(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 563 326**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.03.2012 E 12711561 (6)**

(97) Fecha y número de publicación de la concesión europea: **25.11.2015 EP 2684312**

(54) Título: **Procedimiento para la autentificación, documento con chip RF, lector de chip RF y productos de programa de ordenador**

(30) Prioridad:

10.03.2011 DE 102011013562

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.03.2016

(73) Titular/es:

BUNDESREPUBLIK DEUTSCHLAND, VERTRETEN DURCH DAS BUNDESMINISTERIUM DES INNERN, VERTRETEN DURCH DAS BUNDESAMT FÜR SICHERHEIT (100.0%)
In der Informationstechnik Godesberger Allee 185-189
53175 Bonn, DE

(72) Inventor/es:

KÜGLER, DENNIS y
BENDER, JENS

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento para la autentificación, documento con chip RF, lector de chip RF y productos de programa de ordenador

Para una comunicación fiable entre una primera parte y una segunda parte es necesaria una autentificación mutua. La invención se refiere a un procedimiento para la autentificación, a un documento con chip RF, a un lector de chip RF y a productos de programa de ordenador.

Generalmente, son conocidos dos procedimientos de autentificación. Por una parte, una autentificación basada en contraseña y, por otra parte, una autentificación basada en certificado.

Entre la autentificación basada en contraseña figura el Password Authenticated Connection Establishment (PACE) que se describe en detalle en la Directiva Técnica TR-03110 versión 2.05 de la Oficina Federal de Seguridad en la Técnica de la Información (BSI) "Advanced Security Mechanisms for Machine Readable Travel Documents". Se trata de un acuerdo de claves basado en contraseña. El acuerdo de claves basado en contraseña comprende los pasos: una primera parte y una segunda parte

- generan respectivamente un par de claves efímeras compuesto por una clave efímera privada y una clave efímera pública,
- intercambian su respectiva clave efímera pública y las validan a través de una contraseña común,
- generan y validan a continuación una clave de sesión, sobre cuya base se establece un canal de comunicación seguro.

Los distintos pasos de procedimiento del protocolo PACE se describen en J.-S. Coron y col.: "Supplemental Access Control (PACE v2): Security Analysis of PACE Integrated Mappping", International Association for Cryptologic Research, 2011.

Para la autentificación basada en certificado, una primera parte posee un par de claves estáticas compuesto por una clave estática privada y una clave estática pública, y un certificado sobre la clave estática pública, extendido por una entidad de certificación. A la entidad de certificación está asignada una clave pública conocida por la segunda parte. La autentificación basada en certificado está basada en que la pertenencia del par de claves estáticas a la primera parte es confirmada por una tercera parte fiable, la entidad de certificación, en forma de un certificado. Para ello, el certificado contiene al menos la clave estática pública, la identidad unívoca de la primera parte y una signatura electrónica de la entidad de certificación sobre estos datos. La signatura se puede verificar con la clave pública de la entidad de certificación. En una autentificación subsiguiente, la segunda parte puede comprobar si la primera parte posee la clave privada perteneciente a la clave estática pública contenida en el certificado. Los procedimientos conocidos para la autentificación basada en certificado son la "autentificación de chip" que se describe en detalle en la Directiva Técnica TR-03110 versión 2.05 de la Oficina Federal de Seguridad en la Técnica de la Información (BSI) "Advanced Security Mechanisms for Machine Readable Travel Documents".

Por la Directiva TR-03110 mencionada anteriormente se conoce también un procedimiento que constituye una combinación de la autentificación basada en contraseña y la autentificación basada en certificado. Esta combinación es necesaria entre otras cuando es confidencial la identidad de al menos una parte. La autorización para la comunicación se concede solo por el conocimiento y la comprobación de una contraseña común. Esta contraseña común habitualmente se distribuye entre los participantes en la comunicación, a través de un canal especial, frecuentemente de reducido ancho de banda. A la primera parte puede estar asignado un documento con chip RF con un chip RF en el que están almacenados datos confidenciales. A la segunda parte puede estar asignado un lector para el documento con chip RF. La contraseña común puede estar impresa en el documento con chip RF y transferirse a través de un escáner óptico al lector de chip RF.

Después de la autentificación basada en contraseña, las dos partes saben respectivamente que están comunicando de manera segura con la otra parte que posee la misma contraseña, pero no quién es realmente la otra parte. Esto resulta problemático especialmente cuando se usan contraseñas de grupos, de manera que las contraseñas no se asignan de forma unívoca respectivamente para una combinación de dos partes.

Mediante una autentificación subordinada, basada en certificado, se puede comprobar entonces la identidad unívoca de una parte. La realización de la autentificación basada en certificado después de la autentificación basada en contraseña tiene la ventaja de que la identidad de la parte autentificadora solo se expone cuando se ha detectado que las dos partes básicamente están autorizadas para la comunicación mutua, porque las dos usan la misma contraseña. A causa de la codificación y el aseguramiento de seguridad basado en contraseña, tampoco es posible que terceros accedan a un certificado intercambiado. Además, el acuerdo de claves basado en contraseña garantiza también que la contraseña empleada está protegida contra el acceso de terceros.

Hasta ahora, la implementación ejecuta los dos procedimientos de autentificación completamente uno después de otro. Esto se ilustra en la figura 3. Tanto en el acuerdo de claves basado en contraseña como en la autentificación basada en certificado se generan y se usan pares de claves efímeras. La generación de los pares de claves y la aplicación especialmente de las claves públicas de los pares de claves efímeras son intensivas de cálculo y el

intercambio necesario de las claves públicas de los pares de claves efímeras requiere una comunicación adicional entre las partes.

Otro problema de la realización secuencial es la falta de vínculo entre los dos protocolos, de manera que no queda garantizado que los dos protocolos han sido realizados respectivamente por la misma parte.

Ö. Dagdelen y M. Fischlin tratan en "Security Analysis of the Extended Access Control Protocol for Machine Readable Travel Documents", ISC 2010, el protocolo Extended Access Control (EAC) que para la autentificación mutua entre un terminal y un chip y el establecimiento de un enlace autentificado y codificado usan un protocolo de autentificación de terminal y un protocolo de autentificación de chip. La autentificación del terminal está basada en un certificado y en un par de claves efímeras del terminal.

La invención tiene el objetivo de realizar de manera eficiente y segura un procedimiento para la autentificación para la comunicación fiable.

Según la invención, este objetivo se consigue mediante las características de la reivindicación 1. Además, el objetivo se consigue mediante cada una de las reivindicaciones subordinadas 4, 5, 6 y 7 que se refieren a los productos de fabricación independientes documento con chip RF, producto de programa de ordenador para el documento con chip RF, lector de chip RF y producto de programa de ordenador para el lector de chip RF.

Según la característica d de la reivindicación 1, una parte A calcula una transformación entre el propio par de claves efímeras de la autentificación basada en contraseña y el propio par de claves estáticas de la autentificación basada en certificado, obteniendo un parámetro de la transformación. Mediante la reutilización del propio par de claves efímeras de la autentificación basada en contraseña en la autentificación basada en certificado por una parte se reduce la carga total de cálculo y de comunicación y por otra parte se produce un vínculo entre los dos protocolos, de manera que queda garantizado que los dos protocolos son realizados por la misma parte. De esta manera, se incrementa la seguridad reduciendo al mismo tiempo la carga.

Las ventajas logradas con la invención consisten en que se reduce considerablemente el tiempo necesario para la realización de los dos protocolos. El cálculo y la aplicación de la transformación son mucho más eficientes que la nueva generación de otro par de claves efímeras y la realización subsiguiente de la autentificación. De manera muy ventajosa se suprime completamente la realización del segundo acuerdo de claves y se reutiliza la clave de sesión de la autentificación basada en contraseña. El vínculo entre los dos protocolos se realiza de tal forma que para el cálculo de la transformación es necesario el conocimiento tanto de la clave efímera privada del acuerdo de claves basado en contraseña como de la clave estática privada de la autentificación basada en certificado.

Un primer producto de fabricación independiente es un documento con chip RF con un microordenador con una memoria de mircroordenador, de tal forma que en la memoria de microordenador está almacenado un primer programa de ordenador que está realizado de tal forma que se puede realizar el procedimiento con respecto a la parte A.

Un primer producto de programa de ordenador que presenta un medio legible por ordenador comprende un código de programa para la implementación del primer programa de ordenador en la memoria de microordenador. Para ello sirve un ordenador que se usa en el marco de la fabricación del documento con chip RF.

Un segundo producto de fabricación independiente es un lector de chip RF con un ordenador con una memoria de ordenador, de tal forma que en la memoria de ordenador está almacenado un segundo programa de ordenador que está realizado de tal forma que se puede realizar el procedimiento con respecto a la parte B.

Un segundo producto de programa de ordenador que presenta un medio legible por ordenador comprende un código de programa para la implementación del segundo programa de ordenador en la memoria de ordenador del ordenador del lector de chip RF.

Según una forma de realización ventajosa de la invención, en el paso d) de la reivindicación 1, para el cálculo del parámetro de la transformación, la clave estática privada se proyecta sobre la clave efímera privada. Esto simplifica el cálculo, ya que todos los cálculos directamente dependientes de la clave estática pueden ser precalculados una sola vez.

Según otra forma de realización ventajosa de la invención, en el paso d) de la reivindicación 1, para el cálculo del parámetro de la transformación se usa un número aleatorio adicional que no puede ser influenciado por la primera parte. El número aleatorio adicional puede ser un número que es transmitido por la segunda parte a la primera parte. Esta forma de realización ofrece la ventaja de que el cálculo del parámetro de la transformación no se basa exclusivamente en los pares de claves efímeras y estáticas de la primera parte, sino que también depende de un valor que no está bajo el control de la primera parte. De esta manera, se incrementa la seguridad del procedimiento.

Según otra forma de realización ventajosa de la invención, con respecto al paso f) de la reivindicación 1, la segunda parte aplica el parámetro de la transformación obtenido solo en una de las dos claves públicas de la primera parte y comprueba si es correcta la clave pública transformada obtenida mediante la comprobación de una equivalencia de

la clave pública transformada con la otra clave pública de la parte. Dado que la transformación se aplica solo en una de las dos claves públicas de la primera parte es baja la carga de cálculo. La carga de cálculo sería mayor si el parámetro de la transformación se aplicara en ambas claves públicas de la primera parte. Entonces, se obtendrían dos claves públicas transformadas. La corrección de las dos claves públicas transformadas se podría comprobar mediante la comprobación de la equivalencia entre las dos claves públicas transformadas.

A continuación, se describen en detalle ejemplos de realización de la invención con la ayuda de dibujos. Muestran:

La figura 1, una acción conjunta de una primera parte, una segunda parte y una entidad de certificación, como diagrama;

la figura 2, una secuencia de una autentificación, como diagrama de secuencia;

la figura 3, una secuencia de una autentificación según el estado de la técnica, como diagrama de secuencia.

La figura 1 ilustra un sistema para la autentificación para la comunicación fiable entre una primera parte A y una segunda parte B. El sistema comprende un documento con chip RF y un lector de chip RF. El documento con chip RF está asignado a la primera parte A y el lector de chip RF está asignado a la segunda parte B. El documento con chip RF comprende un microordenador con una memoria de microordenador. En la memoria de microordenador está almacenado un primer programa de ordenador que está realizado de tal forma que se puede realizar un procedimiento para la autentificación con respecto a la parte A. La implementación del primer programa de ordenador en la memoria de microordenador se realizó usando un primer producto de programa de ordenador.

El lector de chip RF comprende un ordenador con una memoria de ordenador. En la memoria de ordenador está almacenado un segundo programa de ordenador que está realizado de tal forma que se puede realizar el procedimiento con respecto a la parte B. La implementación del segundo programa de ordenador en la memoria de ordenador se realizó usando un segundo producto de programa de ordenador.

En cuanto a la parte A, el documento con chip RF es un pasaporte. En cuanto a la parte B, el lector de chip RF es un aparato para funcionarios de fronteras. El fabricante y al mismo el emisor del pasaporte es una entidad de certificación C.

El procedimiento para la autentificación es una combinación de una autentificación basada en contraseña y una autentificación basada en certificado. Para la autentificación basada en certificado, la primera parte A posee un par de claves estáticas y un certificado extendido por la entidad de certificación C.

La segunda parte B conoce la clave pública de la entidad de certificación C. En relación con el presente ejemplo de realización, la clave pública de la entidad de certificación C está almacenada en la memoria de ordenador del ordenador del lector de chip RF.

Como se muestra en la figura 2, en primer lugar, se realiza una autentificación basada en contraseña. La autentificación basada en contraseña se realiza a través del protocolo PACE definido en la directiva Técnica TR-03110 versión 2.05 de la Oficina Federal de Seguridad en la Técnica de la Información (BSI) "Advanced Security Mechanisms for Machine Readable Travel Documents"

En general, es válido que se usan pares de claves basados en logaritmos discretos. La clave privada x es respectivamente un número aleatorio dentro del intervalo de 1 a q-1, siendo q el orden del creador g del grupo matemático empleado (por ejemplo, el grupo multiplicativo de un cuerpo finito o el grupo aditivo de los puntos de una curva elíptica). La clave pública y correspondiente se calcula con: y=g^x. La potenciación (^) representa las x veces de aplicación de la operación de grupo (*) comenzando por el creador g.

Los pasos de la autentificación basada en contraseña son:

a) La primera parte A y la segunda parte B generan respectivamente un par de claves efímeras, compuesto por una clave efímera privada y una clave efímera pública. En lo sucesivo, de designación breve para la clave efímera privada de la parte A sirve xe_A. En lo sucesivo, la clave efímera pública de la parte A se designa por ye_A. xe_B y ye_B corresponden a las claves efímeras privada y pública de la parte B. Los pares de claves efímeras xe_A con ye_A y xe_B con ye_B son adecuados para un acuerdo de claves de Diffie-Hellman.

b) La primera parte A y la segunda parte B intercambian respectivamente la clave efímera pública y las validan mediante una contraseña común. La validación se realiza mediante la realización del protocolo PACE. Como se ve en la figura 1, la contraseña común con respecto a la parte A está almacenada en la disposición de chip RF del documento con chip RF. Además, la contraseña común está impresa en el documento con chip RF. A través de un escáner de contraseña del lector de chip RF, la parte B conoce la contraseña común.

c) la primera parte A y la segunda parte B generan y validan una clave de sesión, sobre cuya base se establece un canal de comunicación seguro. Esto se realiza sobre la base de un secreto común establecido en el protocolo PACE.

A continuación, se realiza una autentificación basada en certificado.

A este respecto, se describen un primer y un segundo ejemplo de realización.

Los pasos del primer ejemplo de realización de la autentificación basada en certificado son:

d) La primera parte A calcula una transformación entre el propio par de claves efímeras de la autentificación basada en contraseña y el propio par de claves estáticas de la autentificación basada en certificado, obteniendo un parámetro de la transformación.

Para el cálculo del parámetro de la transformación, la clave estática privada xs_A se proyecta sobre la clave efímera privada xe_A. Se trata de una proyección biyectiva. La transformación t se calcula con la fórmula: $t = xe_A * xs_A\text{^}(-1)$. En el presente primer ejemplo de realización, el parámetro de la transformación es el valor t calculado. Lo inverso de la clave estática privada $xs_A\text{^}(-1)$ se calcula solo una vez y no se vuelve a calcular de nuevo durante cada autentificación. La transformación es una transformación biyectiva.

e) La primera parte A envía el parámetro de la transformación, en este caso, dado por el valor t determinado en el paso d, junto con el certificado extendido por la entidad de certificación C, a la segunda parte B a través del canal de comunicación seguro.

f) la segunda parte B aplica el parámetro de la transformación obtenido en la clave estática pública ys_A, contenida en el certificado, de la primera parte A y obtiene de esta manera una clave pública transformada yt_A. La fórmula para ello es: $yt_A = ys_A\text{^}t$. Ahora, se ha de comprobar la corrección de la clave pública transformada yt_A. Para ello, la segunda parte comprueba una equivalencia de la clave pública transformada yt_A de la parte A con la clave efímera pública ye_A de la primera parte A, intercambiada previamente en la autentificación basada en contraseña. La segunda parte comprueba: $ye_A = yt_A$.

Divergiendo del presente ejemplo de realización, la segunda parte B también podría aplicar el parámetro de la transformación obtenido en la clave efímera pública ye_A de la primera parte A y comprobar la corrección de la clave pública transformada obtenida, mediante la comprobación de una equivalencia de la clave transformada con la clave estática pública ys_A de la parte A.

g) la segunda parte B valida el certificado recibido de la primera parte A con la clave pública de la entidad de certificación C.

Los pasos del segundo ejemplo de realización de la autentificación basada en certificado son:

d) la primera parte A calcula una transformación entre el propio par de claves efímeras de la autentificación basada en contraseña y el propio par de claves estáticas de la autentificación basada en certificado, obteniendo un parámetro de la transformación.
A diferencia del primer ejemplo de realización, para el cálculo de la transformación se usa adicionalmente un número aleatorio c que no puede ser influenciado por la parte A. Por ejemplo, la segunda parte B puede transmitir previamente a la parte A un número aleatorio c o el número aleatorio c podría calcularse por determinación a partir de la secuencia del protocolo, por ejemplo aplicando una función hash en la clave efímera pública de la parte B.
La primera parte A calcula la transformación t con: $t = xe_A - c* xs_A$.
En el presente ejemplo de realización, el parámetro de la transformación es una tupla con el valor del número aleatorio c y el valor de la transformación. La tupla se abrevia por: (c, t).

e) la primera parte A envía el parámetro de la transformación (c, t), junto con el certificado extendido por la entidad de certificación C, a la segunda parte B a través del canal de comunicación seguro. Dado que se conoce el número aleatorio c de la parte B, basta con que la primera parte transmita a la parte B solo el valor de la transformación t.

f) la segunda parte B aplica el parámetro (c, t) de la transformación obtenido en la clave estática pública ys_A, contenida en el certificado, de la primera parte A y obtiene de esta manera una clave pública transformada yt_A. La fórmula para ello es: $yt_A = g\text{^}t * ys_A\text{^}c$. Ahora, se ha de comprobar la corrección de la clave pública transformada yt_A. Para ello, la segunda parte comprueba una equivalencia de la clave pública transformada yt_A de la parte A con la clave efímera pública ye_A de la primera parte A, intercambiada previamente en la autentificación basada en contraseña. La segunda parte comprueba: $ye_A = yt_A$.

g) la segunda parte B valida el certificado recibido de la primera parte A con la clave pública de la entidad de certificación C.

REIVINDICACIONES

1. Procedimiento para la autentificación para la comunicación fiable entre una primera parte (A) y una segunda parte (B) mediante una combinación de una autentificación basada en contraseña y una autentificación basada en certificado, de tal forma que para la autentificación basada en certificado, la primera parte (A) posee un par de claves estáticas compuesto por una clave estática privada y una clave estática pública, y un certificado sobre la clave estática pública expedido por una entidad de certificación (C), y a la entidad de certificación (C) está asignada una clave pública conocida por la segunda parte (B), de tal forma que

- en primer lugar, se realiza una autentificación basada en contraseña con los siguientes pasos: la primera parte (A) y la segunda parte (B)

  a) generan respectivamente un par de claves efímeras compuesto por una clave efímera privada y una clave efímera pública,
  b) intercambian respectivamente la clave efímera pública y las validan mediante una contraseña común,
  c) generan y validan a continuación una clave de sesión, sobre cuya base se establece un canal de comunicación seguro,

- a continuación, se realiza una autentificación basada en certificado con los siguientes pasos:

  d) la primera parte (A) calcula una transformación entre el propio par de claves efímeras de la autentificación basada en contraseña y el propio par de claves estáticas de la autentificación basada en certificado, obteniendo un parámetro de la transformación,
  e) la primera parte (A) envía el parámetro de la transformación, junto con el certificado expedido por la entidad de certificación (C), a la segunda parte (B) a través del canal de comunicación seguro,
  f) la segunda parte (B) aplica el parámetro de la transformación obtenido en la clave efímera pública y/o en la clave estática pública de la primera parte (A) y obtiene de esta manera al menos una clave pública transformada, cuya corrección se comprueba,
  g) la segunda parte (B) valida el certificado recibido de la primera parte (A) con la clave pública de la entidad de certificación (C), y

- en el paso d) para el cálculo del parámetro de la transformación, la clave estática privada se proyecta sobre la clave efímera privada.

2. Procedimiento según la reivindicación 1, de tal forma que en el paso d) de la reivindicación 1 para el cálculo del parámetro de la transformación se usa un número aleatorio adicional que no puede ser influenciado por la primera parte (A).

3. Procedimiento según la reivindicación 1 o 2, en el que en cuanto al paso f) de la reivindicación 1, la segunda parte (B) aplica el parámetro de la transformación obtenido solo en una de las dos claves públicas de la primera parte (A) y comprueba si es correcta la clave pública transformada obtenida mediante la comprobación de una equivalencia de la clave transformada con la otra clave pública de la primera parte (A).

4. Documento con chip RF con un microordenador con una memoria de microordenador, de tal forma que en la memoria de microordenador está almacenado un primer programa de ordenador que está realizado de tal forma que se puede realizar el procedimiento según una de las reivindicaciones 1 a 3 con respecto a la primera parte (A).

5. Primer producto de programa de ordenador que presenta un medio legible por ordenador, que comprende un código de programa para la implementación del primer programa de ordenador según la reivindicación 4 en la memoria de microordenador.

6. Lector de chip RF con un ordenador con una memoria de ordenador, de tal forma que en la memoria de ordenador está almacenado un segundo programa de ordenador que está realizado de tal forma que se puede realizar el procedimiento según una de las reivindicaciones 1 a 3 con respecto a la segunda parte (B).

7. Segundo producto de programa de ordenador que presenta un medio legible por ordenador, que comprende un código de programa para la implementación del segundo programa de ordenador según la reivindicación 6 en la memoria de ordenador.

Fig. 1

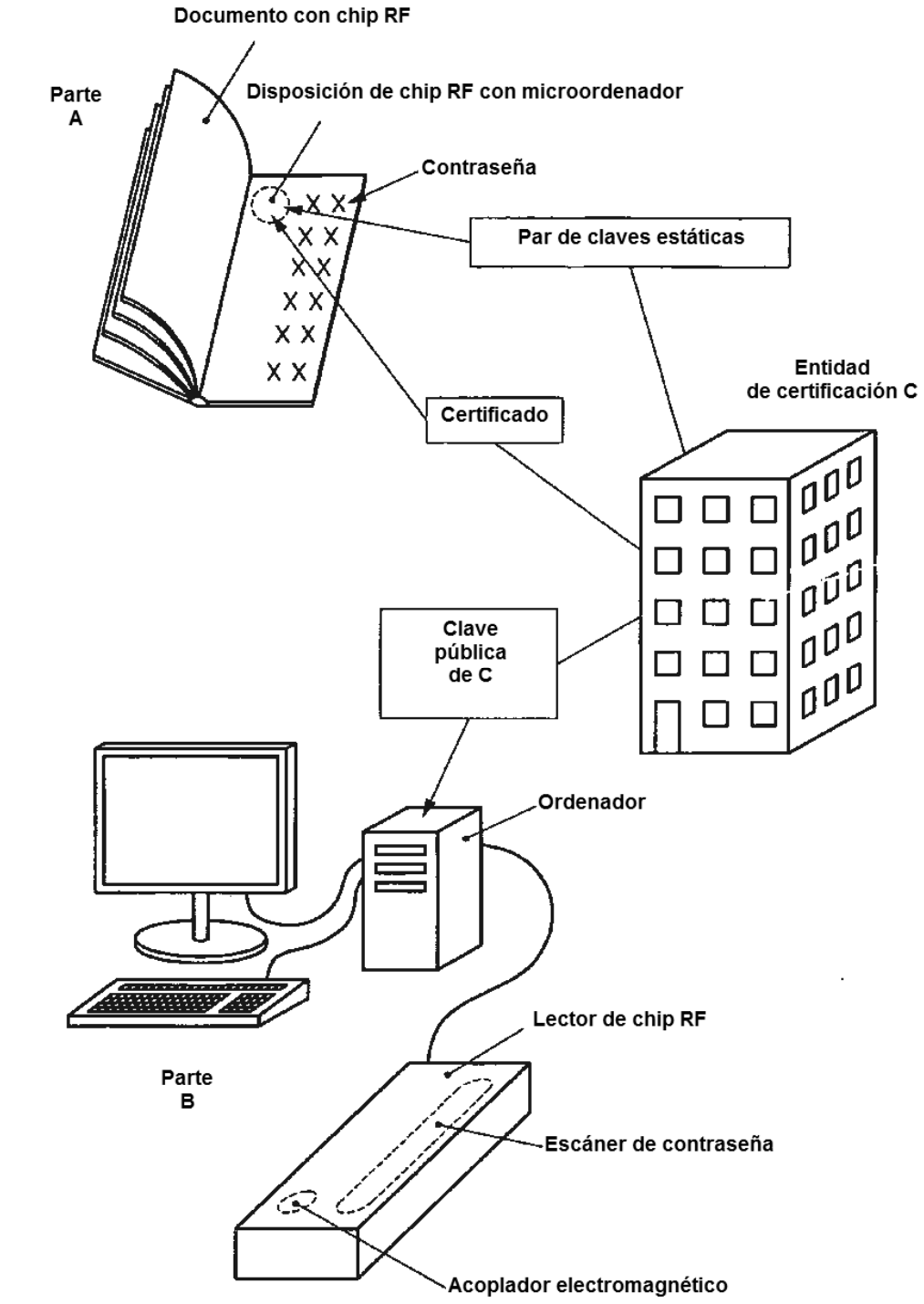

Documento con chip RF
Parte A
Disposición de chip RF con microordenador
Contraseña
Par de claves estáticas
Entidad de certificación C
Certificado
Clave pública de C
Ordenador
Lector de chip RF
Parte B
Escáner de contraseña
Acoplador electromagnético

Fig. 2

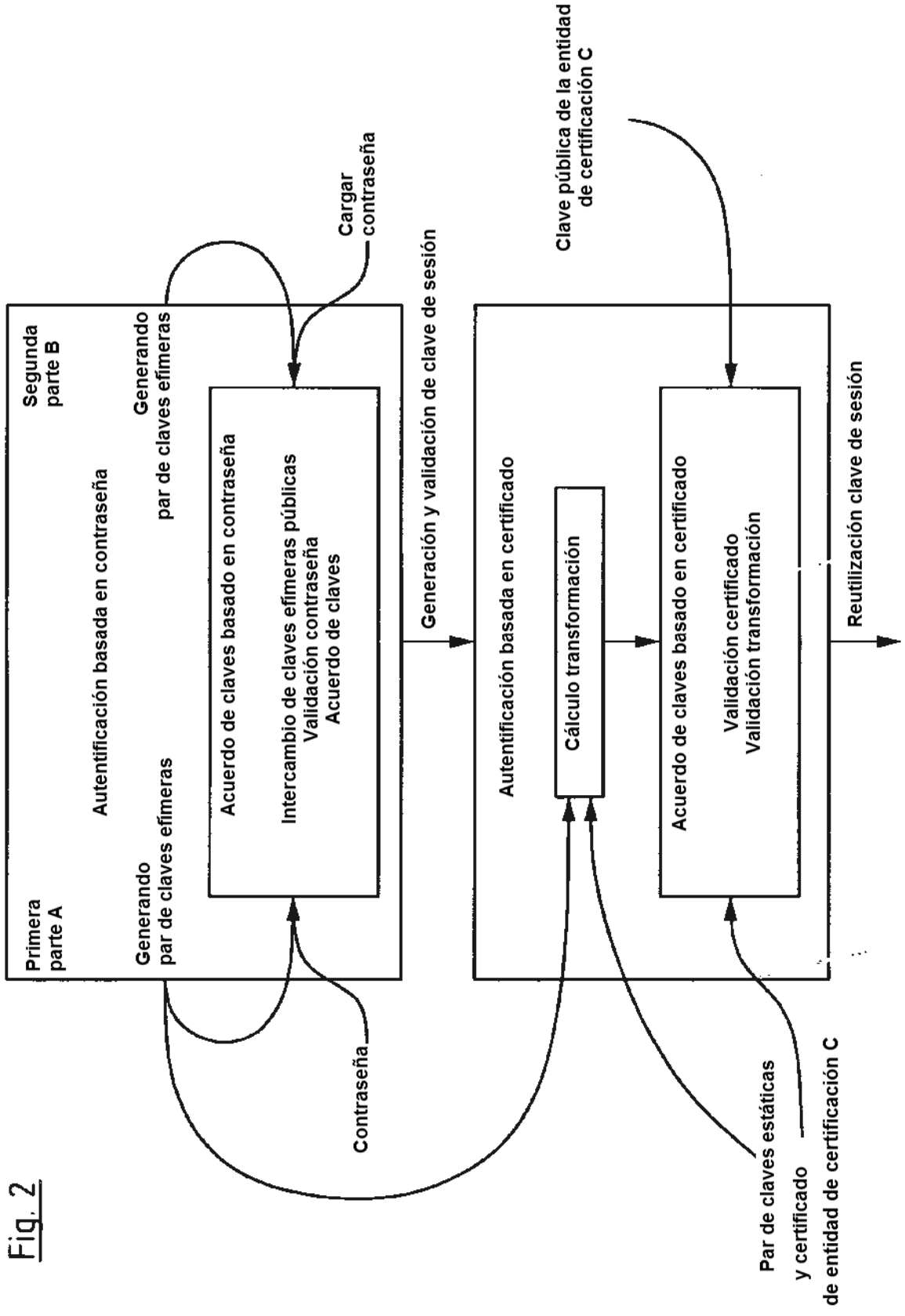
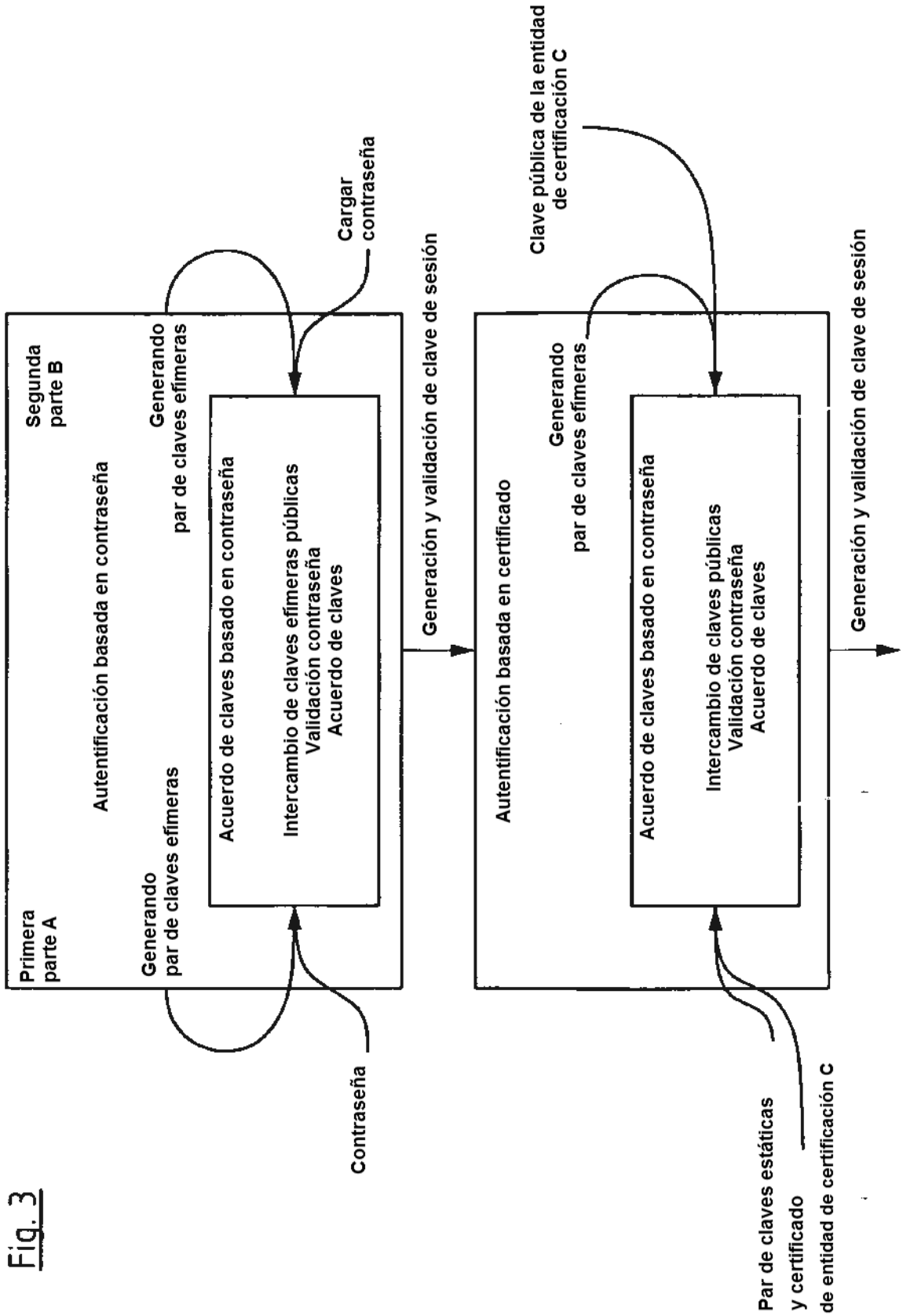

Primera parte A
Segunda parte B
Autentificación basada en contraseña
Generando par de claves efímeras
Generando par de claves efímeras
Acuerdo de claves basado en contraseña
Intercambio de claves efímeras públicas
Validación contraseña
Acuerdo de claves
Cargar contraseña
Contraseña
Generación y validación de clave de sesión
Clave pública de la entidad de certificación C
Autentificación basada en certificado
Cálculo transformación
Acuerdo de claves basado en certificado
Validación certificado
Validación transformación
Reutilización clave de sesión
Par de claves estáticas y certificado de entidad de certificación C

Fig. 3


Primera parte A
Generando par de claves efímeras
Contraseña
Segunda parte B
Autentificación basada en contraseña
Generando par de claves efímeras
Acuerdo de claves basado en contraseña
Intercambio de claves efímeras públicas
Validación contraseña
Acuerdo de claves
Cargar contraseña
Generación y validación de clave de sesión
Autentificación basada en certificado
Par de claves estáticas y certificado de entidad de certificación C
Clave pública de la entidad de certificación C
Generando par de claves efímeras
Acuerdo de claves basado en contraseña
Intercambio de claves públicas
Validación contraseña
Acuerdo de claves
Generación y validación de clave de sesión