica pública no descodificador
- transmissão do centro de gestão para a unidade de segurança da nova chave assimétrica privada por uma mensagem protegida,
- armazenamento desta nova chave assimétrica privada na unidade de segurança.

2. Um método de acordo com a reivindicação 1, caracterizado por a primeira chave ser do tipo simétrico.

3. Um método de acordo com a reivindicação 1, caracterizado por a primeira chave ser do tipo assimétrico, a nova chave assimétrica pública é codificada pela primeira chave privada que corresponde à primeira chave pública do dito descodificador.