(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 790 883**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06Q 20/40 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.12.2016 PCT/FR2016/053614**

(87) Fecha y número de publicación internacional: **29.06.2017 WO17109413**

(96) Fecha de presentación y número de la solicitud europea: **21.12.2016 E 16829417 (1)**

(97) Fecha y número de publicación de la concesión europea: **25.03.2020 EP 3395042**

(54) Título: **Servidor de autenticación para el control de acceso a un servicio**

(30) Prioridad:

21.12.2015 FR 1562946

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.10.2020

(73) Titular/es:

IDEMIA FRANCE (100.0%)
2, Place Samuel de Champlain
92400 Courbevoie, FR

(72) Inventor/es:

GIRODON, STÉPHANE

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Servidor de autenticación para el control de acceso a un servicio

ANTECEDENTES DE LA INVENCIÓN

La presente invención pertenece al campo de los mecanismos de autenticación y se relaciona más en particular con la autenticación para controlar el acceso a un servicio.

La invención puede utilizarse, en particular, para controlar el acceso de un usuario a un servicio en línea accesible a través de una red de telecomunicaciones, tal como Internet, por ejemplo.

Es conocido en el campo de los servicios en línea controlar el acceso de un usuario a dicho servicio por soporte de un mecanismo de autenticación apropiado. En general, la autenticación de un servicio en línea, tal como un servicio comercial en Internet, por ejemplo, requiere que el usuario introduzca un identificador y una contraseña. El acceso al servicio solamente está autorizado si la autenticación se ha aprobado correctamente.

Sin embargo, los mecanismos de autenticación actuales no permiten un control óptimo del acceso a un servicio en línea. Existe un riesgo, en particular, porque es posible para un intruso poder utilizar de manera furtiva el identificador y la contraseña de un usuario que se ha suscrito a un servicio con el fin de obtener acceso no autorizado al servicio en cuestión.

El documento de publicación de solicitud de patente US 2013/0304648 A1 de O'Connell et al. da a conocer un sistema de acceso seguro utilizando una tarjeta inteligente asociada con un sistema de pago bancario.

Actualmente existe la necesidad de una solución que permita un control eficiente y flexible del acceso de un usuario a un servicio en línea accesible a través de una red de telecomunicaciones tal como Internet, a modo de ejemplo.

OBJETO Y RESUMEN DE LA INVENCIÓN

Con este fin, la presente invención se refiere a un servidor de autenticación que comprende:

- un módulo de comunicación capaz de transmitir, a un servidor distante, un identificador bancario de tipo PAN asociado con una tarjeta bancaria, siendo capaz dicho módulo de comunicación, en respuesta a dicho identificador PAN transmitido, de recibir del servidor distante un primer código de acceso para acceder a un servicio;

- un módulo de registro capaz de registrar, en una memoria, un identificador bancario PAN de la tarjeta bancaria, en asociación con una fecha de caducidad de la tarjeta bancaria y del primer código de acceso a un servicio;

- el módulo de comunicación puede recibir una demanda de autenticación procedente de un servidor de acceso que controla el acceso a dicho servicio, comprendiendo dicha demanda un segundo código de acceso y un primer código dinámico de seguridad generado por la tarjeta bancaria;

el servidor de autenticación comprende, además:

- un módulo de verificación configurado para generar un segundo código dinámico de seguridad a partir del identificador bancario PAN y de la fecha de caducidad registrados en dicha memoria, para comparar los códigos de seguridad dinámico primero y segundo, y para detectar que el primer código dinámico de seguridad es válido solamente si coincide con el segundo código dinámico de seguridad; y

- dicho módulo de comunicación está configurado para enviar al servidor de acceso un mensaje de autenticación positiva solamente si:

    - el segundo código de acceso coincide con el primer código de acceso registrado; y

    - el primer código dinámico de seguridad es válido.

La invención permite, de manera ventajosa, asegurar el acceso de un usuario a un servicio, tal como un servicio web a modo de ejemplo. La invención permite la asignación de un código de acceso a un usuario y el almacenamiento, en una base de datos, del código de acceso en asociación con un identificador PAN asociado con la tarjeta inteligente DCVV del usuario y la fecha de caducidad de dicha tarjeta. El usuario puede acceder así posteriormente a un servicio, o realizar una transacción, proporcionando su código de acceso y un código dinámico de seguridad generado por su tarjeta inteligente DCVV. A diferencia de las técnicas convencionales, el usuario no necesita proporcionar su número de cuenta bancaria PAN o la fecha EXP de caducidad de su tarjeta bancaria para acceder al servicio en cuestión. La entidad competente (su banco, por ejemplo) le proporciona un código de acceso para este fin. Por lo tanto, es así

posible limitar la difusión del número de cuenta bancaria PAN y de la fecha de caducidad EXP de la tarjeta bancaria, ya que es probable que estos datos confidenciales sean robados.

La invención puede ofrecer una autenticación mejorada al hacer intervenir un código de acceso estático asignado por una entidad competente al usuario, así como un código dinámico (el código DCVV) que varía con el tiempo.

Además, se puede asignar un código de acceso específico al usuario para cada servicio de entre una pluralidad de servicios. Por lo tanto, es posible ofrecer un control flexible y seguro del acceso de un usuario a una pluralidad de servicios.

De conformidad con una forma de realización particular, el primer código dinámico de seguridad recibido por el módulo de comunicación en la demanda de autenticación es generado por la tarjeta bancaria al ejecutar una función criptográfica a partir del identificador bancario PAN y de la fecha de caducidad y a partir de un dato temporal o un contador del número de primeros códigos dinámicos de seguridad.

Según una forma de realización particular, el módulo de verificación está configurado para generar el segundo código dinámico de seguridad al ejecutar la función criptográfica a partir de dicho identificador bancario PAN y desde la fecha de caducidad registrada en dicha memoria y a partir de un dato temporal o de un contador del número de segundo código dinámico de seguridad.

De conformidad con una forma de realización particular, el módulo de comunicación puede recibir, en datos de transacción bancaria, el identificador PAN que se transmitirá a dicho servidor distante.

Según una forma de realización particular, el módulo de comunicación puede recibir los datos de la transacción bancaria desde el servidor de acceso.

Según una forma de realización particular, el servidor de autenticación es tal que:

- los datos de la transacción bancaria incluyen un tercer código dinámico de seguridad generado por dicho dispositivo, el identificador bancario PAN y la fecha de caducidad;

- el módulo de verificación puede verificar la validez del tercer código dinámico de seguridad;

- dicho módulo de comunicación está configurado para transmitir al servidor distante, solamente si la verificación de validez del tercer código dinámico de seguridad se ha superado con éxito, el identificador PAN y un mensaje que indique que dicho tercer código dinámico de seguridad es válido; y

- dicho módulo de comunicación puede recibir desde el servidor distante, en respuesta al identificador PAN y a dicho mensaje transmitido, dicho primer código de acceso que será registrado por el módulo de registro.

Según una forma de realización particular, el servidor de autenticación es tal que:

- el tercer código dinámico de seguridad es generado por la tarjeta bancaria a partir del identificador PAN y de la fecha de caducidad de la tarjeta bancaria, y a partir de un dato temporal o del contador del número de primeros códigos dinámicos de seguridad;

- el módulo de verificación está configurado para generar un cuarto código dinámico de seguridad a partir del identificador PAN y de la fecha de caducidad de la tarjeta bancaria, y a partir de un dato temporal o del contador del número de segundos códigos dinámicos de seguridad, para comparar los códigos dinámicos de seguridad tercero y cuarto, y para detectar que el tercer código dinámico de seguridad es válido solamente si dicho tercer código dinámico de seguridad coincide con el cuarto código dinámico de seguridad.

De conformidad con una forma de realización particular, el módulo de registro está configurado para registrar un identificador del servicio en asociación con el identificador PAN, la fecha de caducidad y el primer código de acceso de modo que el módulo de verificación sea capaz de determinar el primer código de acceso asociado con dicho servicio.

Según una forma de realización particular, el módulo de registro está configurado para registrar el primer código de acceso en dicha memoria en asociación con una pluralidad de servicios.

Según una forma de realización particular, el servidor de autenticación es tal que:

- el módulo de registro está configurado para registrar una condición temporal en asociación con el identificador PAN, la fecha de caducidad y el primer código de acceso,

- el módulo de verificación se configura para determinar que el primer código de acceso es válido siempre que se cumpla la condición temporal.

Según una forma de realización particular, el módulo de comunicación está configurado para enviar al servidor de acceso un mensaje de autenticación negativa, si el segundo código de acceso no coincide con el primer código de acceso registrado o si el primer código dinámico de seguridad no es válido.

De conformidad con una forma de realización, la invención se pone en práctica por soporte de componentes de software y/o hardware. En este contexto, el término "módulo" puede corresponder, en este documento, también a un componente de software, a un componente de hardware o a un conjunto de componentes de hardware y software.

La invención también se refiere a un sistema para controlar el acceso a un servicio que comprende:

- un servidor de autenticación tal como se definió con anterioridad; y

- un servidor de acceso capaz de controlar el acceso a dicho servicio, estando configurado dicho servidor de acceso para autorizar el acceso a dicho servicio a un usuario asociado con dicho identificador bancario PAN, solamente al recibir el mensaje de autenticación positiva procedente del servidor de autenticación.

En consecuencia, la invención se refiere a un método de autenticación puesto en práctica por un servidor de autenticación, que comprende:

- transmisión, a un servidor distante, de un identificador bancario PAN asociado con una tarjeta bancaria;

- recepción, en respuesta a dicha transmisión, de un primer código de acceso para acceder a un servicio;

- registro del identificador PAN en asociación con el primer código de acceso;

- recepción de una demanda de autenticación procedente de un servidor de acceso que controla el acceso a dicho servicio, comprendiendo dicha demanda un segundo código de acceso y un primer código dinámico de seguridad generado por la tarjeta bancaria al ejecutar una función criptográfica a partir de un dato temporal;

- verificación de la validez del primer código dinámico de seguridad, comprendiendo dicha verificación la generación de un segundo código dinámico de seguridad al ejecutar dicha función criptográfica a partir de un dato temporal y a partir de dicho identificador PAN registrado, la comparación del primero y el segundo códigos dinámicos de seguridad, y la detección de que el primer código dinámico de seguridad es válido solamente si coincide con el segundo código dinámico de seguridad; y

- el envío (C42) al servidor de acceso de un mensaje de autenticación positiva solamente si:

  ° el segundo código de acceso coincide con el primer código de acceso registrado; y

  ° el primer código dinámico de seguridad es válido.

Conviene señalar que las diversas formas de realización mencionadas con anterioridad en relación con el servidor de autenticación de la invención, así como las ventajas asociadas se aplican de manera análoga al método de autenticación de la invención.

En una forma de realización particular, las diferentes etapas del método de autenticación están determinadas por instrucciones de programas informáticos.

En consecuencia, la invención también se refiere a un programa informático en un soporte de información (o soporte de registro), siendo este programa susceptible de ponerse en práctica en un servidor de autenticación o, más generalmente, en un ordenador, comprendiendo este programa instrucciones adaptadas a la puesta en práctica de las etapas de un método de autenticación tal como se definió con anterioridad.

Este programa puede utilizar cualquier lenguaje de programación y tener la forma de código fuente, código objeto o código intermedio entre el código fuente y el código objeto, tal como en una forma parcialmente compilada o en cualquier otra forma deseable.

La invención también se refiere a un soporte de información (o soporte de registro) legible por un ordenador, y que comprende instrucciones de un programa informático tal como se mencionó con anterioridad.

El soporte de información puede ser cualquier entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede incluir un medio de almacenamiento, tal como una memoria ROM, por ejemplo, un CD-ROM o una

memoria ROM de circuito microelectrónico, o también un medio de registro magnético, por ejemplo, un disquete (floppy disc) o un disco duro.

Por otro lado, el soporte de información puede ser un soporte transmisible, tal como una señal eléctrica u óptica, que puede enrutarse a través de un cable eléctrico u óptico, por radio o por otros medios. El programa, según la invención, se puede descargar en particular desde una red del tipo Internet.

De manera alternativa, el soporte de información puede ser un circuito integrado en donde se incorpore el programa, adaptándose el circuito para ejecutar o para ser utilizado en la ejecución del método en cuestión.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Otras características y ventajas de la presente invención surgirán de la descripción que se proporciona a continuación, con referencia a los dibujos adjuntos que ilustran ejemplos de formas de realización desprovistas de cualquier carácter limitativo. En las figuras:

La Figura 1 muestra, de manera esquemática, una tarjeta inteligente de conformidad con una forma de realización particular de la invención;

La Figura 2 representa, de manera esquemática, la estructura de un sistema de control de acceso que comprende un servidor de acceso y un servidor de autenticación de conformidad con una forma de realización particular de la invención;

La Figura 3 representa, de manera esquemática, la estructura de un servidor de autenticación de conformidad con una forma de realización particular de la invención; y

La Figura 4 representa, en forma de diagrama de flujo, las etapas de un método de autenticación de conformidad con una forma de realización particular de la invención.

DESCRIPCIÓN DETALLADA DE VARIAS FORMAS DE REALIZACIÓN

Tal como se indicó con anterioridad, la técnica propuesta se refiere al campo de los mecanismos de autenticación y más en particular, con la autenticación para controlar el acceso a un servicio.

La invención da a conocer un mecanismo de autenticación para controlar el acceso a un servicio en línea, cuyo mecanismo hacer intervenir a un dispositivo electrónico (tal como una tarjeta inteligente, a modo de ejemplo) capaz de generar un código dinámico de seguridad.

Por ejemplo, en el campo de las transacciones bancarias, se conocen las tarjetas inteligentes (denominadas tarjetas bancarias) asociadas con cuentas bancarias. Las operaciones en línea y las transacciones realizadas con una tarjeta bancaria de este tipo se protegen con un código de seguridad asociado con la tarjeta. En general, se dice que estos códigos de seguridad son estáticos, lo que significa que son constantes a lo largo del tiempo o, dicho de otro modo, que su valor permanece idéntico durante toda la vida útil de la tarjeta.

Más recientemente, un método para asegurar transacciones a distancia (en línea o por teléfono, por ejemplo) consiste en utilizar una tarjeta bancaria capaz de generar y mostrar en una pantalla de la tarjeta un código dinámico de seguridad, es decir, un código de seguridad que cambia durante la vida útil de la tarjeta. El sistema de procesamiento informático del servicio financiero de transacciones en línea puede verificar la validez de este código dinámico de seguridad, por ejemplo, en función de un parámetro temporal, para validar o no la transacción. El uso de un código dinámico de seguridad hace posible garantizar que el usuario tenga en su poder la tarjeta bancaria en el momento de la transacción. Si se la roban, el código dinámico de seguridad tiene una utilidad limitada, ya que la validez de este código es solamente temporal.

Se designa un código dinámico de seguridad con el nombre DCVV por "*Dynamic Card Verification Value* - Valor de Verificación de Tarjeta Dinámica". En la presente descripción, una tarjeta inteligente capaz de generar dichos códigos dinámicos de seguridad se denominará tarjeta inteligente DCVV.

Las tarjetas inteligentes de tipo DCVV están inicialmente diseñadas para asegurar una transacción en línea, por ejemplo, una transacción financiera tal como un pago, una consulta bancaria, etc. La presente invención propone el uso de una tarjeta inteligente DCVV para controlar el acceso a un servicio con un nivel de seguridad reforzado.

En la presente descripción, se describen ejemplos de puesta en práctica de la invención en el contexto de la autenticación de un usuario para acceder a un servicio en línea accesible a través de Internet. Sin embargo, se entenderá que la invención se aplica más en general a la autenticación para acceder a cualquier servicio accesible por una red de telecomunicaciones apropiada (Intranet, teléfono, etc.).

A menos que se indique lo contrario, los elementos comunes o similares a varias figuras llevan los mismos signos de referencia y tienen características idénticas o similares, de modo que estos elementos comunes por lo general no se describen de nuevo por razones de simplicidad.

La Figura 1 muestra un dispositivo electrónico 1000 de conformidad con un ejemplo particular para realizar transacciones en línea. Tal como se indica a continuación, este dispositivo electrónico es capaz de generar un código dinámico de seguridad DCVV.

En las formas de realización descritas a continuación, el dispositivo 1000 es una tarjeta inteligente (en inglés *Smart Card*), por ejemplo, una tarjeta bancaria. Sin embargo, son posibles otras puestas en práctica de dicho dispositivo 1000. Como variante, el dispositivo 1000 puede consistir, por ejemplo, en un terminal, por ejemplo, un teléfono móvil, que pone en práctica una aplicación que permite realizar transacciones.

En la forma de realización aquí descrita, la tarjeta inteligente 1000 está, por ejemplo, de conformidad con la norma ISO 7816. En particular, comprende una interfaz de contactos 1300. La tarjeta inteligente 1000 está, por ejemplo, en formato ID-1 (dimensiones: 85,60 x 53,98 mm) y aproximadamente 0,76 mm de grosor. Su cuerpo de tarjeta está realizado, por ejemplo, de materia plástica.

Con referencia siempre a este ejemplo, el nombre NOM del titular de la tarjeta inteligente, un número de cuenta bancaria PAN (por "*Primary Account Number - Número de Cuenta Principal*", de 16 dígitos, por ejemplo) y una fecha de caducidad EXP pueden imprimirse y/o estamparse en relieve en la tarjeta inteligente 1000.

Esta tarjeta inteligente 1000 comprende, en este ejemplo, un controlador 1200 que incluye un módulo capaz de proporcionar la fecha actual, por ejemplo, una señal de reloj CLK, siendo este controlador 1200 capaz de calcular un código dinámico de seguridad DCCV aplicando una función criptográfica F a parámetros de entrada, que incluyen el número de cuenta bancaria PAN, un parámetro temporal y la fecha de caducidad EXP de la tarjeta inteligente 1000. Tal como se indica a continuación, otras formas de calcular un código dinámico de seguridad se pueden considerar al respecto.

El parámetro temporal mencionado con anterioridad representa, por ejemplo, un punto en el tiempo (período temporal, fecha y/o hora, por ejemplo) donde la tarjeta inteligente 1000 genera un código dinámico de seguridad DCCV1 dado. La generación de un código dinámico de seguridad se conoce *per se* y, por lo tanto, no se describirá con más detalle en la presente memoria descriptiva.

En la forma de realización aquí descrita, el código dinámico de seguridad DCCV1 generado por la tarjeta inteligente 1000 varía, por ejemplo, periódicamente, de conformidad con un período predeterminado.

La tarjeta inteligente 1000 incluye, además, en este caso, una pantalla de visualización 1100 capaz de mostrar el código dinámico de seguridad DCCV1. Esta pantalla puede incluir, por ejemplo, 3 o 4 zonas elementales dependiendo de la magnitud de este código dinámico.

En la forma de realización aquí descrita, la tarjeta inteligente 1000 también puede incluir una batería (no ilustrada) y un botón pulsador 1400 para encender o apagar la pantalla 1100 y así controlar la visualización del código dinámico de seguridad DCCV1. Este pulsador o cualquier medio equivalente (botón capacitivo,..) para encender o apagar la pantalla 1100 es opcional. La pantalla de visualización 1100 puede encontrarse en la parte frontal de la tarjeta inteligente 1000 opuesta a aquella donde el número de tarjeta bancaria PAN y la fecha de caducidad EXP están impresos y/o en relieve. De manera alternativa, están en la misma cara.

Se entenderá que el dispositivo 1000 mostrado en la Figura 1 es solamente un ejemplo de realización, siendo posibles otras puestas en práctica en el contexto de la invención. Los expertos en esta técnica comprenderán, en particular, que ciertos elementos del dispositivo 1000 se describen aquí solamente para facilitar la comprensión de la invención, no siendo estos elementos necesarios para poner en práctica la invención.

La Figura 2 muestra, de manera esquemática, un terminal de usuario 2000, un servidor de acceso 3000, un servidor de autenticación 5000 y un servidor distante 6000, de conformidad con una forma de realización particular de la invención. El servidor de acceso 3000 y el servidor de autenticación 5000 conjuntamente forman un sistema de control de acceso SY capaz de controlar el acceso a un servicio S1.

En la presente descripción, se consideran ejemplos de formas de realización en donde un usuario interactúa con el terminal 2000 para acceder al servicio S1, cuyo acceso es controlado por el servidor de acceso 3000. El usuario utiliza la tarjeta inteligente 1000 para registrarse con el servicio S1, posteriormente para autenticarse cuando desee acceder al servicio S1 después del registro.

Más concretamente, en el ejemplo aquí considerado, el terminal 2000 está provisto de una interfaz hombre-máquina HMI, por ejemplo, un ordenador personal, un teléfono inteligente (en inglés, *Smartphone*) o una tableta electrónica.

En este ejemplo, el servidor de acceso 3000 es un servidor que controla el acceso a un servicio web comercial S1, siendo posibles otros tipos de servicios en el contexto de la invención.

En este ejemplo, el servidor distante 6000 es parte de un sistema bancario de la entidad emisora de la tarjeta inteligente 1000.

En este ejemplo, un usuario accede, desde su terminal 2000, al servicio S1 a través de una red de telecomunicaciones 2500 (Internet, a modo de ejemplo), además, en este ejemplo, el servidor de acceso 3000, el dispositivo 5000 y el servidor distante 6000 se comunican entre sí a través de una red de telecomunicaciones 4000 (una red interbancaria, por ejemplo).

El servidor distante 6000 comprende, en este caso, un módulo 6100 para transmitir un código de acceso. Este módulo 6100 es capaz de transmitir al servidor de autenticación 5000, a través de la red 4000, un primer código de acceso CD1 asignado a un usuario para acceder al servicio S1.

En general, el servidor de autenticación 5000 puede verificar la autenticidad del usuario que desea acceder al servicio S1 utilizando su terminal 2000.

Más concretamente, el servidor de autenticación 5000 comprende, en este ejemplo, al menos un procesador 5100 (o más generalmente un controlador), una memoria no volátil M1, una base de datos (o memoria) M2 y una interfaz de comunicación INT.

La memoria M1 es una memoria no volátil regrabable o una memoria de solamente lectura (ROM), constituyendo esta memoria un soporte de registro (o soporte de información) conforme a una forma de realización particular, legible por el servidor de autenticación 5000, y en donde se registra un programa informático PG1 conforme a una forma de realización particular. Este programa informático PG1 incluye instrucciones para la ejecución de un método de autenticación de conformidad con una forma de realización particular. Las etapas de este método se muestran, en una forma de realización particular de la invención, en la Figura 4 descrita más adelante.

La interfaz INT en este ejemplo permite que el servidor de autenticación 5000 se comunique con el servidor distante 6000 y con el servidor de acceso 3000 a través de la red 4000.

En este ejemplo, la base de datos M2 es adecuada para almacenar el primer código de acceso CD1 asignado al usuario del terminal 2000 para acceder al servicio web S1, en asociación con: un identificador asociado con la tarjeta inteligente 1000 (es decir, el identificador PAN de la cuenta bancaria en los ejemplos aquí considerados) y la fecha de caducidad EXP de la tarjeta inteligente 1000. Otros tipos de identificador asociado con la tarjeta inteligente 1000 pueden considerarse en el contexto de la invención.

El procesador 5100 controlado por el programa informático PG1, pone en práctica en este caso una serie de módulos representados en la Figura 3, a saber: un módulo de comunicación 5200, un módulo de registro 5300 y un módulo de verificación 5400.

El módulo de comunicación 5200 puede comunicarse con el terminal de usuario 2000 y con el servidor de autenticación 5000 utilizando la interfaz de comunicación INT.

En este ejemplo particular, el módulo de comunicación 5200 es adecuado para:

- transmitir, al servidor distante 6000, el identificador PAN recibido previamente desde el terminal 2000; y
- en respuesta al identificador PAN transmitido, para recibir del servidor distante 6000 el primer código de acceso CD1 asignado al usuario del terminal 2000 para acceder al servicio web S1.

El módulo de registro 5300 es capaz de registrar el primer código de acceso CD1 en asociación con el identificador PAN recibido. En el ejemplo aquí considerado, los datos en cuestión se registran en la base de datos M2.

En un ejemplo particular, el módulo de comunicación 5200 puede recibir una demanda de autenticación procedente del servidor de acceso 3000, comprendiendo esta demanda un segundo código de acceso (denominado CD2) y un primer código dinámico de seguridad generado por la tarjeta inteligente 1000 (por ejemplo, al ejecutar una función criptográfica a partir del identificador PAN y de la fecha EXP de la tarjeta inteligente 1000, y a partir de un dato temporal).

También en este ejemplo, el módulo de verificación 5400 puede verificar la validez del segundo código de acceso comparándolo con cada código de acceso registrado en la base de datos M2.

El módulo de verificación 5400 también puede verificar la validez del primer código dinámico de seguridad transmitido por el terminal 2000. Para hacerlo, el módulo de verificación 5400 está configurado, en este ejemplo, para generar un

segundo código dinámico de seguridad, para comparar los códigos dinámicos de seguridad primero y segundo, y para detectar, a partir de esta comparación, si el primer código dinámico de seguridad proporcionado por el terminal 2000 es válido. El módulo de verificación 5400 detecta, por ejemplo, que el primer código dinámico de seguridad es válido solamente si coincide con el segundo código dinámico de seguridad. En un ejemplo particular, el primer código dinámico proporcionado por el terminal 2000 se detecta como válido solamente en el caso de la identidad de los primero y segundo códigos dinámicos de seguridad.

En un ejemplo particular, el módulo de verificación 5400 está configurado para generar el segundo código dinámico de seguridad al ejecutar la función criptográfica F a partir de un dato temporal, desde el identificador PAN asociado con la tarjeta inteligente 1000 y desde la fecha de caducidad EXP de la tarjeta inteligente 1000.

Por otro lado, en el ejemplo aquí considerado, el módulo de comunicación 5200 está configurado para enviar al servidor de acceso 3000 un mensaje de autenticación positiva solamente si:

- el primer código dinámico de seguridad generado por la tarjeta inteligente 1000 y enviado por el terminal 2000 es válido; y si

- el segundo código de acceso enviado por el terminal 2000 es válido (es decir, si el segundo código de acceso está registrado como un código de acceso válido en la base de datos M2).

A continuación, se describe una forma de realización particular con referencia a la Figura 4. Más concretamente, el servidor de autenticación 5000 pone en práctica un método de autenticación al ejecutar el programa informático PG1. El servidor de acceso 300 ejecuta aquí un programa informático PG2.

Se supondrá, en esta forma de realización, que el titular de la tarjeta inteligente 1000 interactúa con el terminal 2000 para registrarse primero con el servicio S1, luego para autenticarse para acceder al servicio S1.

Para hacer lo que antecede, el terminal 2000 envía datos (A2) DT1 que comprenden:

- un identificador asociado con la tarjeta inteligente 1000, a saber, el identificador PAN (número de cuenta bancaria) en este ejemplo;

- la fecha de caducidad EXP de la tarjeta inteligente 1000; y

- un código dinámico de seguridad DCVV1 generado previamente por la tarjeta inteligente 1000.

En el ejemplo aquí considerado, los datos DT1 son datos de transacción bancaria.

Estos datos DT1 se transmiten, por ejemplo, al servidor de acceso 3000 en forma de una demanda de registro destinada a registrar al titular de la tarjeta inteligente 1000 con el servicio S1.

En esta forma de realización, el código dinámico de seguridad DCVV1 incluido en los datos DT1 es generado previamente por la tarjeta inteligente 1000 al ejecutar la función criptográfica F a partir del identificador PAN, desde la fecha de caducidad EXP de la tarjeta inteligente 1000 y de un dato temporal. Este dato temporal lo obtiene, por ejemplo, la tarjeta inteligente 1000 a partir de la señal de reloj CLK.

Se supone, por ejemplo, que el usuario que desea registrarse en el servicio S1 utiliza su tarjeta inteligente 1000 con el fin de obtener el código dinámico de seguridad DCVV1, y posteriormente introduce este código dinámico de seguridad DCVV1 en su terminal 2000.

El servidor de acceso 3000 recibe los datos DT1 durante una etapa de recepción B2. El servidor de acceso 3000 luego transmite (B4) estos datos DT1 al servidor de autenticación 5000, que los recibe durante una etapa de recepción C4.

El servidor de autenticación 5000 verifica (C6) entonces la autenticidad de los datos recibidos por DT1.

En este ejemplo particular, el servidor de autenticación 5000 verifica, durante la etapa de verificación C6, si el código dinámico de seguridad DCVV1 es válido. Para hacer lo que antecede, el servidor de autenticación 5000 genera (C8) un código dinámico de seguridad DCVV2 al ejecutar la función criptográfica F a partir de los datos de la transacción bancaria DT1 (más precisamente, el identificador PAN y la fecha de caducidad EXP) recibidos en C4 y a partir de un dato temporal. En este ejemplo, el servidor de autenticación 5000 determina, a partir del identificador PAN recibido, que es la función criptográfica F la que debe ejecutarse. El servidor de autenticación 5000 compara (C10) el código dinámico de seguridad DCVV1 enviado por el terminal 2000 con el código dinámico de seguridad DCVV2 calculado en la etapa C8. El servidor de autenticación 5000 detecta (C12) que el código dinámico de seguridad DCVV1 es válido si dicho código DCVV1 coincide (o es idéntico con) el código dinámico de seguridad DCVV2 obtenido en C8.

Si el resultado de la verificación C6 es positivo (DCVV1 es válido), el servidor de autenticación 5000 continúa con la etapa C14; de lo contrario, el método finaliza.

Durante una etapa de envío C14, el servidor de autenticación 5000 envía al servidor distante 6000 el identificador PAN, estando este último, en este ejemplo, incluido en un mensaje M1. El servidor distante 6000 recibe el mensaje M1 durante una etapa de recepción D14.

El servidor distante 6000 da lugar, entonces, al envío (D16) de un código de acceso CD1 al usuario del terminal 2000. Este código de acceso CD1 se asigna al usuario del terminal 2000 para un acceso posterior al servicio S1. El código de acceso CD1 puede adoptar cualquier forma apropiada (clave criptográfica, cadena de símbolos, etc.).

Se supone en este ejemplo que el código de acceso CD1 es un código único asignado al usuario titular de la tarjeta inteligente 1000 para autenticarse con el servidor de autenticación 3000 con el fin de acceder al servicio S1.

El envío D16 del código de acceso CD1 por el servidor distante 6000 puede llevarse a cabo por cualquier medio adecuado. El código de acceso CD1 puede transmitirse, por ejemplo, a través de un mensaje SMS en el terminal 2000 (o en otro terminal). De manera alternativa, el código de acceso CD1 se envía por correo al usuario.

Además, el servidor distante 6000 envía el código de acceso CD1 al servidor de autenticación 5000 durante una etapa de envío D18. El servidor de autenticación 5000 recibe el código de acceso CD1 durante una etapa de recepción C18.

Durante una etapa de registro C20, el servidor de autenticación 5000 registra, en la base de datos M2, el código de acceso CD1 en asociación con la fecha de caducidad EXP (o más en general, un dato relacionado con la fecha de caducidad EXP) y el identificador PAN de la tarjeta inteligente 1000. Tal como se indica a continuación, datos adicionales, tales como por ejemplo un identificador del servicio S1 en cuestión, pueden registrarse, además, en el caso si fuere necesario en la base de datos M2 en asociación con el código de acceso CD1, la fecha de caducidad EXP y el identificador PAN.

Como resultado de la etapa de registro C20, el usuario se ha registrado para el servicio S1 y tiene un código de acceso CD1 para acceder al servicio S1.

A continuación, se supone que un usuario está intentando acceder al servicio S1 desde el terminal de usuario 2000. Para hacer dicha operación, el terminal 2000 envía (A30) datos DT2 que comprenden un código de acceso que se aquí se denomina CD2, y un código dinámico de seguridad DCVV3. Estos datos DT2 se envían, por ejemplo, en una demanda de acceso.

Los datos DT2 son, por ejemplo, datos de transacción bancaria.

En el ejemplo aquí considerado, el código dinámico de seguridad DCVV3 fue generado previamente por la tarjeta inteligente 1000 al ejecutar la función criptográfica F a partir del identificador PAN de la tarjeta inteligente 1000, de la fecha de caducidad EXP de la tarjeta inteligente 1000 y de un dato temporal. Este dato temporal se obtiene, por ejemplo, por la tarjeta inteligente 1000 a partir de la señal de reloj CLK.

El servidor de acceso 3000 que controla el acceso al servicio S1 recibe los datos DT2 durante una etapa de recepción B30.

Durante una etapa de envío B32, el servidor de acceso 3000 envía al servidor de autenticación 5000 una demanda de autenticación RQ que incluye los datos DT2. El servidor de autenticación 5000 recibe esta demanda RQ durante una etapa de recepción C32.

Durante una etapa C33, el servidor de autenticación 5000 determina si el código de acceso CD2 recibido en C32 es válido comparando el código de acceso CD2 recibido en C32 con el código o códigos de acceso prerregistrados en la base de datos M2. Aquí se supone que el usuario en cuestión es el titular de la tarjeta inteligente 1000 que ha recibido previamente el código de acceso CD1, y que el código de acceso CD2 proporcionado en A30 es idéntico al CD1. Por lo tanto, el servidor de autenticación 5000 determina (C33) que el código de acceso CD2 es válido y continúa con la etapa C34.

El servidor de autenticación 5000 posteriormente verifica (C34) la validez del código dinámico de seguridad DCVV3 recibido en C32. Para hacer lo que antecede, el servidor de autenticación 5000 genera (C36) un código dinámico de seguridad DCVV4 al ejecutar la función criptográfica F a partir de un dato temporal, y a partir del identificador PAN y de la fecha de caducidad EXP registrados todos ellos en la base de datos M2 en asociación con el código de acceso CD2 (idéntico a CD1 en este ejemplo). El servidor de autenticación 5000 determina, por ejemplo, a partir del identificador PAN, que es la función criptográfica F la que debe ejecutarse. El servidor de autenticación 5000 compara (C38) el código dinámico de seguridad DCVV3 recibido en C32 con el código dinámico de seguridad DCVV4 calculado en la etapa C36. El servidor de autenticación 5000 detecta (C42) que el código dinámico de seguridad DCVV3 es

válido solamente si dicho código DCVV3 coincide (o es idéntico con) el código dinámico de seguridad DCVV4 obtenido en C36.

El servidor de autenticación envía (C44) al servidor de acceso 3000 un mensaje M2 de autenticación positiva solamente si determina (C42) que se cumplen las dos condiciones siguientes:

(1) el código de acceso CD2 es válido (dicho de otro modo, que el código de acceso CD2 coincide (o es idéntico con) el código de acceso CD1); y

(2) el código dinámico de seguridad DCVV3 es válido.

En el ejemplo aquí considerado, se supone que el servidor de autenticación 5000 detecta en C42 que se cumplen las dos condiciones (1) y (2) anteriores, además, el servidor de autenticación 5000 activa el envío C44 del mensaje de autenticación positiva M2.

Al recibir (B44) el mensaje M2, el servidor de acceso 3000 determina (B46) que la demanda de acceso del usuario desde el terminal 2000 es legítima y, por lo tanto, autoriza (B46) el acceso del usuario al servicio S1 en cuestión.

Si, por el contrario, el servidor de autenticación 5000 detecta en C42 que al menos una de las condiciones (1) y (2) definidas con anterioridad no se cumplen, envía en C44 un mensaje M3 de autenticación negativa al recibir (B44) el mensaje M3, el servidor de acceso 3000 determina (B46) que la demanda de acceso del usuario desde el terminal 2000 no es legítima y, por lo tanto, rechaza (B46) el acceso del usuario al servicio S1 en cuestión.

De conformidad con la forma de realización descrita con referencia a la Figura 4, es posible, por ejemplo, prever la forma de realización del siguiente escenario operativo:

- un usuario en A2 utiliza su tarjeta bancaria tipo DCVV para adquirir un artículo en un sitio web comercial (por ejemplo, la compra de un ticket en el sitio web de un servicio de transporte);
- el usuario recibe luego un código de acceso CD1 enviado en D16 por su banco por correo o SMS;
- posteriormente, el usuario utiliza en A30 su código de acceso CD1 y un código dinámico de seguridad generado por su tarjeta bancaria DCVV para recuperar su artículo desde un terminal que pertenece a la red del comerciante (recupera, por ejemplo, un ticket de transporte de un terminal que pertenece a una red de servicios de transporte).

La invención permite, de manera ventajosa, asegurar el acceso de un usuario a un servicio, tal como por ejemplo un servicio web. La invención prevé la asignación de un código de acceso a un usuario y el almacenamiento, en una base de datos, del código de acceso en asociación con un identificador PAN asociado con la tarjeta inteligente DCVV del usuario y la fecha de caducidad de dicha tarjeta. El usuario puede acceder posteriormente a un servicio, o realizar una transacción, proporcionando su código de acceso y un código dinámico de seguridad generado por su tarjeta inteligente DCVV. A diferencia de las técnicas convencionales, el usuario no necesita proporcionar su número de cuenta bancaria PAN o la fecha de caducidad EXP de su tarjeta bancaria al acceder al servicio en cuestión. La entidad competente le proporciona un código de acceso para este fin (su banco, por ejemplo). Por lo tanto, es posible así limitar la difusión del número de cuenta bancaria PAN y de la fecha de caducidad EXP de la tarjeta bancaria, ya que es probable que estos datos confidenciales sean robados. Para hacer lo que antecede, los datos DT2 enviados por el terminal 2000 durante la etapa A30 (Figura 4) no incluyen el identificador bancario PAN de la tarjeta bancaria 1000 ni la fecha de caducidad EXP de dicha tarjeta bancaria 1000. De manera similar, la demanda de autenticación RQ recibida por el servidor de autenticación 5000 en la etapa C32 (Figura 4) no incluye dicho identificador bancario PAN de la tarjeta bancaria 1000 ni dicha fecha de caducidad EXP de la tarjeta bancaria 1000. El servidor de autenticación 5000 encuentra el identificador PAN y la fecha de caducidad EXP a partir del código de acceso proporcionado por el usuario, consultando su memoria M2 tal como se explicó con anterioridad haciendo referencia a la etapa C34.

La invención puede ofrecer una autenticación mejorada al hacer intervenir un código de acceso estático asignado por una entidad competente al usuario, así como un código dinámico (el código DCVV) que varía en el transcurso del tiempo.

Además, se puede asignar un código de acceso específico al usuario para cada servicio de entre una pluralidad de servicios. Por lo tanto, es posible ofrecer un control flexible y seguro del acceso de un usuario a una pluralidad de servicios.

Se entenderá que se pueden prever diversas formas de realización alternativas de los ejemplos descritos con anterioridad en el contexto de la invención.

De conformidad con una forma de realización particular, el servidor de autenticación 5000 registra en C20 (Figura 4) un identificador del servicio en cuestión, en asociación con el código de acceso CD1 y el identificador PAN. Por ejemplo, es posible registrar en la base de datos M2, para un mismo identificador PAN, diferentes códigos de acceso

correspondientes a los servicios respectivos. En un ejemplo particular, la demanda RQ recibida en C32 por el servidor de autenticación 5000 incluye el identificador del servicio al que el usuario desea acceder.

De conformidad con una forma de realización particular, un mismo código de acceso CD1, denominado código de acceso universal, se asigna a un usuario para acceder a una pluralidad de servicios. En un ejemplo particular, dicho código de acceso universal CD1 se registra por el servidor de autenticación 5000 en la base de datos M2 en asociación con el identificador PAN del usuario. De manera ventajosa, un banco u otro puede ofrecer un servicio de autenticación (basado en el servidor de autenticación 5000, y posiblemente el servidor distante 6000) universal y de alto nivel de seguridad para los usuarios y los proveedores de servicios S1. Esta forma de realización tiene la ventaja de que los usuarios solamente necesitan memorizar un único código de acceso CD1 para acceder a una pluralidad de servicios S1 (por ejemplo, para todos los servicios a los que el usuario está autorizado para acceder), se ofrece un alto nivel de seguridad mediante el uso del código dinámico de seguridad DCVV (habida cuenta de su aspecto dinámico y su generación criptográfica).

De conformidad con una forma de realización particular, el servidor de autenticación M2 registra en la base de datos M2 un código de acceso universal CD1 (que permite el acceso a una pluralidad de servicios) en asociación con el identificador PAN del usuario y cada identificador de entre una pluralidad de servicios a los que el usuario está autorizado para acceder. Como variante, no se registra ningún identificador de servicio y el servicio de autenticación ofrecido por el banco, u otro, a partir del código de acceso CD1, es válido para todos los servicios posibles.

Según una forma de realización particular, el código de acceso CD1 asignado al usuario es válido solamente durante un período temporal dado. Por lo tanto, es posible adaptar con el tiempo los derechos de acceso de una pluralidad de usuarios a un servicio dado. Según un ejemplo particular, se registra una condición temporal en la base de datos M2 en asociación con el código de acceso CD1, el identificador PAN y la fecha de caducidad EXP. En este caso, el servidor de autenticación 5000 detecta en C42 que la autenticación ha pasado satisfactoriamente solamente si se cumple la condición temporal.

Se observará que, en las formas de realización descritas con anterioridad, el usuario se registra con el servicio S1 enviando un código dinámico de seguridad DCVV, además de su identificador PAN. Según una variante, el terminal 2000 no envía el código dinámico de seguridad DCVV en A2 (Figura 4), si fuere necesario, la autenticación del usuario puede llevarse a cabo de una manera diferente.

Según una forma de realización particular, durante la fase de registro de usuario para el servicio S1, el servidor de autenticación 5000 y/o el servidor distante 6000 pueden recibir el identificador PAN sin pasar por el terminal 2000 y/o sin pasar por el servidor de acceso 3000. Por lo tanto, en un ejemplo particular descrito con referencia a la Figura 4, el servidor de autenticación 5000 recibe en C4 el identificador PAN directamente desde el terminal 2000 sin pasar por el servidor de acceso 3000, o sin pasar ni por el terminal 2000 ni por el servidor de acceso 3000. Del mismo modo, según una variante, el servidor distante 6000 puede recibir (D14) el identificador PAN directamente desde el terminal 2000 o desde el servidor de acceso 3000.

El usuario puede, por ejemplo, ir a su banco, conectarse a un servicio en línea, tal como un servicio de banca electrónica, o incluso conectarse al servidor distante 6000 con un terminal que no sea el terminal 2000. Para autenticarse y así obtener su código de acceso CD1, el usuario puede usar, por ejemplo, el código PIN secreto de su tarjeta bancaria 1000 o presentar un documento de identidad, siendo posibles otros métodos de autenticación.

De conformidad con una forma de realización particular descrita con referencia a la Figura 4, durante la fase de registro de usuario para el servicio S1, el usuario de la tarjeta inteligente 1000 puede preguntarle a su banco (o cualquier otro organismo competente), o al servidor distante 6000, para proporcionarle el código de acceso CD1 sin que sea necesario que el usuario proporcione el identificador PAN de su tarjeta inteligente 1000. En respuesta a esta demanda, el banco o el servidor distante 6000 puede, por ejemplo, transmitir el código de acceso CD1 al servidor de autenticación 5000, al terminal 2000 o incluso directamente al usuario. El usuario puede, por ejemplo, realizar esta demanda presentándose a su banco o conectándose a un servicio en línea tal como un servicio de banca electrónica. Con el fin de obtener su código de acceso CD1, el usuario se autentica de cualquier manera apropiada, tal como presentando un código de acceso de banca electrónica o un documento de identidad.

De conformidad con una forma de realización particular descrita con referencia a la Figura 4, durante la fase de registro de usuario para el servicio S1, el terminal 2000, o posiblemente el servidor de acceso 3000, envía directamente al servidor de autenticación 5000 el código de acceso CD1 y el identificador PAN asociado, de modo que el servidor de autenticación 5000 memoriza en su base de datos M2 el código de acceso CD1 en asociación con el identificador PAN. En este caso, el servidor distante 6000 no es necesario. Para hacer lo que antecede, durante la fase de registro para el servicio S1, el servidor de acceso 3000 puede, por ejemplo, determinar el código de acceso CD1 a partir del identificador PAN recibido en B2 desde el terminal 2000 (Figura 4). Para este fin, el servidor de acceso 3000 contiene, por ejemplo, en la memoria, el código de acceso CD1 asociado con el identificador PAN del usuario. Según otro ejemplo, durante su fase de registro para el servicio S1, el propio usuario proporciona el código de acceso CD1 y su identificador PAN al servidor de autenticación 5000, posiblemente pasando por el terminal 2000 y/o por el servidor de

acceso 3000. El usuario puede, por ejemplo, introducir el código de acceso CD1 de su elección, así como el identificador PAN de su tarjeta 1000, en su terminal 2000 durante su fase de registro.

En las formas de realización descritas con anterioridad, la tarjeta inteligente 1000 y el módulo de verificación 5400 utilizan cada uno un dato temporal (o parámetro temporal) para generar cada código dinámico de seguridad DCVV. Los expertos en esta técnica entenderán que estos datos temporales deben sincronizarse para permitir la comparación de estos códigos dinámicos de seguridad. En la práctica, para superar estos problemas de sincronización, el módulo de verificación 5400 puede configurarse para generar varios códigos dinámicos de seguridad mediante el uso de diferentes parámetros temporales (por ejemplo, varios parámetros temporales sucesivos a lo largo del tiempo) para la verificación de un único código dinámico de seguridad. En este caso, la autenticación se supera con éxito tan pronto como uno de los códigos dinámicos de seguridad generados por el módulo de verificación 54000 corresponde al código dinámico de seguridad generado por la tarjeta inteligente 1000.

Como variante, el dato temporal se puede sustituir por un contador que se incrementa:

- en el lateral de la tarjeta inteligente 1000: cada vez que la tarjeta genera un nuevo código dinámico de seguridad DCVV, por ejemplo, cuando el usuario presiona el pulsador 1400; y

- en el lado del servidor de autenticación 5000 (más en particular su módulo de verificación 5400): cada vez que este último genera un código dinámico de seguridad DCVV para verificar la validez de un código dinámico de seguridad DCVV generado por las tarjetas inteligentes 1000.

De nuevo, el experto en esta técnica comprenderá que estos contadores deben estar sincronizados para permitir la comparación de estos códigos. En la práctica, para superar estos problemas de sincronización, el servidor de autenticación puede generar varios códigos dinámicos de seguridad utilizando diferentes valores de contador, el código dinámico de seguridad se considera válido tan pronto como uno de estos segundos códigos dinámicos de seguridad corresponde al código dinámico de seguridad generado por la tarjeta inteligente.

A continuación, consideramos una variante de las formas de realización descritas con anterioridad con referencia particular a la Figura 4. De conformidad con esta variante, el servidor de acceso 3000 también desempeña la función del servidor distante 6000 (dicho de otro modo, los servidores 3000 y 6000 forman un solo y único servidor) en el sentido de que es el servidor de acceso 3000 el que, durante la fase de registro de usuario para el servicio S1, obtiene el código de acceso CD1 y proporciona este último para el servidor de autenticación 5000. De conformidad con esta variante, el operador del servicio S1 puede decidir qué código de acceso CD1 se asigna a cada uno de los usuarios del servicio S1.

De conformidad con una puesta en práctica particular de esta variante, durante la fase de registro de usuario para el servicio S1, el terminal 2000 transmite los datos de transacción DT1 al servidor de acceso 3000 tal como ya se describió con referencia a las etapas A2 y B2 ilustradas en la Figura 4. Los datos DT1 incluyen, en particular, el identificador PAN y la fecha de caducidad EXP de la tarjeta inteligente 1000. En este ejemplo, estos datos DT1 están acompañados por un identificador, denominado identificador de acceso, del usuario para identificarse con el servicio S1 (por ejemplo, un identificador de perfil o inicio de sesión). En respuesta a los datos así recibidos, el servidor de acceso genera (u obtiene) el código de acceso CD1 asignado al usuario para acceder al servicio S1, luego transmite, al servidor de autenticación 5000, este código de acceso CD1 (estático) con el identificador PAN y la fecha de caducidad EXP, así como posiblemente el código dinámico DCVV1 generado por la tarjeta inteligente 1000 cuando dicho código dinámico se utiliza para autenticar al usuario durante la fase de registro. El servidor de acceso 6000 también registra (en una base de datos, por ejemplo) el código de acceso CD1 asignado al usuario en asociación con el identificador de acceso del usuario (su identificador de perfil, por ejemplo). Durante la fase de registro, el servidor de autenticación 5000, por lo tanto, no necesita solicitar el código de acceso CD1 al servidor distante 6000 tal como se describió con anterioridad haciendo referencia a las etapas C14 y C18 ilustradas en la Figura 4. De conformidad con esta variante, el servidor de autenticación realiza las etapas C6 y C12 tal como se describió con anterioridad con referencia a la Figura 4 para verificar la validez del código dinámico DCVV1 proporcionado por el usuario (en el caso de que dicho código dinámico se utilice durante el registro) y, si este código DCVV1 es válido, continúe con la etapa C20 tal como se describió con anterioridad (Figura 4) con el fin de registrar, en su base de datos M2, el código de acceso CD1 en asociación con el identificador PAN y la fecha de caducidad EXP. El servidor de autenticación 5000 también puede registrar datos adicionales (identificador de servicio, etc.) en asociación con estos datos, de manera análoga a la forma de realización descrita con anterioridad con referencia a la Figura 4. Tal como fue ya indicado, se puede considerar que el terminal 2000 no envíe un código DCVV1 dinámico durante el registro, pudiendo realizarse la autenticación del usuario de una manera diferente si fuere necesario.

Aún de conformidad con una puesta en práctica particular de esta variante, durante la fase de acceso al servicio S1, el terminal 2000 transmite al servidor de acceso 3000 datos de transacción aquí indicados como DT3, de manera similar a las etapas A30 y B30 ilustradas en la Figura 4. Los datos DT3 incluyen, en particular, el código dinámico DCVV3 generado por la tarjeta inteligente 1000, así como el identificador de acceso utilizado por el usuario del terminal 2000 para identificarse con el servicio S1. De conformidad con esta puesta en práctica, el servidor de acceso 3000 determina, a partir del identificador de acceso proporcionado en los datos DT3, el código de acceso CD1 previamente

registrado durante la fase de registro de usuario para el servicio S1. Para hacer lo que antecede, el servidor de acceso 3000 consulta, por ejemplo, su base de datos. El servidor de acceso 3000 luego transmite al servidor de autenticación 5000, en una demanda de autenticación RQ2 (similar a la demanda RQ mostrada en la Figura 4), el código de acceso CD1 en asociación con el código dinámico DCVV3 proporcionado por el usuario. El servidor de autenticación 5000 luego verifica el código de acceso CD1 proporcionado por el servidor de acceso 3000 de manera similar a la etapa C33 descrita con anterioridad con referencia a la Figura 4, y luego verifica la validez del código dinámico DCVV3 de forma similar a la etapa C34 (Figura 4). Si el código de acceso proporcionado y el código dinámico DCVV3 suministrado por el servidor de acceso 3000 son válidos, el servidor de autenticación 5000 envía al servidor de acceso 3000 un mensaje M2 de autenticación positiva de manera análoga a las etapas C42- C44 ya descritas con referencia a la Figura 4. Conviene señalar que, de manera similar a las formas de realización precedentes, los datos DT3 enviados por el terminal 2000 y la demanda de autenticación RQ2 enviada por el servidor de acceso 3000 al servidor de autenticación 5000 no incluye ni el identificador bancario PAN de la tarjeta bancaria 1000 ni la fecha de caducidad EXP de la tarjeta bancaria 1000. El servidor de autenticación 5000 encuentra, al consultar su memoria M2, el identificador PAN y la fecha de caducidad EXP a partir del código de acceso CD1 proporcionado por el servidor de acceso 3000, y luego utiliza el identificador PAN y la fecha de caducidad EXP para verificar la validez del código dinámico DCVV3 de manera similar a la etapa de verificación C34 ilustrada en la Figura 4.

La variante anterior es ventajosa porque no es necesario hacer intervenir a un servidor distante 6000 (Figura 2), que pertenezca, por ejemplo, a una red bancaria, para proporcionar al servidor de autenticación 5000, durante la fase de registro, el código de acceso asignado a un usuario para acceder al servidor S1. Por otro lado, cuando el usuario desea acceder al servicio S1, simplemente proporciona su identificador de acceso (inicio de sesión o equivalente) y un código DCVV dinámico generado por su tarjeta bancaria 1000 para autenticarse. Es el servidor de acceso 3000 quien se encarga de deducir, a partir del identificador de acceso proporcionado por el usuario, el código de acceso CD1 previamente asignado al usuario, luego transmite este código de acceso CD1 al servidor autenticación 5000 para que este último pueda verificar la validez del código dinámico DCVV proporcionado por el usuario. De manera ventajosa, el usuario no necesita proporcionar el código de acceso CD1 al servidor de acceso 3000 para acceder al servicio S1 en cuestión (dicho de otro modo, los datos DT3 no necesitan incluir el código de acceso), lo que permite simplificar todavía más el procedimiento de autenticación desde el punto de vista del usuario. El usuario no tiene necesariamente conocimiento del código de acceso CD1 asignado por el servidor de acceso durante la fase de registro.

Un experto en esta técnica entenderá que las formas de realización y variantes descritas con anterioridad solamente constituyen ejemplos no limitativos de puestas en práctica de la invención. En particular, un experto en esta técnica puede prever cualquier adaptación o combinación de las formas de realización y variantes descritas con anterioridad con el fin de dar respuesta a una necesidad muy particular.

REIVINDICACIONES

1. Servidor de autenticación (5000) que incluye:

- un módulo de comunicación (5200) capaz de transmitir, a un servidor distante (6000), un identificador bancario de tipo PAN asociado con una tarjeta bancaria (1000), siendo capaz dicho módulo de comunicación (5200), en respuesta a dicho identificador PAN transmitido, para recibir del servidor distante (6000) un primer código de acceso (CD1) para acceder a un servicio (S1);

- un módulo de registro (5300) capaz de registrar, en una memoria, el identificador bancario PAN de la tarjeta bancaria (1000), en asociación con una fecha de caducidad (EXP) de la tarjeta bancaria y el primer código de acceso (CD1) a un servicio (S1);

- siendo el módulo de comunicación (5200) capaz de recibir una demanda de autenticación procedente de un servidor de acceso (3000) que controla el acceso a dicho servicio (S1), comprendiendo dicha demanda un segundo código de acceso (CD2) y un primer código dinámico de seguridad (DCVV3) generado por la tarjeta bancaria (1000);

comprendiendo el servidor de autenticación, además:

- un módulo de verificación (5400) configurado para generar un segundo código dinámico de seguridad (DCVV4) a partir del identificador bancario PAN y la fecha de caducidad (EXP) registrada en dicha memoria, para comparar los primero y segundo códigos dinámicos de seguridad, y para detectar que el primer código dinámico de seguridad (DCVV3) es válido solamente si coincide con el segundo código dinámico de seguridad (DCVV4); y

- estando dicho módulo de comunicación (5200) configurado para enviar al servidor de acceso (3000) un mensaje de autenticación positiva (M2) solamente si:

    ° el segundo código de acceso (CD2) coincide con el primer código de acceso registrado (CD1); y

    ° el primer código dinámico de seguridad (DCVV3) es válido.

2. Servidor de autenticación según la reivindicación 1, en donde el primer código dinámico de seguridad (DCVV3) recibido por el módulo de comunicación (5200) en la demanda de autenticación es generado por la tarjeta bancaria (1000) al ejecutar una función criptográfica a partir del identificador bancario PAN y de la fecha de caducidad (EXP), y a partir de un dato temporal o de un contador del número de primeros códigos dinámicos de seguridad (DCVV3).

3. Servidor de autenticación según la reivindicación 2, en donde el módulo de verificación (5400) está configurado para generar el segundo código dinámico de seguridad (DCVV4) al ejecutar la función criptográfica a partir de dicho identificador bancario PAN y de la fecha de caducidad (EXP) registrados en dicha memoria y a partir de un dato temporal o de un contador del número de segundo código dinámico de seguridad (DCVV4).

4. Servidor de autenticación según una cualquiera de las reivindicaciones 1 a 3, en donde el módulo de comunicación (5200) puede recibir, en datos de transacción bancaria (DT1), el identificador de PAN que se transmitirá a dicho servidor distante (6000).

5. Servidor de autenticación según la reivindicación 4, en donde el módulo de comunicación (5200) puede recibir los datos de la transacción bancaria (DT1) desde el servidor de acceso (3000).

6. Servidor de autenticación según la reivindicación 4 o 5, en donde:

- los datos de la transacción bancaria (DT1) comprenden un tercer código dinámico de seguridad (DCCV1) generado por dicha tarjeta bancaria (1000), el identificador bancario PAN y la fecha de caducidad (EXP);

- el módulo de verificación (5400) puede verificar la validez del tercer código dinámico de seguridad (DCVV1);

- estando dicho módulo de comunicación (5200) configurado para transmitir al servidor distante (6000), solamente si la verificación de validez del tercer código dinámico de seguridad (DCVV1) se ha superado con éxito, el identificador PAN y un mensaje (M1) que indica que dicho tercer código dinámico de seguridad (DCVV1) es válido; y

- dicho módulo de comunicación (5200) puede recibir del servidor distante (6000), en respuesta al identificador y a dicho mensaje (M1) transmitido, dicho primer código de acceso (CD1) para ser registrado por el módulo de registro (5300).

7. Servidor de autenticación según la combinación de las reivindicaciones 2, 3 y 6, en donde:

- el tercer código dinámico de seguridad (DCVV1) se genera por la tarjeta bancaria (1000) a partir del identificador PAN y de la fecha de caducidad (EXP) de la tarjeta bancaria (100), a partir de un dato temporal o del contador para el número de primeros códigos dinámicos de seguridad (DCVV3);

- el módulo de verificación (5400) está configurado para generar un cuarto código dinámico de seguridad (DCVV2) a partir del identificador PAN y de la fecha de caducidad (EXP) de la tarjeta bancaria (100), y a partir de un dato temporal o del contador del número de segundos códigos dinámicos de seguridad (DCVV4), para comparar los códigos de seguridad dinámicos tercero y cuarto, y para detectar que el tercer código dinámico de seguridad (DCVV1) es válido solamente si dicho tercer código dinámico de seguridad (DCVV1) coincide con el cuarto código dinámico de seguridad (DCVV2).

8. Servidor de autenticación según una cualquiera de las reivindicaciones 1 a 7, en donde el módulo de registro (5300) está configurado para registrar un identificador (IDS1) del servicio (S1) en asociación con el identificador PAN, la fecha de caducidad (EXP) y el primer código de acceso (CD1) de modo que el módulo de verificación (5400) pueda determinar el primer código de acceso (CD1) asociado con dicho servicio (S1).

9. Servidor de autenticación según una cualquiera de las reivindicaciones 1 a 8, en donde el módulo de registro (5300) está configurado para registrar el primer código de acceso (CD1) en dicha memoria en asociación con una pluralidad de servicios.

10. Servidor de autenticación según una cualquiera de las reivindicaciones 1 a 9, en donde:

- el módulo de registro (5300) está configurado para registrar una condición temporal en asociación con el identificador PAN, la fecha de caducidad (EXP) y el primer código de acceso (CD1),

- estando el módulo de verificación (5400) configurado para determinar que el primer código de acceso (CD1) es válido siempre que se cumpla la condición temporal.

11. Servidor de autenticación (5000) según una cualquiera de las reivindicaciones 1 a 10, en donde el módulo de comunicación está configurado para enviar al servidor de acceso (3000) un mensaje de autenticación negativo, si el segundo código de acceso (CD2) no coincide con el primer código de acceso (CD1) registrado o si el primer código dinámico de seguridad (DCVV3) no es válido.

12. Sistema de control de acceso a un servicio (SY) (S1) que comprende:

- un servidor de autenticación (5000) según una cualquiera de las reivindicaciones 1 a 11; y

- un servidor de acceso (3000) capaz de controlar el acceso a dicho servicio (S1), estando configurado dicho servidor de acceso para autorizar el acceso a dicho servicio a un usuario asociado con dicho identificador PAN, solamente al recibir el mensaje de autenticación positiva del servidor de autenticación.

13. Método de autenticación puesto en práctica por un servidor de autenticación (5000), que comprende:

- transmisión (C14), a un servidor distante (6000), de un identificador bancario PAN asociado con una tarjeta bancaria (1000);

- recepción (C18), en respuesta a dicha transmisión (C14), de un primer código de acceso (CD1) para acceder a un servicio (S1);

- registro (C20) del identificador PAN en asociación con el primer código de acceso (CD1);

- recepción (C32) de una demanda de autenticación (RQ) procedente de un servidor de acceso (3000) que controla el acceso a dicho servicio (S1), comprendiendo dicha demanda un segundo código de acceso (CD2) y un primer código dinámico de seguridad (DCVV3) generado por la tarjeta bancaria (1000) al ejecutar una función criptográfica a partir de un dato temporal;

- verificación (C34) de la validez del primer código dinámico de seguridad (DCVV3), comprendiendo dicha verificación la generación (C36) de un segundo código dinámico de seguridad (DCVV4) al ejecutar dicha función criptográfica a partir de un dato temporal y a partir de dicho identificador PAN registrado, siendo la comparación (C38) del primer y segundo código dinámico de seguridad, y la detección (C34) de que el primer código dinámico de seguridad (DCVV3), es válido solamente si coincide con el segundo código dinámico de seguridad (DCVV4); y

- el envío (C42) al servidor de acceso (3000) de un mensaje de autenticación positiva (M2) solamente si:

- el segundo código de acceso (CD2) coincide con el primer código de acceso registrado (CD1); y
- el primer código dinámico de seguridad (DCVV3) es válido.

14. Programa informático (PG2; PG3) que comprende instrucciones para la ejecución de las etapas de un método de conformidad con la reivindicación 13 cuando dicho programa es ejecutado por un ordenador.

15. Soporte de registro (M1) legible por un ordenador en donde se registra un programa informático (PG2; PG3) que comprende instrucciones para la ejecución de las etapas de un método de conformidad con la reivindicación 13.

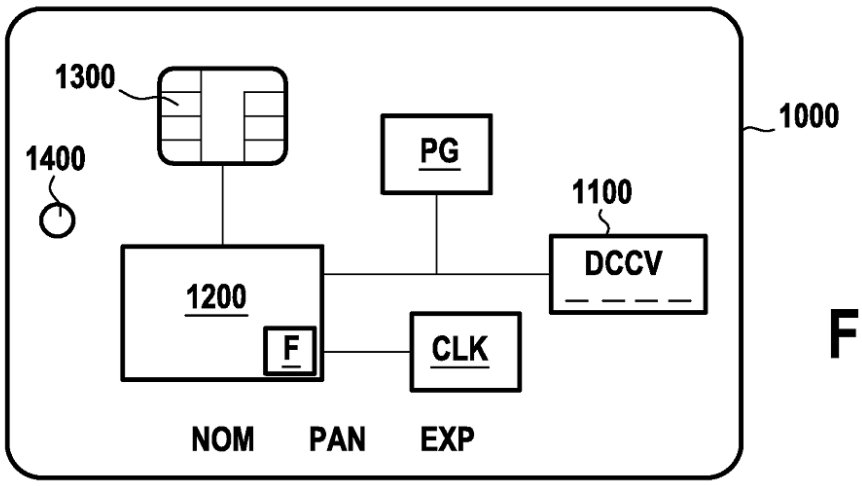

FIG.1

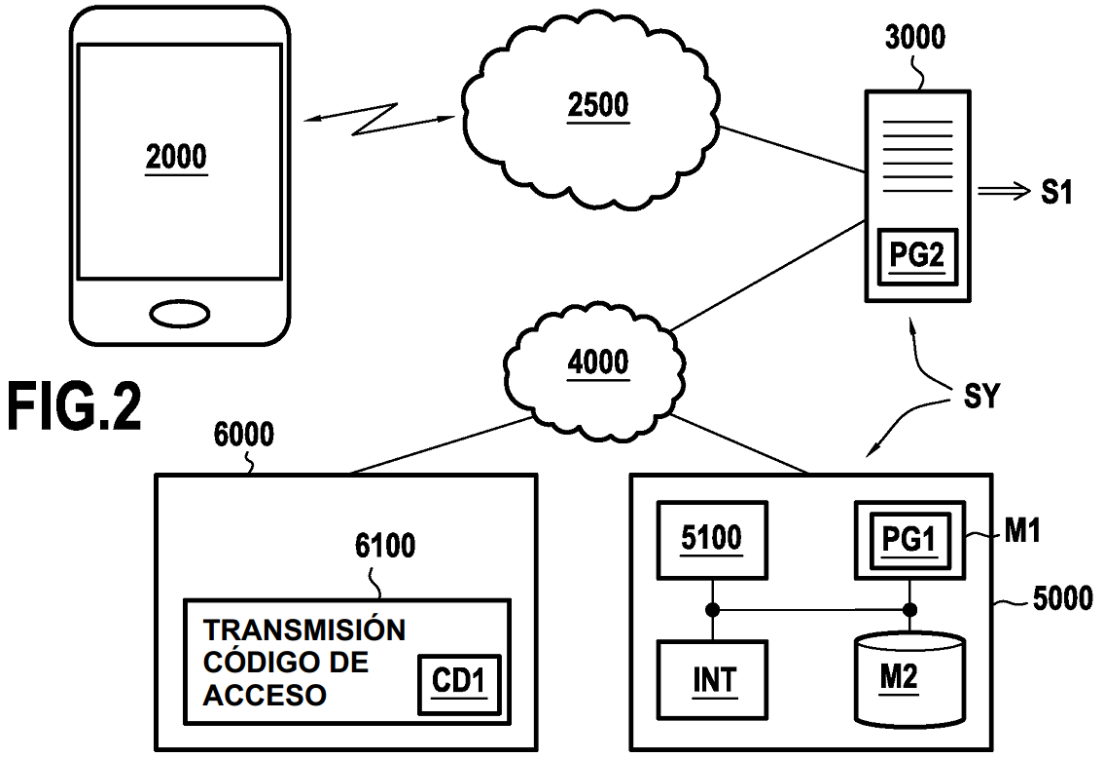

FIG.2

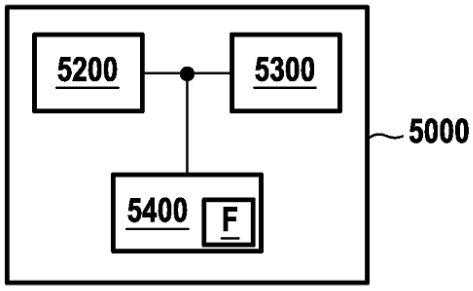

FIG.3

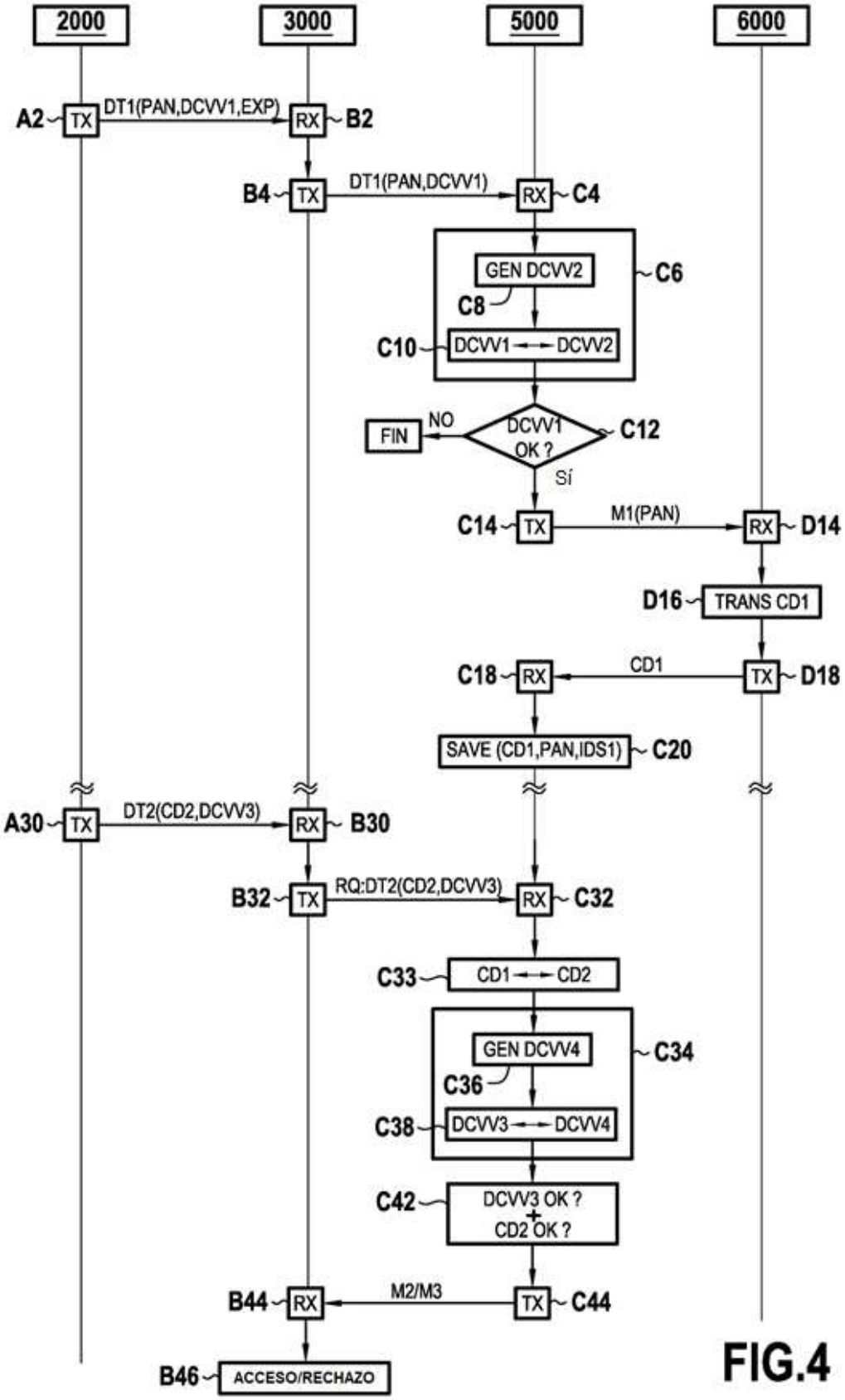
2000
3000
5000
6000
A2
TX
DT1(PAN,DCVV1,EXP)
RX
B2
B4
TX
DT1(PAN,DCVV1)
RX
C4
GEN DCVV2
C6
C8
C10
DCVV1 ↔ DCVV2
FIN
NO
DCVV1 OK ?
C12
Sí
C14
TX
M1(PAN)
RX
D14
D16
TRANS CD1
C18
RX
CD1
TX
D18
SAVE (CD1,PAN,IDS1)
C20
A30
TX
DT2(CD2,DCVV3)
RX
B30
B32
TX
RQ:DT2(CD2,DCVV3)
RX
C32
C33
CD1 ↔ CD2
GEN DCVV4
C34
C36
C38
DCVV3 ↔ DCVV4
C42
DCVV3 OK ?
+
CD2 OK ?
B44
RX
M2/M3
TX
C44
B46
ACCESO/RECHAZO

FIG.4