



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 367 635**

51 Int. Cl.:
G07C 9/00 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **04742504 .6**

96 Fecha de presentación : **14.04.2004**

97 Número de publicación de la solicitud: **1618535**

97 Fecha de publicación de la solicitud: **25.01.2006**

54 Título: **Procedimiento de control de acceso seguro.**

30 Prioridad: **28.04.2003 FR 03 05153**

45 Fecha de publicación de la mención BOPI:
07.11.2011

45 Fecha de la publicación del folleto de la patente:
07.11.2011

73 Titular/es: **MORPHO**
27, rue Leblanc
75015 Paris, FR

72 Inventor/es: **Lambert, Laurent y**
Fondeur, Jean-Christophe

74 Agente: **De Elzaburu Márquez, Alberto**

ES 2 367 635 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimiento de control de acceso seguro

La presente invención se refiere a un procedimiento de control de acceso seguro.

- 5 Hoy día, controlar el acceso a un lugar protegido o a un sistema informático es primordial. Este control de acceso pasa por la definición de una lista de personas autorizadas. Una vez registrados los parámetros de acceso, el sistema de control de acceso autoriza el acceso solamente en función de informaciones recibidas de acuerdo con las condiciones de acceso establecidas previamente. Este procedimiento de control de acceso comprende generalmente una fase de identificación y una fase de verificación. Este procedimiento es denominado en lo que sigue, procedimiento de identificación consolidada.
- 10 Un procedimiento de identificación consolidada puede ser realizado, por ejemplo, con la ayuda de medios biométricos. Este es el caso, por ejemplo, de los procedimientos de identificación consolidada que consisten, por una parte, en identificar por una toma de huella digital a la persona que solicita el acceso y, por otra, en verificar el carácter vivo del dedo portador de esta huella digital. Un sistema de este tipo se presenta por ejemplo en forma de sensores de huella digital que comprenden medios ópticos previstos para realizar una imagen de una persona y medios eléctricos previstos para realizar mediciones eléctricas del dedo portador de esta huella. Con la ayuda de un dispositivo de tratamiento vinculado al portador, la imagen de la huella es comparada en un banco de imágenes con el fin de identificar a la persona poseedora del dedo correspondiente, y las mediciones eléctricas son comparadas entre sí o con otras características extraídas de la imagen de la huella del dedo con el fin de verificar si este dedo es vivo.
- 15 La solicitud internacional WO 95/26013 describe un procedimiento de identificación consolidada de este tipo que consiste en autorizar el acceso de una persona cuando ésta ha sido identificada por una toma de medición de identificación y esta información ha sido validada por una toma de medición u otras varias tomas de mediciones y en rechazar el acceso en caso contrario.
- 20 Por estos procedimientos de identificación consolidada de dos fases, los intentos de fraude son limitados. Sin embargo, se ha constatado que el número de intentos reducía la fiabilidad del sistema, pudiendo por ejemplo un defraudador que haya conseguido ser identificado como una persona autorizada, hacer validar esta identificación y así corromper el sistema al cabo de algunas decenas de intentos.
- 25 El objetivo de la invención es, por tanto, mejorar la seguridad de los procedimientos de identificación consolidada evitando que numerosos intentos permitan burlarla.
- 30 Se conoce una solución para asegurar las transacciones bancarias que pueden parecerse a la identificación consolidada de persona. Por ejemplo, la solicitud de patente americana US2002138444 describe un sistema en el cual, después de haber introducido una tarjeta bancaria en un terminal, se realiza una verificación en una lista de tarjetas bloqueadas y si la tarjeta no está bloqueada, el usuario debe introducir su código PIN. Si el código no es correcto, el número de identificación de la tarjeta queda registrado en la lista de las tarjetas bloqueadas.
- 35 El problema encontrado por este sistema es que una vez bloqueada una tarjeta, el usuario ya no puede utilizar su tarjeta, haciendo al sistema ciertamente seguro pero poco sensible.
- El objetivo de la presente invención es, por tanto, mejorar la seguridad de los procedimientos de identificación consolidada evitando que numerosos intentos permitan burlarla, al tiempo que una persona, de la cual ha sido identificada y validada una característica, pero que esté presente en la lista de revocación, no sea objeto de un rechazo sistemático.
- 40 A tal efecto, la presente invención se refiere a un procedimiento de identificación consolidada de una persona de acuerdo con el objeto de la reivindicación independiente 1.
- De acuerdo con otra característica de la invención, un medio de identificación es elegido entre los medios de reconocimiento de huella digital, de iris, de voz, o un código secreto y un medio de medición es elegido entre los medios de medición de impedancia, de inductancia, de presión sanguínea o de temperatura.
- 45 De acuerdo con otra característica de la invención, el citado procedimiento consiste en comparar los resultados de medición obtenidos por el citado o cada medio de identificación con datos preestablecidos y en identificar a una persona cuando los resultados de medición correspondan a datos preestablecidos para la citada persona.
- De acuerdo con otra característica de la invención, el citado procedimiento consiste en validar una identificación de una persona cuando los resultados de medición obtenidos por el citado o cada medio de medición correspondan a criterios de aceptabilidad.
- 50 De acuerdo con otra característica de la invención, la citada característica registrada en la citada lista de revocación es al menos el resultado de una toma de medición que permita una identificación o una información deducida del citado resultado.

De acuerdo con otra característica de la invención, la citada información es la identidad de la persona identificada.

Las características de la invención anteriormente mencionadas, así como otras se pondrán de manifiesto de modo más claro con la lectura de la descripción que sigue de un ejemplo de realización, realizándose la citada descripción en relación con los dibujos anejos, en los cuales:

5 La Fig. 1 representa un organigrama de las etapas del procedimiento de identificación consolidada de acuerdo con un primer modo de realización de la invención.

La Fig. 2 representa un organigrama de las etapas del procedimiento de identificación consolidada de acuerdo con un segundo modo de realización de la invención.

10 La Fig. 3 representa un organigrama de las etapas del procedimiento de identificación consolidada de acuerdo con un tercer modo de realización de la invención.

El procedimiento de acuerdo con la invención es un procedimiento de control de acceso basado en el principio de un procedimiento de identificación consolidada. El procedimiento de identificación consolidada ilustrado en la Fig. 1 comprende un conjunto de medios de toma de medición que reagrupan medios de identificación M_i previstos para identificar a una persona que solicita un acceso a un sistema, así como medios de medición M_m previstos para efectuar mediciones en esta persona que solicita el acceso, con el fin de caracterizarla.

15 Un medio de identificación M_i es por ejemplo un sensor de huella digital, un sensor de huella de iris, un sensor de voz o un dispositivo de entrada de un código secreto, etc. Un medio de medición M_m es por ejemplo un sensor que efectúe mediciones de impedancia Z , de inductancia L , de presión sanguínea P° , de temperatura T° o de cualquier otra característica ligada a la persona que solicita el acceso.

20 En el procedimiento de acuerdo con un primer modo de realización de la invención, la primera etapa consiste en realizar al menos dos tomas de medición P_1 y P_2 . Una de las tomas de medición, por ejemplo P_1 , es necesariamente una toma de medición realizada con la ayuda de un medio de identificación M_i , mientras que la otra toma de medición P_2 y las otras tomas de medición, si existen otras, son realizadas cada una con la ayuda de un medio elegido entre el conjunto de los medios de identificación M_i y el conjunto de los medios de medición M_m propuestos anteriormente. Así, se puede utilizar en P_1 una toma de huella digital y en P_2 una toma de huella de iris o, en P_1 una toma de huella digital y en P_2 una toma de huella óptica, etc.

25 Se puede también efectuar en P_1 una toma de huella digital del pulgar de la mano derecha acoplada en P_2 a mediciones de impedancia de este pulgar.

30 Se observará que las tomas de medición P_1 y P_2 pueden ser realizadas tanto de manera sucesiva como de manera aproximadamente simultánea. En el caso de dos tomas de medición sucesivas, estas tomas están ligadas entre sí por una lógica de relación de orden y/o de relación temporal. Así, por ejemplo, cuando un grupo de personas autorizadas efectúa en dos etapas sucesivas las dos tomas de medición P_1 y P_2 , cada persona es reconocida en la segunda toma de medición P_2 como la persona ya reconocida en la primera toma P_1 .

35 Cada toma P_1 , P_2 da un resultado RP_1 , RP_2 . El resultado RP_1 obtenido por la toma de medición P_1 destinada a identificar a la persona que solicita el acceso es sometido a una etapa denominada de identificación. Esta etapa consiste en verificar que el resultado RP_1 corresponde a una persona autorizada. Si, al final de la etapa de identificación, la respuesta es negativa, dicho de otro modo si la persona que solicita el acceso no ha sido reconocida como una persona autorizada, entonces el acceso de esta persona es rechazado inmediatamente. Si, en el caso contrario, la persona que solicita el acceso ha sido reconocida como una persona autorizada, los resultados RP_1 y RP_2 de las dos tomas de mediciones P_1 y P_2 son sometidos una etapa de validación. Esta etapa consiste en verificar que existe una coherencia entre los resultados de las tomas RP_1 y RP_2 . Por coherencia, se entiende de manera general el establecimiento de una relación esperada entre los resultados de las tomas RP_1 y RP_2 .

40 En un modo de realización ilustrativo, el resultado RP_1 es considerado como bueno, si hay identificación, es decir si el sistema reconoce que la huella digital del pulgar derecho de la persona que solicita el acceso corresponde a una huella de una persona autorizada. El resultado RP_2 es considerado como bueno, si los valores de impedancia medidos en el pulgar derecho corresponden a valores considerados como pertenecientes a una persona viva. Finalmente, la coherencia de los resultados RP_1 y RP_2 entre sí es verificada y considerada como buena, si el pulgar portador de la huella digital reconocida, presenta valores de impedancia medidos considerados como pertenecientes a una persona viva o a valores prerregrados considerados como propios de la persona identificada.

45 Si las condiciones de identificación y de coherencia no son validadas, entonces el acceso es rechazado a la persona solicitante. Por ejemplo, este rechazo puede ser además objeto de una inscripción en una lista de revocación, de al menos una característica identificada durante la toma de medición P_1 . Esta característica o estas características pueden ser un resultado de toma de medición o de una información deducida de un resultado de una toma de medición. Así, entre las características que pueden ser inscritas en la lista, se puede encontrar por ejemplo la identidad de la persona reconocida, una huella digital, un código secreto, etc. Esta característica o estas características pue-

den ser las de las víctimas de defraudadores como las de los defraudadores. Esta o estas características deben permitir reconocer más fácilmente a un defraudador durante un nuevo intento de éste.

5 Por el contrario, si las condiciones de identificación y de coherencia son validadas, entonces se verifica que al menos una de las características obtenidas de las tomas de medición y susceptibles de estar en la lista de revocación no se encuentra en esta lista de revocación. Si en la lista de revocación no está presente ninguna característica obtenida de las tomas de medición y susceptible de estar en la lista de revocación, entonces el acceso es autorizado. Si, en el caso contrario, al menos una característica obtenida de las tomas de medición está presente en la lista de revocación, entonces el acceso puede ser rechazado a la persona que le solicita.

10 Por ejemplo, si la huella del pulgar derecho tomada durante la toma de medición P1 validada por una toma de medición P2, se encuentra después de consulta de la lista de revocación, ya registrada en esta lista, la persona que solicita el acceso con esta huella puede ser inmediatamente rechazada.

15 Una vez constituida la lista de revocación, cualquier persona que se presente a las tomas de medición P1 y P2 con al menos una de las características inscritas en la lista de revocación, pudiendo ser esta persona tanto la persona poseedora de esta identidad como un defraudador, podrá ver rechazar su acceso. El acceso, así, puede ser hacerse muy difícil para defraudadores que efectuaran varios intentos.

20 En un ejemplo de realización ilustrado en la Fig. 2, se instaura un número n predefinido de intentos de acceso. Este número predefinido es por ejemplo igual a tres. En este ejemplo de realización, las etapas que preceden a la etapa de validación así como las etapas que siguen a la aceptación de la validación son idénticas a las descritas para el primer modo de realización. Por el contrario, en este ejemplo de realización en caso de ausencia de validación, se verifica que el número de intentos n es diferente de un valor nulo. Si este es el caso, se disminuye el número n de intentos en una unidad y se rechaza el acceso a la persona que solicita este acceso. Si este no es el caso, es decir si el número n es igual a un valor nulo, se inscribe entonces como en el primer modo de realización al menos una característica obtenida de las tomas de mediciones P1 y P2 en una lista de revocación, y después se rechaza el acceso a la persona que le solicita. Además, a cada nuevo intento de acceso, después de identificación de la persona, el número de intentos n asociado a la citada persona es obtenido por relación con esta identificación y es memorizado para a continuación ser tenido en cuenta en caso de ausencia de validación.

25 En este ejemplo de realización, los intentos de acceso son contabilizados y la ausencia de validación sancionada al cabo del número de intentos predefinido por una inscripción en la lista de revocación.

30 Se propone igualmente otro modo de realización de la invención. En este modo de realización ilustrado en la Fig. 3, una característica identificada y después validada, pero presente en la lista de revocación, no es objeto de un rechazo sistemático.

35 En efecto, la presencia de esta característica en la lista de revocación va seguida, en este modo de realización de la invención, de una nueva toma de medición P_i por un medio de identificación M_i , diferente de la primera toma de medición P1. Esta otra toma de medición P_i reemplaza a la primera toma de medición P1 obtenida por un medio de identificación. El procedimiento comienza de nuevo desde el principio y las diferentes etapas del procedimiento tienen en cuenta los resultados obtenidos por las tomas de mediciones P_i y P2.

40 En el ejemplo ilustrativo elegido, si la huella del pulgar derecho está presente en la lista de revocación, la persona que solicita el acceso podrá efectuar una nueva toma de medición, ya sea con un medio de identificación M_i idéntico, pero por ejemplo con el índice, o bien con un medio de identificación M_i diferente, por ejemplo con la huella del iris de su ojo derecho, etc.

Se observará que la elección del nuevo medio de identificación M_i puede ser dejada a la persona que solicita el acceso, o bien ser propuesta por el sistema que pone en práctica el procedimiento.

45 En el ejemplo ilustrativo elegido, la presencia en la lista de revocación de la huella de pulgar identificada durante la toma de medición P1 puede ser objeto de otra toma de medición por un medio de identificación M_i como por ejemplo una toma de huella de iris. La huella del iris reemplaza entonces a la huella del pulgar en el procedimiento.

Con el fin de limitar el número de intentos de identificación, se predetermina un número m de intentos de identificación. De esta manera, después de cada cambio de medio de identificación, se verifica que el número m de intentos de identificación es diferente de un valor nulo. Si este número m es diferente de un valor nulo entonces se disminuye en una unidad este número m y se empieza de nuevo el procedimiento, si no el acceso es rechazado.




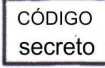
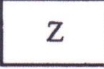
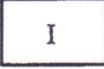
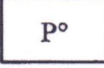
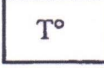
50 Asimismo, igual que en el ejemplo de realización precedente, la etapa de validación va seguida de una verificación de un número n de intentos predeterminados que conducen a un rechazo inmediato en el caso en que n sea diferente de cero, o a una inscripción en la lista de revocación y a un rechazo en el caso contrario.

Se observará que los valores de m y n son conocidos en la etapa de identificación debido a la correspondencia hecha entre la identidad de la persona y el número n o m .

- 5 Para cada uno de los modos de realización expuestos, la persona reconocida a través de la característica rechazada debe ser entonces reautorizada de manera controlada para ser de nuevo considerada y reconocida por el sistema como una persona autorizada de acceso. Esta reautorización puede obtenerse por dos métodos. El primer método consiste en borrar de la lista de revocación las características ligadas a la citada persona, y después en revalidarlas de manera que éstas sean reconocidas de nuevo como pertenecientes a una persona autorizada. El segundo método consiste, por una parte, en suprimir definitivamente la autorización a las citadas características inscritas en la lista de revocación y, por otra, en autorizar otras características ligadas a la citada persona no inscritas en la lista de revocación.
- 10 Se observará que las informaciones contenidas en la citada lista de revocación pueden ser centralizadas en un archivo informático consultable a distancia por el sistema encargado de comunicar con la citada lista.

REIVINDICACIONES

1. Procedimiento de identificación consolidada de una persona que consiste en autorizar el acceso a esta persona a continuación de la ejecución con éxito del conjunto de etapas siguiente:
 - 5 - una etapa de una primera toma de medición, denominada medición de identificación de la citada persona, realizada por un medio de identificación (Mi),
 - una etapa de toma de al menos otra medición por al menos otro medio de medición (Mm),
 - una etapa de identificación de la persona sometida a la toma de medición de identificación,
 - una etapa de rechazo de acceso en el caso en que la persona no sea identificada, si no
 - 10 - una etapa de validación de acceso de la citada persona cuando ésta ha sido identificada por la citada toma de medición de identificación y los resultados de la citada identificación y los de la citada toma de medición o de las citadas otras tomas de medición son coherentes, y
 - una etapa de rechazo de acceso en caso de acceso no validado durante la etapa de validación, caracterizado porque
 - 15 - en caso de acceso validado, el conjunto de la etapas comprende además una etapa de verificación de que al menos una característica de la citada persona obtenida de las citadas tomas de mediciones no pertenece a una lista de revocación, y porque
 - si ninguna característica de la citada persona pertenece a la lista de revocación, el acceso es autorizado a esta persona,
 - 20 - si al menos una característica de la citada persona pertenece a la lista de revocación, se ejecuta de nuevo el conjunto de las etapas reemplazando el medio de identificación (Mi) de la etapa de primera toma de medición por un medio de identificación diferente del utilizado durante la ejecución precedente de esta etapa de primera toma de medición, y el acceso es autorizado a esta persona si esta nueva ejecución del citado conjunto de etapas termina de modo satisfactorio, y si existe una incoherencia entre dos tomas de mediciones después de un número predefinido de intentos de acceso sin éxito, al menos una característica de la citada persona es inscrita en la lista de revocación, y
 - 25 el acceso es rechazado a esta persona.
2. Procedimiento de acuerdo con la reivindicación 1, caracterizado porque la citada o cada otra toma de medición es realizada por un medio de identificación (Mi) o por un medio de medición (Mm).
3. Procedimiento de acuerdo con una de las reivindicaciones precedentes, caracterizado porque un medio de identificación (Mi) es elegido entre los medios de reconocimiento de huella digital, de iris, de voz o un código secreto y porque un medio de medición (Mm) es elegido entre los medios de medición de impedancia (Z), de inductancia (I), de presión sanguínea (P°) o de temperatura (T°).
- 30 4. Procedimiento de acuerdo con una de las reivindicaciones precedentes, caracterizado porque la citada etapa de identificación consiste en comparar los resultados de medición (RP1, RP2) obtenidos por el citado o cada medio de identificación (Mi) con datos preestablecidos y en identificar a una persona cuando los resultados de medición (RP1, RP2) corresponden a datos preestablecidos para la citada persona.
- 35 5. Procedimiento de acuerdo con una de las reivindicaciones precedentes, caracterizado porque la etapa de validación consiste en comparar los resultados de medición (RP1, RP2) obtenidos por el citado o cada medio de medición (Mm) con valores predeterminados correspondientes a criterios de aceptabilidad.
- 40 6. Procedimiento de acuerdo con una de las reivindicaciones precedentes, caracterizado porque la citada característica registrada en la citada lista de revocación es al menos el resultado de una toma de medición que permite una identificación o una información deducida de este resultado.
7. Procedimiento de acuerdo con la reivindicación 6, caracterizado porque la citada información es la identidad de la persona identificada.

	Mi	Mm
	   	   
P1	X	
P2	X	X

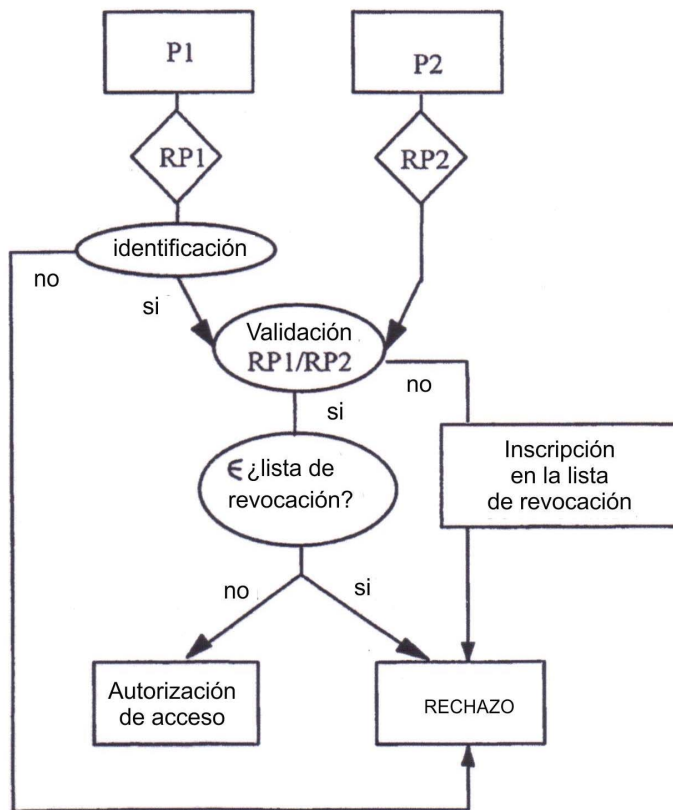


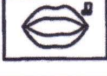


FIG. 1

	Mi	Mm
	 	<div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid black; padding: 2px;">Z</div> <div style="border: 1px solid black; padding: 2px;">I</div> </div>
	 <div style="border: 1px solid black; padding: 2px;">CÓDIGO secreto</div>	<div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid black; padding: 2px;">P°</div> <div style="border: 1px solid black; padding: 2px;">T°</div> </div>
P1	X	
P2	X	X

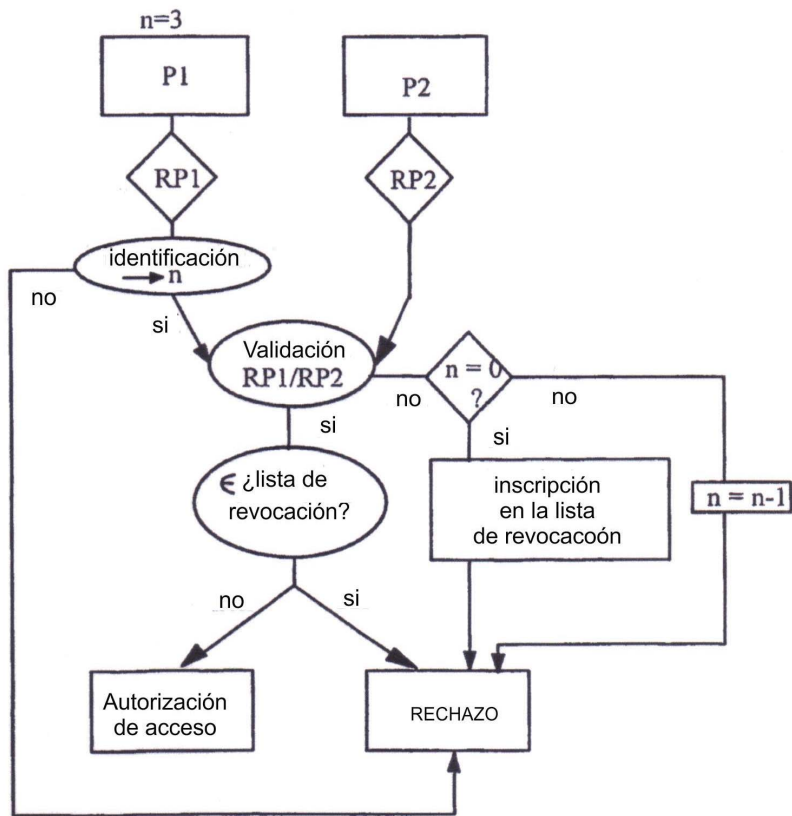





FIG. 2

	Mi	Mm
	   CÓDIGO secreto ...	Z I P° T° ...
P1	×	
P2	×	×
Pi	×	

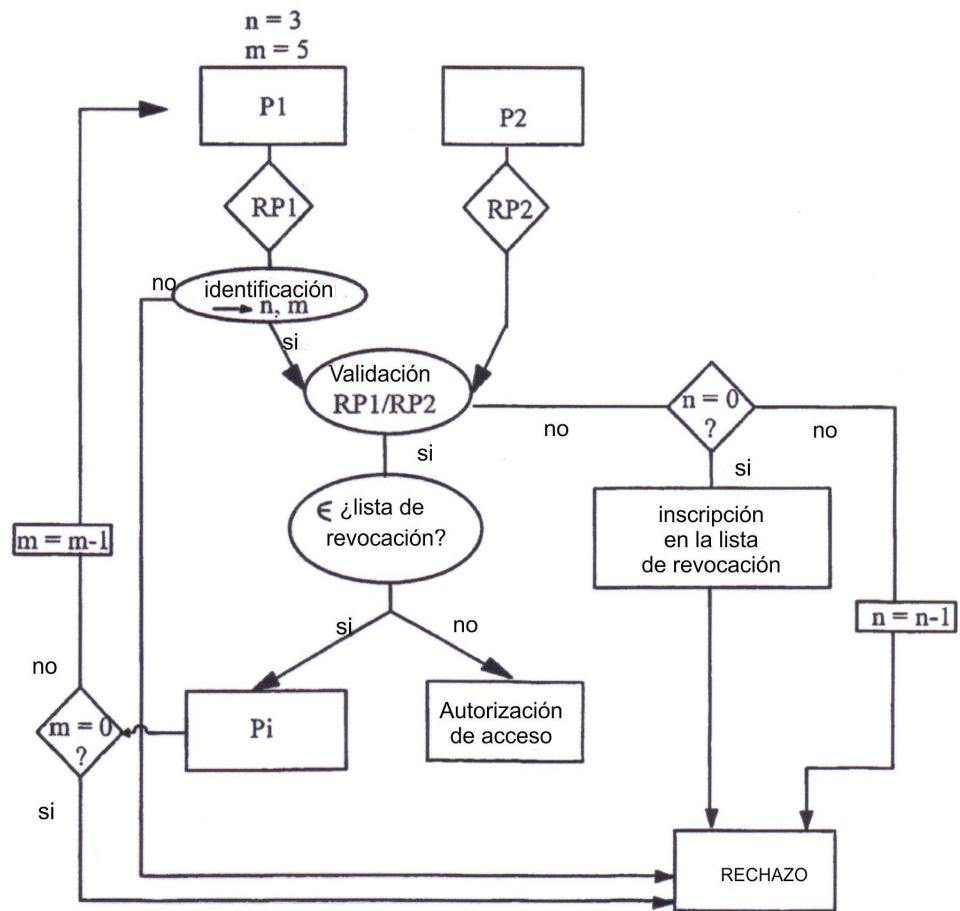


FIG. 3