(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 572 146**

(51) Int. CI.:

***G06F 21/33*** (2013.01)
***G06F 21/10*** (2013.01)
***G06F 21/44*** (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.05.2005 E 05742473 (1)**

(97) Fecha y número de publicación de la concesión europea: **30.03.2016 EP 1756694**

(54) Título: **Método de autenticación para autenticar un primer participante para un segundo participante**

(30) Prioridad:

**04.06.2004 EP 04102536**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**30.05.2016**

(73) Titular/es:

**KONINKLIJKE PHILIPS N.V. (100.0%)**
**HIGH TECH CAMPUS 5**
**5656 AE EINDHOVEN, NL**

(72) Inventor/es:

**MAES, MAURICE J. J. J-B;**
**SKORIC, BORIS;**
**STARING, ANTONIUS A. M. y**
**TALSTRA, JOHAN C.**

(74) Agente/Representante:

**ISERN JARA, Jorge**

## DESCRIPCIÓN

Método de autenticación para autenticar un primer participante para un segundo participante

Campo de la invención

La presente invención se refiere a los sistemas de protección de copia, y más específicamente a un método de autenticación para autenticar un primer participante para un segundo participante, donde se realiza una operación con la condición de que la autenticación se realice correctamente.

Antecedentes de la invención

En diversos sistemas de protección de copia (CPS) en los que el contenido tiene que transferirse a través de un canal de comunicaciones de acceso público, tal como un enlace inseguro entre ordenadores o una interfaz de unidad/host en un PC, se produce un procedimiento en el que un dispositivo de hardware y una aplicación de software tienen que probarse entre sí que son fiables. Este procedimiento se denomina autenticación. Una etapa importante en el proceso de autenticación es un intercambio mutuo de certificados de clave pública. Un certificado de clave pública es un certificado pequeño, firmado digitalmente por una autoridad de certificación bien conocida y de confianza (CA), que atestigua el hecho de que un determinado dispositivo o aplicación con un número de identificación ID tiene una clave pública (PK). A continuación en el presente documento, el dispositivo y la aplicación se denominan también como participantes. La PK de la CA se conoce comúnmente, y puede usarse por cualquier participante para verificar la firma de la CA en el certificado.

Para activar este proceso, cada participante contiene un número de claves secretas denominadas claves privadas. Estas claves y el flujo de control que usan deberían estar bien protegidos con el fin de evitar que los piratas informáticos sorteen los CPS. Sin embargo, a largo plazo, es probable que se pirateen algunos o incluso muchos dispositivos, así como aplicaciones, tales como el software de reproducción, y por lo tanto se realice la copia de contenido no autorizado.

Con el fin de realizar dicha copia no autorizada más difícil, ha llegado a usarse la llamada revocación. Una lista de revocación de certificados (CRL) se prepara, conteniendo información sobre qué participantes se revocan. Como una parte del procedimiento de autenticación, todos los participantes están obligados a leer la CRL, y si al menos uno de los dos participantes que interactúan se revoca se interrumpe el procedimiento. Hay dos tipos de CRL. Una lista blanca (WL) que enumera todos los participantes que son compatibles en un momento determinado de tiempo. Una lista negra (BL) que enumera todos los dispositivos que se han revocado. Para los fines de esta solicitud, no hay diferencia en la información que contienen la WL y la BL, ya que el conocimiento de todos los dispositivos revocados determina que todavía son compatibles, y viceversa.

Sin embargo, hay diferencias en la forma en que se interpretan y se usan. Cuando se usa un BL, un primer participante, o participante que verifica, que desea determinar que un segundo participante o participante que demuestra, no está revocado, tiene que obtener la BL completa. Cuando se usa un WL, el participante que verifica solo tiene que obtener la parte de la WL que se refiere al participante que demuestra. Por lo tanto el uso de una lista blanca es ventajoso en términos de los requisitos de almacenamiento y las cargas de bus de transmisión en los CPS. Esto es de particular importancia cuando el participante que verifica es un dispositivo que tiene poca potencia de cálculo, tal como una unidad óptica. El procesamiento y el análisis de una BL larga serían gravosos para un dispositivo de este tipo.

Sin embargo, una lista blanca simple requiere que cada participante tenga su propio certificado que acredite su estado de no revocación, lo que resulta en una sobrecarga de red o almacenamiento de disco excesivos. Para mitigar este inconveniente, es útil un enfoque de dos etapas como se desvela en los documentos WO03/10788 (expediente del mandatario PHNL020543) y WO03/10789 (expediente del mandatario PHNL020544). El participante que demuestra no solo suministra su certificado de clave pública, sino también un certificado de grupos (GC). El GC es una prueba concisa del hecho de que uno o más grupos, a uno de los cuales pertenece el participante que demuestra, no se han revocado. El mismo GC puede usarse por muchos participantes, es decir, todos los participantes que se mencionan en el GC. Efectivamente la totalidad de la CRL se ha dividido en los GC, que se firman individualmente y que se distribuyen a los participantes comunicantes. Una forma de usar los GC, de acuerdo con las solicitudes de patente internacionales mencionadas anteriormente, es indicar los límites superior e inferior de cada grupo representado en el GC. Cuando un participante de un grupo específico pierde su condición de participante autorizado, se generarán uno o más nuevos GC. Una mejora adicional se describe en la solicitud de patente europea 04101104.0 (expediente del mandatario PHNL040332). Esta mejora comprende la generación de una representación codificada de longitud de ejecución de un estado de autorización de un número de dispositivos.

Con el fin de tener un buen efecto de prevención de pirateo usando los CG, debería forzarse a los participantes a usar los GC más recientes, con el fin de usar una información de revocación que no esté fuera de fecha. De lo contrario, la herramienta de revocación es de poca utilidad. En el documento US 5.949.877 se desvela un método en

el que se comparan unas fechas de creación relativas de las CRL. La lista de revocación de un participante que verifica se actualiza cuando el participante recibe una lista más reciente.

En una implementación de las intenciones del documento US 5.949.877, cada GC lleva un número de secuencia (SeqNo) que indica el momento en que se ha creado el GC por la CA. Por lo tanto, un SeqNo superior corresponde a un tiempo más reciente. Normalmente, como se ha ejemplificado anteriormente, se genera un nuevo conjunto de GC después de una revocación, llevando cada GC un SeqNo aumentado. Los participantes compatibles tienen que comparar el SeqNo de un GC recibido con cierta medida de "frescura". Normalmente, esta medida es un número de validez (VN), de tal manera que los GC con SeqNo ≥ VN se aceptarán como unos certificados válidos y los GC con SeqNo < VN se rechazarán. Hay varias maneras para que un participante encuentre nuevos GC y VN, tales como a través de unas conexiones en línea, a través de unos discos y por el contacto con otros participantes. Todos los participantes compatibles almacenan un VN, posiblemente el más alto descubierto hasta ahora. Debido a la disparidad en la potencia de procesamiento entre los PC y, al menos algunos periféricos normalmente de bajo consumo, tales como por ejemplo, los dispositivos ópticos, el almacenamiento de los GC se maneja de manera diferente. Por lo tanto, las aplicaciones almacenan un conjunto completo de los GC que llevan el SeqNo más alto descubierto hasta ahora, mientras que tales periféricos no almacenan los GC.

Sin embargo, el uso de los VN puede provocar situaciones no deseadas. Considérese, por ejemplo, una comparación de un SeqNo y un VN en una situación de reproducción. Como un primer enfoque, se supone que una unidad siempre almacena el SeqNo más alto visto hasta ahora en un registro VN de la misma, y que la unidad, durante el procedimiento de autenticación, exige que el GC de la aplicación de reproducción tenga SeqNo ≥ VN. Esta manera de usar los SeqNo y los VN se considera, por ejemplo, como una opción para una normalización de BD-ROM (Disco ROM Blu-ray). Entonces, podría ocurrir una seria molestia al usuario en situaciones fuera de línea como se describirá a continuación.

Ahora considérese un uso alternativo de los SeqNo - VN, de acuerdo con una segunda aproximación. Durante el procedimiento de autenticación para la reproducción, un dispositivo usa el VN entregado a través del disco, que se va a reproducir. El GC de la aplicación solo se acepta si tiene SeqNo ≥ $VN_{disc}$. Este enfoque es una manera más fácil de usarse.

Sin embargo, desde el punto de vista de los propietarios del contenido, el segundo enfoque tiene un serio inconveniente. Si se piratea una aplicación "App", sus secretos pueden usarse para construir una aplicación pirateada de contenido robado "Copia", que a continuación se distribuye a través de Internet. La CA revocará la App enumerando las aplicaciones como no autorizadas en todas las futuras WL; dicha App todavía está autorizada en los GC con SeqNo = X, pero revocada en todos los GC con SeqNo > X. A continuación, a pesar de esta revocación, siempre puede usarse la Copia para robar el contenido de todos los discos con $VN_{disc}$ ≤ X. En el primer enfoque esto es mucho más difícil, ya que el pirata tendría que aislar su dispositivo de todos los nuevos discos.

Considérese de nuevo el primer enfoque. Un usuario con un ordenador portátil y una App de software de reproducción ha comprado un nuevo disco. Resulta que el disco tiene un VN que es más alto que el SeqNo de la App, y por lo tanto se deniega la aplicación. A continuación, el usuario tendrá que actualizar la App descargando (posiblemente gratis) un programa de reemplazo. Sin embargo, si el usuario no tiene acceso a Internet en el momento, lo que ocurriría con bastante frecuencia para el propietario de un ordenador portátil, no es posible la actualización. Además de las molestias que esto pueda provocar, el usuario no será capaz de reproducir los discos viejos, ya que la unidad de disco del ordenador portátil ha almacenado el VN del disco y no permitirá que se ejecute la App. En otras palabras, los discos que han trabajado siempre dejan de funcionar repentinamente, hasta que el usuario sea capaz de descargar el software actualizado. Hay varias otras situaciones, bastante comunes, en las que el VN de la unidad se verá aumentado de tal manera que la ejecución de una aplicación de software se bloquea hasta que el usuario pueda actualizar la aplicación. Una situación de este tipo es en la que una unidad extraíble se comunica con una aplicación que tiene un SeqNo que es mayor que el VN de la unidad, mientras que interactúa con el otro PC. Otra situación de este tipo similar es en la que múltiples aplicaciones de software en el mismo PC se comunican con la misma unidad pero no están manteniendo un ritmo igual.

A pesar de que el primer enfoque dará lugar algunas veces a una situación en la que la aplicación del usuario dejará de funcionar a pesar de que no se haya revocado, será probablemente el más usado. A continuación se planteará una demanda de un desarrollo que reduce la molestia del usuario.

Sumario de la invención

Es un objeto de la presente invención proporcionar un método de autenticación que sirva mejor que la técnica anterior descrita anteriormente a los fines de tanto los usuarios como de los propietarios de contenido.

El objeto se consigue de acuerdo con un método como se define en la reivindicación 1 del conjunto adjunto de reivindicaciones.

Por lo tanto, en un primer aspecto de la misma, la invención proporciona un método de autenticación para autenticar un primer participante para un segundo participante, en el que se realiza una operación con la condición de que la autenticación se realice correctamente, comprendiendo las etapas de:

- verificar si el primero participante está autenticado; y
- si el primer participante no está autenticado, entonces clasificar el primer participante para una sub-autorización, en el que, si se clasifica el primer participante para la sub-autorización, entonces todavía se realizará la operación.

Autenticado significa que se cumplen un conjunto (uno o más) de los criterios primarios o principales que se comprueban durante el procedimiento de autenticación de los mismos. Si el primer participante, tal como una aplicación de software o un dispositivo, no está autenticado, la operación condicional todavía puede realizarse, bajo ciertas condiciones. Si se cumplen esas condiciones determinadas, se concede una sub-autorización.

De este modo, este método, por ejemplo, permite el uso de al menos algunas aplicaciones que se habrían rechazado en los métodos de la técnica anterior. Mediante las opciones apropiadas de las condiciones para la sub-autorización, se evita la molestia de usuario fuera de línea mencionada anteriormente. Ejemplos de implementación son evidentes a partir de las realizaciones de la siguiente manera.

De acuerdo con una realización del método de autenticación, un certificado de compatibilidad está implicado en el proceso de autenticación. Por lo tanto, solo se autentican los participantes compatibles.

De acuerdo con una realización del método de autenticación, también está implicada en el procedimiento de autenticación una fecha de una medida de emisión que se incluye en el certificado. La fecha de medida de emisión está relacionada con el tiempo, tal como la fecha en que se ha emitido el certificado. Por ejemplo, la fecha de medida de emisión podría ser un número de secuencia, que se aumenta cada vez que se emite un nuevo certificado.

De acuerdo con una realización del método de autenticación, la clasificación para una sub-autorización depende del resultado de la comparación. Por ejemplo, mediante una elección apropiada de la medida de comparación, un uso de las medidas es para controlar la edad que se acepta de los certificados.

De acuerdo con una realización del método de autenticación, se define un intervalo de números de validez permitidos. Este intervalo puede usarse para definir unos límites superior e inferior, que estrechan las posibilidades para conceder una sub-autorización, a pesar de que está incluida en la definición que el intervalo puede cubrir cualquier parte (o incluso todas) de la serie existente de números.

De acuerdo con una realización del método de autenticación, se define un número de validez mínimo. Si la fecha de la medida de emisión es menor que el número de validez mínimo no se concederá ninguna sub-autorización. Esto se usa preferentemente para evitar que los participantes que tienen certificados demasiado viejos se les concedan una sub-autorización.

De acuerdo con una realización del método de autenticación, se clasifica el primer participante para un sub-asignación aunque no es compatible de acuerdo con el certificado. Sin embargo, la sub-autorización solo se concederá siempre y cuando la fecha de la medida de emisión sea lo suficientemente alta, es decir, que el certificado y, en consecuencia, la incompatibilidad, sea lo suficientemente reciente. Por supuesto, de nuevo, no se especifica el valor máximo pero, preferentemente, se elige relativamente alto.

De acuerdo con una realización del método de autenticación, dos números de validez diferentes, es decir, un número actual y un número anterior, del segundo participante se usan como los valores límite del intervalo. De ese modo es posible hacer el intervalo en función de las actualizaciones de los números de validez del segundo participante.

De acuerdo con una realización del método de autenticación, se usa un contador de gracia para controlar el número de veces que se sub-autorizan el primer participante, y otros primeros participantes, si los hay. En una realización, el contador se disminuye cada vez que se concede al primer participante una sub-autorización. Por ejemplo, esto puede usarse para establecer el contador, en un cierto punto del tiempo, a un número predefinido, y detener la concesión de la sub-autorización cuando el contador llega a cero. Con el fin de que el primer participante vuelva a autenticarse o sub-autorizarse, tiene que renovar el certificado.

En un segundo aspecto de la misma, la presente invención proporciona un dispositivo digital que está dispuesto para actuar como un participante en un proceso de autenticación, en el que se usan unos certificados de compatibilidad para determinar la compatibilidad de los participantes implicados en el proceso de autenticación. El dispositivo comprende una primera zona de memoria que contiene una medida de comparación, que se asocia con el tiempo, y que también se usa en dicho proceso de autenticación, una segunda zona de memoria que contiene una lista limitada de otros participantes que se han implicado en un proceso de autenticación con el dispositivo, y una tercera zona de memoria, que contiene unos certificados de compatibilidad que se refieren a los participantes de dicha lista.

De acuerdo con este segundo aspecto, la invención reduce sustancialmente la molestia de usuario cuando el dispositivo está fuera de línea, al menos en lo que respecta a los problemas encontrados debido a un certificado que es un poco viejo. Aunque la memoria está limitada, la probabilidad es alta de que un certificado, que se refiere al participante a implicarse en el procedimiento de autenticación con el dispositivo digital, se actualice al mismo tiempo que el número de comparación del dispositivo digital. Ya que entonces el certificado es accesible para ese participante, también la probabilidad de un procedimiento de autenticación con éxito es alta. Hay que tener en cuenta que las enseñanzas de este segundo aspecto pueden usarse en combinación con las enseñanzas del primer aspecto. En un tercer aspecto de la misma, la presente invención proporciona un método de autenticación para autenticar un primer participante para un segundo participante, que comprende las etapas de:

- verificar si el primer participante está autenticado; y
- si el primer participante no está autenticado, introducir una identificación del primer participante en un almacenamiento local que contiene una lista de los primeros participantes no autentificados, almacenamiento que es accesible para el segundo participante,

en el que dicha etapa de verificación comprende una etapa de verificar si el primer participante es un miembro de dicha lista.

De acuerdo con este tercer aspecto, localmente se mantiene una clase de lista de revocación de los participantes no autenticados, lista que es accesible para al menos el segundo participante. Por lo tanto, la invención es ventajosa, entre otras cosas, desde una perspectiva de propietario de contenido. Un participante 7 que una vez que se ha introducido en la lista no puede usarse con independencia del tipo de contenido o portador de contenido. Por ejemplo, se elimina el inconveniente del segundo enfoque tratado anteriormente en los antecedentes de la invención.

Estos y otros aspectos de la invención serán evidentes a partir de y se aclararán con referencia a las realizaciones descritas en lo sucesivo en el presente documento.

Breve descripción de los dibujos

La invención se describirá ahora con más detalle y con referencia a los dibujos adjuntos en los que:

La figura 1 muestra, en una vista en perspectiva, un sistema en el que se emplea un método de acuerdo con la presente invención;
La figura 2 es un diagrama de bloques que ilustra cómo una realización del método funciona en el sistema de la figura 1;
La figura 3 es un diagrama de bloques de unas partes relevantes de una realización de un dispositivo digital de acuerdo con la presente invención, y
La figura 4 es un diagrama de bloques de unas partes relevantes de una realización de un dispositivo, que está dispuesto para emplear otra realización de un método de autenticación.

Descripción de las realizaciones preferidas

Un primer participante y un segundo participante se implican en un procedimiento de autenticación, en el que una operación se va a realizar si la autenticación tiene éxito. Para ejemplificar los fines, en una primera realización del método de acuerdo con la presente invención, se supone que el primer participante es una aplicación de software, que el segundo participante es un dispositivo, y que la operación a realizarse es acceder a unos contenidos. Más específicamente, se supone que la aplicación quiere acceder al contenido, que el acceso se aprueba de manera condicional por el dispositivo.

Como parte de la autorización de acceso al contenido, puede necesitarse actualizar la información de derechos de uso asociada con el contenido. Por ejemplo, puede ser necesario disminuirse un contador que indica cuántas veces puede accederse al contenido. Un derecho de reproducción de una sola vez puede necesitar eliminarse o tener su estado establecido a ‘no válido’ o ‘usado’. Un denominado ticket también podría usarse. Véase la patente de Estados Unidos 6.601.046 (expediente del mandatario PHA 23636) para obtener más información sobre el acceso basado en tickets. Esta actualización de los derechos de uso puede hacerse mediante el primer participante o mediante el segundo participante.

Tal como se entiende por los expertos en la materia, existen numerosas combinaciones de diferentes tipos de participantes y de diferentes tipos de operaciones, etc., que están abarcados por el alcance de la presente invención. Unos cuantos ejemplos son los procedimientos de autenticación entre dispositivos móviles y los dispositivos fijos, y entre los PC y los servidores en una red.

Cuando se va a usar una aplicación de software para acceder al contenido de una unidad de contenido recibido por un dispositivo, tiene lugar un procedimiento de autenticación con el fin de autorizar la aplicación para un acceso de este tipo. Una situación típica, como se asume al describir esta realización, es en la que se usa la aplicación para

reproducir el contenido que está almacenado en una unidad de contenido constituida por un disco, que se introduce en un dispositivo constituido por una unidad de disco. Para mejorar la comprensión de esta realización, se considera un sistema como se muestra en la figura 1 y la figura 2. El sistema comprende un ordenador, tal como un ordenador portátil, 101, que tiene la aplicación (App) 103 instalada en el mismo, y una unidad de disco extraíble 105 conectada al mismo. Un disco 107 va a insertarse en la unidad de disco 105. La unidad 105 se comunica con el ordenador 101 a través de un bus de interfaz 109, y el contenido del disco 107 se transfiere a la unidad 105 a través de un enlace óptico 111. Normalmente, el contenido del disco se escanea ópticamente y se convierte en señales electrónicas por medio de un transductor optoelectrónico 113.

La unidad 105 tiene contador de gracia k 115, un registro de número de validez actual (CurrVN) 117, y un registro de número de validez anterior (PrevVN) 119. La aplicación App 103 contiene un certificado de compatibilidad que es un certificado de grupos (GC) 121 de un grupo de aplicaciones y dispositivos que incluye la App 103. El GC 121 tiene una fecha de medida de emisión que es un número de secuencia (SeqNo) 123, cuyo valor está en función del momento en el tiempo cuando se genera el GC 121. El contenido de los registros CurrVN y PrevVN 117, 119 está comprendido en una medida de comparación que se usa para las comparaciones con la fecha de la medida de emisión, es decir, el número de secuencia, como se explicará a continuación.

Cuando se inserta un disco 107 en la unidad 105, y se decide que la aplicación 103 debería usarse para reproducir los contenidos del disco 107, se inicia un procedimiento de autenticación. El disco 107 comprende un número de validez VN que se presenta a la unidad 105. Además comprende un conjunto completo de GC, es decir, todos los certificados emitidos hasta ahora. El VN se compara con el CurrVN 117 de la unidad 105. En general, si el disco es nuevo VN > CurrVN. A continuación, el registro CurrVN 117 se actualiza con el VN, y el conjunto de los GC se almacena en la unidad, y/o en un dispositivo, tal como un PC, al que la unidad 105 está montada o conectada. Como una parte del procedimiento de autenticación, la App 103 tiene que demostrar a la unidad 105 que está autenticada para usarse para acceder al contenido. En el caso básico mencionado anteriormente, el SeqNo del GC 121 se compara con el CurrVN, esto determina que son iguales, también se determina que la App es todavía compatible de acuerdo con el nuevo GC que se refiere a la App 103, y en consecuencia se verifica que la App 103 está autenticada. Por lo tanto, se permite acceder a la App a los contenidos del disco 107.

Sin embargo, en varias situaciones, como también se ha descrito en los antecedentes anteriores, no hay una actualización completa del CurrVN y del GC, por ejemplo, debido a la falta de recursos de memoria en la unidad 105 que eviten la copia de los nuevos GC, mientras que el CurrVN se actualiza con un VN más alto. Además, si la App ya no es compatible de acuerdo con el nuevo GC, esta no se autentica.

De acuerdo con el presente método, en circunstancias específicas, aunque la App no esté autenticada, todavía se permite el acceso. Para los fines de esta aplicación esto se denomina sub-autorización. Sin embargo, ya que una sub-autorización proporciona a la aplicación las mismas ventajas que si estuviese autentificada, aunque los criterios para la autenticación no sean compatibles, algunas limitaciones se asocian a la concesión de la sub-autorización, haciéndola dependiente del tiempo y del número. Por lo tanto, el número de secuencia y los números de validez son elementos asociados con el tiempo, ya que los valores de los mismos están en función de cuando se generan en el tiempo. Como tales, pueden usarse para determinar un período de gracia, como se describirá a continuación. El contador de gracia k es el elemento número, pero también está relacionado con el tiempo de una manera, ya que cuando ha contado hasta un número final ha pasado una cantidad de tiempo, aunque por lo general indefinido. Esto será evidente a partir de la descripción siguiente.

Como una primera etapa de dicho procedimiento de autenticación, el SeqNo 123 se compara con el CurrVN 117. Si SeqNo > CurrVN, entonces:

- el valor de CurrVN se almacena en PrevVN;
- el valor de SeqNo se almacena en CurrVN; y
- el contador de gracia k se establece en k0,

en la que k0 indica un número predefinido de reproducciones bajo una sub-autorización, como se explicará a continuación. A continuación, se comprueba si el GC de la App indica que la App es compatible o no revocada. Si la App no se revoca, entonces se determina, por la unidad 105, que la App se autentica y se admite el acceso al contenido, es decir, la reproducción. Si, por el contrario, la App se revoca, se concederá una sub-autorización. A continuación, se seguirá permitiendo la reproducción, pero solo para k0 tiempos. A tal fin, como un etapa de esta parte de la autenticación, k se disminuye, es decir, k → k-1.

Si SeqNo < CurrVN, entonces, en una siguiente etapa el SeqNo 123 se compara con el PrevVN 119. Si SeqNo < PrevVN, entonces, la App 103 no está autenticado para la unidad 105. Por lo tanto, el usuario no puede acceder al contenido hasta que se haya actualizado la aplicación de software App 103 a una versión más reciente que tenga un GC que lleve un SeqNo suficientemente alto.

Si el SeqNo 123 está incluido en el intervalo de números de validez, es decir, si PrevVN ≤ SeqNo < CurrVN, independientemente del estado de revocación, en una siguiente etapa se comprueba si k > 0. Si es así, entonces la

App se clasifica para una sub-autorización, k se reduce y se permite la reproducción. Si k = 0, entonces no se concede la sub-autorización y se deniega el acceso al contenido. El resultado es el mismo para la combinación de SeqNo = CurrVN, y la App 103 que se revoca. Por último, si SeqNo = CurrVN, y la App no se revoca, entonces la aplicación se autentica. Los contadores no se modifican.

El valor de PrevVN determina el tiempo que una aplicación puede usarse y puede seguir usándose. Sin embargo, ya que PrevVN es solo un número por detrás de CurrVN en un caso típico con un usuario que usa continuamente nuevos discos, nada sino más bien nuevas aplicaciones serán útiles. En una realización alternativa, el número de validez mínimo del intervalo no es el PrevVN sino el número de validez anterior al anterior PrevPrevVN, que es una etapa más atrás del CurrVN. En esta realización, el PrevPrevVN se usa para las comparaciones con el SeqNo en lugar de con el PrevVN. Una ventaja es una mayor probabilidad de que el usuario pueda seguir usando su aplicación de reproducción personalizada durante el período de gracia, al tiempo que se evita el uso de herramientas de pirateo muy antiguas.

En otra realización alternativa, no existe el contador del PrevVN. Esto corresponde a fijar permanentemente el PrevVN a cero. En esta realización es absolutamente cierto que el usuario puede seguir usando su aplicación de reproducción personalizada durante el período de gracia.

En una realización de un dispositivo digital de acuerdo con esta invención, el dispositivo digital 300 es un dispositivo de tipo de pocos recursos, tal como una unidad óptica típica. Tiene muy poca capacidad de memoria para almacenar, por lo general en una memoria cache, la lista completa de los GC. Sin embargo, tiene una cantidad limitada de memoria 301, y más específicamente una memoria de acceso aleatorio no volátil (NVRAM), que es capaz de contener algunos GC. Además, la unidad 300 mantiene una lista de los participantes, es decir, aplicaciones o dispositivos, con los que ha participado en un procedimiento de autenticación. Preferentemente, esta lista es una lista primero en entrar, primero en salir (FIFO), ya que a lo largo del tiempo, normalmente, solo puede contener una parte de todos los participantes. Como se muestra en la figura 3, la unidad 300 tiene un primera zona de memoria 303 que contiene una medida de comparación, que en esta realización es un número de validez VN, una segunda zona de memoria 305 que contiene la lista FIFO, y una tercera zona de memoria 307, que contiene los GC que se refieren a los participantes de la lista FIFO en 305.

Cuando la unidad 300 actualiza su VN, también almacena los GC que se refieren a los participantes de la lista FIFO en la tercera zona de memoria 307. Cuando un participante de la lista FIFO participa en un procedimiento de autenticación con la unidad 300, al igual que anteriormente, el SeqNo del GC correspondiente se compara con el VN de la unidad 300. Con el fin de que el participante pueda autenticarse, tiene que tenerse en cuenta como compatible en el GC, y tiene que satisfacerse SeqNo ≥ VN. Normalmente, ya que el participante está en la lista FIFO su GC se ha actualizado junto con el VN de la unidad 300, y por lo tanto su SeqNo es lo suficientemente alto. Sin embargo, si el participante no está en la lista FIFO existe una probabilidad aumentada de una autenticación sin éxito. Hay que tener en cuenta que, en esta realización del dispositivo, el procedimiento de autenticación que el dispositivo inicia o en el que participa puede ser como en cualquiera de las realizaciones descritas anteriormente.

De acuerdo con la presente invención, se proporciona también un procedimiento de autenticación entre los participantes primero y segundo, en el que se verifica si el primer participante está autenticado. Si el primer participante no está autenticado, se introduce una identificación del primer participante en un almacenamiento local que contiene una lista de los primeros participantes no autenticados, almacenamiento que es accesible para el segundo participante. La verificación comprende una prueba de compatibilidad y una prueba de si el primer participante es un miembro de la lista de no autenticación. Esta lista local puede considerarse como una BL local. Un dispositivo que está equipado y actúa de acuerdo con esta realización se muestra más esquemáticamente en la figura 4. El dispositivo 400, tal como una unidad de disco óptico, tiene una memoria 401 que comprende un primera zona de memoria 403, que contiene un número de validez VN, y una segunda zona de memoria 405 que contiene la BL local. Siempre que un primer participante, tal como una aplicación, falla al autenticar a la unidad 400 de su identificación (ID) se almacena en la BL local en la segunda zona de memoria 405. Siempre que una aplicación intenta autenticar a la unidad 400, usando un GC diciendo que es compatible, y que comprende un SeqNo ≥ VN, la unidad prueba si la aplicación se produce en la BL local. Si es así, la unidad 400 aborta la autenticación, de otro modo se autentica la aplicación. Esta realización es de un valor específico si la primera memoria es volátil y toma el valor del VN disponible actualmente en el disco presente.

El método puede implementarse como un programa informático que comprende partes de código ejecutable que realizan las etapas de acuerdo con el método. El programa se carga en y se ejecuta por, el dispositivo, tal como la unidad de disco descrita anteriormente, que tiene la función de verificar la compatibilidad de la aplicación de software.

La invención puede encontrar una aplicación en las redes domésticas. Una red doméstica típica incluye un número de dispositivos, por ejemplo, un receptor de radio, un sintonizador/decodificador, un reproductor de CD, un par de altavoces, un televisor, un VCR, una grabadora digital, un teléfono móvil, un reproductor de cintas, un ordenador personal, un asistente digital personal, una unidad de visualización portátil, y así sucesivamente. Estos dispositivos están, en general, interconectados para permitir que un dispositivo, por ejemplo, la televisión, controle a otro, por

ejemplo, el VCR. Un dispositivo, tal como, por ejemplo, el sintonizador/decodificador o decodificador (STB), es por lo general el dispositivo central, que proporciona un control central sobre los otros. El contenido, que comprende normalmente cosas como música, canciones, películas, programas de TV, imágenes, juegos, libros y similares, pero que también puede incluir servicios interactivos, se recibe a través de una pasarela residencial o un decodificador externo. El contenido también podría introducirse en el hogar a través de otras fuentes, tales como unos medios de almacenamiento como discos o usando dispositivos portátiles.

La red doméstica puede funcionar como un dominio autorizado. En este tipo de sistemas de protección de contenido (como el SmartRight de Thomson, o el DTCP de DTLA), un conjunto de dispositivos puede autenticarse entre sí a través de una conexión bidireccional. Basándose en esta autenticación, los dispositivos confiarán entre sí y esto les permitirá intercambiar contenido protegido. En las licencias que acompañan al contenido, se describe qué derechos tiene el usuario y qué operaciones se permiten realizar en el contenido.

Algunas arquitecturas específicas de los dominios autorizados se han descrito en la solicitud de patente internacional WO 03/098931 (expediente del mandatario PHNL020455), la solicitud de patente europea número de serie 03100772.7 (expediente del mandatario PHNL030283), la solicitud de patente europea número de serie 03.102.281,7 (expediente del mandatario PHNL030926), la solicitud de patente europea número de serie 04100997.8 (expediente del mandatario PHNL040288) y F. Kamperman y W. Jonker, P. Lenoir, y B. vd Heuvel, Secure content management in authorized domains, Proc. IBC2002, páginas 467-475, Septiembre de 2002.

Hay que tener en cuenta, que para los fines de esta solicitud, y en particular con respecto a las reivindicaciones adjuntas, la palabra "comprende" no excluye otros elementos o etapas, que la palabra "un" o "una", no excluye una pluralidad, que por sí misma será evidente para los expertos en la materia.

En la reivindicación de dispositivo que enumera varios medios, varios de estos medios pueden realizarse por uno y el mismo elemento de hardware. El mero hecho de que determinadas medidas se mencionen en las reivindicaciones dependientes diferentes entre sí, no indica que una combinación de estas medidas no pueda usarse de manera ventajosa.

**REIVINDICACIONES**

1. Un método de autenticación para autenticar un primer participante para un segundo participante, en el que se realiza una operación con la condición de que la autenticación se realice correctamente, que comprende las etapas de:

- verificar si el primer participante está autenticado o no, comprendiendo la verificación
- comparar una fecha de la medida de emisión de un certificado de compatibilidad con una medida de comparación del segundo participante, comprendiendo la medida de comparación un intervalo de números de validez permitidos, definido por un número de validez mínimo y un número de validez máximo, en el que dicho primer participante se autentica solo si se determina por la comparación de que la fecha de la medida de emisión no está fuera de la fecha establecida por el número de validez máximo, y
- verificar si el primer participante es compatible o no de acuerdo con un certificado de compatibilidad que se refiere al primer participante, en el que se autentica al primer participante solo si es compatible; y
- si el primer participante no está autenticado, entonces clasificar el primer participante para una sub-autorización en función del valor de un contador de gracia asociado con un número de veces que los primeros participantes se han clasificado para la sub-autorización, en el que, si el primer participante se clasifica para la sub-autorización, la operación todavía se realiza y el contador de gracia se reduce, en el que dicha clasificación del primer participante para una sub-autorización depende del resultado de una etapa de
- comparar una fecha de medida de emisión del certificado de compatibilidad con la medida de comparación del segundo participante, no clasificándose el primer participante para dicha sub-autorización si la fecha de la medida de emisión es menor que el número de validez mínimo de dicho intervalo de números de validez permitidos.

2. Un método de autenticación de acuerdo con la reivindicación 1, en el que dicha clasificación del primer participante para una sub-autorización depende del resultado de una etapa de

- comparar una fecha de medida de emisión del certificado de compatibilidad con una medida de comparación del segundo participante.

3. Un método de autenticación de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que un número de validez máximo de dicho intervalo de números de validez permitidos es un número de validez actual almacenado en el segundo participante.

4. Un método de autenticación de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que un número de validez mínimo de dicho intervalo de números de validez permitidos es un número de validez anterior almacenado en el segundo participante.

5. Un método de autenticación de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que dicho certificado de compatibilidad es un certificado de grupos.

6. Un método de autenticación de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que la operación comprende acceder a un contenido.

7. Un método de autenticación de acuerdo con la reivindicación 6, en el que dicho contenido se almacena en un disco óptico.

8. Un método de autenticación de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que dicho primer participante es una aplicación de software y dicho segundo participante es un dispositivo.

9. Un método de autenticación de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que el segundo participante contiene una lista limitada de los primeros participantes, que comprende las etapas de: almacenar, en el segundo participante, un conjunto actualizado de certificados de compatibilidad que contienen los certificados de compatibilidad que se refieren a los primeros participantes de dicha lista de primeros participantes.

10. Un método de autenticación de acuerdo con la reivindicación 9, que comprende la etapa de:

- actualizar, en el segundo participante, una medida de comparación, que está asociada con el tiempo, y que se usa también en dicho procedimiento de autenticación, en el que almacenar el conjunto actualizado de certificados de compatibilidad está en relación con dicha actualización.

11. Un dispositivo digital que está dispuesto para actuar como un segundo participante en un método de autenticación para autenticar un primer participante para un segundo participante, realizando el dispositivo una operación con la condición de que la autenticación se realice correctamente, en el que se usan certificados para determinar la compatibilidad de los participantes implicados en el procedimiento de autenticación, en el que el dispositivo comprende un primera zona de memoria que contiene una medida de comparación, comprendiendo la medida de comparación un intervalo de números de validez permitidos, definido por un número de validez mínimo y

un número de validez máximo, y que también se usa en dicho procedimiento de autenticación, estando dispuesto el dispositivo digital para:

- verificar si el primer participante está autenticado o no, comprendiendo la verificación
- comparar una fecha de la medida de emisión de un certificado de compatibilidad con la medida de comparación, en el que solo se autentica dicho primer participante si se determina por la comparación que la fecha de la medida de emisión no está fuera de la fecha establecida por el número de validez máximo, y
- verificar si el primer participante es compatible o no de acuerdo con un certificado de compatibilidad que se refiere al primer participante, en el que solo se autentica el primer participante si es compatible; y
- si el primer participante no está autenticado, entonces clasificar el primer participante para una sub-autorización en función del valor de un contador de gracia asociado con un número de veces que los primeros participantes se han clasificado para la sub-autorización, en el que, si el primer participante se clasifica para la sub-autorización, la operación todavía se realiza y el contador de gracia se reduce, en el que dicha clasificación del primer participante para una sub-autorización depende del resultado de una etapa de
- comparar una fecha de una medida de emisión del certificado de compatibilidad con la medida de comparación del segundo participante, no clasificándose el primer participante para dicha sub-autorización si la fecha de medida de emisión es menor que el número de validez mínimo de dicho intervalo de números de validez permitidos.

12. Un dispositivo digital de acuerdo con la reivindicación 11, que comprende una segunda zona de memoria que contiene una lista limitada de otros participantes que han estado implicados en un procedimiento de autenticación con el dispositivo, y una tercera zona de memoria, que contiene los certificados de compatibilidad que se refieren a los participantes de dicha lista.

13. Un dispositivo digital de acuerdo con la reivindicación 12, en el que el dispositivo está dispuesto para:

cuando está disponible una medida de comparación más reciente, actualizar la primera memoria con dicha medida de comparación más reciente y, junto con dicha actualización, actualizar la tercera zona de memoria con los certificados de compatibilidad más recientes que se refieren a los participantes de dicha lista.

14. Un dispositivo digital de acuerdo con la reivindicación 12 o 13, que está dispuesto para actualizar dicha lista de los otros participantes con el participante actual cuando está implicado en un procedimiento de autenticación.

15. Un método de autenticación para autenticar un primer participante para un segundo participante de acuerdo con una cualquiera de las reivindicaciones 1-10, que comprende las etapas de:

- verificar si el primer participante está autenticado; y
- si el primer participante no está autenticado, introducir una identificación del primer participante en un almacenamiento local que contiene una lista de los primeros participantes no autentificados, almacenamiento que es accesible para el segundo participante,

en el que dicha etapa de verificación comprende una etapa de verificar si el primer participante es un miembro de dicha lista.

16. Un método de autenticación de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que el segundo participante obtiene dicha medida de comparación a partir de un soporte de datos.

17. Un producto de programa informático, que puede cargarse directamente en la memoria interna de un dispositivo digital, que comprende unas partes de código de software para hacer que el dispositivo realice las etapas del método de autenticación de acuerdo con una cualquiera de las reivindicaciones 1-10, 15 y 16.

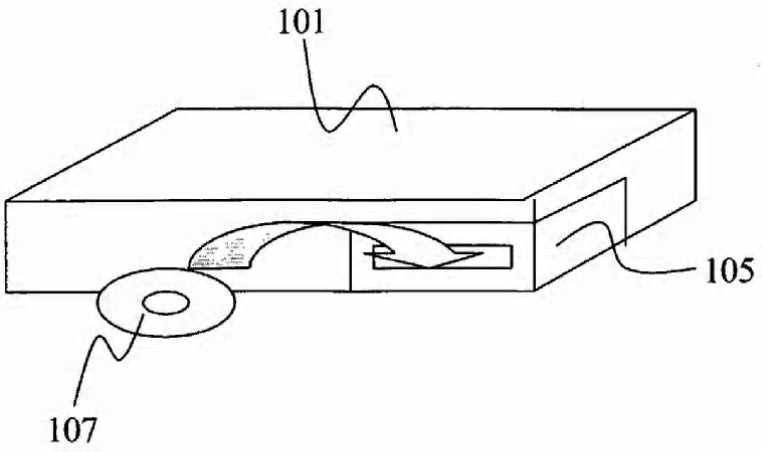


Fig. 1

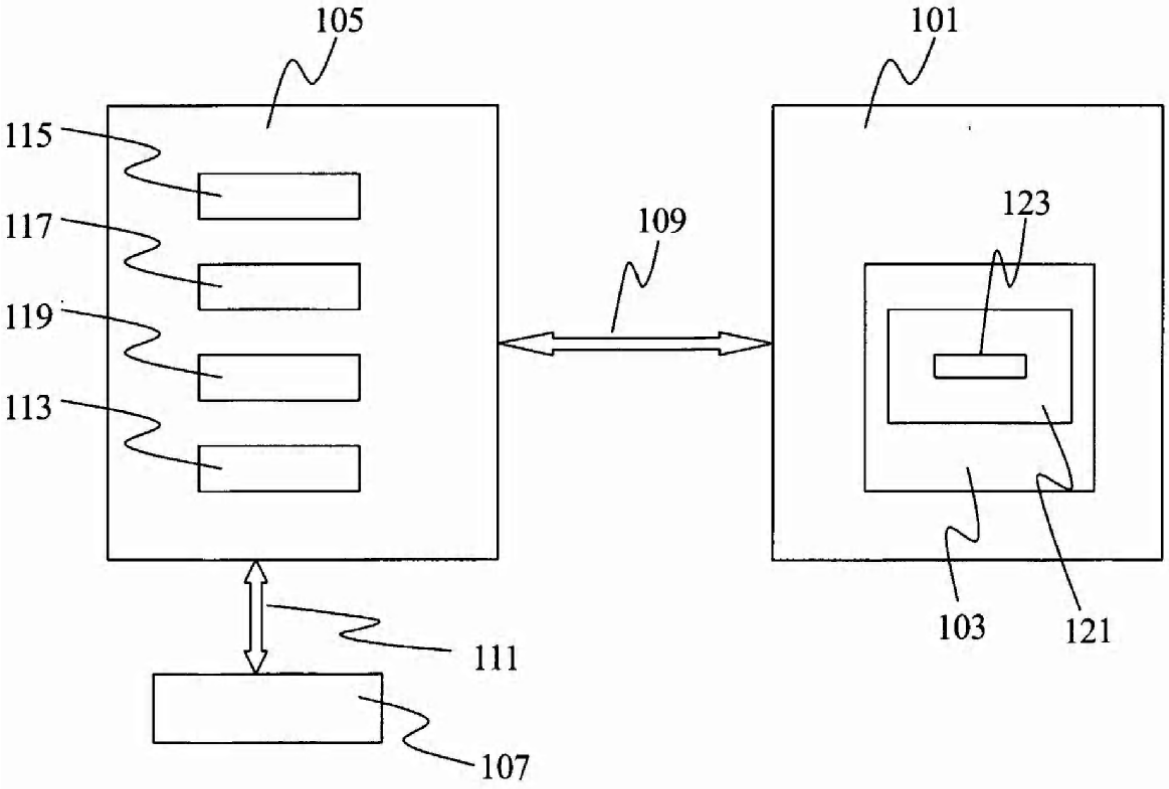


Fig. 2

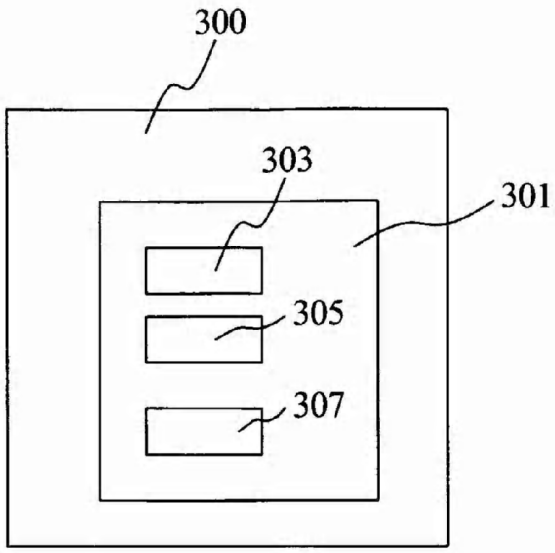


Fig. 3

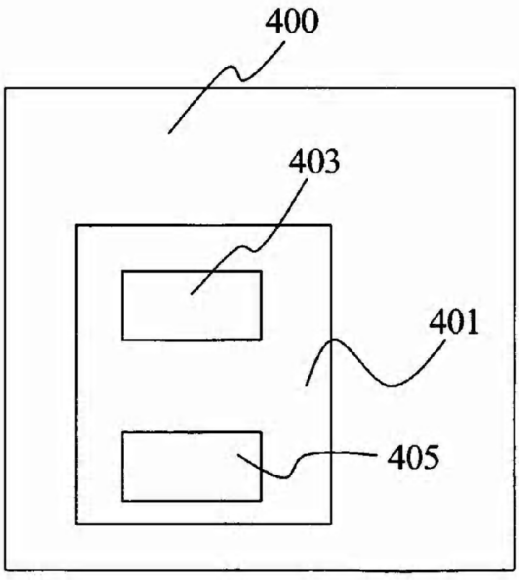


Fig. 4