(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 690 366**

(51) Int. CI.:

G06F 21/77 (2013.01)
H04L 9/32 (2006.01)
H04L 9/30 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.10.2008 E 13155103 (8)**

(97) Fecha y número de publicación de la concesión europea: **29.08.2018 EP 2595085**

(54) Título: **Procedimiento para proteger una tarjeta de chip frente a un uso no autorizado, tarjeta de chip y terminal de tarjetas de chip**

(30) Prioridad:

29.10.2007 DE 102007000589

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.11.2018

(73) Titular/es:

BUNDESDRUCKEREI GMBH (100.0%)
Oranienstrasse 91
10969 Berlin, DE

(72) Inventor/es:

NGUYEN, KIM y
BYSZIO, FRANK

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento para proteger una tarjeta de chip frente a un uso no autorizado, tarjeta de chip y terminal de tarjetas de chip

La invención se refiere a un procedimiento para la protección de una tarjeta de chip frente a un uso no autorizado, a una tarjeta de chip y a un terminal de tarjetas de chip.

Para la activación de una función de tarjeta de chip puede ser necesaria previamente una identificación del usuario con respecto a la tarjeta de chip, como es conocido en sí por el estado de la técnica. La identificación de usuario más común es la introducción de una identificación secreta, que en general es designada como PIN ("Personal Identificación Number", número de identificación personal) o como CHV ("Card Holder Verification", verificación del titular de la tarjeta). Tales identificaciones se componen en general de una cadena de caracteres numéricos o alfanuméricos. Para la identificación del usuario, la identificación es introducida por el usuario a través del teclado de un terminal de tarjetas de chip o de un ordenador al que está conectado un lector de tarjetas de chip y luego enviada a la tarjeta de chip. Esta compara la identificación introducida con la identificación almacenada y, a continuación, notifica el resultado al terminal o al ordenador mediante la emisión de una señal correspondiente.

En cuanto a los tipos de PIN se puede distinguir entre fijos y variables. Un PIN fijo no puede ser modificado por el usuario y debe ser aprendido de memoria por este. Si se da a conocer, entonces el usuario de la tarjeta debe destruir su tarjeta de chip para evitar el uso indebido por parte de personas no autorizadas, y conseguir una nueva tarjeta de chip con otro PIN fijo. Del mismo modo, el usuario necesita una nueva tarjeta de chip si él o ella ha olvidado el PIN fijo.

Un PIN variable puede ser modificado a discreción por el usuario. Para cambiar el PIN por razones de seguridad siempre es necesario dar el PIN válido en ese momento, ya que de lo contrario un atacante podría sustituir cualquier PIN existente por el suyo propio.

La situación es diferente con los llamados SUPERPIN o PUK ("Personal Unlocking Key", Clave de desbloqueo personal). Por regla general estos tienen más dígitos que el propio PIN, y son utilizados para reiniciar un contador de introducciones erróneas (también denominado "contador de intentos erróneos") que está en su máximo valor. Con el PUK se transfiere inmediatamente también un nuevo PIN a la tarjeta de chip, porque un contador de intentos erróneos reiniciado no vale de nada si se ha olvidado el PIN. Y este es por lo general el caso cuando el contador de intentos erróneos ha alcanzado su valor máximo.

También hay aplicaciones que utilizan PIN provisionales. La tarjeta de chip es personalizada con un PIN aleatorio que recibe el usuario de la tarjeta en una carta de PIN. No obstante, en la primera introducción la tarjeta le requiere sustituir el PIN personalizado por el suyo propio. En un procedimiento similar denominado "procedimiento de PIN sin valor atribuido", a la tarjeta de chip se le reasigna un PIN trivial, como por ejemplo "0000", e igualmente en el primer uso es forzado por la tarjeta de chip a un cambio (véanse en relación a ello también los documentos DE 35 23 237 A1, DE 195 07 043 A1, DE 195 07 044 C2, DE 198 50 307 C2, EP 0 730 253 B1). Por tales procedimientos se tiene una llamada función de primer usuario que proporciona al usuario autorizado la seguridad de que antes de su primer uso no ha tenido lugar ningún uso no autorizado de la tarjeta de chip por un tercero.

Por el documento DE 198 50 307 C2 es conocido un procedimiento para la protección frente a un uso no autorizado de tarjetas de chip. La tarjeta de chip tiene una función de primer usuario, que cuando se utilizan por primera vez los datos y/o las funciones de la tarjeta de chip requiere la especificación de un número secreto (PIN) personal, que puede ser elegido a discreción por el usuario, de modo que por la introducción del número secreto personal los datos y/o las funciones de la tarjeta de chip se ponen en el estado de uso. Una variación posterior del número secreto personal es posible por un código de desbloqueo de orden superior.

Por el estado de la técnica se han dado a conocer también ya procedimientos para la verificación de una identificación en los que no es necesaria la transmisión de la propia identificación, como por ejemplo Strong Password Only Authentication Key Exchange (SPEKE), Diffie-Hellman Encripted Key Exchange (DH-EKE), protocolo Bellovin-Merritt o Password Authenticated Connection Establishment (PACE). El protocolo SPEKE se da a conocer, por ejemplo en www.jablon.org/speke97.html, los documentos US 6.792.533 B2 y US 7.139.917 B2. Entre otros, igualmente por www.jablon.org/speke97.html es conocido el protocolo DH-EKE. Entre otros, por el documento US 5.241.599 es conocido el protocolo Bellovin-Merritt. Por www.heise.de/security/news/meldung/85024 es conocido el protocolo PACE, que es especialmente adecuado para la criptografía de curvas elípticas.

Una visión general sobre los fundamentos del cifrado simétrico se puede obtener por ejemplo del documento "Applied Cryptography" de Bruce Schneier (1996), publicado por John Wiley and Sons.

Además, el documento "Kryptographie und elliptische Kurven" de Christian Hainz (2001-04-01, páginas 2-14) da una visión general sobre el uso de curvas elípticas en la criptografía, por ejemplo en el contexto de un procedimiento de intercambio de claves de Diffie-Hellman.

El documento DE 103 38 643 A1 da a conocer un procedimiento para la identificación segura de objetos, que puede ser empleado por ejemplo para la identificación amigo-enemigo. Para ello son variadas las frecuencias de emisión empleadas para la transmisión de una secuencia de mensajes parciales, siendo fijada la serie de frecuencias empleada por un usuario y comunicada al segundo usuario por una ruta segura.

El documento DE 198 50 308 A1 describe también un procedimiento para la protección de tarjetas de chip frente a uso indebido en aparatos ajenos al sistema. Así, por ejemplo, en el marco de un procedimiento desafío-respuesta es solicitada por la tarjeta de chip una identificación de un terminal y comparada con la identificación que está almacenada en la tarjeta de chip.

Por el documento EP 1 552 484 A0 es conocido un ordenador al que está asociado un módulo de identidad del suscriptor (SIM) como es utilizado en un teléfono móvil GSM. El SIM puede ser autenticado a través de la red telefónica, de la misma manera que los SIM para usuarios de auriculares de teléfono en una red y puede igualmente autenticar a un usuario de un ordenador personal o al propio ordenador personal.

El documento EP 1 909 431 A1 da a conocer un procedimiento que comprende la conexión de un procesador principal (HP2) a un controlador mediante una unidad de conexión (C1) y la transmisión de datos secretos, es decir, de una clave de encriptación pública, a un control, siendo almacenados los datos por el control.

En relación a esto la invención tiene por objeto proporcionar un procedimiento mejorado para la protección de una tarjeta de chip frente a un uso no autorizado. La invención tiene además por objeto proporcionar una tarjeta de chip mejorada y un terminal de tarjetas de chip mejorado.

Los objetos subyacentes a la invención se resuelven, respectivamente, con las características de las reivindicaciones independientes. Formas de realización preferidas se especifican en las reivindicaciones dependientes.

Según la invención se proporciona un procedimiento para la protección de una tarjeta de chip frente a un uso no autorizado. El procedimiento implica, además de la propia tarjeta de chip, un terminal de tarjetas de chip.

Por "terminal de tarjetas de chip" se entiende aquí cualquier aparato que esté realizado para la comunicación con una tarjeta de chip para, por ejemplo dirigir comandos de tarjeta de chip a la tarjeta de chip y recibir respuestas correspondientes de la tarjeta de chip. La comunicación entre la tarjeta de chip y el terminal de tarjetas de chip puede en este caso ser: con contacto, de forma inalámbrica, por ejemplo a través de un procedimiento de RFID, o selectivamente con contacto o de forma inalámbrica, en particular a través de una interfaz llamada de modo dual. En cuanto al terminal de tarjetas de chip puede tratarse de un aparato lector de tarjetas de chip llamado de clase 1, 2 o 3, con o sin un teclado propio o un ordenador al que está conectado un aparato lector de tarjetas de chip. En cuanto al terminal de tarjetas de chip puede tratarse también de un terminal previsto para un determinado propósito, como por ejemplo un terminal de banco para la realización de transacciones bancarias, un terminal de pago, por ejemplo para comprar entradas electrónicas, o un terminal de acceso para liberar el acceso a un área protegida.

Por el término "protección de una tarjeta de chip" se entiende aquí la protección de la tarjeta de chip en conjunto o la protección de una o varias de las funciones de la tarjeta de chip. Por ejemplo, según la invención se protege una función de la tarjeta de chip que merece especialmente la pena ser protegida, como por ejemplo una función de firma para la generación de una firma electrónica, una función de pago, una función de autenticación o similares.

De acuerdo con una forma de realización del procedimiento según la invención, el usuario autorizado recibe del centro emisor de la tarjeta de chip una identificación secreta, que en general es denominada PIN. Para utilizar la tarjeta de chip, en primer lugar se debe introducir una identificación en el terminal de tarjetas de chip, que en lo que sigue es designado por PIN'. Solo cuando el PIN' es idéntico al PIN debe ser posible utilizar la tarjeta de chip o la función de tarjeta de chip protegida.

Para ello el terminal de tarjetas de chip genera un texto cifrado a partir de al menos un primer parámetro de comunicación con ayuda de una primera clave simétrica. En cuanto a la primera clave simétrica puede tratarse del propio PIN' o de una clave simétrica derivada del PIN'. Por ejemplo, el PIN' sirve como un llamado valor semilla (“seed”) para la generación de la primera clave simétrica por el terminal de tarjetas de chip.

El al menos un parámetro de comunicación se proporciona de manera que por él pueda ser definido un primer canal de comunicación protegido entre el terminal de tarjetas de chip y la tarjeta de chip. Para poder formar este primer canal de comunicación protegido entre la tarjeta de chip y el terminal de tarjetas de chip, en primer lugar el texto cifrado del primer parámetro de comunicación, obtenido con ayuda de la primera clave simétrica, es transmitido a través de un canal de comunicación predefinido desde el terminal de tarjetas de chip a la tarjeta de chip. Por tanto, este canal de comunicación predefinido se define de forma estándar para establecer una comunicación inicial entre el terminal de tarjetas de chip y la tarjeta de chip.

Después de la transferencia del texto cifrado a través de este canal de comunicación predefinido desde el terminal de tarjetas de chip a la tarjeta de chip, por parte de la tarjeta de chip es realizado el intento de desencriptar este

texto cifrado con ayuda de una segunda clave simétrica. Esta desencriptación se consigue solo cuando la segunda clave simétrica es igual a la primera clave, es decir, si se satisface la condición PIN' = PIN.

Por tanto, el establecimiento de una conexión de comunicación a través del primer canal de comunicación protegido solo es posible si se satisface la condición PIN' = PIN, ya que la tarjeta de chip solo en este caso tiene conocimiento del primer parámetro de comunicación por el cual puede ser fijado el primer canal de comunicación protegido.

En cuanto al primer parámetro de comunicación puede tratarse, por ejemplo, de la indicación de una frecuencia de transmisión, de un esquema de salto en frecuencia, de un procedimiento de codificación y/o de un procedimiento de modulación.

Si por el contrario no se satisface la condición PIN' = PIN, entonces la primera clave derivada del PIN' no coincide con la segunda clave de la tarjeta de chip. Esto tiene como consecuencia que la desencriptación del texto cifrado recibido del terminal de tarjetas de chip por la tarjeta de chip con ayuda de la segunda clave no produce el primer parámetro de comunicación, sino por ejemplo, un segundo parámetro de comunicación que difiere del primer parámetro de comunicación.

Mediante el segundo parámetro de comunicación puede ser definido un segundo canal de comunicación que es diferente del primer canal de comunicación. Cuando la tarjeta de chip recibe una señal por el primer canal de comunicación, esta, sin embargo, es ignorada ya que la tarjeta de chip espera una señal por el segundo canal de comunicación. Como resultado, no se produce así comunicación entre el terminal de tarjetas de chip y la tarjeta de chip cuando no se cumple la condición PIN' = PIN.

Según una forma de realización de la invención, en cuanto al parámetro de comunicación puede tratarse de una clave pública de un par de claves asimétricas del terminal de tarjetas de chip. Para el establecimiento de una clave simétrica para la comunicación entre el terminal de tarjetas de chip y la tarjeta de chip, por ejemplo de acuerdo con el método de Diffie-Hellman, la clave pública del terminal de tarjetas de chip es desencriptada con la primera clave simétrica obtenida a partir de la primera identificación y enviada a la tarjeta de chip a través del canal de comunicación predefinido.

Solo cuando se satisface la condición PIN' = PIN, la tarjeta de chip recibe la clave pública correcta del terminal de tarjetas de chip. El terminal de tarjetas de chip a partir de la clave pública de la tarjeta de chip, que por ejemplo es consultada de un servidor de claves, genera de acuerdo con el método de Diffie-Hellman la tercera clave, mientras que la tarjeta de chip a partir de su clave privada y del texto cifrado desencriptado con ayuda de la segunda clave simétrica genera una cuarta clave igualmente de acuerdo con el método de Diffie-Hellman, de modo que la cuarta clave solo es igual a la tercera clave, si se cumple la condición PIN' = PIN.

La tercera y la cuarta clave simétrica idénticas sirven para la encriptación de señales, en particular comandos de tarjeta de chip y respuestas a tales comandos de tarjeta de chip que son intercambiados entre el terminal de tarjetas de chip y la tarjeta de chip a través del primer canal de comunicación. Este primer canal de comunicación está definido por lo menos, además, por la tercera clave, con ayuda de la cual es encriptada la comunicación a través del primer canal de comunicación con un método de encriptación simétrica.

De acuerdo con una forma de realización de la invención es utilizado un procedimiento de criptografía de logaritmo discreto (DLC) para la generación de una tercera clave por el terminal de tarjetas de chip y de una cuarta clave por la tarjeta de chip, de modo que la cuarta clave solo es igual a la tercera clave cuando se satisface la condición PIN' = PIN.

Para el establecimiento de la tercera clave pueden utilizarse en principio cualesquiera procedimientos de criptografía de logaritmo discreto como están descritos, por ejemplo, en la norma del Nacional Institute of Standars and Technology (NIST), NIST Special Publication 800-56A, de marzo de 2007, así como en Standards for Efficient Cryptography, SEC1: Elliptic Curve Cryptography, Certicon Research, 20 de septiembre de 2000, versión 1.0. Tales procedimientos requieren la generación de los llamados parámetros de dominio para la generación de la tercera y cuarta clave idénticas por el terminal de tarjetas de chip o la tarjeta de chip.

De acuerdo con una forma de realización de la invención, se emplea como DLC un procedimiento de criptografía de curvas elípticas (ECC), en particular Diffie-Hellman de curvas elípticas (ECDH).

De acuerdo con una forma de realización de la invención, la primera identificación, es decir el PIN' que es introducido en el terminal de tarjetas de chip, es utilizado como un llamado valor semilla para la derivación de la primera clave simétrica. De esta forma es generada una clave de mayor longitud de lo que sería el caso con el uso de la primera identificación directamente como clave.

Según una forma de realización de la invención en la tarjeta de chip es almacenada una segunda identificación, es decir el PIN, a partir del cual puede ser derivada la segunda clave para la desencriptación del texto cifrado recibido inicialmente del terminal de tarjetas de chip. Para la derivación de la segunda clave a partir de la segunda identificación puede ser empleada la segunda identificación como valor semilla.

De acuerdo con una forma de realización de la invención, no es almacenado en la tarjeta de chip el propio PIN, sino solo la segunda clave. La segunda clave está almacenada preferentemente en una zona de memoria no volátil protegida de la tarjeta de chip. Así pues, a diferencia del estado de la técnica no es necesario el almacenamiento del PIN como valor de referencia en la tarjeta de chip.

De acuerdo con una forma de realización de la invención, la tarjeta de chip tiene un contador de intentos erróneos. Si debido a una introducción errónea del PIN' no coinciden el primer y el segundo canal de comunicación, entonces la tarjeta de chip incrementa o disminuye el contador de intentos erróneos con cada mensaje que recibe la tarjeta de chip en otro canal de comunicación que no sea el segundo o el predefinido. Aquellos mensajes que recibe la tarjeta de chip en otro canal de comunicación que no sea el segundo o el predefinido son por lo demás ignorados por la tarjeta de chip. Si el número de intentos erróneos excede de un valor umbral predeterminado, entonces la tarjeta de chip en conjunto o una determinada función de la tarjeta de chip es bloqueada de forma reversible o irreversible.

De acuerdo con una forma de realización de la invención, la tarjeta de chip tiene una función de primer usuario. La tarjeta de chip sin usar se encuentra en su estado de primer uso, en el que está fijado un parámetro de comunicación determinado para una primera elección del primer canal de comunicación. La tarjeta de chip pasa desde su estado de primer uso a un estado de uso cuando por primera vez recibe un comando de tarjeta de chip en este primer canal de comunicación. Para continuar con el uso de la tarjeta de chip debe entonces ser elegido otro parámetro de comunicación por parte del terminal de tarjetas de chip.

En otro aspecto, la invención se refiere a una tarjeta de chip con una interfaz para la comunicación con un terminal de tarjetas de chip a través de un canal de comunicación predefinido, y varios otros canales de comunicación, medios para la desencriptación con ayuda de una segunda clave simétrica de un texto cifrado recibido en el canal predefinido que es encriptado con ayuda de una primera clave simétrica, de modo que de la desencriptación resulta al menos un parámetro de comunicación si una primera identificación introducida previamente en el terminal de tarjetas de chip es correcta, siendo fijado de forma unívoca por el parámetro de comunicación uno de los otros canales de comunicación para la comunicación protegida entre la tarjeta de chip y el terminal de tarjetas de chip.

En otro aspecto la invención se refiere a un terminal de tarjetas de chip con medios para introducir una primera identificación, medios para generar un texto cifrado a partir de al menos un primer parámetro de comunicación con ayuda de una primera clave simétrica derivada de la primera identificación, de modo que con ayuda del parámetro de comunicación puede ser definido un primer canal de comunicación protegido entre el terminal de tarjetas de chip y la tarjeta de chip, y medios para enviar el texto cifrado a la tarjeta de chip a través de un canal de comunicación predefinido.

En otro aspecto la invención se refiere a un procedimiento en el que en cuanto al procedimiento de criptografía de logaritmo discreto se trata de un procedimiento de criptografía de curvas elípticas.

En otro aspecto la invención se refiere a un procedimiento en el que en cuanto al procedimiento de criptografía de logaritmo discreto se trata de un método de Diffie-Hellman de curvas elípticas.

En otro aspecto la invención se refiere a un procedimiento en el que la primera identificación es usada como valor semilla para la derivación de la primera clave simétrica por el terminal de tarjetas de chip.

En otro aspecto la invención se refiere a un procedimiento en el que en la tarjeta de chip está almacenada una segunda identificación (140), de la cual puede ser derivada la segunda clave.

En otro aspecto la invención se refiere a un procedimiento en el que la segunda clave está almacenada en una zona de memoria no volátil protegida de la tarjeta de chip.

En otro aspecto la invención se refiere a un terminal de tarjetas de chip, en el que en cuanto al primer parámetro de comunicación se trata de la indicación de una frecuencia de transmisión, de un esquema de salto en frecuencia, de un procedimiento de codificación y/o de un procedimiento de modulación.

A continuación se explicarán en detalle formas de realización de la invención con referencia a los dibujos. Muestran:

Figura 1, un diagrama de bloques de una primera forma realización de una tarjeta de chip según la invención y de un terminal de tarjetas de chip,

Figura 2, un diagrama de flujo de una forma de realización de un procedimiento según la invención,

Figura 3, un diagrama de bloques de otra forma de realización de una tarjeta de chip según la invención y de un terminal de tarjetas de chip, y

Figura 4, un diagrama de flujo de otra forma de realización de un procedimiento según la invención.

En las siguientes figuras, los elementos correspondientes entre sí de las diferentes formas de realización están caracterizados con los mismos símbolos de referencia.

La figura 1 muestra un diagrama de bloques de un terminal de tarjetas de chip 100. El terminal de tarjetas de chip 100 tiene una interfaz 102 para la comunicación con una tarjeta de chip 104 que tiene una interfaz 106 correspondiente. Preferiblemente, las interfaces 102 y 106 están realizadas para una comunicación inalámbrica, por ejemplo por radio, en particular por un procedimiento RFID.

Las interfaces 102 y 106 están constituidas, por ejemplo, de tal manera que entre las interfaces 102, 106 pueden formarse diferentes canales de comunicación, diferenciándose estos canales de comunicación entre sí en un plano físico y/o lógico. Por ejemplo, pueden formarse canales de comunicación de diferentes frecuencias de transmisión. También pueden formarse canales de comunicación en base a diferentes esquemas de salto de frecuencia. Por "salto de frecuencia" se entienden aquí procedimientos de salto de frecuencia según los cuales las frecuencias utilizadas para la transmisión de datos son modificadas continuamente de acuerdo con un esquema definido.

Las interfaces 102, 106 también pueden estar realizadas de tal manera que puedan ser formados diferentes canales de comunicación con ayuda de diferentes métodos de codificación y/o métodos de modulación, como por ejemplo modulación de frecuencia, modulación de amplitud, modulación de fase, modulación de ancho de impulsos u otros métodos de modulación.

Los diferentes canales de comunicación que pueden ser establecidos entre las interfaces 102 y 106 son designados en lo que sigue como el "conjunto de canales de comunicación".

Uno de los canales de comunicación 108 del conjunto de canales de comunicación está predefinido para la comunicación inicial entre el terminal de tarjetas de chip 100 y la tarjeta de chip 104. Por ejemplo, el canal de comunicación está predefinido con respecto a su frecuencia de transmisión, así como el método de modulación y codificación que se va a emplear.

El canal de comunicación predefinido sirve para la transmisión de un texto cifrado 110 del al menos un parámetro de comunicación K1 desde el terminal de tarjetas de chip 100 a la tarjeta de chip 104 para comunicar a la tarjeta de chip 104, cuál de los canales de comunicación 112 del conjunto de canales de comunicación debe ser empleado para la posterior comunicación con el terminal de tarjetas de chip 100.

Por tanto, el parámetro de comunicación K1 incluye un dato que especifica unívocamente este canal de comunicación 112. Este dato puede tomar la forma de una palabra de código. En la tarjeta de chip 104 puede estar almacenada en una memoria no volátil una llamada tabla de consulta en la que a las posibles palabras de código se les asigna, respectivamente, una especificación de uno de los canales de comunicación del conjunto de canales de comunicación.

Para la selección de un canal de comunicación del conjunto de canales de comunicación pueden ser utilizados todos los posibles canales de comunicación disponibles que se puedan formar entre las interfaces 102, 106 o una selección de los mismos, de modo que entonces a cada uno de los canales de comunicación del conjunto de canales de comunicación, que realmente puede ser usado para la comunicación entre las interfaces 102, 106, se le asigna una palabra de código única que puede ser transmitida como parámetro de comunicación 110 desde el terminal de tarjetas de chip 100 a la tarjeta de chip 104.

El terminal de tarjetas de chip 100 tiene una interfaz de usuario 114, por ejemplo un teclado o una interfaz gráfica de usuario, mediante los cuales puede ser introducida una primera identificación 116. Esta primera identificación se designará en lo que sigue como PIN' sin limitación de la generalidad.

El terminal de tarjetas de chip 100 tiene al menos un procesador 118 para la ejecución de un programa de aplicación 120. El programa de aplicación 120 puede provocar la generación de un comando de tarjeta de chip 122 para invocar una determinada función de tarjeta de chip 124 de la tarjeta de chip 104. Por ejemplo, el programa de aplicación 120 necesita la función de tarjeta de chip 124 para una comprobación de autenticidad, para la generación de una firma digital, para la comprobación de una autorización, en particular de una autorización de acceso, la ejecución de una transacción financiera o similares.

El procesador 118 sirve además para la ejecución de las instrucciones de programa de un módulo de comunicación 126, que sirve para seleccionar el canal de comunicación 112 del conjunto de canales de comunicación y con ello para seleccionar el parámetro de comunicación 110. La selección del parámetro de comunicación 110 puede realizarse de acuerdo con un esquema predeterminado, o aleatoriamente, en particular pseudoaleatoriamente. Por ejemplo, en el módulo de comunicación 126 está almacenada una lista de diferentes parámetros de comunicación 110, que es procesada cíclicamente.

El procesador 118 sirve además para la ejecución de instrucciones de programa 128 para una encriptación simétrica de los parámetros de comunicación 110. La encriptación se realiza con ayuda del PIN'. Para ello, las instrucciones de programa 128 pueden incluir un generador de claves 130.

El generador de claves 130 puede estar realizado de tal manera que a partir del PIN' como valor semilla genere una primera clave simétrica, que es designada en lo que sigue como S1. La clave S1 se utiliza para la encriptación simétrica del parámetro de comunicación K1 seleccionado por el módulo de comunicación 126.

El texto cifrado del parámetro de comunicación K1 que resulta de la encriptación simétrica con la clave S1 es transmitido a través del canal de comunicación predefinido 108 desde la interfaz 102 a la interfaz 106.

La tarjeta de chip 104 tiene un procesador 132 que sirve para la ejecución de las instrucciones de programa de un módulo de comunicación 134. El módulo de comunicación 134 está realizado para el procesamiento del parámetro de comunicación K1 eventualmente recibido del terminal de tarjetas de chip 100. El módulo de comunicación 134 puede acceder, por ejemplo con el parámetro de comunicación K1 como clave, a una tabla de asignación, en particular una tabla de consulta, para buscar los parámetros del canal de comunicación 112 seleccionados por el terminal de tarjetas de chip 100, como por ejemplo su frecuencia de transmisión y/o el método de codificación y modulación que se va a utilizar.

El procesador 132 sirve además para la ejecución de instrucciones de programa 136 para la desencriptación simétrica del texto cifrado 110 que ha recibido la tarjeta de chip 104 del terminal de tarjetas de chip 100. Por ejemplo, la tarjeta de chip 104 tiene una zona de memoria protegida 138, en la que está almacenada una segunda identificación 140. La segunda identificación se denomina de aquí en adelante PIN sin limitación de generalidad. El PIN es comunicado al usuario autorizado de la tarjeta de chip con la entrega de la tarjeta de chip 104 por separado, por ejemplo en forma de una llamada carta de PIN.

Las instrucciones de programa 136 pueden incluir un generador de claves 142, que utiliza el PIN como el llamado valor semilla para derivar a partir de él una segunda clave. Esta segunda clave se designa en lo que sigue por S2.

Alternativamente, la segunda clave S2 puede estar almacenada en la zona de memoria protegida 138 de la tarjeta de chip 104 en lugar del PIN 140. Entonces es innecesario el generador de claves 142, así como un almacenamiento del PIN 140 en la tarjeta de chip 104. En contraste con el estado de la técnica, en la tarjeta de chip 104 no necesariamente tiene que estar almacenado el PIN 140 como valor de referencia para la comprobación de la corrección del PIN' 116.

La tarjeta de chip 104 puede presentar además un contador de intentos erróneos 144. El contador de intentos erróneos 144 está realizado de manera que es contado cada intento erróneo de la tarjeta de chip 104. El número de intentos erróneos es comparado con un valor umbral predeterminado. Cuando se alcanza este valor umbral, al menos la función de tarjeta de chip 124 que está asociada al contador de intentos erróneos 144, es bloqueada de forma reversible o irreversible.

La tarjeta de chip 104 puede presentar además una función de primer uso. Por ejemplo, el estado de primer uso de la tarjeta de chip 104 puede ser definido por un parámetro de comunicación determinado, que especifica uno de los canales de comunicación del conjunto que debe ser empleado para la primera utilización de la tarjeta de chip.

Para usar la tarjeta de chip 104 se procede como sigue: un usuario introduce el PIN' 116 en el terminal de tarjetas de chip 100 a través de la interfaz de usuario 114. Esto puede tener lugar por una demanda correspondiente del programa de aplicación 120. El módulo de comunicación 126 selecciona a continuación un primer parámetro de comunicación de los posibles parámetros de comunicación, por ejemplo de la lista predeterminada de parámetros de comunicación, esto es, el parámetro de comunicación K1.

El generador de claves 130 genera la clave S1 a partir del PIN'. El parámetro de comunicación K1 es encriptado a continuación por la ejecución de las instrucciones de programa 128 con ayuda de la clave simétrica S1. El texto cifrado 110 del parámetro de comunicación K1 que resulta de ello es enviado entonces a través del canal de comunicación predefinido 108 desde la interfaz 102 a la interfaz 106 de la tarjeta de chip 104.

En caso necesario, la tarjeta de chip 104 deriva la clave S2 a partir del PIN o accede directamente a la zona de memoria protegida 138 mediante la clave S2. Con ayuda de la clave S2 se lleva a cabo el intento de una desencriptación del texto cifrado 110 del parámetro de comunicación K1 recibido desde el terminal de tarjetas de chip 100 mediante la ejecución de las instrucciones de programa 136 por la tarjeta de chip 104.

El resultado de este intento de desencriptación es un segundo parámetro de comunicación que es designado en lo que sigue por K2, y que es transferido al módulo de comunicación 134. Este parámetro de comunicación K2 solo es idéntico al parámetro de comunicación K1 si se cumple la condición PIN' = PIN, ya que solo entonces la clave S1, que ha sido utilizada para la encriptación simétrica, puede ser igual a la clave S2 que se utilizó para la desencriptación simétrica del texto cifrado del parámetro de comunicación K1.

A través del parámetro de comunicación K2 puede ser definido un segundo canal de comunicación 146, concretamente de modo que el módulo de comunicación 134 accede con el parámetro de comunicación K2 a su tabla de asignación. Este segundo canal de comunicación 146 es de nuevo idéntico al primer canal de comunicación 112, solo si se cumple la condición PIN' = PIN.

Después de la transferencia del texto cifrado del parámetro de comunicación K1 a través del canal de comunicación predefinido 108, el terminal de tarjetas de chip 100 genera el comando de tarjeta de chip 122 que es enviado a través del primer canal de comunicación 112 desde la interfaz 102 a la interfaz 106. La tarjeta de chip 104 o su módulo de comunicación 134 están ajustados para la recepción en el segundo canal de comunicación 146 debido al parámetro de comunicación K2.

Cuando el segundo canal de comunicación 146 coincide con el primer canal de comunicación 112, entonces el comando de tarjeta de chip 122 es procesado por la tarjeta de chip 104 y es invocada la función de tarjeta de chip 124. Como resultado, la tarjeta de chip 104 genera una respuesta al comando de tarjeta de chip 122 y transmite esta respuesta a través del primer canal de comunicación 112 de vuelta al terminal de tarjetas de chip 100.

Si por el contrario, el segundo canal de comunicación 146 no es idéntico al primer canal de comunicación 112, entonces la tarjeta de chip 104 ignora el comando de tarjeta de chip recibido en el primer canal de comunicación 112 e incrementa el contador de intentos erróneos 144.

Por ejemplo, el canal de comunicación 108 está definido por una frecuencia de transmisión de 9 GHz, el canal de comunicación 112 por una frecuencia de transmisión de 10 GHz y el canal de comunicación 146 por una frecuencia de transmisión de 11 GHz, de modo que las frecuencias de transmisión de los canales de comunicación 112 y 146 difieren entre sí, ya que el PIN' introducido en el terminal de tarjetas de chip 100 no es igual al PIN. Cuando la tarjeta de chip 104 recibe en este caso una señal a la frecuencia de 10 GHz desde el terminal de tarjetas de chip 100, aunque ha esperado una recepción a la frecuencia de 11 GHz, esta señal es ignorada y el contador de intentos erróneos se incrementa. De esta forma se tiene una verificación implícita del PIN' sin que el PIN' tuviera que ser comparado directamente con el PIN, y sin que el PIN deba ser almacenado en la tarjeta de chip.

La figura 2 muestra un diagrama de flujo correspondiente. En la etapa 200 se introduce el PIN' en el terminal de tarjetas de chip. A continuación, en la etapa 202 por el terminal de tarjetas de chip 100 es establecido el parámetro de comunicación K1 para seleccionar uno de los canales de comunicación del conjunto de canales de comunicación. En la etapa 204, el parámetro de comunicación K1 es encriptado simétricamente con ayuda del PIN'. Esto puede realizarse de modo que a partir del PIN' con ayuda de un generador de claves sea derivada la clave simétrica S1, que luego sirve para la encriptación del parámetro de comunicación K1.

En la etapa 206, el texto cifrado del parámetro de comunicación K1 generado con ayuda de la clave S1 es transmitido a través de un canal de comunicación predefinido desde el terminal de tarjetas de chip a la tarjeta de chip.

La tarjeta de chip 104 acomete en la etapa 208, el intento de una desencriptación del parámetro de comunicación K1 basada en el PIN. El PIN correcto puede estar almacenado en una zona de memoria protegida de la tarjeta de chip, y se utiliza para derivar una clave simétrica S2. Alternativamente, también puede estar almacenada directamente la clave S2 en la zona de memoria protegida de la tarjeta de chip.

La desencriptación del texto cifrado del parámetro de comunicación K1 con la clave S2 tiene como resultado un parámetro de comunicación K2. Por este parámetro de comunicación K2 puede ser definido un segundo canal de comunicación del conjunto. Solo si el PIN' es correcto, es decir si se cumple la condición PIN' = PIN, los canales de comunicación especificados por los parámetros de comunicación K1 y K2 son idénticos

En la etapa 210, el terminal de tarjetas de chip genera un comando de tarjeta de chip y envía este a la tarjeta de chip a través del primer canal de comunicación especificado por el parámetro de comunicación K1 (etapa 212). En la etapa 214, la tarjeta de chip solo puede recibir el comando de tarjeta de chip, si el segundo canal de comunicación, al que adaptada la tarjeta de chip para la recepción, es idéntico al primer canal de comunicación, es decir, si se cumple la condición PIN' = PIN. En el caso contrario, la tarjeta de chip ignora el texto cifrado recibido en el primer canal de comunicación e incrementa su contador de intentos erróneos.

En cuanto al parámetro de comunicación K1 puede tratarse en una forma de realización de la invención de una clave pública del terminal de tarjetas de chip. El texto cifrado de esta clave pública, que ha sido generado por encriptación simétrica con ayuda de la clave S1, es transmitido desde el terminal de tarjetas de chip a la tarjeta de chip. La tarjeta de chip recibe solo entonces la clave pública correcta del terminal de tarjetas de chip, cuando a su vez se satisface la condición PIN' = PIN, ya que solo entonces se consigue la desencriptación del texto cifrado con ayuda de la clave S2 (véase la forma de realización de la figura 1). La clave pública de la tarjeta de chip puede ser consultada, por ejemplo, de un servidor de claves externo a través de una red, en particular internet.

A partir de la clave privada del terminal de tarjetas de chip y de la clave pública de la tarjeta de chip, el terminal de tarjetas de chip puede derivar una clave simétrica S3 según el método de Diffie-Hellman. En consecuencia, la tarjeta de chip a partir de la clave pública del terminal de tarjetas de chip y de su clave privada puede derivar igualmente una clave simétrica S4 de acuerdo con el método de Diffie-Hellman. Las claves S3 y S4 son idénticas, si se cumple la condición PIN' = PIN.

En esta forma de realización el primer canal de comunicación (véase el canal de comunicación 112 de la figura 1) es definido al menos de forma complementaria mediante la clave simétrica S3 = S4. El comando de tarjeta de chip

enviado a la tarjeta de chip por el terminal de tarjetas de chip es encriptado concretamente con la clave simétrica S3, y entonces solo puede ser desencriptado, es decir recibido, por la tarjeta de chip, cuando el comando de tarjeta de chip puede ser desencriptado con ayuda de la clave S4. De lo contrario, el comando de tarjeta de chip es ignorado y el contador de intentos erróneos se incrementa.

La figura 3 muestra una forma de realización de una tarjeta de chip según la invención y de un terminal de tarjetas de chip según la invención, en el que se emplea un procedimiento de criptografía de logaritmo discreto para la generación de las claves S3 o S4. Además, en la forma de realización de según la figura 1, el procesador 118 sirve para la ejecución de instrucciones de programa 148, a través de las cuales se tiene un llamado esquema de establecimiento de clave para la generación de la clave simétrica S3.

El esquema de establecimiento de clave trabaja de acuerdo con un procedimiento de criptografía de logaritmo discreto (DLC), en particular de la criptografía de curvas elípticas (ECC), preferiblemente de acuerdo con un método de Diffie-Hellman de curvas elípticas (ECDH). Para generar la clave simétrica S3 las instrucciones de programa 148 producen en primer lugar un primer parámetro de dominio que en adelante se denomina D1.

Además, el módulo de comunicación 126 puede generar un primer parámetro de canal KA1 o leerlo de una lista predeterminada, que por ejemplo especifica las propiedades físicas del primer canal de comunicación. El primer parámetro de canal KA1 corresponde al parámetro de canal K1 en la forma de realización de la figura 1.

Los parámetros de dominio D1 y el o los parámetros de canal KA1 son encriptados con ayuda de la clave S1 por las instrucciones de programa 128. El texto cifrado 110 obtenido a partir de KA1, D1 con ayuda de la clave S1 es transmitido a través del canal de comunicación predefinido 108 desde la interfaz 102 a la interfaz 106.

La tarjeta de chip 104 desencripta el texto cifrado 110 con la ayuda de la clave simétrica S2. Como resultado de la desencriptación, la tarjeta de chip 104 recibe el segundo parámetro de canal KA2, que corresponde al parámetro de comunicación K2 en la forma de realización de la figura 1. Además, la tarjeta de chip recibe el parámetro de dominio D2. El parámetro de canal KA2 es procesado por el módulo de comunicación 134 para determinar, por ejemplo, la especificación física del segundo canal de comunicación 146.

La tarjeta de chip 104 tiene además en la forma de realización de la figura 1 instrucciones de programa 150, que corresponden en su funcionalidad a las instrucciones de programa 148, y por las que por el lado de la tarjeta de chip es implementado el esquema de establecimiento de clave.

Por el lado del terminal de tarjetas de chip mediante la ejecución de las instrucciones de programa 148 a partir de los parámetros de dominio D1 se deriva la clave simétrica S3, que es almacenada en una memoria 152 del terminal de tarjetas de chip 100. Por consiguiente, por la ejecución de las instrucciones de programa 150 por el lado de la tarjeta de chip 104 a partir de los parámetros de dominio D2 es derivada una clave simétrica S4 que es almacenada en una memoria 154 de la tarjeta de chip 104.

El comando de tarjeta de chip 122 es encriptado con la clave simétrica S3 antes de su envío por el terminal de tarjetas de chip y, a continuación es transmitido a través del primer canal de comunicación 112 especificado por el parámetro de canal KA1. La recepción del comando de tarjeta de chip 122 por la tarjeta de chip 104 solo es posible si se tiene tanto KA2 = KA1 como D2 = D1, lo que a su vez solo es posible cuando se cumple la condición PIN' = PIN.

Es particularmente ventajoso en esta forma de realización que la transferencia de los parámetros de dominio D1 a través del canal de comunicación predefinido 108 no pueda ser espiada por un tercero, ya que la transmisión de los parámetros de dominio D1 se realiza en forma encriptada.

La figura 4 muestra un diagrama de flujo correspondiente. En la etapa 400 es introducido un PIN' en el terminal de tarjetas de chip por un usuario. Del PIN' es derivada la clave simétrica S1.

En la etapa 402 se inicia el esquema de establecimiento de clave. A continuación, en la etapa 404 es generado un conjunto de parámetros de dominio D1. Con ayuda de los parámetros de dominio D1 es generada la clave simétrica S3 por el terminal de tarjetas de chip. Además, en la etapa 406 por el terminal de tarjetas de chip el parámetro de canal KA1 es generado o leído de una lista predeterminada.

En la etapa 408, los parámetros de dominio D1 y/o los parámetros de canal KA1 son encriptados con la clave S1. Por ejemplo, los parámetros de dominio D1 y el parámetro de canal KA1 pueden ser concatenados, resultando de ello un único parámetro de comunicación, que a continuación es encriptado con la clave S1. Alternativamente, solo los parámetros de dominio D1 o solo el parámetro de canal KA1 o un subconjunto respectivo de los parámetros de dominio y/o de canal son encriptados con la clave S1. El texto cifrado resultante de la encriptación con la clave S1, así como los parámetros de dominio y/o de canal sin encriptar que quedan eventualmente, son transmitidos en la etapa 410 desde el terminal de tarjetas de chip a la tarjeta de chip a través del canal predefinido (véase el canal de comunicación 108 de las figuras 1 y 3).

En la etapa 412, la tarjeta de chip intenta desencriptar el texto cifrado con ayuda de la clave S2. De esta forma la tarjeta de chip 104 obtiene los parámetros de canal KA2 y los parámetros de dominio D2. A partir de los parámetros de dominio D2 la tarjeta de chip 104 deriva la clave S4.

En la etapa 414, el terminal de tarjetas de chip 100 genera un comando de tarjeta de chip, que es encriptado con la clave S3 (etapa 416) para transmitir este a través del primer canal de comunicación definido por el parámetro de canal KA1 (véase el canal de comunicación 112 en las formas de realización de las figuras 1 y 3). El terminal de tarjetas de chip 100 envía el comando de tarjeta de chip en la etapa 418.

Una recepción correcta de este texto cifrado por la tarjeta de chip en la etapa 420 solo es posible cuando el segundo canal de comunicación 146 coincide con el primer canal de comunicación 112, es decir, cuando KA2 = KA1, y cuando además es posible desencriptar el comando de tarjeta de chip con la clave S4, es decir, cuando S4 = S3. Las condiciones KA2 = KA1 y S4 = S3 solo puede cumplirse si ha sido introducido por el usuario el PIN' correcto en el terminal de tarjetas de chip, es decir, si PIN' = PIN.

Lista de símbolos de referencia

100	terminal de tarjetas de chip
102	interfaz
104	tarjeta de chip
106	interfaz
108	canal de comunicación predefinido
110	parámetro de comunicación
112	primer canal de comunicación
114	interfaz de usuario
116	PIN’
118	procesador
120	programa de aplicación
122	comando de tarjeta de chip
124	función de tarjeta de chip
126	módulo de comunicación
128	instrucciones de programa
130	generador de claves
132	procesador
134	módulo de comunicación
136	instrucciones de programa
138	zona de memoria protegida
140	PIN
142	generador de claves
144	contador de intentos erróneos
146	segundo canal de comunicación
148	instrucciones de programa
150	instrucciones de programa
152	memoria
154	memoria

REIVINDICACIONES

1. Procedimiento para la protección de una tarjeta de chip (104) frente a un uso no autorizado, con las siguientes etapas:

- introducción de una primera identificación (116) en un terminal de tarjetas de chip (100),
- generación de un texto cifrado a partir de al menos un primer parámetro de comunicación (K1; KA1, D1) con ayuda de una primera clave simétrica (S1) derivada de la primera identificación, pudiendo ser definido con ayuda del parámetro de comunicación un primer canal de comunicación protegido (112) entre el terminal de tarjetas de chip y la tarjeta de chip,
- transmisión del texto cifrado a través de un canal de comunicación predefinido (108) desde el terminal de tarjetas de chip a la tarjeta de chip,
- intento de desencriptación del texto cifrado con ayuda de una segunda clave simétrica (S2) por la tarjeta de chip, de modo que entonces el resultado de la desencriptación solo es el primer parámetro de comunicación cuando la primera clave simétrica es igual a la segunda clave simétrica, de modo que el primer canal de comunicación protegido solo puede ser definido entre el terminal de tarjetas de chip y la tarjeta de chip cuando la primera identificación es correcta.

2. Procedimiento según la reivindicación 1, en el que en cuanto al primer parámetro de comunicación se trata de la indicación de una frecuencia de transmisión, de un esquema de salto en frecuencia, de un procedimiento de codificación y/o de un procedimiento de modulación.

3. Procedimiento según la reivindicación 1 o 2, en el que en cuanto al primer parámetro de comunicación se trata de una clave pública del terminal de tarjetas de chip, de modo que en el caso de que la desencriptación del texto cifrado tenga éxito, la tarjeta de chip deriva a partir de la clave pública de acuerdo con el método de Diffie-Hellman (DH) otra clave simétrica (S4) para encriptar la comunicación entre el terminal de tarjetas de chip y la tarjeta de chip, en el que el terminal de tarjetas de chip determina una clave pública de la tarjeta de chip y a partir de la clave pública de la tarjeta de chip deriva otra clave simétrica (S3) para encriptar la comunicación entre el terminal de tarjetas de chip y la tarjeta de chip de acuerdo con el método de Diffie-Hellman (DH), en el que el primer canal de comunicación está definido por la encriptación con las otras claves simétricas (S3, S4).

4. Procedimiento según la reivindicación 1 o 2, en el que en cuanto al primer parámetro de comunicación se trata de un primer parámetro de dominio (D1) para la ejecución de un procedimiento criptográfico de logaritmo discreto para la generación de una tercera clave simétrica (S3) por el terminal de tarjetas de chip y de una cuarta clave simétrica (S4) por la tarjeta de chip, en el que la tercera y cuarta claves simétricas son idénticas cuando la primera identificación es correcta, estando previstas la tercera y la cuarta clave simétrica para la encriptación de la comunicación entre el terminal de tarjetas de chip y la tarjeta de chip a través del primer canal de comunicación protegido.

5. Procedimiento según una de las reivindicaciones anteriores, en el que el resultado de la desencriptación es un segundo parámetro de comunicación (K2; D2, KA2) no correcto cuando la primera identificación no es correcta, en el que un segundo canal de comunicación (146) no correcto puede ser definido por la tarjeta de chip mediante el segundo parámetro de comunicación, con las siguientes etapas adicionales:

- envío de un comando de tarjeta de chip (122) desde el terminal de tarjetas de chip a la tarjeta de chip a través del primer canal de comunicación protegido,
- la tarjeta de chip ignora el comando de tarjeta de chip y se reduce el número de intentos erróneos restantes, de modo que la tarjeta de chip o una función de tarjeta de chip de la tarjeta de chip es bloqueada cuando se sobrepasa un número de intentos erróneos predeterminado.

6. Tarjeta de chip con:

- una interfaz (106) para la comunicación a través de un canal de comunicación predefinido (108) y varios canales de comunicación adicionales (112, 146, ...) con un terminal de tarjetas de chip (100),
- medios (132, 136) para la desencriptación, con ayuda de una segunda clave simétrica (S2), de un texto cifrado recibido en el canal predefinido que está encriptado con ayuda de una primera clave simétrica, de modo que la desencriptación da como resultado al menos un parámetro de comunicación (K2; KA2, D2) si una primera identificación (116) introducida previamente en el terminal de tarjetas de chip es correcta, siendo fijado unívocamente por el parámetro de comunicación uno de los otros canales de comunicación para la comunicación protegida entre la tarjeta de chip y el terminal de tarjetas de chip,
- una función de primer usuario, de modo que en un estado de primer uso está fijado un determinado parámetro de comunicación para una primera elección del primer canal de comunicación, y en el que la tarjeta de chip

pasa de su estado de primer uso a un estado de uso cuando recibe por primera vez un comando de tarjeta de chip (122) en este primer canal de comunicación.

7. Tarjeta de chip según la reivindicación 6, en la que en cuanto al primer parámetro de comunicación se trata de la indicación de una frecuencia de transmisión, de un esquema de salto en frecuencia, de un procedimiento de codificación y/o de un procedimiento de modulación.

8. Tarjeta de chip según la reivindicación 6 o 7, en la que por el primer parámetro de comunicación es indicada una clave pública y con medios (132) para la ejecución de un método de Diffie-Hellman para la derivación de otra clave simétrica (S4) con ayuda de la clave pública.

9. Tarjeta de chip según la reivindicación 6, 7 u 8, con medios (150) para la ejecución de un procedimiento criptográfico de logaritmo discreto para la generación de la otra clave simétrica (S4), en el que la otra clave simétrica está prevista para la encriptación simétrica de la comunicación entre el terminal de tarjetas de chip y la tarjeta de chip a través del canal de comunicación definido (112).

10. Tarjeta de chip según una de las reivindicaciones anteriores 6 a 9, con una zona de memoria no volátil protegida para almacenar una segunda identificación (140) a partir de la cual puede ser derivada la segunda clave.

11. Tarjeta de chip según una de las reivindicaciones anteriores 6 a 10, con una zona de memoria no volátil protegida para el almacenamiento de la segunda clave.

12. Tarjeta de chip según una de las reivindicaciones anteriores 6 a 11, con un contador de intentos erróneos (144) para el bloqueo de la tarjeta de chip si el número de intentos erróneos ha alcanzado un valor umbral predeterminado, en la que un mensaje recibido por la tarjeta de chip que es enviado a la tarjeta de chip por uno de los otros canales de comunicación que no son el canal de comunicación definido, se cuenta como intento erróneo.

13. Tarjeta de chip según una de las reivindicaciones anteriores 6 a 12, en la que se trata de un documento, en particular de un documento de valor o de seguridad, un carnet, unos medios de pago, una tarjeta de firma o similar.

14. Terminal de tarjetas de chip con:

- medios (114) para la introducción de una primera identificación (116),
- medios para la generación de un texto cifrado a partir de al menos un primer parámetro de comunicación (K1; KA1, D1) con ayuda de una primera clave simétrica (S1) derivada de la primera identificación, en el que con ayuda del parámetro de comunicación puede ser definido un primer canal de comunicación protegido (112) entre el terminal de tarjetas de chip y la tarjeta de chip (104),
- medios para el envío del texto cifrado a la tarjeta de chip a través de un canal de comunicación predefinido (108).

15. Terminal de tarjetas de chip según la reivindicación 14, con medios (148) para la generación de parámetros de dominio (D1) para la ejecución de un procedimiento criptográfico de logaritmo discreto para derivar una clave simétrica adicional (S3) para la encriptación de la comunicación entre el terminal de tarjetas de chip y la tarjeta de chip, de modo que el primer parámetro de comunicación indica los parámetros de dominio.

Fig. 1

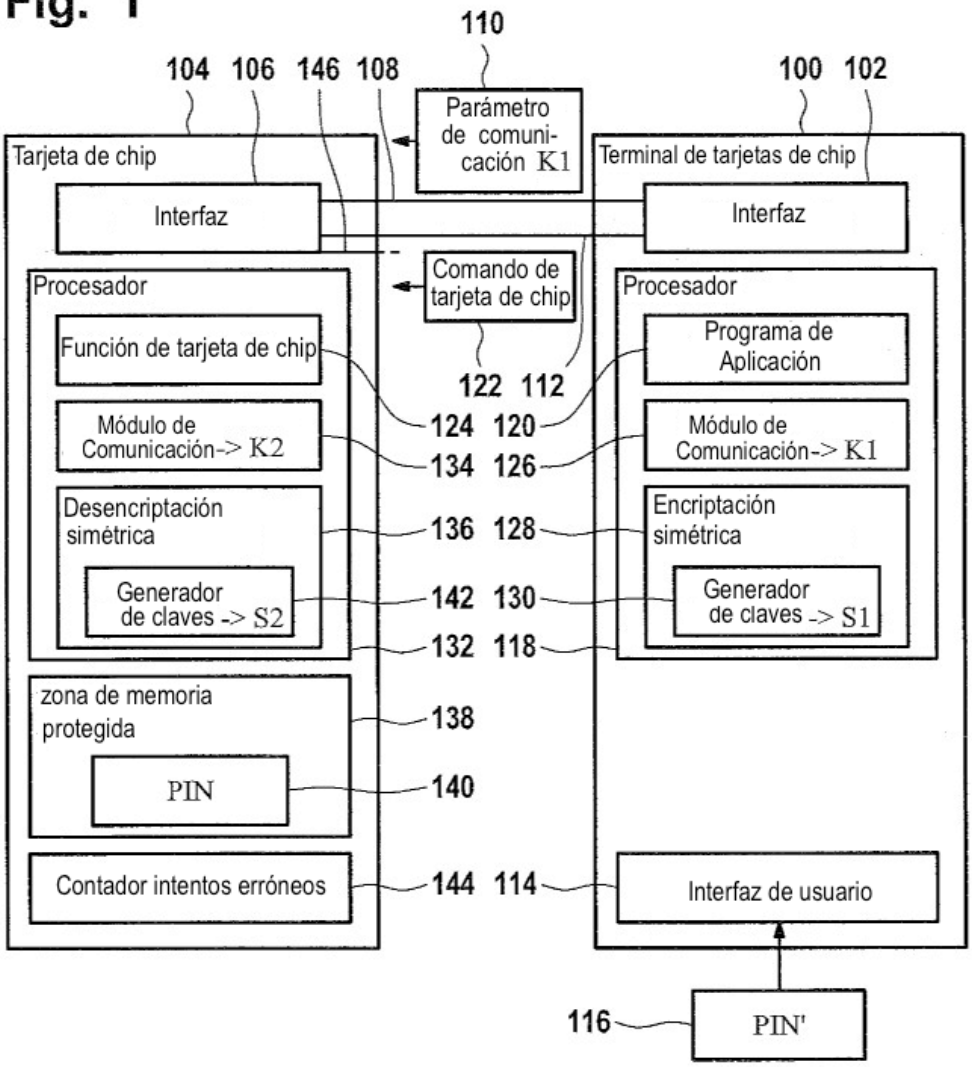

110
104 106 146 108
100 102
Parámetro de comunicación K1
Tarjeta de chip
Terminal de tarjetas de chip
Interfaz
Interfaz
Comando de tarjeta de chip
Procesador
Procesador
Función de tarjeta de chip
Programa de Aplicación
122 112
Módulo de Comunicación-> K2
Módulo de Comunicación-> K1
124 120
134 126
Desencriptación simétrica
Encriptación simétrica
136 128
Generador de claves -> S2
Generador de claves -> S1
142 130
132 118
zona de memoria protegida
138
PIN
140
Contador intentos erróneos
144 114
Interfaz de usuario
116
PIN'

Fig. 2

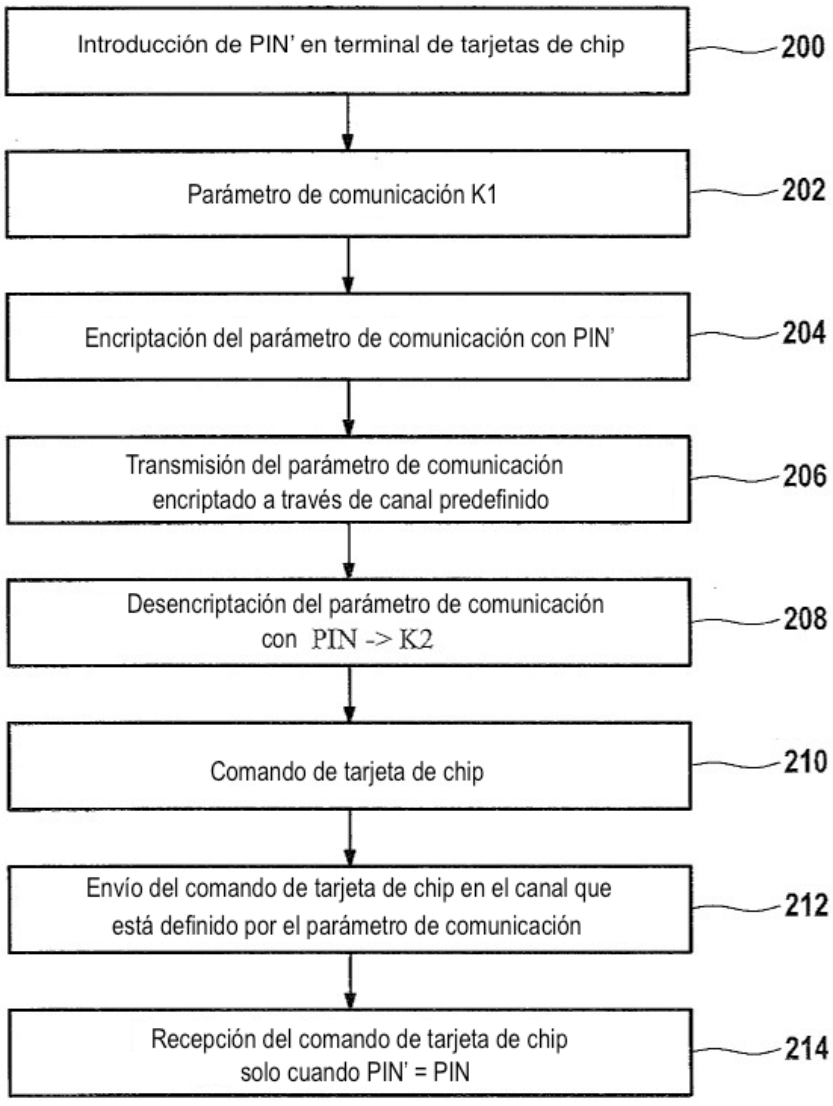

Introducción de PIN' en terminal de tarjetas de chip
200
Parámetro de comunicación K1
202
Encriptación del parámetro de comunicación con PIN'
204
Transmisión del parámetro de comunicación encriptado a través de canal predefinido
206
Desencriptación del parámetro de comunicación con PIN -> K2
208
Comando de tarjeta de chip
210
Envío del comando de tarjeta de chip en el canal que está definido por el parámetro de comunicación
212
Recepción del comando de tarjeta de chip solo cuando PIN' = PIN
214

Fig. 3

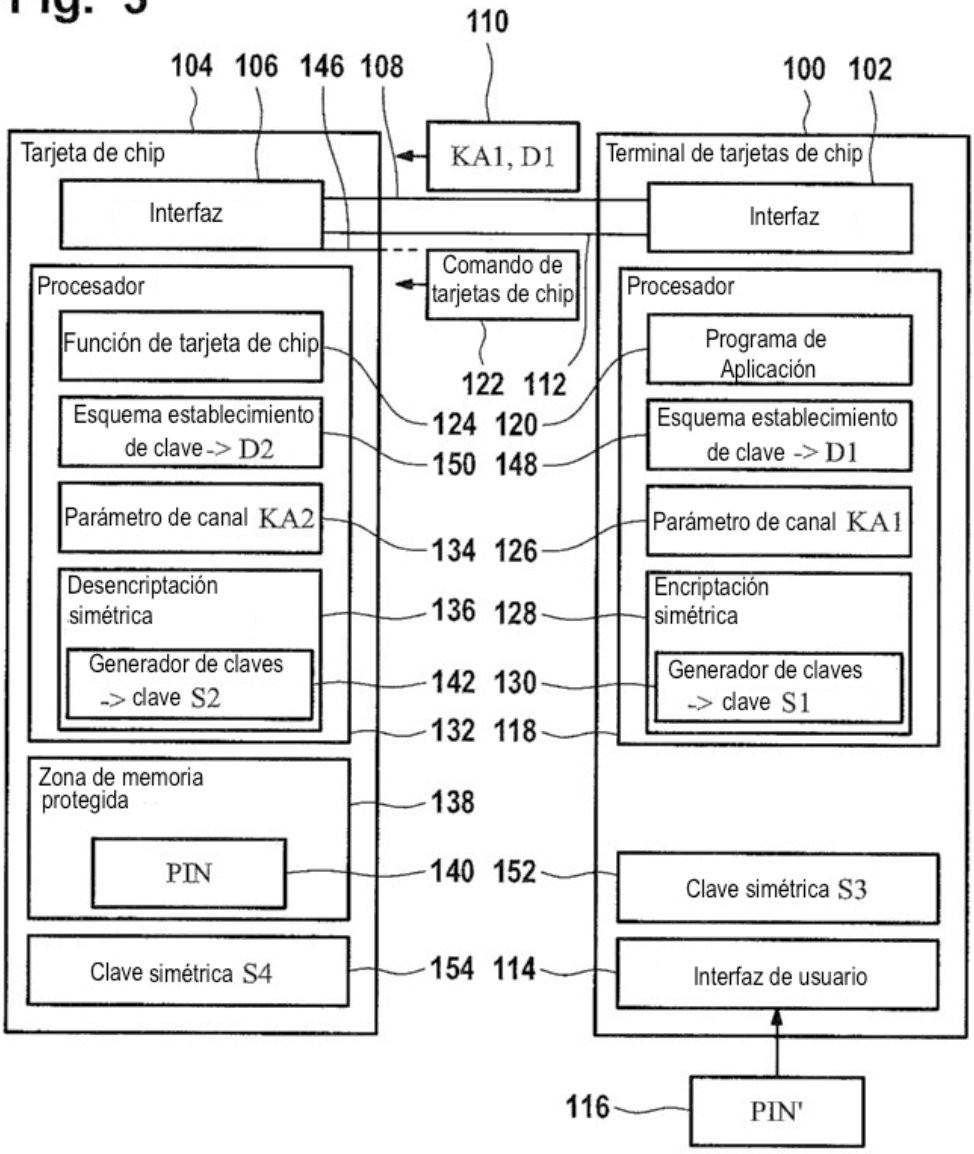
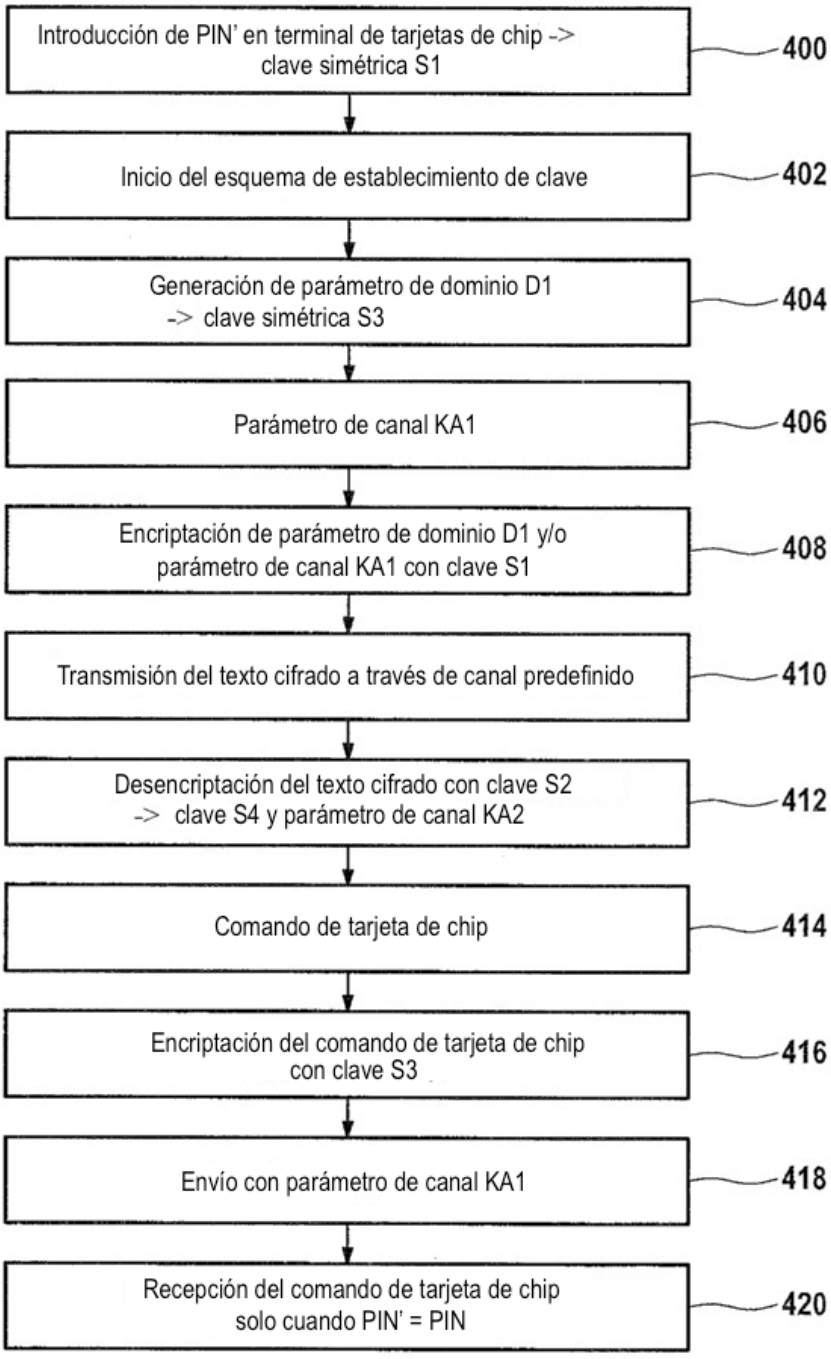

110
104
106
146
108
100
102
Tarjeta de chip
KA1, D1
Terminal de tarjetas de chip
Interfaz
Interfaz
Comando de tarjetas de chip
Procesador
Procesador
Función de tarjeta de chip
Programa de Aplicación
122
112
Esquema establecimiento de clave -> D2
Esquema establecimiento de clave -> D1
124
120
150
148
Parámetro de canal KA2
Parámetro de canal KA1
134
126
Desencriptación simétrica
Encriptación simétrica
136
128
Generador de claves -> clave S2
Generador de claves -> clave S1
142
130
132
118
Zona de memoria protegida
138
PIN
140
152
Clave simétrica S3
Clave simétrica S4
154
114
Interfaz de usuario
116
PIN'

Fig. 4


Introducción de PIN' en terminal de tarjetas de chip -> clave simétrica S1
400
Inicio del esquema de establecimiento de clave
402
Generación de parámetro de dominio D1 -> clave simétrica S3
404
Parámetro de canal KA1
406
Encriptación de parámetro de dominio D1 y/o parámetro de canal KA1 con clave S1
408
Transmisión del texto cifrado a través de canal predefinido
410
Desencriptación del texto cifrado con clave S2 -> clave S4 y parámetro de canal KA2
412
Comando de tarjeta de chip
414
Encriptación del comando de tarjeta de chip con clave S3
416
Envío con parámetro de canal KA1
418
Recepción del comando de tarjeta de chip solo cuando PIN' = PIN
420