(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 603 585**

(51) Int. CI.:

H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.09.2010 E 10012098 (9)**

(97) Fecha y número de publicación de la concesión europea: **17.08.2016 EP 2306668**

(54) Título: **Sistema y procedimiento de transacción segura en línea**

(30) Prioridad:

30.09.2009 FR 0904662

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.02.2017

(73) Titular/es:

INGENICO GROUP (100.0%)
28-32 Boulevard de Grenelle
75015 Paris, FR

(72) Inventor/es:

MARTIN, PATRICE;
CHOISET, BRUNO y
COGNEAU, LAURENT

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Sistema y procedimiento de transacción segura en línea

La presente invención se refiere al campo de las transmisiones seguras de datos a través de al menos una red de comunicación como, por ejemplo, la red Internet. Las transmisiones permiten, por ejemplo, llevar a cabo operaciones "en línea" (u "on line", según la terminología en inglés), conectándose al menos a un servidor por medio de al menos un terminal adecuado, a través de al menos una red de comunicación.

La presente invención se aprovecha de las tarjetas chip seguras como, por ejemplo, las "tarjetas bancarias" o las "tarjetas de pago con chip", especialmente las conocidas con el nombre de EMV (para “Europay MasterCard Visa"), que permiten proteger los pagos realizados por medio del chip (por ejemplo, del tipo ISO 7816) de la tarjeta que comprende al menos una clave de encriptación y, en su caso, por medio del código de identificación asociado (número de identificación personal, PIN para "Personal Identification Number" según la terminología en inglés). Cabe señalar que la presente invención se adapta particularmente para llevar a cabo transacciones en línea, pero también puede ser utilizada para diversos tipos de intercambio seguro de información. De este modo, por ejemplo, la presente invención está adaptada para el uso de otras tarjetas como, por ejemplo, las tarjetas sanitarias, las tarjetas de los profesionales de la salud (CPS) o cualquier otro tipo de tarjeta cuyo chip almacene al menos una clave encriptada, con el fin de proteger los intercambios de datos de cualquier tipo (estando estos intercambios reagrupados aquí bajo el término "transacción"). De hecho, la invención puede, en su caso, evolucionar según el cambio de las normas de las tarjetas, especialmente las tarjetas EMV, y se hablará en la presente solicitud en general de "tarjeta segura" para referirse a este tipo de tarjetas chip que contienen al menos una clave simétrica de encriptación almacenada en el chip y provistas con capacidades criptográficas por clave simétrica, En cambio con las tarjetas de tipo PKI (“Public Key Infrastructure", según la terminología en inglés, que se refiere a una infraestructura que permite la gestión y uso de certificados digitales que vinculan las claves públicas con la identidad de un usuario) conocidas de la técnica anterior que utilizan claves asimétricas y tienen los inconvenientes mencionados más adelante.

Un problema en el ámbito de las transacciones seguras se refiere a los ataques posibles, por ejemplo, por piratas informáticos, para obtener los datos sensibles de las transacciones, como las informaciones bancarias, etc. Muchos de los ataques informáticos se basan en la ingeniería social (es decir, la falta de conocimientos técnicos por parte del público, que no conoce los mecanismos de seguridad y puede, por consiguiente, utilizar los mecanismos de forma que corran el riesgo de dejarlos vulnerables). En particular, se conocen los virus informáticos, que son programas informáticos escritos con el fin de propagarse a otros ordenadores insertándose en programas legítimos llamados "anfitriones". También pueden tener el efecto, buscado o no, de dañar perturbando más o menos seriamente el funcionamiento del ordenador infectado. Se pueden propagar a través de cualquier medio de intercambio de datos digitales como Internet, pero también disquetes, CD-ROM, dispositivos USB, etc. Existen, también, los ataques conocidos con el nombre de "suplantación de la identidad" o "cebo" ("phishing”, según la terminología en inglés) utilizados por los estafadores para obtener informaciones personales con el fin de cometer una usurpación de la identidad. La técnica consiste en hacer creer a la víctima que se está dirigiendo a un tercero de confianza (banco, administración, etc.) con el fin de sonsacarle informaciones personales (contraseña, número de tarjeta de crédito, fecha de nacimiento, etc.). La suplantación de la identidad puede hacerse por correo electrónico, por sitios webs falsificados o por otros medios electrónicos. Se conocen también los ataques llamados de “redireccionamiento malicioso” ("pharming" en inglés), que explotan las vulnerabilidades del DNS ("Domain Name System", según la terminología en inglés) para recuperar los datos de una víctima. Se trata de un tipo de suplantación de la personalidad que permite robar informaciones después de haber atraído a la víctima a un sitio web camuflado, incluso aunque el nombre del dominio esté escrito correctamente. Los piratas informáticos habrán cambiado previamente la correspondencia entre el nombre del dominio y la dirección IP. De ese modo, por ejemplo, www.mabanque.fr no apuntará ya hacia la dirección IP del servidor de "Mi Banco", sino a otro servidor fraudulento. Otros tipos de ataques son conocidos con el nombre de “registrador de pulsaciones en el teclado” ("keylogger", según la terminología en inglés) por los cuales el equipo o software espía registra las pulsaciones en el teclado de un ordenador en ciertas condiciones y las transmite, en especial para permitir un uso fraudulento. También, se sabe de los ataques conocidos como el "intermediario" (“hombre en el medio”, HDM, en francés) (o "man in the middle attack", MITM, según la terminología en inglés) que tiene como fin interceptar las comunicaciones entre dos partes sin que ni una ni otra puedan dudar de que el canal de comunicación (CS) entre ellas se ha visto comprometido. El atacante debe, en primer lugar, ser capaz de observar e interceptar los mensajes de una víctima con la otra. El ataque "intermediario" es particularmente aplicable en el protocolo original de intercambio de las claves Diffie-Hellman, cuando se utiliza sin autenticación. También se sabe de los ataques conocidos con el nombre de "el hombre del navegador" (o "man in the browser", según la terminología en inglés), que es una forma reciente de amenazas vinculadas a los ataques de intermediario (hombre del medio), y se basan en un troyano (software malicioso aparentemente legítimo diseñado para ejecutar acciones sin el conocimiento del usuario, utilizando por lo general derechos que pertenecen a su entorno para desviar, difundir o destruir las informaciones, o incluso para abrir una puerta trasera que permita a un atacante tomar el control remoto de un ordenador). Estos ataques infectan, por ejemplo, un navegador de internet y permiten modificar páginas, modificando el contenido o las transacciones o insertar otras transacciones, todo ello de un modo totalmente invisible para el usuario y la aplicación anfitriona. Estos ataques son particularmente peligrosos porque generalmente tienen éxito, incluso cuando se utilizan mecanismos de seguridad como SSL, PKI ("Public Key Infrastructure", según la terminología en inglés que se refiere a una

infraestructura que permite la gestión y utilización de certificados digitales que vinculan las claves públicas con la identidad de un usuario) y/o el uso de autenticación de dos o tres factores.

Se conocen en la técnica anterior diversas soluciones para realizar transacciones seguras por internet. Sin embargo, la mayor parte de las soluciones conocidas son vulnerables a al menos uno de los ataques conocidos. Se conocen, por ejemplo, las soluciones que utilizan "clave de protección" (material informático, como una clave para conectarse a un ordenador, por ejemplo de USB, "Universal Serial Bus") u objetos portátiles o tarjetas chip y/o lectores de tarjetas chip dispuestos para proteger las operaciones. Sin embargo, este tipo de solución tiene el inconveniente de utilizar certificados, tales como protocolos SSL/TLS, por ejemplo, cuyo usuario no puede generalmente verificar la autenticidad y que son, por consiguiente, vulnerables a algunos de los ataques descritos. Además, estas soluciones tienen el inconveniente de requerir el despliegue de una infraestructura de red que soporte el uso de estos dispositivos para la autenticación (gestión de los certificados distribuidos, etc.). En efecto, diversos protocolos relativamente seguros, como SSL/TLS, se abandonan debido a los problemas de ingeniería social antes mencionados, porque los usuarios aceptan cualquier certificado que se les presente.

También se conocen soluciones que consisten en la creación de un canal seguro (o "túnel" seguro), es decir, un canal (CS) de comunicación encriptada, entre las 2 entidades relacionadas en el momento de la transacción (por ejemplo, banco-usuario). Sin embargo, este tipo de solución tiene también el inconveniente de quedar vulnerable a ciertos ataques porque el canal seguro se basa en el uso de certificados tales como los protocolos SSL/TLS.

Por último, se conocen, en especial de los documentos WO 2005/001618, EP 1850297 y WO 01/82246, soluciones conocidas que son compatibles con el Programa de Autenticación por Tarjeta (PAC, o CAP para "Chip Authentication Program" según la terminología en inglés) y que usan un lector de tarjeta bancaria conectado al terminal (ordenador, por ejemplo) del usuario y en el que éste último inserta una tarjeta bancaria para permitir la firma de las transacciones por el chip de esta tarjeta. Sin embargo, este tipo de solución tiene el inconveniente de ser vulnerable a ciertos ataques ya que las informaciones sensibles circulan por el terminal que pide al lector la firma de la transacción por la tarjeta. Por ejemplo, un problema con esta solución está vinculado a la ingeniería social, ya que es debido al hecho de que el usuario no verifica generalmente las informaciones en el lector y se conforma con validar la transacción fiándose de lo que se visualiza en su terminal, cuando un ataque, por ejemplo, del tipo hombre del navegador, haya podido desviar las informaciones a validar en el lector a la vez que se visualizan informaciones normales en el terminal.

En este contexto, existe la necesidad de soluciones sencillas, económicas y fáciles de utilizar, especialmente por el público en general, lo que permite proteger las transacciones en línea, a diferencia de las soluciones conocidas a menudo demasiado caras, demasiado complejas de utilizar y de ejecutar por el público en general, sobre todo a causa de los problemas vinculados a la ingeniería social.

Un objetivo de la presente invención es, por consiguiente, superar al menos algunos inconvenientes de la técnica anterior proporcionando un sistema que permita inicializar transacciones seguras en línea.

Este objetivo se logra mediante un sistema de inicialización de transacción segura en línea, a través de al menos una red de comunicación, conteniendo el sistema al menos un equipo de un proveedor de servicios que comprende al menos un servidor dispuesto para gestionar transacciones en línea, por el intercambio de datos representativos de las transacciones, comprendiendo dicho equipo también al menos un módulo de seguridad dispuesto para proteger esas transacciones, caracterizado porque:

- dicho sistema contiene al menos un lector de tarjeta chip que accede al equipo proveedor a través de dicha red de comunicación y que comprende medios de procesamiento dispuestos para, por una parte, intercambiar datos con al menos un chip de al menos una tarjeta segura, con el fin de obtener del chip, y transmitir al módulo de seguridad los datos, denominados públicos, representativos de al menos una información vinculada a la tarjeta y, por otra parte, para generar, en cooperación con dicho chip, al menos una clave de sesión, y transmitir al módulo de seguridad los datos encriptados utilizando esta clave de sesión,
- el módulo de seguridad está dispuesto para calcular dicha clave de sesión a partir de dichos datos públicos recibidos y al menos una clave de encriptado,
- el cálculo de la clave de sesión por el lector y el módulo de seguridad que permite la inicialización de la transacción mediante el establecimiento de un canal de comunicación seguro en el que los datos representativos de la transacción podrán circular en forma encriptada por dicha clave de sesión.

Según otra característica, el chip de la tarjeta está dispuesto para generar, a partir de al menos una clave de encriptado almacenada en el chip, al menos un criptograma utilizado por los medios de procesamiento del lector dispuestos para generar la clave de sesión utilizada en el establecimiento del canal seguro.

Según otra característica:

- el módulo de seguridad utiliza al menos una clave, denominada clave madre utilizada para la generación de las claves de las tarjetas seguras suministradas por el proveedor de servicios, denominadas claves hijas, siendo cada una de las tarjetas suministradas identificable a partir de al menos una información contenida en los datos públicos,
- los medios de procesamiento del lector transmiten al módulo de seguridad los datos públicos que le permiten hallar la clave de encriptado a utilizar para el cálculo de la clave de sesión.

Según otra característica, el equipo del proveedor de servicio contiene al menos una base de datos que almacenan las claves de encriptado de las tarjetas seguras suministradas por el proveedor de servicio, el módulo de seguridad que accede a esta base de datos para encontrar, en función de los datos públicos recibidos del lector de la tarjeta chip, la clave de encriptado a utilizar para el cálculo de la clave de sesión.

Según otra característica, el lector y el equipo proveedor están conectados a través de una comunicación segura según un protocolo de tipo SSL/TLS dentro de la cual quedará establecido el canal seguro.

Según otra característica, los medios de procesamiento del lector están dispuestos para recibir del módulo de seguridad y tratar al menos una petición de inicialización del canal seguro que comprende un número impredecible y que provoca la consulta del chip por el lector, para obtener al menos un criptograma y los datos representativos de las informaciones vinculadas a la tarjeta, lo que permite a los medios de procesamiento del lector generar la clave de sesión que sirve para establecer el canal de comunicación seguro y transmitir al módulo de seguridad, por una parte, los datos representativos de informaciones vinculadas a la tarjeta y, por otra parte, dichos datos encriptadas con esta clave de sesión, que contienen los datos relativos al número impredecible.

Según otra característica, la inicialización de la transacción responde a una transmisión al servidor del equipo proveedor de al menos una parte de los datos representativos de la transacción, por un servidor de terceros que gestiona un sitio internet al que el usuario se ha conectado.

Según otra característica, el servidor del equipo proveedor está dispuesto para gestionar el establecimiento y la utilización del canal seguro tratando y conservando un número impredecible, la clave de sesión, un número de sesión generado en el establecimiento del canal seguro y que está vinculado al número impredecible y a un contador de transacción de la tarjeta, así como un número de secuencia incrementado en cada petición enviada al lector durante cada sesión.

Según otra característica, el módulo de seguridad del equipo proveedor está dispuesto para almacenar la clave de sesión en los medios de memorización y/o para encriptar la clave de sesión utilizando una clave, denominada clave maestra, y transmitirla al servidor para el almacenamiento en forma encriptada en los medios de memorización.

Otro objetivo de la presente invención es superar al menos algunos inconvenientes de la técnica anterior proponiendo un sistema que permita proteger las transacciones en línea.

Este objetivo se consigue mediante un sistema de transacción segura, que contiene un sistema de inicialización según la invención, en el que el lector y el módulo de seguridad están dispuestos para encriptar y desencriptar, mediante dicha clave de sesión, los datos representativos de la transacción que se intercambian durante la transacción, circulando entonces estos datos por el canal de comunicación seguro con estos encriptados/desencriptados.

Según otra característica, el servidor está dispuesto para requerir del módulo de seguridad, en cada transmisión de datos con el lector, un encriptado/desencriptado por dicha clave de sesión de los datos transmitidos, estando el lector dispuesto para encriptar/desencriptar también los datos intercambiados durante la transacción.

Otro objetivo de la presente invención es superar al menos algunos inconvenientes de la técnica anterior proponiendo un procedimiento que permita la inicialización de transacciones seguras en línea.

Este objetivo se consigue mediante un procedimiento de inicialización de transacción segura en línea, a través de al menos una red de comunicación, ejecutada por un sistema de inicialización de transacción segura según la invención, caracterizado porque contiene al menos una etapa de establecimiento de al menos un canal de comunicación segura entre el módulo de seguridad y el lector que se ejecuta por medio de las siguientes etapas:

- generación de al menos una clave de sesión, mediante los medios de procesamiento del lector, en cooperación con la tarjeta, después del encriptado de los datos utilizando esta clave de sesión,
- obtención, por el lector, a partir del chip de la tarjeta, de los datos representativos de las informaciones vinculadas a la tarjeta,
- transmisión, del lector al módulo de seguridad, de los datos representativos de las informaciones vinculadas a la tarjeta y de los datos encriptados utilizando la clave de sesión,
- generación, mediante el módulo de seguridad, de la clave de sesión a partir de al menos una clave de encriptado del módulo de seguridad y de los datos recibidos.

Según otra característica, la etapa de generación de al menos una clave de sesión, mediante los medios de procesamiento del lector está precedida por una etapa de generación (51), por el chip de la tarjeta, de al menos un criptograma a partir de la clave de encriptado almacenada en el chip y de la transmisión de este (estos) criptograma (criptogramas) al lector generando la clave de sesión a partir de este (estos) criptograma (criptogramas).

Según otra característica, el procedimiento contiene al menos una etapa de entrada, por el usuario de la tarjeta, de al menos un código de identificación personal de usuario, y de autenticación de ese código por el chip de la tarjeta, permitiendo esta etapa de entrada/autenticación al menos una etapa de firma de datos por el chip.

Según otra característica, el procedimiento contiene al menos una etapa de recepción y procesamiento, por los medios de procesamiento del lector, de al menos una petición de inicialización del canal seguro enviada por el módulo de seguridad, que comprende un número impredecible y provocando la consulta del chip por el lector, para obtener al menos un criptograma y los datos representativos de las informaciones vinculadas a la tarjeta, permitiendo esta etapa la etapa de generación de la clave de sesión que se utiliza para establecer el canal de comunicación seguro y la transmisión al módulo de seguridad, por una parte, de los datos representativos de las informaciones vinculadas a la tarjeta y, por otra parte, dichos datos encriptados utilizando esta clave de sesión, que contiene datos relativos al número impredecible.

Otro objetivo de la presente invención es superar al menos algunos inconvenientes de la técnica anterior proporcionando un procedimiento que permita proteger las transacciones en línea.

Este objetivo se consigue mediante un procedimiento de transacción segura, caracterizado porque contiene las etapas del procedimiento de inicialización según la invención y al menos una etapa de transmisión de datos entre el módulo de seguridad y el lector, en forma encriptada utilizando dicha clave de sesión, ejecutada en un sistema de transacción segura según la invención.

Según otra característica, el servidor está dispuesto para requerir del módulo de seguridad, en cada etapa de transmisión de datos con el lector, un encriptado/desencriptado por dicha clave de sesión de los datos transmitidos, estando el lector dispuesto para encriptar/desencriptar también los datos intercambiados durante la transacción.

Otras características y ventajas de la presente invención aparecerán más claramente de la lectura de la siguiente descripción, hecha con referencia a los dibujos adjuntos, en los que:

- la figura 1 muestra una realización del sistema según la invención,
- la figura 2 muestra una realización del procedimiento según la invención,
- la figura 3 muestra una realización del procedimiento según la invención, hasta el establecimiento del canal seguro,
- la figura 4 muestra la continuación de la realización del procedimiento de la figura 3, a partir del establecimiento del canal seguro.

La presente invención se refiere, por una parte, a un sistema y a un procedimiento de inicialización de transacción segura en línea, por medio del establecimiento de un canal seguro descrito a continuación. La presente invención se refiere, por otra parte, a un sistema y a un procedimiento de transacción segura en línea, es decir, transmisiones de datos seguras, que se basan en dicho canal seguro. Como ejemplos ilustrativos y no limitantes, los datos transmitidos podrán referirse a operaciones que permitan la consulta y gestión de operaciones bancarias corrientes en línea ("e-banking (banca electrónica)") y/o que permitan la suscripción a productos financieros en línea ("e-subscription (suscripción electrónica)") y/o que permitan la validación de solicitudes de retención ante un destinatario autorizado como, por ejemplo, con los títulos interbancarios de pago, TIP ("e-billing", “facturación electrónica” en inglés) o y/o que permitan el pago de compras en línea ("e-commerce (comercio electrónico)"), utilizando por ejemplo un protocolo de pago seguro en Internet tal como el protocolo de "3D-securo". La invención es particularmente ventajosa porque se propone proteger las transacciones mediante un mecanismo resistente a la mayor parte de los ataques conocidos y que permiten atenerse a los problemas de ingeniería social. El término "transacción" se refiere, en la presente solicitud, cualquier tipo de transmisión de datos a través de al menos una red de comunicación, siendo estas transmisiones seguras por medio de la presente invención. De este modo, el término "transacción" podrá referirse a una transacción, por ejemplo, de tipo bancario (por ejemplo, un pago en línea, etc.), pero la verdad es que podrá referirse a otros tipos de transmisiones de datos (por ejemplo, en el caso de envío de informaciones personales, en particular durante el uso de una tarjeta sanitaria u otra). Estas "transacciones" se designan en el presente documento de ser efectuadas entre al menos un usuario y al menos una entidad designada por el término "proveedor de servicio" (por ejemplo, un establecimiento bancario, una organización privada o pública, etc.), que posee un equipo (un conjunto de dispositivos, por ejemplo) específico para la ejecución de la invención, designado con el término "equipo (4) proveedor" (o "equipo (4) del proveedor de servicio"), como se detalla a continuación. El proveedor del servicio habrá proporcionado a los usuarios de la presente invención una tarjeta (2) denominada "segura" (como se explica más adelante) y un lector (1) de tarjeta específico, para permitirle realizar las transacciones en línea. La tarjeta (2) y el lector (1) se diseñan como de ser "suministrados" por el proveedor de servicio pero se mostrará de la lectura de la presente solicitud que la invención no se limita a la forma en la que los usuarios los han obtenido, siendo este término utilizado para explicar que el proveedor de servicio conoce las tarjetas de los usuarios (por ejemplo por medio de al menos una base de datos que almacenan identificadores de usuario y de tarjetas), como se explica en detalle a continuación y posee un equipo (4) proveedor dispuesto para cooperar con los lectores (1) de tarjeta durante las transacciones, como se explica a continuación.

Como se mencionó anteriormente, la presente invención permite varios tipos de transacciones tales como, a modo de ejemplos ilustrativos y no limitativos, los conocidos con los nombres de "banca electrónica", "suscripción electrónica", "facturación electrónica" o "comercio electrónico". El comercio electrónico utiliza, por ejemplo, el protocolo "3D-seguro" que permite una autenticación del tenedor de una tarjeta de pago de las compras realizadas en los sitios web, y consiste en asociar el procedimiento de autorización financiera con una autenticación en línea basada en un modelo que contiene 3 ámbitos (el ámbito del comprador, es decir, en general, el ámbito del comerciante y de la sociedad que le afilió a la red de pago; el ámbito del emisor, es decir, en general, el ámbito del

titular de la tarjeta y de la sociedad (a menudo su banco) que emitió la tarjeta, el ámbito de la interoperabilidad, es decir, en general, el del operador de la red de pago que asegura la interoperabilidad entre los dos primeros ámbitos y se asegura de que los flujos financieros desembocan allá donde deben desembocar). Este protocolo se basa en los mensajes enviados a través de comunicaciones seguras, por ejemplo, por medio de protocolos de tipo SSL ("Secure Sockets Layer", según la terminología en inglés) o TLS ("Transport Layer Security", según la terminología de inglés) que garantizan la autenticación del servidor y del cliente por certificados digitales. Cabe señalar que la presente invención puede ser compatible con la Programa de Autenticación por Tarjeta (PAC, o CAP para el "Chip Authentication Program ", según la terminología en inglés), que proporciona las especificaciones técnicas relativas a la utilización de tarjetas chip bancarias para la autenticación de los usuarios y de las transacciones bancarias en línea y por teléfono. También se adoptó como contraseña de autenticación dinámica (DPA). Los clientes de los bancos que recibieron un lector CAP de su banco pueden insertar su tarjeta bancaria en el lector CAP, con el fin de participar en uno de los protocolos de autenticación respaldados por estas especificaciones. El CAP es una forma de autenticación que utiliza dos factores a la vez, porque deben ser presentados tarjeta chip y un PIN válido para que una transacción dé resultado, según varios procedimientos admitidos. Sin embargo, como se ha mencionado en el preámbulo de la presente solicitud, los procedimientos admitidos por las especificaciones CAP tienen el inconveniente de quedar vulnerables a algunos ataques mientras que la presente invención cumple con los requisitos de seguridad CAP pero permite proteger todavía más las transacciones.

Además, como se mencionó anteriormente, la presente invención se aprovecha de las tarjetas chip designadas aquí con el término "tarjeta chip segura" que almacenan al menos una clave simétrica de encriptado e contienen un chip provisto de capacidades criptográficas que utiliza claves simétricas. Podrá tratarse, en particular, de tarjetas bancarias, es decir, tarjetas chip de pago tal como las conocidas con el nombre de EMV (para "Europay MasterCard Visa") que permiten proteger los pagos realizados por medio del chip (por ejemplo, del tipo ISO 7816) de la tarjeta que contiene al menos una clave de encriptado simétrico. Sin embargo, la invención no se limita a las tarjetas bancarias (o tarjeta sanitaria u otras) citadas aquí como ejemplo ilustrativo y no limitativo pues la invención solo necesita, en lo que se refiere a la tarjeta, que el chip almacene una clave simétrica de encriptado y los datos relativos a la tarjeta, y que posea al menos capacidad de encriptado simétrico (como por ejemplo, con al menos una aplicación específica implantada en el chip de la tarjeta) que se ejecutan en respuesta a las órdenes recibidas de un lector que acceda a la tarjeta. Cabe señalar que como alternativa, es posible que el lector y la tarjeta interactúen a través de una comunicación sin contacto (sin estar la tarjeta, necesariamente, insertada en el lector, pero que este último pueda acceder a ella). El término "tarjeta segura" se utilizará en la presente descripción para designar este tipo de tarjetas. La presente invención no requiere, por consiguiente, el despliegue de nuevas entidades de encriptado (como las "claves de protección", las claves USB de encriptado u otro dispositivo a conectar a un terminal y que almacene una clave de encriptado) y prevé la utilización de tarjetas seguras que permiten una autenticación sólida y mutua entre el equipo proveedor (4) y el chip (20) de la tarjeta, como se detalla a continuación. Por consiguiente, la invención puede aprovecharse de las tarjetas que ya se están utilizando y que ya tienen los medios necesarios para su implantación (en términos de la tarjeta: capacidades de criptografía simétrica, clave de encriptado y los datos acerca de la tarjeta) como, por ejemplo, las tarjetas bancarias de tipo EMV. Cabe señalar que en el caso de tarjetas seguras que requieren la introducción de un código PIN (como las tarjetas EMV), se obtiene incluso una sólida y mutua autenticación entre el proveedor y el propio usuario. Mediante los medios aplicados en la presente invención, el usuario tiene la seguridad de realizar una transacción con su proveedor de servicio y este último tiene también la seguridad de una transacción con su cliente (el usuario o al menos un usuario autorizado, siempre que al usuario no le hayan robado su tarjeta y el código PIN asociado).

La presente invención requiere el uso de un lector (1) de tarjeta segura, que contiene medios (12) de procesamiento de datos dispuestos para dialogar con el chip (20) de la tarjeta (2), en particular para obtener del chip (20) las firmas de los datos para el establecimiento del canal seguro y para realizar las transacciones realizadas en línea. Además, estos medios (12) de procesamiento de datos se disponen para realizar operaciones criptográficas sobre los datos suministrados por el chip y para transmitir al equipo (4) proveedor los datos encriptados a través de un canal seguro (CS).

El lector (1) está (o sus medios de procesamiento están) dispuesto (dispuestos) además para el establecimiento de un canal (CS) de comunicación seguro (o "túnel seguro") con al menos un módulo (o dispositivo) de seguridad del equipo (4) proveedor en modo conectado (es decir, durante una comunicación con el equipo proveedor por medio de al menos una red de comunicación), por ejemplo, según un algoritmo 3DES, por ejemplo en el modo CBC, y con una clave de sesión (Kses) previamente generada. Como se mencionó anteriormente, la presente invención utiliza una de las funcionalidades de las tarjetas seguras permitidas por al menos una clave de encriptado almacenada en el chip y proporcionada por el (o conocido del) proveedor de servicio. Cabe señalar que el algoritmo de cifrado 3DES (denominado también "Triple DES") que es un algoritmo de cifrado simétrico que encadena tres aplicaciones sucesivas del algoritmo DES (para “Data Encryption Standard", según la terminología en inglés, que es un algoritmo de cifrado por bloques) en el mismo bloque de datos de 64 bits, con 2 ó 3 claves DES diferentes solo se cita aquí a modo de ejemplo ilustrativo y no limitativo. Asimismo, el modo CBC ("Cipher Block Chaining" según la terminología en inglés o "encadenamiento de los bloques") que consiste en aplicar a cada bloque una "OR exclusivo” con el cifrado del bloque precedente antes de que él mismo sea cifrado y que utiliza un vector de inicialización para hacer único cada mensaje, citado aquí sólo como ejemplo ilustrativo y no limitativo. En efecto, se entenderá de la lectura de la presente solicitud que los procedimientos de encriptado utilizados podrán evolucionar en función de las normas

y que algunas realizaciones de la presente invención se aprovechan de los dispositivos de seguridad ya en uso en las tarjetas seguras.

Los sistemas de inicialización y de transacción segura en línea utilizan, de una manera conocida de por sí, al menos una red (RC) de comunicación. Por ejemplo, esta red puede ser de tipo Internet. En diversas alternativas, la invención puede utilizar varias redes. Además, las redes implicadas pueden ser de varios tipos, como por ejemplo una red de telefonía móvil (como por ejemplo las redes de tercera generación) que permiten una comunicación de banda ancha con terminales tales como, por ejemplo, teléfonos móviles u ordenadores provistos de medios de comunicación adaptados, etc. Más habitualmente, puede ser una red de tipo Internet, por ejemplo, alámbrica.

También de manera conocida de por sí, las transacciones en línea se realizan generalmente a partir de un terminal (3), tal como un ordenador, por ejemplo, pero se pueden realizar desde otros tipos de terminales, tales como los teléfonos móviles que contienen medios de comunicación y al menos una aplicación de navegación en la red, conocida con el nombre de navegador (o "browser", según la terminología en inglés). Cabe señalar que dicho terminal se designa aquí como "terminal de usuario", pero es evidente que dicho terminal puede ser propiedad de cualquier entidad, que puede corresponder a diversos tipos de terminales y que esta designación no debe interpretarse de manera limitativa. En general, es evidente que la navegación en una red de tipo internet se puede realizar desde diversos tipos de terminales y la invención no debe limitarse a los ejemplos no limitativos dados aquí con fines ilustrativos. En cambio, la presente invención que requiere el uso de un lector (1) de tarjeta segura, es necesario que el terminal (3) pueda bien contener dicho lector directamente en el terminal o bien estar conectado a ese lector por medio de al menos un conector adaptado (por ejemplo, mini-USB, como se encuentra con frecuencia incluso en terminales móviles) y controladores ("drivers" según la terminología en inglés) que permiten el control de un lector de ese tipo, siendo los detalles relativos al diálogo entre el terminal y el lector, en función de las transmisiones de datos en la red (a través del navegador) proporcionados más adelante en la presente descripción. En el presente documento no se darán detalles de la disposición física de los terminales y de los lectores (ni de los controladores ni de otros medios utilizados), ya que el especialista entenderá de la lectura de la invención las disposiciones que son posibles sin apartarse del espíritu de la invención. Además, la invención prevé también realizaciones que permiten prescindir de un terminal (3) en el que se debe conectar el lector (1). En estas realizaciones, el lector (1) será provisto de medios de comunicación en al menos una red (RC) de comunicación. Este lector (1), denominado "comunicante" puede, en algunas alternativas, incorporar al menos una aplicación que permita navegar por la red de comunicación, para permitir al usuario conectarse al menos al equipo (4) proveedor. Las versiones mejoradas permitirán la conexión a otros servidores (por ejemplo, sitios de compras, etc.). En otras alternativas, el lector (1) no dispondrá de un navegador (en su definición común de software de navegación) pero será configurado para poder conectarse directamente al equipo (4) proveedor, por ejemplo, a través de medios de comunicación (por ejemplo, de medios de comunicación inalámbricos como una red de telefonía móvil) y a través de medios de memorización que almacenan los datos que le permiten conectarse a ese equipo. Tales datos pueden contener, por ejemplo, al menos una URL ("Universal Resourdes Locator", en inglés) que indica la dirección de al menos un servidor del equipo (4) proveedor, posiblemente con un nombre de usuario y una contraseña. Estos datos pueden, por ejemplo, ser almacenados en los medios de memorización del propio lector (1) o en el chip (20) de la tarjeta (2) segura (y extraídos por el lector para la comunicación con el proveedor). Por consiguiente, el especialista entenderá de la lectura de la presente solicitud que la invención puede, de hecho, utilizar un dispositivo tal como un lector de tarjeta segura que se puede conectar a un terminal comunicante o formar el mismo dicho terminal comunicante y que, en el caso de que el propio lector forme un terminal comunicante, el navegador y el módulo de puerta de enlace (descritos más adelante en la presente solicitud) pueden omitirse ya que estos últimos se utilizan, respectivamente, para conectarse al equipo (4) proveedor y controlar la transmisión de los datos del navegador entre el terminal y el lector. Sin embargo, en algunas realizaciones, el navegador y el módulo de puerta de enlace pueden implantarse a pesar de todo en este tipo de lector comunicante, para permitir más funcionalidades (especialmente en el caso en el que el navegador sea un verdadero software de navegación que requiera la integración de un módulo de puerta de enlace como se ha descrito en la presente solicitud).

Por otra parte, también se sabe que las transacciones en línea utilizan al menos un equipo (4) de un proveedor de servicio (por ejemplo, un establecimiento bancario o un organismo privado o público) que comprende al menos un servidor (40) dispuesto para gestionar las comunicaciones, y en particular las transacciones, con los navegadores (N) de los terminales (3). Las transacciones en línea, tales como las dadas como ejemplo ilustrativo y no limitativo, en la presentación del ámbito técnico ("banca electrónica", etc.), requieren generalmente la conexión del usuario (a través del navegador de un terminal o, según las alternativas descritas anteriormente, a través del lector comunicante) con el servidor (40) para permitir una autenticación de usuario y una autorización de la transacción por el servidor (40). Además, el equipo proveedor (4) contiene también, en general, en la técnica anterior al menos un módulo de seguridad (41) que está dispuesto para desencriptar y verificar las firmas de transacciones proporcionadas por las tarjetas (pudiendo este módulo, por ejemplo, ser implantado en al menos un servidor del equipo (4) proveedor). Este módulo de seguridad (41) puede, a modo de ejemplo ilustrativo y no limitativo, contener, por ejemplo, como se conoce en el ámbito bancario, un "entorno criptográfico", que podrá ser, por ejemplo, como los conocidos con el nombre de HSM (para “Hardware Security Module", según la terminología en inglés) que permiten las operaciones de desencriptado de las firmas de las transacciones y de la verificación de esas firmas. En general, un servidor del equipo (4) proveedor podrá, en su caso, almacenar los datos relativos a las transacciones y/o a su encriptado. De manera conocida de por sí, el equipo proveedor (4) puede contener un primer servidor, denominado

frontal (como se muestra en la figura 1) al que se conectan los usuarios para realizar transacciones, y un segundo servidor, denominado servidor (40) de operaciones, que gestiona los inicios de sesión de los usuarios y los intercambios de datos requeridos en función de las transacciones solicitadas (por el usuario o por un servidor de un sitio de compras, por ejemplo), transmitiendo los datos sensibles al módulo de seguridad (41) para el cifrado/descifrado. El especialista comprenderá, por consiguiente, que el equipo proveedor (4) podrá contener al menos un servidor (40) (por ejemplo, un único servidor que cumple las funciones del servidor frontal y del servidor de operaciones) y al menos un módulo (41) de seguridad (por ejemplo, "entorno criptográfico", por ejemplo de tipo HSM), implantado en el mismo servidor o (como se muestra en la figura 1) en al menos un dispositivo diferente.

En algunas realizaciones, el lector (1) y el equipo proveedor (4) están conectados a través, respectivamente, de los medios de comunicación, implantados directamente en el lector o a través de un terminal (3), por ejemplo mediante un navegador (N) y los medios de comunicación de al menos un servidor (40), a través de una comunicación segura según un protocolo de tipo SSL/TLS dentro del cual está abierto el canal (CS) seguro. Se sabe en este ámbito que las conexiones de los usuarios en los servidores de su proveedor (proveedores) de servicio (servicios) (por ejemplo, un establecimiento bancario) se transfieren por conexiones seguras (por ejemplo, según el protocolo https). La presente invención permite el uso de protocolos de seguridad, por ejemplo del tipo SSL/TLS para proteger la sesión de comunicación, pero permite además crear un canal (CS) seguro dentro de esta sesión, para proteger aún más las informaciones sensibles intercambiadas, por ejemplo para permitir resistir principalmente los ataques "hombre en el medio" u "hombre en el navegador". En otras realizaciones, la comunicación con el equipo (4) proveedor podrá hacerse según otros tipos de protocolos, principalmente los protocolos no seguros, ya que el establecimiento del canal (CS) seguro se realiza desde el principio de la comunicación para que ningún dato sensible circule "en abierto" por la red. Por ejemplo, desde que el lector (1) se activa (por ejemplo, cuando se conecta a un terminal comunicante o cuando accede a la tarjeta), se conecta (mediante sus medios de comunicación o los del terminal) con el equipo (4) proveedor a través de la red (RC) de comunicación (por ejemplo, mediante una URL almacenada en los medios de memorización y extraída por el lector) para establecer el canal seguro.

Se comprende, por consiguiente, que los sistemas de inicialización y de transacción segura en línea, a través de al menos una red (RC) de comunicación que contiene al menos un lector (1) de tarjeta (2) segura, que se comunica (por ejemplo, a través de un terminal (3) que contiene medios (30) de procesamiento de datos que ejecutan al menos un navegador (N) dispuesto para comunicarse a través de dicha red (RC), o directamente mediante los medios de comunicación) con al menos un equipo (4) de un proveedor de servicio que comprende al menos un servidor (40) dispuesto para gestionar las transacciones con los lectores (1) o navegadores (N) de terminales (3) de los usuarios, por el intercambio de datos representativos de transacciones, y al menos un módulo de seguridad (41), dispuesto para proteger estas transacciones (en cooperación con el lector).

Más concretamente, los sistemas según la invención están dispuestos para el establecimiento de un canal (CS) seguro entre el lector (1) de la tarjeta (2) segura y el módulo de seguridad (41), por medio de al menos una clave de encriptado (CF) y de los datos (D_chip) representativos de al menos una información asociada a la tarjeta, almacenadas en el chip de la tarjeta segura. Esta clave de encriptado corresponde a un "secreto compartido" por la tarjeta y el equipo (4) proveedor y se utiliza para generar por ambas partes una clave de sesión (Kses) que permite el encriptado de los datos de las transacciones transmitidas a través del canal seguro. De este modo, el módulo de seguridad (41) (o servidor) y el lector (1) utilizan la misma clave de sesión para encriptar/desencriptar los datos que se intercambian para la transacción. Se comprende, por consiguiente, que por estos encriptados/desencriptados efectuados por ambas partes, se establece un canal seguro (CS) entre las dos entidades para permitir que los datos sensibles no puedan ser violados. Estos datos (D_chip) representativos de las informaciones vinculadas a la tarjeta corresponden a los datos "públicos" porque no son sensibles y pueden, por consiguiente, circular sin encriptar por la red. Estos datos (D_chip) públicos se envían al equipo (4) proveedor para que pueda identificar la tarjeta (2) y realizar las mismas operaciones criptográficas que la tarjeta (2) y el lector (1). En el presente documento, mediante la expresión "establecimiento de un canal seguro" se entiende el hecho de que el equipo (4) proveedor (especialmente el módulo (41) de seguridad) y el lector (1) se conectan para calcular una misma clave de sesión (Kses) que utilizan para encriptar/desencriptar los datos de las transacciones intercambiadas más adelante, en tránsito por el canal (CS) seguro. La presente invención se refiere, por consiguiente, a un procedimiento y a un sistema de inicialización de transacciones seguras que se basan en el establecimiento de un canal seguro (CS) para las transacciones. Una vez establecido este canal (CS), la transacción se inicializa y puede ejecutarse a través del canal seguro. La presente invención también se refiere, por consiguiente, a un procedimiento y un sistema de transacciones seguras que se basan en dicha inicialización mediante el establecimiento de un canal seguro (CS). La presente invención propone, por consiguiente, sistemas resistentes a los diversos tipos de ataques conocidos que utilizan, de manera ventajosa, los mecanismos de seguridad ya en uso en las tarjetas seguras, pero aprovechándose de ellas a distancia en relación con el equipo del proveedor de servicio por medio de al menos un canal (CS) seguro que permita garantizar la seguridad de las transacciones, o incluso su total confidencialidad en ciertas realizaciones que se detallan más adelante. En efecto, en lugar de proponer una simple firma de las transacciones por la tarjeta (2) (mediante el lector), realizada al final de la transacción para validar esta última, como en la técnica anterior (particularmente en los sistemas de tipo CAP), se propone inicializar la transacción estableciendo un canal seguro (CS) que se basa en los mismos mecanismos criptográficos, pero cuyo uso se modifica para la aplicación de la presente invención. El uso de estos mecanismos criptográficos se modifica, en particular, debido a que el (los) criptograma (criptogramas) generado (generados) por la tarjeta (2) son utilizados por

el lector (1) para generar una clave de sesión (Kses), por ejemplo, mediante la concatenación de dos criptogramas proporcionados por la tarjeta (2). Por otra parte, el módulo de seguridad está aquí dispuesto para generar también la misma clave sesión (Kses) que luego se utilizará por este último y por el lector para encriptar/desencriptar los datos que deben intercambiarse para la transacción propiamente dicha. En cambio, en la técnica anterior, especialmente en los sistemas CAP, la tarjeta envía simplemente un criptograma al final de la transacción al módulo de seguridad (41) que verifica simplemente si el criptograma es correcto. Además, el uso de estos mecanismos se modifica durante las transacciones pues las operaciones de encriptado/desencriptado se realizan por ambas partes para los envíos de datos a través del canal seguro (CS), tanto desde el servidor al lector como desde el lector al servidor. En la técnica anterior, especialmente en los sistemas CAP, el servidor no encripta los datos a enviar a la tarjeta o al lector. Se comprende, por consiguiente, que el encriptado por el módulo de seguridad de los datos enviados al lector que los desencripta es un uso ventajoso y nuevo de los mecanismos de los que se conoce sólo una parte. Además, el establecimiento del canal seguro se basa en el intercambio de informaciones entre la tarjeta (mediante el lector) y el servidor. Cuando todos los datos relativos a la transacción sólo se introducen, se procesan y/o se visualizan en el lector (y nada en el terminal al que el lector puede estar conectado), la invención permite una total confidencialidad de los datos, además de la seguridad proporcionada por el canal seguro (CS), como se detalla más adelante.

El sistema de inicialización según la invención contiene al menos un lector (1) de tarjeta chip con acceso al equipo (4) proveedor a través de dicha red (RC) de comunicación y que comprende medios (12) de procesamiento dispuestos para, por una parte, intercambiar datos con al menos un chip (20) de al menos una tarjeta (2) segura, con el fin de obtener del chip (20), y transmitir al módulo de seguridad (41), los datos (D_chip), denominados públicos, representativos de al menos una información asociada con la tarjeta (2) y, por otra parte, generar, en cooperación con dicho chip (20), al menos una clave de sesión (Kses), y transmitir al módulo de seguridad (41), los datos encriptados mediante esta clave de sesión (Kses). El módulo de seguridad (41) está dispuesto para calcular dicha clave de sesión (Kses), a partir de dichos datos públicos (D_chip) recibidos y de al menos una clave de encriptado (CF).

Este cálculo de la clave de sesión (Kses) por el lector (1) y el módulo de seguridad (41) que permite la inicialización de la transacción mediante el establecimiento de un canal (CS) para la comunicación segura en el que los datos representativos de la transacción podrán circular en forma encriptada por dicha clave de sesión (Kses).

Para el cálculo de la clave de sesión (Kses) a partir de los datos recibidos, el módulo de seguridad (41) puede realizar los mismos cálculos que el lector (1) y la tarjeta (2). Por ejemplo, el lector puede generar la clave de sesión a partir de al menos un criptograma (ARQC, AAC) generado por el chip (20) de la tarjeta (2), como se detalla en la presente solicitud, y el módulo de seguridad (41) puede también generar al menos un criptograma (ARQC, AAC), y después calcular la clave de sesión (Kses) a partir de este (estos) último (últimos).

El sistema según algunas realizaciones se describirá ahora con referencia a la figura 1. Cabe señalar que las diversas realizaciones descritas en la presente solicitud se pueden combinar entre sí a menos que no se mencione explícitamente lo contrario, o que no sean compatibles entre sí y/o que su combinación no funcione, ya sea por el sistema o por el procedimiento.

El sistema de transacción según la presente invención contiene, por consiguiente, al menos un lector (1) de una tarjeta chip conectado al terminal (3) usuario y que comprende medios (12) de procesamiento dispuestos especialmente para intercambiar datos con una tarjeta (2) segura de un usuario a la que accede el lector (debido a que la tarjeta está insertada en el lector o debido a una lectura a distancia en el caso de tarjetas y lectores denominados "sin contacto"). El lector (1) puede también contener medios (10) de representación visual y medios (11) de entrada (tal como una pantalla y una pluralidad de teclas, o incluso una pantalla táctil), para permitir al usuario verificar las informaciones visualizadas y entrar o validar los datos, según las diversas realizaciones. Los medios (12) de procesamiento del lector (1) están dispuestos también para realizar un procesamiento local de los datos como, por ejemplo, las operaciones de cifrado (encriptado) o descifrado (desencriptado) de los datos representativos de una transacción, por ejemplo en función de los mensajes intercambiados con la tarjeta o con el equipo (4) proveedor. Cabe señalar que la tarjeta (2) con chip (20) se llama "de un usuario" y se sabe en este ámbito que pertenecen exclusivamente a un usuario. Sin embargo, también se sabe que las tarjetas seguras, por ejemplo del tipo EMV, que tienen varios titulares, y esta designación no debe interpretarse, por consiguiente, de manera limitativa sino para sugerir que permite la identificación (completamente fiable en algunos casos) del usuario que hace uso de ella como un usuario autorizado (por la verificación del código PIN, en concreto). Las tarjetas (2) seguras son conocidas de la técnica anterior y contienen al menos un chip (20) que permite firmar las transacciones, en particular una vez realizada la autenticación de su usuario, por validación de un código de identificación personal válido (código PIN, para "Personal Identification Number", según la terminología en inglés). No se darán detalles, por consiguiente, sobre el funcionamiento de estas tarjetas más allá de las etapas más específicas en la implantación de la presente invención.

Los medios (12) de procesamiento del lector (1) de la tarjeta segura están, además, dispuestos para generar, en cooperación con el chip (20) de la tarjeta (2), al menos una clave de sesión (Kses). Para generar una clave de sesión (Kses), el lector (1) obtiene de la tarjeta (2) una serie de datos que se detallan más adelante según diversas realizaciones. En particular, la clave de sesión (Kses) es generada por el lector (1) en cooperación con el chip (20) que almacena al menos una clave de encriptado (CF) y datos (D_chip) públicos. Los medios (12) de procesamiento

del lector (1) pueden, por ejemplo, ejecutar al menos una aplicación específica para la implantación de la invención (principalmente para el establecimiento del canal seguro mediante el encriptado/desencriptado de los datos). En algunas realizaciones, los medios (12) de procesamiento del lector (1) están dispuestos para recibir del módulo de seguridad (41), y procesar al menos una petición de establecimiento (inicialización) del canal (CS) seguro, provocando la consulta del chip (20) por el lector (1) para obtener al menos un criptograma (AAC, ARQC) y los datos (D_chip) representativos de las informaciones asociadas a la tarjeta (2), lo que permite a los medios (12) de procesamiento del lector (1) generar la clave de sesión (Kses) que sirve para establecer el canal (CS) de comunicación seguro y transmitir al módulo de seguridad (41), por una parte, los datos (D_chip) representativos de las informaciones asociadas a la tarjeta (2) y, por otra parte, dichos datos encriptados utilizando esta clave de sesión (Kses). En algunas realizaciones, esta petición de establecimiento del canal puede contener un número impredecible (UN) aumentando la seguridad como se detalla más adelante. En este caso, los datos encriptados por el lector (1) utilizando la clave de sesión (Kses) contendrán los datos relativos a ese número impredecible (UN). Por ejemplo, el lector genera un número de sesión (Nses) que puede, por ejemplo, corresponder a una concatenación de ese número impredecible (UN) con un contador de transacción (conocido con el nombre de ATC en el ámbito de la banca) y puede cifrar este número de sesión (Nses) por la clave de sesión (Kses) para enviarlo al módulo de seguridad (41). Al establecer el canal (CS) seguro, el lector (1) puede solicitar la introducción del código PIN por parte del usuario, con el fin de autentificar a éste último para acondicionar la generación del (de los) criptograma (criptogramas). En respuesta al pedido de establecimiento del canal, el lector envía al equipo (4) proveedor al menos los datos (D_chip) representativos de las informaciones asociadas a la tarjeta (2). Estos datos pueden ser enviados sin encriptado previo por el lector (1), como se mencionó anteriormente. El módulo de seguridad (41) está dispuesto para calcular la clave de sesión (Kses) a partir de al menos una clave de encriptado (CF) y los datos (D_chip) públicos que le son transmitidos por el lector (1), que los ha obtenido ante el chip (20) de la tarjeta (2). Estos intercambios de datos permiten, por consiguiente, la inicialización de la transacción dado que esta clave de sesión (Kses) permite el establecimiento de canal seguro (CS) entre el módulo de seguridad (41) y el lector (1) por medio de encriptados/desencriptados de los datos intercambiados entre estos últimos. Los datos intercambiados para permitir la transacción (por ejemplo, para definir diversos parámetros de la transacción, para validar la transacción, etc.) se encriptan entonces desde el principio (por el lector y el módulo de seguridad) a diferencia de algunas soluciones de la técnica anterior (principalmente CAP) donde solo la validación de la transacción se basa en una firma por la propia tarjeta (2) (y no un encriptado por ambas partes por el módulo de seguridad y el lector).

En algunas realizaciones, el chip (20) de la tarjeta (2) está, de hecho, dispuesto para generar, a partir de la clave de encriptado (CF), al menos un criptograma (AAC, ARQC) utilizado por los medios (12) de procesamiento del lector (1) para generar la clave de sesión (Kses) que sirve para el establecimiento del canal (CS) seguro. El (los) criptograma (criptogramas) generado (generados) por la tarjeta puede (o pueden) ser, por ejemplo, del tipo de los criptogramas conocidos con el nombre de AAC (para “Application Authentication Cryptogram”, según la terminología en inglés) y/o con el nombre de ARQC (para “Authorization ReQuest Cryptogram” según la terminología en inglés) convencionalmente conocidos en este ámbito. En algunas alternativas de realización, el chip puede generar los dos tipos de criptogramas y será su confluencia lo que permita al lector (1) generar la clave de sesión (Kses) (por ejemplo, por una concatenación de dos criptogramas).

En algunas realizaciones, el módulo de seguridad (41) utiliza al menos una clave, denominada clave madre (CM) que se utiliza para la generación de las claves (CF) de las tarjetas (2) seguras proporcionadas por el proveedor de servicio, denominadas claves hijas (CF), siendo cada una de las tarjetas (2) proporcionadas identificables a partir de al menos una información contenida en los datos (D_chip) públicos.

En estas realizaciones, los medios (12) de procesamiento del lector (1) transmiten al módulo de seguridad (41) los datos (D_chip) públicos para que pueda encontrar la clave de encriptado (CF) que se utilizará para calcular la clave de sesión (Kses) y permitir así el encriptado/desencriptado de los datos representativos de la transacción, transmitidos a través del canal (CS) seguro. Según un ejemplo particular, el módulo de seguridad (41) utiliza un algoritmo, por ejemplo, del tipo 3DES, para generar las claves de encriptado (CF) a partir de la clave madre (CM) y de los datos (D_chip) públicos. Dicho algoritmo permite, por consiguiente, al módulo de seguridad (41), por medio de los datos (D_chip) públicos que recibe del lector, encontrar la clave hija a utilizar a partir de la clave madre (CM). Para mayor seguridad, cabe señalar que la clave madre (CM) utilizada por el módulo de seguridad (41), se puede almacenar en forma encriptada por al menos una clave de encriptado, denominada clave secreta (SK). Cabe señalar también que la clave de encriptado (CF) solo está realmente presente de forma furtiva en el módulo de seguridad (41), cuando se calcula la clave de sesión (Kses).

En algunas realizaciones correspondientes a una alternativa a las realizaciones del párrafo anterior, el equipo (4) del proveedor de servicio contiene al menos una base de datos que almacenan las claves de encriptado (CF) de las tarjetas (2) seguras proporcionadas por el proveedor de servicio, accediendo el módulo de seguridad (41) a esta base de datos para encontrar, en función de los datos (D_chip) públicos recibidos del lector (1) de la tarjeta chip, la clave (CF) a utilizar para calcular la clave de sesión (Kses). Para mayor seguridad, cabe señalar aquí que las claves de encriptado (CF) conservadas en el módulo de seguridad (41) pueden ser almacenadas en forma encriptada, por al menos una clave de encriptado, denominada clave secreta (SK).

En algunas realizaciones, los datos (D_chip) representativos de las informaciones vinculadas a la tarjeta (2) pueden ser representativos de al menos una información que permite al menos identificar la tarjeta utilizada para la

transacción. Según diversas realizaciones, estos datos también pueden representar al menos una información relativa a las posiciones (o valores) de los contadores. Estos datos pueden ser, por ejemplo, como los actualmente conocidos en el ámbito de las tarjetas bancarias, que contienen un número de cuenta primaria (PAN, de "Primary Account Number", en inglés) que puede ser utilizado por el módulo de seguridad (41) para encontrar la clave hija (a partir de la clave madre o entre las claves hijas almacenadas, según los 2 ejemplos descritos en los 2 párrafos anteriores). Otros datos utilizables por el módulo de seguridad (41) en la presente invención, para encontrar el (los) criptograma (criptogramas), son datos conocidos con el identificador IAD (para "Issuer Authentication Data" según la terminología en inglés) y que pueden contener los datos representativos de las informaciones conocidas con los acrónimos KDI ("Key Derivation Index", según la terminología en inglés), CVN (para "Cryptogram Version Number", según la terminología de inglés) y CVR (para "Card Verification Result" según la terminología en inglés). Además, estos datos pueden contener también datos conocidos con los nombres ingleses de "Card Risk Management Data Object List 1" (CDOL1), "Card Risk Management Data Object List 2" (CDOL2), "Application Transacción Counter (contador de transacciones de la aplicación" (ATC) y "Primary Account Number Sequence (secuencia del número de cuenta primaria" (PSN). Cabe señalar que los ejemplos de datos representativos de las informaciones asociadas a la tarjeta que se dan aquí no son limitativos y solo representan ejemplos seleccionados, en particular en el ámbito de la banca, para detallar la manera en que el módulo de seguridad (41) puede calcular la clave de sesión que permite el cifrado de los datos que circulan por el canal (CS) seguro.

Cualquiera o todos estos datos (D_chip) de la tarjeta (2) permite al módulo de seguridad (41) calcular la clave de sesión (Kses). Asimismo, según diversas realizaciones, los datos públicos (D_chip) representan al menos una información asociada a la tarjeta y permiten al menos identificar la tarjeta (2). Por ejemplo, el módulo de seguridad (41) puede estar dispuesto para:

- encontrar la clave de encriptado (CF) a utilizar por al menos una parte de estos datos (D_chip), por ejemplo, el PAN de la tarjeta (2) que les transmite el lector (1),
- generar al menos un criptograma (AAC, ARQC) a partir de al menos una parte de estos datos (D_chip) y de la clave de encriptado (CF), por ejemplo mediante la ejecución de al menos una aplicación tal como la utilizada por la tarjeta para generar el (los) criptograma (criptogramas),
- calcular la clave de sesión (Kses) de la misma manera que el lector (1) a partir del (de los) criptograma (criptogramas) (AAC, ARQC), por ejemplo, por medio de una aplicación al menos parcialmente equivalente a la del lector.

En algunas realizaciones, el establecimiento del canal (CS) seguro es iniciado por el equipo (4) proveedor (cuando el lector (1) se haya conectado con este último o cuando una solicitud de transacción es recibida por este último). Por ejemplo, cuando las tarjetas (2) contienen varias aplicaciones para generar los criptogramas (lo que permite aumentar el nivel de seguridad), el equipo (4) proveedor (ya sea el servidor (40) de las operaciones, ya sea el módulo (41) la seguridad) puede enviar un orden de inicialización del canal (CS) seguro al lector (1), especificando al menos una aplicación a utilizar para generar los criptogramas, por medio de al menos un identificador de aplicación (AID, para "Application IDentifier", según la terminología en inglés). Se sabe que los chips (20) de las tarjetas (2) seguras almacenan a veces al menos una lista que da un orden de prioridad a sus aplicaciones. El identificador de la aplicación permite que el chip no utilice las aplicaciones en este orden sino en función de lo que le es indicado por el equipo (4) proveedor. Como alternativa, el equipo (4) proveedor puede almacenar las mismas listas y el identificador de aplicación transmitido puede, por consiguiente, indicar simplemente el número de aplicación en la lista. En otras alternativas más simples, las listas del equipo (4) proveedor permiten prescindir de dicho identificador de aplicación. En otras realizaciones, el canal (CS) seguro se podría iniciar por el lector (1) que transmita al equipo (4) proveedor dicho identificador de aplicación que le es suministrado por la tarjeta (2) cuando genera al menos un criptograma o que habrá utilizado para indicar a la tarjeta qué aplicación utilizar para generar el (los) criptograma (criptogramas). Cabe señalar que los mismos mecanismos para identificar la aplicación se pueden utilizar para informar al lector acerca de la aplicación que se debe utilizar para generar la clave de sesión (en el caso de que contuviera varias aplicaciones para esta función) o para informar al equipo (4) proveedor sobre la aplicación que ha utilizado.

Algunas realizaciones contienen un mecanismo que permite aumentar aún más la seguridad del encriptado. Este mecanismo se basa en un número impredecible (UN) mencionado anteriormente, que es generado por el equipo (4) proveedor (por el servidor (40) de las operaciones o por el módulo (41) de seguridad), al establecer el canal (CS) seguro. Este número impredecible (UN) es transmitido al lector (1) para formar una incertidumbre de la cual se generará la clave de sesión (Kses). Alternativamente, el número impredecible (UN) puede ser generado por la tarjeta (2) o el lector (1), o incluso ser introducido por el usuario en el lector (1) y transmitido al equipo (4) proveedor, pero la seguridad mejora cuando es el servidor quien lo envía al lector. En algunas realizaciones que combinan las realizaciones o las alternativas de las realizaciones anteriores, para poder aumentar aún más el nivel de seguridad, el número impredecible (UN) y el identificador de aplicación se transmiten ambos en el momento del establecimiento (inicialización) del canal (CS) seguro (ya sea a solicitud del lector o del proveedor).

Se comprende, por consiguiente, que en algunas realizaciones particularmente seguras, el lector (1) puede solicitar al chip (20) de la tarjeta generar un primer criptograma (por ejemplo ARQC) especificando un número impredecible (UN). El chip (20) devolverá entonces un primer criptograma, por ejemplo, con un contador de transacción (ATC, por ejemplo) y con datos del tipo IAD (por ejemplo, DKI, CVN y CVR). El lector puede entonces solicitar al chip (20) de la tarjeta generar un segundo criptograma (por ejemplo, AAC) especificando, por ejemplo, el número impredecible (UN) de nuevo. El chip (20) devolverá entonces un segundo criptograma, por ejemplo, con un contador de transacción

(ATC, por ejemplo) y con los datos del tipo IAD (por ejemplo, DKI, CVN y CVR). El lector (1) puede generar entonces la clave de sesión (Kses) concatenando los criptogramas primero y segundo.

Por otra parte, en algunas realizaciones, el lector (1) está dispuesto para generar un número de sesión (Nses). Este número de sesión (Nses) está vinculado al número impredecible (UN) y al contador de transacción (por ejemplo ATC) asociado con un identificador de usuario de la tarjeta (2). Asimismo, el lector (1) genera el número de sesión (Nses) por la combinación del número impredecible (UN) y el contador de transacción (por ejemplo, por medio de una concatenación).

En estas realizaciones, una vez calculada la clave de sesión, el lector puede transmitir el número de sesión (Nses) al equipo (4) proveedor, en forma encriptada por la clave de sesión (Kses). Este número de sesión (Nses) permite a continuación al equipo (4) proveedor identificar el lector (1) con el que las transacciones están en marcha. El servidor (40) de operaciones puede utilizar este número de sesión (Nses) para rastrear las operaciones realizadas. Por ejemplo, el servidor (40) de operaciones puede solicitar encriptados/desencriptados al módulo de seguridad que le indica el número de sesión. Además, el equipo (4) proveedor puede ser dispuesto para generar un número de secuencia (Nseq) asociado a cada transacción e incrementado en cada petición enviada al lector (1). De este modo, se mantiene un registro de cada orden (Nseq) para cada operación (Nses). Los datos que circulan a través del canal seguro pueden, por consiguiente, estar siempre acompañados de un número de sesión (Nses), de un número de secuencia (Nseq) y estar encriptados por la clave de sesión (Kses).

Una vez establecido el canal (CS) seguro, el lector (1) puede dialogar con el equipo (4) proveedor de forma segura y acceder a la tarjeta (2) para obtener diversos tipos de datos. En algunas realizaciones, los medios (12) de procesamiento del lector (1) están dispuestos para recibir al menos un mensaje encriptado que requiere la consulta del chip (20), procedente del equipo proveedor (4), y desencriptar este mensaje utilizando la clave de sesión (Kses), de manera que envíe a la tarjeta (2) al menos una petición de APDU de consulta del chip (20).

En general, el lector está dispuesto para responder a órdenes o peticiones (por ejemplo, a través de estos mensajes encriptados) enviadas por el equipo (4) proveedor (por ejemplo, el servidor (40) de operaciones). Estas peticiones pueden referirse, como ejemplos ilustrativos y no limitativos, a:

- una solicitud de confirmación de la conexión del lector (1) en el terminal (3) y/o una solicitud de identificación del lector (sin necesitar el intercambio con la tarjeta)
- una orden de inicialización del canal seguro,
- una solicitud de representación visual de las informaciones enviadas por el equipo (4) proveedor, para confirmación (validación) por el usuario,
- una solicitud de representación visual de una invitación para la entrada de datos por parte del usuario,
- una solicitud de firma de datos,
- las solicitudes de consulta del chip (petición APDU), por ejemplo, recibidas en forma de mensaje encriptado, desencriptados por el lector que interroga al chip.

En algunas realizaciones, el servidor (40) de operaciones del equipo proveedor (4) está dispuesto para gestionar el establecimiento y la utilización del canal (CS) seguro conservando (almacenando) el número impredecible (UN), el número de secuencia (Nseq) asociado con cada transacción e incrementado en cada petición enviada al lector (1), y el número de sesión (Nses).

En algunas realizaciones, el módulo de seguridad (41) del equipo proveedor (4) está dispuesto para almacenar la clave de sesión (Kses) en los medios de memoria y/o para encriptar la clave de sesión (Kses) utilizando una clave, denominada clave maestra (KM), y transmitirla al servidor (40) para almacenamiento en forma encriptada ($[Kses]_{KM}$) en los medios de memorización. Asimismo, por ejemplo, el servidor (40) de operaciones, encargado de la gestión de las comunicaciones con el usuario (a través del terminal y del lector) conserva la clave de sesión (pero en forma encriptada por la clave del módulo de seguridad para mayor seguridad, ya que el servidor no puede ser tan seguro como el módulo de seguridad) y la reenvía al módulo de seguridad a cada solicitud de encriptado/desencriptado. Los intercambios con el usuario no tienen entonces que ser seguidos por el módulo de seguridad que simplemente realiza las operaciones de encriptado/desencriptado en respuesta a las solicitudes del servidor (40) de operaciones que gestiona las otras operaciones, principalmente identificando la transacción en marcha con el número de sesión (Nses) y la petición en marcha con el número de secuencia (Nseq).

El equipo (4) proveedor, principalmente el servidor (40) de operaciones está dispuesto, por consiguiente, para recoger estos datos (D_chip) representativos de las informaciones vinculadas a la tarjeta (2) y, en algunas realizaciones, para conservar los elementos siguientes asociados con la operación (al menos el tiempo de la operación):

- el criptograma ($[Kses]_{KM}$) de la clave de sesión (Kses), devuelto por el módulo de seguridad (41),
- el n.º de sesión (Nses), que puede, por ejemplo, estar constituido por 4 octetos del UN y 2 octetos del ATC asociado con el identificador del titular,
- n.º de secuencia (Nseq) durante una sesión (operación), por ejemplo, constituida por 2 octetos e incrementada en cada petición u orden enviada al lector (1).

Además, el servidor (40) de operaciones puede estar dispuesto para verificar la consistencia de la información

controlando que un número de sesión correcto (en comparación con el n.º conservado) esté presente cuando el descifrado de los datos recibidos del lector (1), y para verificar que el número de secuencia (Nseq) esté estrictamente creciendo en una sesión. Por último, también puede estar dispuesto para verificar en los datos (D_chip) que se ha completado la autenticación del titular (PIN).

Los datos sobre la transacción se pueden almacenar también, especialmente para prever los casos de oposición, aunque la validación de las transacciones realizadas por el usuario autentificado por su código pueda hacer que las transacciones no sean rechazables.

En algunas realizaciones en las que la invención utiliza un navegador (software de navegación ejecutado por los medios de procesamiento del terminal (3) de usuario o del lector (1) directamente), la invención prevé un módulo de puerta de enlace (ME) que permite transmitir los datos recibidos desde el equipo (4) proveedor al lector (1). De hecho, los navegadores (N) conocidos no permiten, en la actualidad, transmitir los datos recibidos a través de una red de comunicación hacia un lector de tarjetas. En el caso de un navegador ejecutado por los medios (30) de procesamiento de un terminal (3) de usuario, se necesitará al menos un módulo (ME) de puerta de enlace ejecutado por esos medios (30) de procesamiento. En el caso de un lector de comunicación mencionado anteriormente, este módulo, opcionalmente, se puede omitir. Este módulo de puerta de enlace está dispuesto para controlar los intercambios de los datos que circulan por el canal (CS) seguro entre el módulo de seguridad (41) y el lector (1), transmitiendo al lector (1) los datos recibidos del equipo proveedor (principalmente el servidor (40) de operaciones) por el navegador (N). En algunas realizaciones, este módulo de puerta de enlace (ME) puede ejecutarse dentro del entorno de software proporcionado por el navegador. Por ejemplo, este módulo de puerta de enlace puede ser un módulo de extensión ("plug-in (enchufable)", según la terminología en inglés) del navegador (N). Se puede implantar en forma de una aplicación, por ejemplo de tipo JAVA®. La invención puede, por consiguiente, prever diversos tipos de implantación, tal como los módulos enchufables, o de código descargable o en el futuro, los navegadores pueden contener una función de este tipo. Alternativamente, también es posible que el lector y/o la tarjeta almacene (almacenen) los datos que permiten la instalación en el terminal de este módulo. De este modo, el terminal (3) de usuario, en el momento de la conexión del lector o/y cuando el lector acceda a la tarjeta, pueda encontrarse provisto automáticamente del módulo de puerta de enlace permitiendo las transmisiones de datos en el canal seguro.

Por ejemplo, tal módulo (ME) de puerta de enlace puede permitir que el navegador verifique la presencia del lector, confirmando al navegador esta presencia o, en caso de ausencia o respuesta inadecuada, provocando la representación visual de un mensaje que invite al usuario a conectar el lector. En general, el módulo de puerta de enlace será responsable de transmitir al lector las solicitudes recibidas por el navegador, tales como las solicitudes detalladas anteriormente como ejemplos ilustrativos y no limitativos (consulta del chip, validación de los datos, firma de los datos, invitación a la entrada, etc.) y se encargará de transmitir la (o las) respuesta (respuestas) del lector (1) al navegador.

En algunas realizaciones, al menos una parte de los datos representativos de la transacción, transmitidos al servidor (40) del equipo proveedor (4), son introducidos por el usuario en los medios de entrada del terminal (3), a través de las informaciones visualizadas por el navegador (N) en los medios de representación visual del terminal (3). Estas realizaciones no garantizan necesariamente la confidencialidad ya que varios tipos de ataques permitirán violar la confidencialidad, o incluso permiten alterar los datos de entrada. Sin embargo, incluso si los datos de entrada en el navegador son alterados, podrá garantizarse mediante la presente invención la seguridad de las transacciones si el usuario utiliza el lector (1) para introducir, verificar los datos relativos a la transacción y para validar la transacción ya que los datos de la transacción habrán sido encriptados para circular por el canal (CS) seguro sin que puedan ser alterados. La invención podrá prever visualizar a través del navegador un mensaje informando al usuario de la necesidad de verificar y validar las informaciones sobre el lector. En algunas realizaciones que permiten una confidencialidad total de las informaciones y una total seguridad, los datos son introducidos por el usuario en el lector (1). En algunas realizaciones, al menos una parte de los datos representativos de la transacción, transmitidos al servidor (40) del equipo proveedor (4), son introducidos por el usuario en los medios (11) de entrada del lector (1) de la tarjeta chip. Se comprende, por consiguiente, que en algunas alternativas de la invención, la seguridad y la confidencialidad total de las transacciones está garantizada por el hecho de que todos los datos circulan por el canal seguro entre el lector y el equipo proveedor.

En algunas realizaciones, la inicialización de la transacción que sigue a una transmisión al servidor (40) del equipo proveedor (4) de al menos una parte de los datos representativos de la transacción, por un servidor (5) de terceros que gestiona un sitio internet al que se ha conectado el usuario. De ese modo, la inicialización se produce cuando el usuario intenta realizar una transacción. La propia transacción puede pasar entonces por el canal seguro (CS). En algunas realizaciones, al menos parte de los datos representativos de la transacción se transmiten al servidor (40) del equipo proveedor (4) por un servidor (5) de terceros que gestiona un sitio internet en el que el usuario se ha conectado. De la presente descripción se comprende que el usuario puede conectarse al servidor (5) de terceros desde su lector/terminal en el caso en que el lector esté integrado en un terminal comunicante o conectarse al servidor (5) de terceros desde su terminal en el caso de que el lector esté conectado a dicho terminal. La conexión del usuario se hace a través del navegador (N) del terminal (3), para realizar una transacción, seleccionado por los medios de entrada del terminal (3). De ese modo, la invención permite también la compra de artículos en línea. El equipo proveedor (4) que recibe los datos relativos a una transacción del servidor (5) de terceros al que está conectado el navegador (N) puede conectarse con el lector para establecer el canal seguro y que ya no haya datos

sensibles accesible en la red.

La invención se refiere también a un procedimiento de inicialización de transacción segura en línea y a un procedimiento de transacción segura en línea cuya realización se muestra en la figura 2. Estos procedimientos son implantados por los sistemas según la invención. El procedimiento de transacción contiene al menos una etapa de transmisión (91) de datos cifrados, por dicha clave de sesión (Kses) entre el módulo de seguridad (41) y el lector (1), después de un etapa de establecimiento (90) de al menos un canal (CS) de comunicación seguro entre el módulo de seguridad (41) y el lector (1). Esta etapa de establecimiento (90) del canal (CS) seguro se ejecuta por medio de las siguientes etapas previas:

- generación (52) de al menos una clave de sesión (Kses), por los medios (12) de procesamiento del lector (1), en cooperación con la tarjeta (2), después del encriptado de los datos utilizando esta clave de sesión (Kses),
- obtención (53), por el lector (1), a partir del chip (20) de la tarjeta (2), de los datos (D_chip) representativos de las informaciones asociadas a la tarjeta (2),
- transmisión (54), desde el lector (1) al módulo de seguridad (41), de los datos (D_chip) representativos de las informaciones asociadas a la tarjeta (2) y de los datos encriptados utilizando la clave de sesión (Kses),
- generación (55), por el módulo de seguridad (41), de la clave de sesión (Kses) a partir de al menos una clave de encriptado (CF) del módulo de seguridad (41) y de los datos (D_chip) recibidos.

Después de esta etapa de establecimiento (90) del canal (CS) de comunicación seguro, la transacción puede tener lugar en una secuencia determinada (en función del tipo de transacción), de manera completamente segura, por medio de al menos una etapa de transmisión (91) de datos cifrados entre el módulo de seguridad (41) y el lector (1). Se comprende, por consiguiente, que la presente invención presenta la ventaja de proteger los datos transmitidos desde el inicio de la transacción en lugar de sólo proteger la validación de la transacción mediante una firma (criptográfica) como en la técnica anterior. En algunas realizaciones, la etapa de generación (52) de al menos una clave de sesión (Kses), por los medios (12) de procesamiento del lector (1) está precedida por una etapa de generación (51), por el chip (20) de la tarjeta (2), de al menos un criptograma (AAC, ARQC) a partir de la clave de encriptado (CF) almacenada en el chip (20) y de transmisión de este (estos) criptograma (criptogramas) al lector (1) que genera la clave de sesión (Kses) a partir de este (estos) criptograma (criptogramas) (AAC, ARQC).

En algunas realizaciones, el procedimiento contiene al menos una etapa de entrada (50) por el usuario de la tarjeta (2), de al menos un código de identificación personal (PIN) del usuario, y de autenticación de este código por el chip (20) de la tarjeta. Esta etapa de entrada/autenticación (50) puede ser ejecutado en el establecimiento del canal seguro, para que el usuario se autentifique desde el principio y que los intercambios de datos necesarios en la transacción se realicen a través del canal que se haya establecido mediante la autenticación del usuario de la tarjeta. Esta etapa permite, por consiguiente, al menos una etapa de firma (60) de los datos por el chip (20). Por ejemplo, cuando el lector requiere criptogramas del chip para el cálculo de la clave de sesión, el chip efectúa las firmas haciendo al menos un criptograma y el lector genera la clave de sesión, como se mencionó anteriormente. En el caso de una autenticación en el momento de establecer el canal seguro (CS), esta firma (60) para la inicialización de la transacción se distingue de las firmas utilizadas habitualmente en este ámbito, en particular en la CAP, ya que estas firmas clásicas se realizan al final de la transacción para validar esta última (mediante el envío de un criptograma) mientras que la firma de inicialización de estas realizaciones se realiza para el establecimiento del canal, antes de cualquier intercambio de datos, lo que asegura favorablemente la transacción. Sin embargo, la presente invención permite también la ejecución de otra etapa de firma al final de la transacción. Por ejemplo, después de que se haya establecido el canal y una vez que la mayor parte de las etapas necesarias para la transacción hayan tenido lugar a través del canal por el intercambio de datos en forma encriptada, es posible solicitar de nuevo la entrada del código PIN por parte del usuario al final de la transacción, por ejemplo, a través de la representación visual de un resumen de las informaciones de la transacción y de una invitación a introducir el PIN para una firma del tipo utilizado habitualmente en la CAP. En general, el procedimiento puede también contener al menos una etapa de validación por parte del usuario de las informaciones visualizadas y/o introducidas en el lector y que corresponden a los datos representativos de la transacción.

En algunas realizaciones, el procedimiento contiene al menos una etapa de encapsulación/desencapsulación (58) de los datos representativos de la transacción que circulan a través del canal (CS) seguro.

En algunas realizaciones, la etapa de generación (52) de al menos una clave de sesión (Kses), por los medios (12) de procesamiento del lector (1) está precedida por un etapa de generación (51), por el chip (20) de la tarjeta (2), de al menos un criptograma (AAC, ARQC) a partir de la clave de encriptado (CF) almacenada en el chip (20) y de transmisión de este (estos) criptograma (criptogramas) al lector (1) generando la clave de sesión (Kses) a partir de este (estos) criptograma (criptogramas) (AAC, ARQC). Por ejemplo, el lector concatena dos criptogramas diferentes generados.

En algunas realizaciones, el procedimiento contiene al menos una etapa de recepción y procesamiento, por los medios (12) de procesamiento del lector (1), de al menos una petición de inicialización del canal (CS) seguro enviado por el módulo de seguridad (41), que comprende un número impredecible (UN) y provocando la consulta del chip (20) por el lector (1) para obtener al menos un criptograma (AAC, ARQC) y los datos (D_chip) representativos de las informaciones vinculadas a la tarjeta (2), esta etapa que permite la etapa de generación (52) de la clave de sesión (Kses) que sirve para establecer el canal (CS) de comunicación seguro y la transmisión (54) al módulo de

seguridad (41), por una parte, de los datos (D_chip) representativos de las informaciones vinculadas a la tarjeta (2) y, por otra parte, dichos datos encriptados utilizando la clave de sesión (Kses), que contienen los datos relativos al número impredecible (UN).

El procedimiento de transacción segura según la invención contiene las etapas del procedimiento de inicialización y al menos una etapa de transmisión (91) de datos entre el módulo de seguridad (41) y el lector (1), en forma encriptada utilizando dicha clave de sesión (Kses), ejecutada en un sistema de transacción segura según la invención.

En algunas realizaciones, el servidor (40) está dispuesto para requerir del módulo de seguridad (41), en cada etapa de transmisión (91) de datos con el lector (1), de un encriptado/desencriptado por dicha clave de sesión (Kses) de los datos transmitidos, estando el lector (1) dispuesto para encriptar/desencriptar también los datos intercambiados durante la transacción.

De la lectura de la presente solicitud, se entenderá que la etapa (90) de inicialización del canal seguro, por el intercambio de los datos necesarios puede contener también las etapas de transmisión de datos representativos del número impredecible (UN), del identificador de aplicación (AID), del número de sesión (Nses), del número de secuencia (Nseq), etc., mencionados previamente. También se comprende que, una vez terminada la inicialización (90) del canal, el procedimiento puede llevarse a cabo con al menos una iteración de la etapa de transmisión (91) de datos encriptados utilizando la clave de sesión. Cada iteración de esta transmisión (91) está vinculada con al menos una etapa de encriptado/desencriptado (910) de los datos transmitidos. De ese modo, se comprende que la invención se refiere, en primer lugar, a un procedimiento y a un sistema de inicialización de transacción en los que el establecimiento (90), o inicialización, del canal seguro (CS) se lleva a cabo por la ejecución de las etapas descritas anteriormente para permitir que las dos entidades utilicen la misma clave de sesión y que la invención se ocupe también de un procedimiento y un sistema de transacción seguro en los que las transmisiones (91) de los datos representativos de la transacción estén vinculados con al menos una etapa de encriptado/desencriptado (910) de los datos transmitidos por dicha clave de sesión (Kses). Es por el hecho de que los datos estén encriptados por lo que se entiende que circulan por un canal seguro.

En general, se comprende que la invención permite la ejecución de etapas relativas a tales transacciones como, por ejemplo, las transferencias bancarias en línea, los pagos en línea (por ejemplo, de tipo 3D-seguro), las modificaciones del código PIN en línea (haciéndose el envío del nuevo código de entrada en forma encriptada por la clave de sesión a través del canal seguro). Cabe señalar que la presente invención permite, por supuesto, la transmisión de otro tipo de datos que los que se refieren al código PIN ya que el término "transacción" se refiere aquí abarcando cualquier tipo de transmisión de datos. En el caso de un cambio de código PIN de una tarjeta segura, el nuevo código PIN transmitido de forma cifrada a través del canal seguro es descifrado por el módulo (41) de seguridad y puede ser almacenado por el equipo (4) proveedor. En el ámbito bancario, los cambios de código PIN requieren el uso de una petición específica de la tarjeta, conocida con el nombre de "secure messaging (mensajería segura)". La invención puede integrar esta funcionalidad utilizando el envío, por el equipo (4) proveedor que haya recibido el nuevo código PIN elegido por el usuario (entrada en el lector), de tal petición que contenga el nuevo código PIN y que permita el cambio del código PIN por la tarjeta.

Los diversos tipos de transacciones posibles mediante la ejecución del procedimiento podrán llevarse a cabo según varias secuencias, al alcance del especialista. Las figuras 3 y 4 muestran la secuencia de una operación de transferencia, en el ejemplo descrito anteriormente de un equipo (4) proveedor que comprende un primer servidor, denominado frontal, al cual accede el navegador (N) del terminal (3) al que está conectado un lector (1) que accede al chip (20) de la tarjeta (2) y un servidor (40) de operaciones que gestionan todas las operaciones y que preguntan al módulo de seguridad (41) para los encriptados/desencriptados. La figura 3 muestra la secuencia hasta el establecimiento (90) del canal seguro (CS), en un ejemplo de realización adaptado a una operación de transferencia. La figura 4 muestra la continuación de la realización del procedimiento de la figura 3, a partir del establecimiento (90) del canal seguro (CS). La figura 3 muestra, por consiguiente, una realización del procedimiento de inicialización de transacción y la figura 4 muestra, por consiguiente, una realización del procedimiento de transacción. En este ejemplo de las figuras 3 y 4, se considera que la sesión de "banca electrónica" ya está en marcha: el usuario ya ha sido autentificado por un procedimiento establecido por el banco y desea realizar una operación del tipo transferencia bancaria durante su sesión. Su lector está conectado, y su tarjeta insertada. En este ejemplo, el procedimiento para ejecutar dicha operación de transferencia se desarrollará de la forma siguiente:

- Envío (61) por el equipo (4) proveedor (el servidor frontal web, por ejemplo) de una invitación a una entrada de los campos de la operación hacia el terminal (3);
- Entrada (62) de los datos de la operación por el usuario en el terminal (3);
- Envío (63) de los datos de la operación y petición de confirmación del terminal (3) hacia el servidor Frontal Web;

Cabe señalar que la entrada puede hacerse de hecho en el lector (1) en lugar de en el terminal. En este caso, las etapas anteriores serán complementar por las etapas de transmisiones, por medio del módulo de puerta de enlace (ME), los datos entre el terminal y el lector. Cabe señalar también que se han omitido aquí todas las etapas realizados por el módulo de puerta de enlace y que solo se menciona el terminal (3) para mayor claridad y simplicidad. El procedimiento continúa con:

- Envío (64) de los datos de la operación del Frontal Web al servidor (40) de la operación;

- Orden (65) de inicialización del canal seguro, por el servidor de operación hacia el terminal (3);
- Prueba (66) de la presencia del lector por el terminal (3);
- Prueba (67) de la presencia de la tarjeta por el lector (1);
- Orden (68) de inicialización (90) del canal seguro por el terminal (3) hacia el lector (1);
- Intercambio (intercambios) (69) entre el lector y la tarjeta (por las peticiones descritas anteriormente, en particular aquí para una solicitud de introducción del código PIN);
- Entrada (70) del código PIN por parte del usuario, después de una invitación en la representación visual del lector (1);
- Intercambio (intercambios) (71) entre el lector y la tarjeta (por las peticiones descritas anteriormente, en particular para la verificación del código PIN de la tarjeta);
- Generación (52) de la clave de sesión (Kses) por el lector (1) para el establecimiento (90) el canal seguro (CS), por ejemplo, con Generación (51) del criptograma (criptogramas) por la tarjeta (2), Generación de un número de sesión N(ses), y después Encriptado (910) del número de sesión N(ses);
- Obtención (53) de los datos (D_chip) de la tarjeta (2) por el lector (1);
- Transmisión (54) de los datos (D_chip) representativos de las informaciones vinculadas a la tarjeta (2), del lector (1) al módulo de seguridad (41), aquí principalmente por medio de:
    - Envío (72) de los datos (D_chip) de la tarjeta y el número de sesión (Nses) cifrado por la clave de sesión (Kses) por el lector (1) hacia el terminal (3);
    - Envío (73) de los datos (D_chip) de la tarjeta y, en su caso, el número de sesión (Nses) cifrado por la clave de sesión (Kses), por el terminal (3) hacia el servidor (40) de operaciones;
- Orden (74) de creación de la clave de sesión (Kses) a partir de los datos (D_chip) de la tarjeta, por el servidor de operación hacia el módulo de seguridad (41);
- Generación (55), por el módulo de seguridad (41), de la clave de sesión (Kses) a partir de una clave de encriptado (CM) del módulo de seguridad (41) y de los datos (D_chip) recibidos,
- Envío (75) de la clave de sesión (Kses) cifrada por la clave maestra (KM) por el módulo de seguridad (41) hacia el servidor de operación (para el almacenamiento y la reutilización en las etapas siguientes de la transacción, en su caso con el número de sesión y el número de secuencia).

El Canal (CS) seguro se activa entonces (establecimiento (90) mediante las generaciones (52 y 55) de ambas partes. El procedimiento de inicialización se ha completado en esta realización y el procedimiento de transacción puede entonces continuar (figura 4) por:

- Orden (76) de cifrado (910) de los datos de la operación para su representación visual en la pantalla del lector, por el servidor de operación hacia el módulo de seguridad (41),
- Transmisión (91) de los datos de la transacción encriptados utilizando la clave de sesión (Kses) aquí principalmente por medio de:
    - Envío (77) de la cadena cifrada de caracteres por la clave de sesión por el módulo de seguridad (41) hacia el servidor de operación;
    - Orden (78) de solicitud de confirmación de las informaciones cifradas por la clave de sesión por el servidor de operación hacia el terminal (3);
    - Orden (79) de solicitud de confirmación de las informaciones cifradas por la clave de sesión, por el terminal (3) hacia el lector (1);
- Representación visual (80) en el lector (1) de las informaciones cifradas y Validación/Anulación (81) por el usuario en función de las informaciones visualizadas.

Cabe señalar que el procedimiento puede contener varias iteraciones sucesivas de las diversas etapas, incluidas las transmisiones (91) que pueden contener diversas peticiones tales como las descritas anteriormente, especialmente con respecto a la orden (79), la representación visual (80) y la validación/anulación (81): por ejemplo, una iteración para solicitar la validación/anulación de la cuenta a ser cargada, una iteración para solicitar la validación/anulación de la cuenta que se le atribuye, etc. Según diversas alternativas, se podrá de hecho tener una sola orden (79) enviada para varios requerir varias representaciones visuales (80) y validaciones (81) y etapas o varias órdenes para varias etapas de validación/anulación). Cabe señalar también que la encapsulación/desencapsulación (58) no se menciona aquí para simplificar la descripción de la secuencia de las etapas.

El procedimiento de transacción continúa entonces con una transmisión (91) en el otro sentido, aquí, en particular aquí gracias a:

- Envío (82) de las informaciones validadas, firmadas por la tarjeta y después cifradas por el lector (1) con la clave de sesión, hacia el terminal (3);
- Envío (83) de las informaciones validadas, firmadas por la tarjeta y después cifradas por el lector (1) con la clave de sesión, por el terminal (3) hacia el servidor de operación;
- Orden (84) de descifrado de las informaciones validadas, firmadas por la tarjeta y después cifradas con la clave de sesión por el servidor de operación hacia el módulo de seguridad (41);

Para ayudar a conservar un registro de las operaciones, el procedimiento puede continuar con una etapa de envío (85) de las informaciones validadas y de la firma en abierto para el archivo, del módulo de seguridad (41) hacia el servidor (40) de operación. El servidor (40) de operación puede entonces realizar una Operación de reconocimiento, por ejemplo, con el envío (86), al menos al terminal (3), de una confirmación de operación (confirmación de la

transacción realizada).

Al leer este ejemplo ilustrativo anterior y los medios específicos descritos en la presente solicitud, el especialista comprenderá las etapas, especialmente entre las descritas anteriormente, que se pueden ejecutar mediante diversas operaciones como, por ejemplo, transacciones bancarias (pago en línea) o los envíos seguros de datos (por ejemplo, representativos de informaciones sobre la salud del usuario, etc.)

El módulo de seguridad (41) está dispuesto al menos para permitir una iniciación de transacción por medio de al menos una función de inicialización del canal seguro, por ejemplo ejecutada a continuación de una orden de creación del canal (CS) seguro que proviene del servidor (40) de operaciones. Por ejemplo, esta función puede tener, como parámetros de entrada, datos representativos de informaciones vinculadas a la tarjeta (D_chip) para la constitución de la clave de sesión y, como valores de retorno, la clave de sesión (Kses) cifrada por la clave maestra (KM) del módulo de seguridad (41): $[Kses]_{KM}$. Cabe señalar que, según diversas realizaciones, los valores devueltos pueden también contener el número impredecible (UN) y/o el identificador de aplicación (AID) mencionado anteriormente o que el servidor de operaciones pueda generar esta función de inicialización del canal seguro transmitiéndola al lector después de haber añadido allí el número impredecible (UN) y/o el identificador de aplicación (AID).

En algunas realizaciones, el módulo de seguridad (41) está dispuesto también para permitir una transacción segura por medio de al menos una función de cifrado/descifrado (encriptado/desencriptado) por ejemplo ejecutada después de:

- Una orden de encriptado (cifrado), por ejemplo enviada al módulo de seguridad por el servidor (40) de operaciones. Por ejemplo, esta función puede tener en parámetros $[Kses]_{KM}$ la clave de sesión cifrada por la clave maestra del módulo de seguridad, así como los datos a cifrar y, en los valores devueltos, los datos cifrados por la clave de sesión (Kses).
- Una orden de desencriptado (descifrado), por ejemplo enviada al módulo de seguridad por el servidor (40) de operaciones. Por ejemplo, esta función puede tener, en parámetros, la clave de sesión cifrada por la clave maestra del módulo de seguridad ($[Kses]_{KM}$) así como los datos a descifrar y, en valores devueltos, los datos en abierto (descifrados).

Además, dependiendo de las aplicaciones y la arquitectura (del equipo) del proveedor de servicio, la invención puede también incluir otros datos y funciones conocidas por el especialista (clave de transporte, transcifrado...) y que son específicas de cada proveedor de servicio.

La presente invención implica "medios de procesamiento de datos" en varios dispositivos (servidor, terminal, lector, tarjeta, etc.). El especialista comprenderá al leer la presente solicitud que dichos medios de procesamiento de datos se refieren, para la tarjeta segura, el chip que contiene al menos un microprocesador que permite el procesamiento de los datos. Además, el chip permite almacenar diversos tipos de datos, tales como los representativos de informaciones vinculadas a la tarjeta, pero también los datos que permiten la ejecución de la aplicación (aplicaciones) específica (específicas) (para la firma de las transacciones en particular). Por otra parte, el especialista comprenderá que, para los servidores, los terminales y el lector, tales medios pueden contener también al menos un microprocesador, por ejemplo montado sobre una placa madre. En general, los medios de procesamiento de datos pueden contener al menos un circuito electrónico y/o al menos un procesador. Dependiendo de los recursos informáticos necesarios, son posibles varias alternativas al alcance del especialista. Del mismo modo, las diversas tareas y funciones descritas aquí pueden de hecho ser realizadas por varios dispositivos diferentes que cooperan para formar la entidad que se está describiendo (servidor, terminal, etc.). De hecho, es posible, por ejemplo, que varios servidores cooperen para llevar a cabo las tareas necesarias dentro del sistema al que pertenecen, como se explica, por ejemplo, para los servidores del equipo (4) proveedor, y la invención no debe ser limitada a la presencia de un único servidor, por ejemplo. Del mismo modo, el término servidor es particularmente claro para las aplicaciones descritas aquí, pero se entenderá que la invención se puede ejecutar también sustituyendo el equipo proveedor (servidores) por al menos un terminal de un usuario (que contendrá entonces los medios específicos descritos para el equipo proveedor, después de haber configurado con anterioridad la tarjeta y ese terminal para permitir la ejecución de la invención. Además, la invención ejecuta, en diversas realizaciones, las aplicaciones de software y la manera en la que estas aplicaciones se ejecutan debe entenderse que no se limitan a su ejecución en un solo dispositivo, ya que los medios de procesamiento pueden ser distribuidos a través de múltiples dispositivos. De este modo, las aplicaciones descritas aquí pueden también provenir de fuentes dispares (especialmente en el caso del código descargable) y es una interpretación funcional que deberá aplicarse, ya que lo que importa es la ejecución de las funciones descritas aquí.

En particular, la invención ejecuta medios específicos, principalmente en el terminal usuario (módulo de puerta de enlace para el navegador), en el equipo proveedor (al menos el módulo de seguridad y un servidor para los intercambios), en el lector (aplicación específica). La invención puede, por consiguiente, involucrar también a cada uno de esos elementos por separado, con sus medios específicos descritos aquí.

Debe ser evidente para los expertos en la técnica que la presente invención permite realizaciones con otras numerosas formas específicas sin apartarse del ámbito de aplicación de la invención reivindicada. En consecuencia, las presentes realizaciones se deben considerar ilustrativas, pero pueden ser modificadas en el ámbito definido por

el alcance de las reivindicaciones adjuntas, y la invención no debe ser limitada a los detalles dados anteriormente.

REIVINDICACIONES

1. Lector (1) de tarjeta chip para transacciones seguras en línea, a través de al menos una red (RC) de comunicación, por el intercambio de datos representativos de transacciones con al menos un equipo (4) de un proveedor de servicios que comprende al menos un servidor (40) dispuesto para gestionar las transacciones en línea y al menos un módulo de seguridad (41) que asegura estas transacciones en cooperación con el lector (1), caracterizado por que comprende medios (12) de procesamiento que están adaptados para:
- intercambiar, antes de cualquier transacción, los datos con al menos un chip (20) de al menos una tarjeta (2) segura, con el fin de obtener, del chip (20), y transmitir, al módulo de seguridad (41), los datos (D_chip), denominados públicos, representativos de al menos una información vinculada a la tarjeta (2),
- gestionar, antes de cualquier transacción, en cooperación con dicho chip (20), al menos una clave de sesión (Kses), y transmitir al módulo de seguridad (41) los datos encriptadas utilizando esta clave de sesión (Kses), con el fin de que el módulo de seguridad (41) puede calcular dicha clave de sesión (Kses), a partir de dichos datos públicos (D_chip) recibidos y de al menos una clave de encriptado (CF),
- intercambiar los datos representativos de la transacción con el módulo de seguridad (41), en forma encriptada por dicha clave de sesión (Kses), formando de este modo un canal (CS) de comunicación seguro para la transacción.

2. Lector (1) de tarjeta chip según la reivindicación 1, caracterizado por que los medios (12) de procesamiento del lector (1) están adaptados para generar la clave de sesión (Kses) en cooperación con el chip (20) de la tarjeta (2), requiriendo del chip (20) de la tarjeta (2) que genere, a partir de al menos una clave de encriptado (CF) almacenada en el chip (20), al menos un criptograma (AAC, ARQC) utilizado por el lector (1) para generar la clave de sesión (Kses) que sirve para el establecimiento del canal (CS) seguro.

3. Sistema de transacción segura en línea, a través de al menos una red (RC) de comunicación, conteniendo el sistema al menos un equipo (4) de un proveedor de servicio que comprende al menos un servidor (40) dispuesto para gestionar transacciones en línea, por el intercambio de datos representativos de las transacciones con al menos un lector (1) de tarjeta (2) chip, comprendiendo dicho equipo (4) también al menos un módulo de seguridad (41), dispuesto para proteger estas transacciones, caracterizado por que:
- dicho sistema contiene al menos un lector (1) de tarjeta chip según una de las reivindicaciones 1 y 2,
- el módulo de seguridad (41) calcula dicho clave de sesión (Kses), a partir de dichos datos públicos (D_chip) recibidos y de al menos una clave de encriptado (CF),
- el lector (1) y el módulo de seguridad (41) encriptan y desencriptan, por dicha clave de sesión (Kses), los datos representativos de la transacción que se intercambian durante la transacción, formando así un canal (CS) de comunicación seguro para la transacción.

4. Sistema según la reivindicación 3, caracterizado por que:
- el módulo de seguridad (41) utiliza al menos una clave, denominada clave madre (CM) que se utiliza para la generación de las claves (CF) de las tarjetas (2) seguras proporcionadas por el proveedor de servicio, denominadas claves hijas (CF), siendo cada una de las tarjetas (2) proporcionadas identificables a partir de al menos una información contenida en los datos (D_chip) públicos,
- los medios (12) de procesamiento del lector (1) transmiten al módulo de seguridad (41) los datos (D_chip) públicos para que pueda encontrar la clave de encriptado (CF) a utilizar para calcular la clave de sesión (Kses).

5. Sistema según una de las reivindicaciones 3 y 4, caracterizado por que el equipo (4) del proveedor de servicio contiene al menos una base de datos que almacena las claves de encriptado (CF) de las tarjetas (2) seguras proporcionadas por el proveedor de servicio, accediendo el módulo de seguridad (41) a esta base de datos para encontrar, en función de los datos (D_chip) públicos recibidos del lector (1) de tarjeta chip, la clave de encriptado (CF) a utilizar para calcular la clave de sesión (Kses).

6. Sistema según una de las reivindicaciones 3 a 5, caracterizado por que el lector (1) y el equipo proveedor (4) están vinculados a través de una comunicación segura según un protocolo de tipo SSL/TLS dentro del cual se establece el canal (CS) seguro.

7. Sistema según una de las reivindicaciones 3 a 6, caracterizado por que los medios (12) de procesamiento del lector (1) están dispuestos para recibir el módulo de seguridad (41) y tratar al menos una petición de inicialización del canal (CS) seguro que comprende un número impredecible (UN) y que provoca la consulta del chip (20) por el lector (1), para obtener al menos un criptograma (AAC, ARQC) y los datos (D_chip) representativos de las informaciones vinculadas a la tarjeta (2), lo que permite a los medios (12) de procesamiento del lector (1) generar la clave de sesión (Kses) que sirve para establecer el canal (CS) de comunicación seguro y de transmitir al módulo de seguridad (41), por una parte, los datos (D_chip) representativos de las informaciones vinculadas a la tarjeta (2) y, por otra parte, dichos datos encriptados utilizando esta clave de sesión (Kses), que contiene los datos relativos al número impredecible (UN).

8. Sistema según una de las reivindicaciones 3 a 6, caracterizado por que la inicialización de la transacción hecha a continuación de una transmisión al servidor (40) del equipo proveedor (4) de al menos una parte de los datos representativos de la transacción, por un servidor (5) de terceros que gestiona un sitio de Internet al que se ha conectado el usuario.

9. Sistema según una de las reivindicaciones 3 a 8, caracterizado por que el servidor de (40) del equipo proveedor (4) está dispuesto para gestionar el establecimiento y la utilización del canal (CS) seguro procesando y conservando un número impredecible (UN), la clave de sesión (Kses), un número de sesión (Nses) generado en el establecimiento del canal seguro (CS) y que está vinculado al número impredecible (UN) y un contador de transacción de la tarjeta (2), así como un número de secuencia (Nseq) incrementado en cada petición enviada al lector (1), durante cada sesión.

10. Sistema según una de las reivindicaciones 3 a 8, caracterizado por que el módulo de seguridad (41) del equipo proveedor (4) está dispuesto para almacenar la clave de sesión (Kses) en medios de memorización y/o para encriptar la clave de sesión (Kses) utilizando una clave, denominada clave maestra (KM), y transmitirla al servidor (40) para el almacenamiento en forma encriptada en los medios de memorización.

11. Sistema según una de las reivindicaciones 3 a 10, caracterizado por que el servidor (40) está dispuesto para requerir del módulo de seguridad (41), en cada transmisión de datos con el lector (1), un encriptado/desencriptado por dicha clave sesión (Kses) de los datos transmitidos, estando el lector (1) dispuesto para encriptar/desencriptar también los datos intercambiados durante la transacción.

12. Procedimiento de inicialización de transacción segura en línea, a través de al menos una red (RC) de comunicación, ejecutada utilizando al menos un lector según una de las reivindicaciones 1 y 2, caracterizado por que contiene al menos una etapa de establecimiento (90) de al menos un canal (CS) de comunicación segura entre el módulo de seguridad (41) y el lector (1) que se ejecuta mediante los siguientes etapas:
- generación (52) de al menos una clave de sesión (Kses), por los medios (12) de procesamiento del lector (1), en cooperación con la tarjeta (2), y después el encriptado de los datos utilizando esta clave de sesión (Kses)
- obtención (53), por el lector (1), a partir del chip (20) de la tarjeta (2), de los datos (D_chip) representativos de las informaciones vinculadas a la tarjeta (2),
- transmisión (54), del lector (1) al módulo de seguridad (41), de los datos (D_chip) representativos de las informaciones vinculadas a la tarjeta (2) y de los datos encriptados utilizando la clave de sesión (Kses).
- generación (55), por el módulo de seguridad (41), de la clave de sesión (Kses) a partir de al menos una clave de encriptado (CF) del módulo de seguridad (41) y de los datos (D-chip) recibidos.

13. Procedimiento según la reivindicación 12, caracterizado por que la etapa de generación (52) de al menos una clave de sesión (Kses), por los medios (12) de procesamiento del lector (1) está precedida por una etapa de generación (51), por el chip (20) de la tarjeta (2), de al menos un criptograma (AAC, ARQC) a partir de la clave de encriptado (CF) almacenada en el chip (20) y de la transmisión de este (estos) criptograma (criptogramas) al lector (1) que genera la clave de sesión (Kses) a partir de este (estos) criptograma (criptogramas) (AAC, ARQC).

14. Procedimiento según una de las reivindicaciones 12 y 13, caracterizado por que contiene al menos una etapa de entrada (50), por el usuario de la tarjeta (2), de al menos un código de identificación personal (PIN) del usuario, y la autenticación de ese código por el chip (20) de la tarjeta, permitiendo esta etapa de entrada/autenticación (50) al menos una etapa de firma (60) de los datos por el chip (20).

15. Procedimiento según una de las reivindicaciones 12 a 14, caracterizado por que contiene al menos una etapa de recepción y procesamiento, por los medios (12) de procesamiento del lector (1), de al menos una petición de inicialización del canal (CS) seguro enviado por el módulo de seguridad (41) que comprende un número impredecible (UN) y que provoca la consulta del chip (20) por el lector (1), para obtener al menos un criptograma (AAC, ARQC) y los datos (D_chip) representativos de las informaciones vinculadas a la tarjeta (2), permitiendo esta etapa la etapa de generación (52) de la clave de sesión (Kses) que sirve para establecer el canal (CS) seguro de comunicación y la transmisión (54) al módulo de seguridad (41), por una parte, los datos (D_chip) representativos de las informaciones vinculadas a la tarjeta (2) y, por otra parte, dichos datos encriptados utilizando esta clave de sesión (Kses), que contiene los datos relativos al número impredecible (UN).

16. Procedimiento de transacción segura en línea, caracterizado por que contiene las etapas del procedimiento de inicialización según una de las reivindicaciones 12 a 15 y al menos una etapa de transmisión (91) de los datos entre el módulo de seguridad (41) y el lector (1), en forma encriptada utilizando dicha clave de sesión (Kses).

17. Procedimiento según la reivindicación 16, caracterizado por que el servidor (40) está dispuesto para requerir del módulo de seguridad (41), en cada etapa de transmisión (91) de los datos con el lector (1), un encriptado/desencriptado por dicha clave de sesión (Kses) de los datos transmitidos, estando el lector (1) dispuesto para encriptar/desencriptar también los datos intercambiados durante la transacción.

FIGURA 1

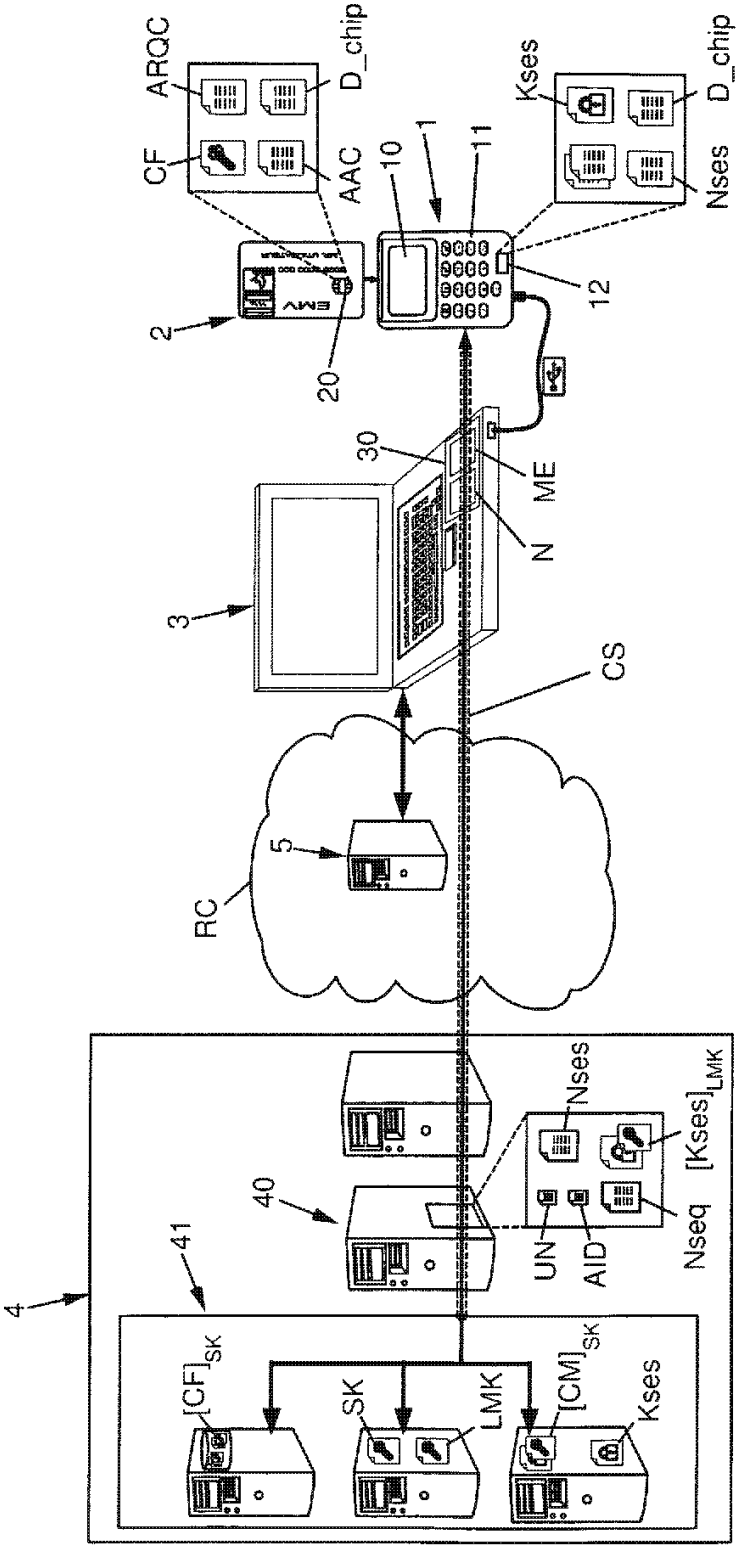

ARQC
D_chip
CF
AAC
Kses
D_chip
Nses
10
1
11
12
2
20
30
ME
N
3
CS
RC
5
4
41
40
Nses
[Kses]LMK
Nseq
UN
AID
[CF]SK
SK
LMK
[CM]SK
Kses

FIGURA 2

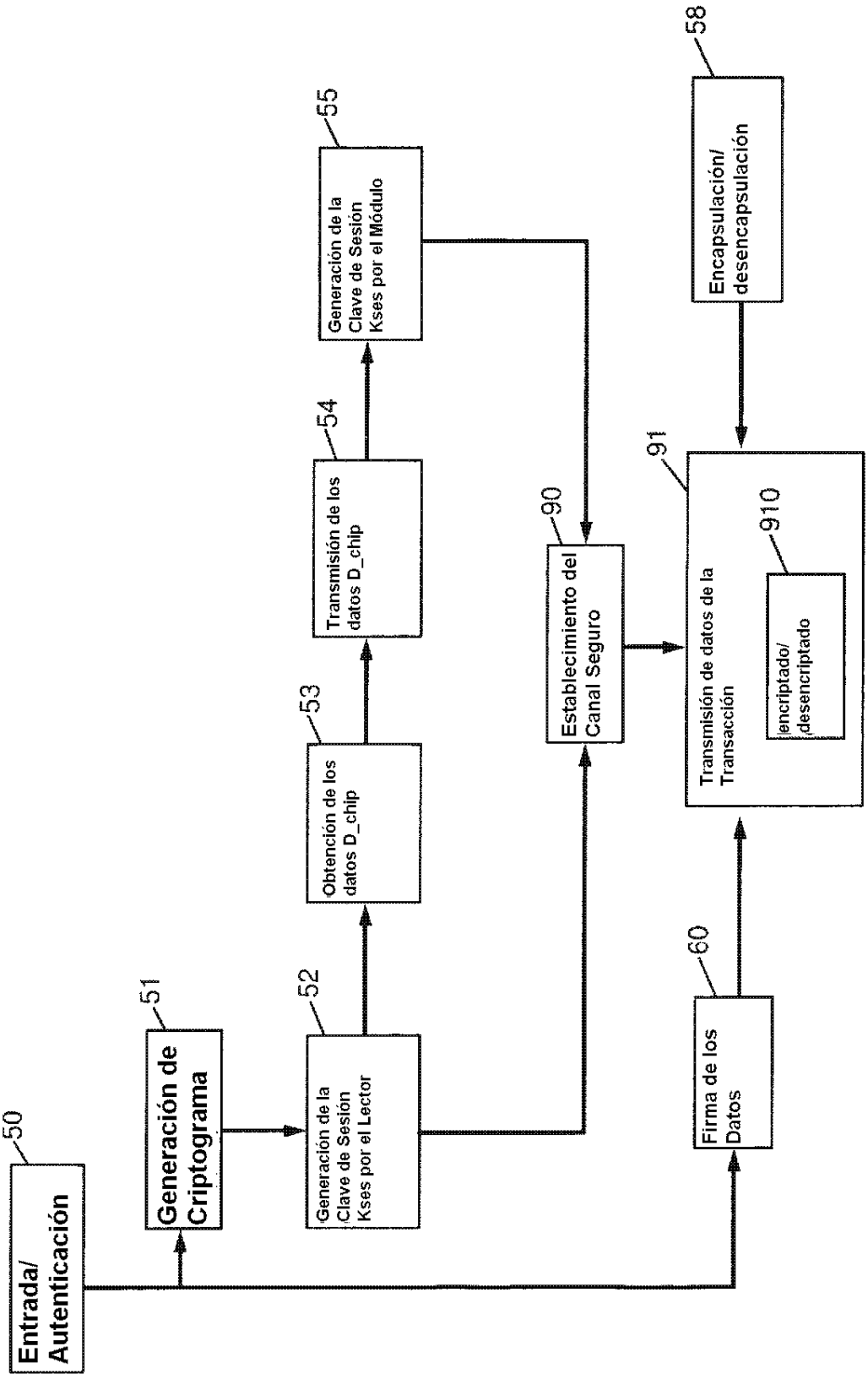

Entrada/ Autenticación
50
Generación de Criptograma
51
Generación de la Clave de Sesión Kses por el Lector
52
Obtención de los datos D_chip
53
Transmisión de los datos D_chip
54
Generación de la Clave de Sesión Kses por el Módulo
55
Establecimiento del Canal Seguro
90
Transmisión de datos de la Transacción
91
encriptado/ desencriptado
910
Encapsulación/ desencapsulación
58
Firma de los Datos
60

FIGURA 3

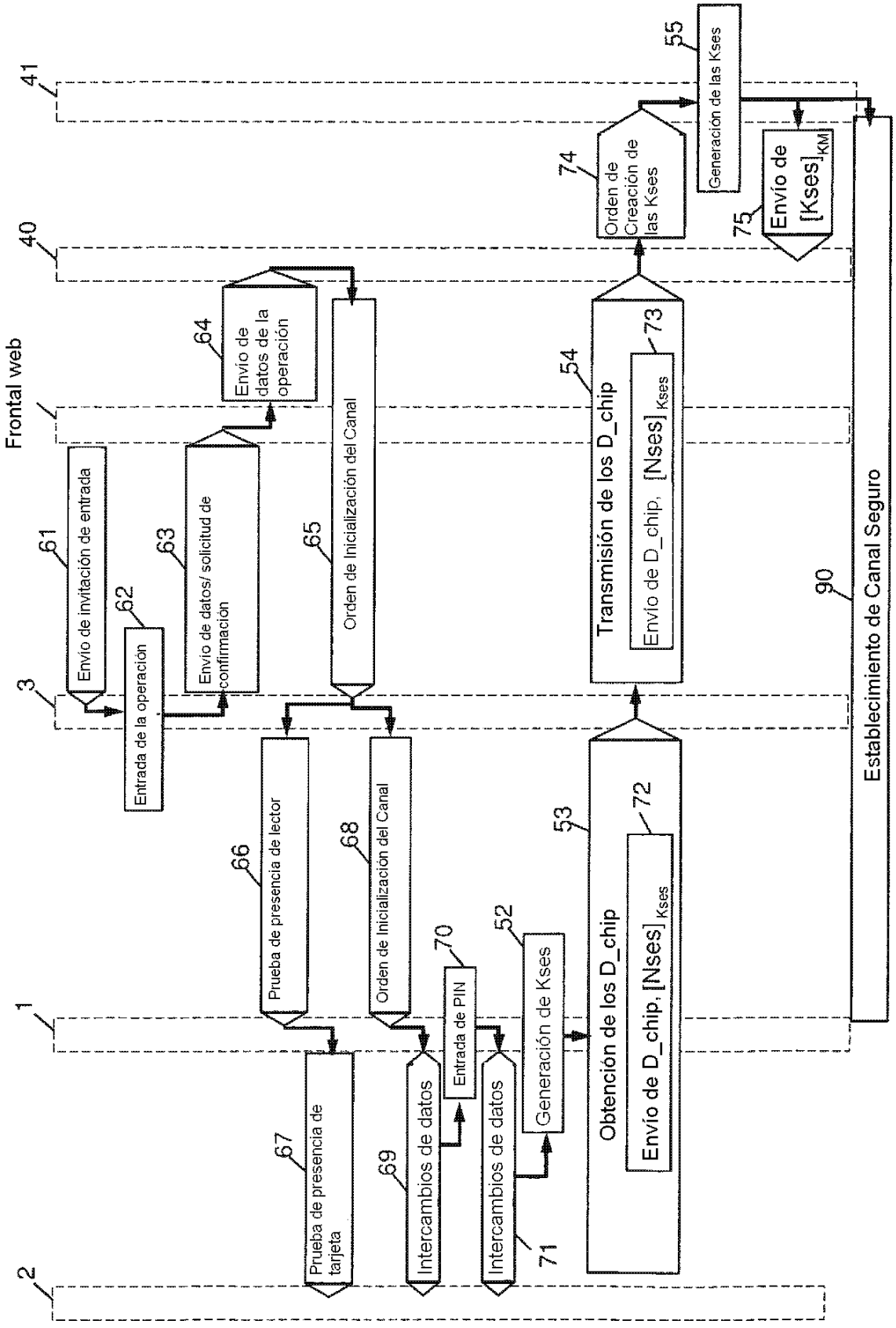
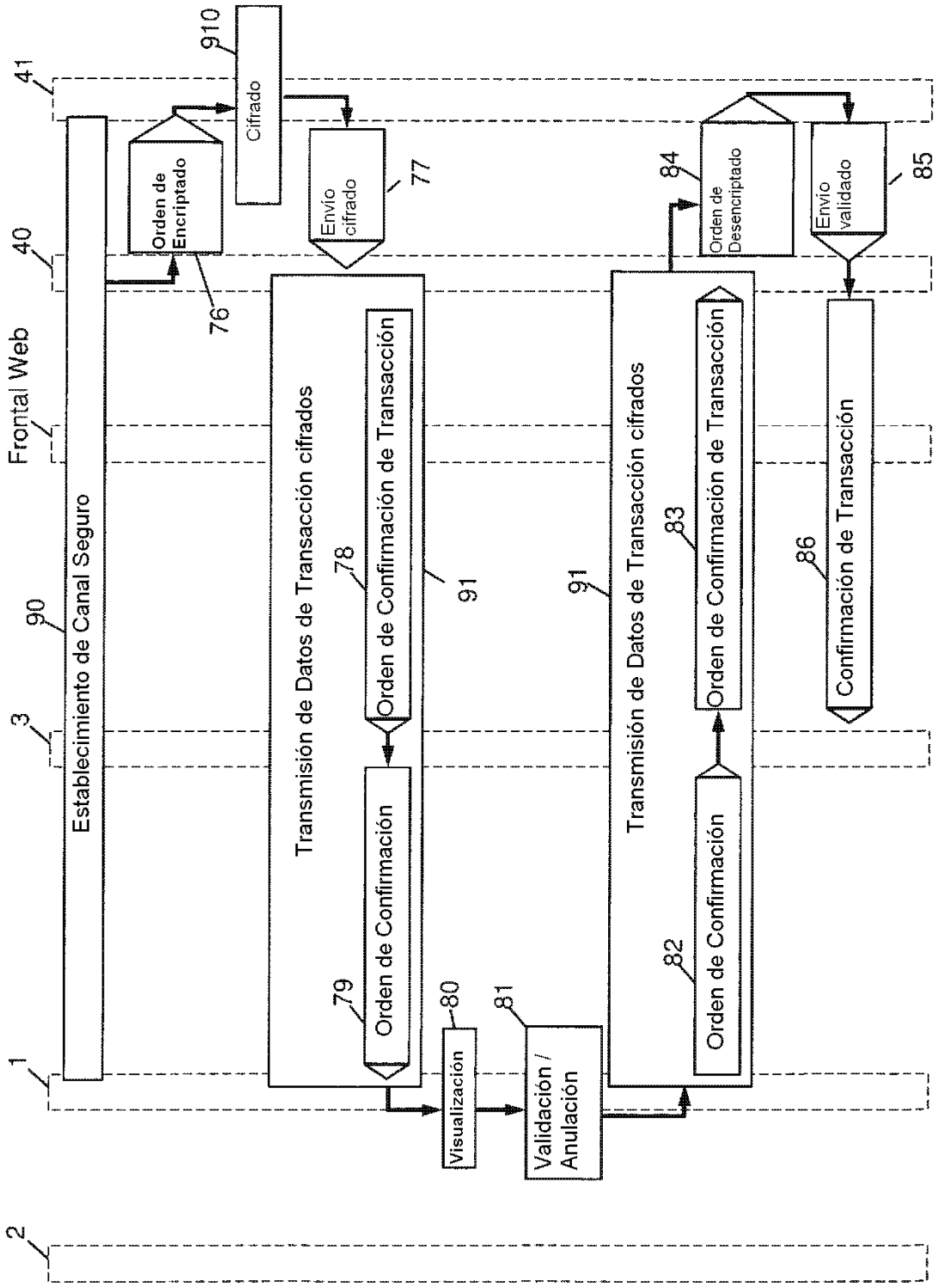

41
40
Frontal web
3
1
2
55
Generación de las Kses
74
Orden de Creación de las Kses
75
Envío de [Kses]KM
64
Envío de datos de la operación
65
Orden de Inicialización del Canal
54
Transmisión de los D_chip
73
Envío de D_chip, [Nses]Kses
61
Envío de invitación de entrada
62
Entrada de la operación
63
Envío de datos/ solicitud de confirmación
90
Establecimiento de Canal Seguro
66
Prueba de presencia de lector
68
Orden de Inicialización del Canal
53
Obtención de los D_chip
72
Envío de D_chip, [Nses]Kses
52
Generación de Kses
70
Entrada de PIN
67
Prueba de presencia de tarjeta
69
Intercambios de datos
71
Intercambios de datos

FIGURA 4


1
2
3
40
41
Frontal Web
Establecimiento de Canal Seguro
90
910
Cifrado
Orden de Encriptado
76
Envío cifrado
77
Transmisión de Datos de Transacción cifrados
78
Orden de Confirmación de Transacción
91
Orden de Confirmación
79
80
Visualización
81
Validación / Anulación
82
Orden de Confirmación de Transacción
83
Transmisión de Datos de Transacción cifrados
91
84
Orden de Desencriptado
Envío validado
85
Confirmación de Transacción
86