(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 558 542**

(51) Int. CI.:

G06F 21/34 (2013.01)
G06Q 20/34 (2012.01)
G06Q 20/40 (2012.01)
G07C 9/00 (2006.01)
G07F 7/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **15.02.2008 E 08709620 (2)**

(97) Fecha y número de publicación de la concesión europea: **21.10.2015 EP 2122527**

(54) Título: **Dispositivo y método de autenticación**

(30) Prioridad:

20.02.2007 GB 0703245

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.02.2016

(73) Titular/es:

CRYPTOMATHIC LTD (100.0%)
329 CAMBRIDGE SCIENCE PARK MILTON ROAD
CAMBRIDGE, CAMBRIDGESHIRE CB4, GB

(72) Inventor/es:

TULIANI, JONATHAN ROSHAN

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Dispositivo y método de autenticación

La presente invención se refiere a un dispositivo y método de autenticación, en particular a dispositivos y métodos para la generación de contraseñas dinámicas, y a tarjetas que llevan el dispositivo y al software que implementa el método.

La autenticación de usuarios remotos es una parte esencial de muchas aplicaciones basadas en la web y en la red. Los nombres de usuarios y contraseñas tradicionales ofrecen una solución barata pero débil. Se obtiene frecuentemente una seguridad más alta enviando a los usuarios un "identificador" un dispositivo pequeño, portátil que genera contraseñas aparentemente aleatorias que son válidas solamente para un único uso: las denominadas contraseñas de un uso (OTP del inglés "One-Time Passwords"). Mediante la presentación de una OTP al sistema el usuario demuestra la posesión del identificador, que cuando se combina con una contraseña estática tradicional proporciona una autenticación fuerte, de dos factores.

Existen una amplia variedad de identificadores en el mercado, basados principalmente en tecnología propietaria, específica del vendedor. Por ejemplo, RSA SecureID, VASCO Digipass, Secure Computing y Active Identity. Está teniendo lugar actualmente un esfuerzo en la comunidad comercializadora de identificadores, denominado Iniciativa para Autenticación Abierta (OATH, del inglés "Open Authentication") [http://www.openauthentication.org]. Esta busca promover normas para identificadores que generen OTP y la infraestructura necesaria para su despliegue y uso.

Al mismo tiempo, la necesidad de una autenticación fuerte en el sector financiero ha conducido a MasterCard a ser la pionera en una normativa alternativa, basada en una variante de la tarjeta de pago "Chip y PIN" estándar (Figura 1). En este esquema, denominado programa de autenticación por chip (CAP, del inglés "Chip Authentication Program") [Chip Authentication Program Function Architecture, MasterCard International, septiembre de 2004], se usa un lector de tarjetas portátil (Figura 2) para crear unas OTP basada en las funciones del núcleo dentro de la tarjeta. Los lectores de tarjeta son anónimos e intercambiables, y el concepto demanda un despliegue amplio para hacer los artículos comunes en cada hogar u oficina, eliminando así la necesidad de que los usuarios individuales lleven su lector de tarjeta con su persona.

Sin embargo, CAP es un sistema cerrado, propietario y no es compatible con otros sistemas. En el futuro, pueden llegar a ser ampliamente disponibles lectores de tarjetas compatibles con CAP, pero solo serán útiles con tarjetas Chip y PIN compatibles con CAP aprobadas por sus bancos emisores, dado que solamente el banco emisor tiene acceso a la información necesaria para verificar una OTP generada por la tarjeta.

Se describirá un medio para el aprovechamiento de los lectores de tarjetas CAP estándar junto con una tarjeta personalizada, no de pago, para generar unas OTP compatibles con OATH. Una ventaja de este enfoque es que se puede usar la infraestructura OATH estándar para el despliegue de las tarjetas y la validación de las OTP resultantes, mientras que el coste de los identificadores se reduce al coste de una tarjeta-chip, mediante el aprovechamiento de la base lectora de la tarjeta ya establecida. Más generalmente, describiremos la sustitución del algoritmo en los dispositivos de tarjeta y lector basados en la contraseña de un uso. Las tarjetas pueden proporcionarse para trabajar con, por ejemplo, esquemas RSA SecureID, VASCO DigiPass, Secure Computing o ActivIdentity en lugar de o además de OATH.

Se describirá un circuito integrado para la generación de una contraseña dinámica para un primer esquema criptográfico, siendo adecuado el circuito para su uso con un dispositivo diseñado para un segundo, diferente esquema criptográfico, comprendiendo el circuito: una entrada de fuente de alimentación para el suministro de alimentación al circuito integrado; una interfaz para la transmisión de datos a, y la recepción de datos desde, el circuito integrado; y un procesador conectado a una memoria, almacenando la memoria códigos de control del procesador para controlar al procesador, cuando se ejecuta, para generar una contraseña dinámica de acuerdo con el primer esquema criptográfico y a continuación producir datos de criptograma intermedio adecuados para la salida hacia dicho dispositivo de modo que el procesamiento realizado por el dispositivo de acuerdo con el segundo esquema criptográfico dé como resultado que el dispositivo genere la contraseña dinámica original de acuerdo con el primer esquema criptográfico.

Se describirá un método de producir la salida de datos de pseudo-criptograma que corresponden a una contraseña dinámica de acuerdo con un primer esquema criptográfico, siendo adecuados los datos para su salida a un dispositivo diseñado para un segundo esquema criptográfico, diferente, comprendiendo el método la generación de la contraseña dinámica de acuerdo con el primer esquema criptográfico y a continuación la generación de datos de criptograma intermedio mediante la inversión del procesamiento realizado por el dispositivo de acuerdo con el segundo esquema criptográfico y produciendo la salida de dichos datos de criptograma intermedio, de modo que el dispositivo en procesamiento de los datos genera la contraseña dinámica original de acuerdo con el primer esquema criptográfico.

De acuerdo con un aspecto de la presente invención, se proporciona un aparato para la generación de datos de

criptograma intermedio que corresponden a una contraseña para un primer esquema criptográfico, siendo adecuado el aparato para su uso con un dispositivo diseñado para un segundo, diferente esquema criptográfico, comprendiendo el aparato: una interfaz de comunicación para la comunicación con uno de dichos dispositivos; y un procesador conectado a una memoria, almacenando la memoria códigos de control del procesador para controlar el procesador, cuando se ejecuta, para: generar una contraseña de acuerdo con el primer esquema criptográfico; y generar los datos de criptograma intermedio que corresponden a dicha contraseña, siendo adecuados los datos de criptograma intermedio para producir la salida hacia dicho dispositivo de modo que, cuando dicho dispositivo procesa dichos datos de criptograma intermedio de acuerdo con el segundo esquema criptográfico, dicho dispositivo genera dicha contraseña.

Preferiblemente la contraseña comprende una contraseña dinámica, o una contraseña que es generada mediante la inclusión de bits desde un contador o reloj binario dentro del cálculo de criptograma, y en el caso de que se use un contador el incremento del contador cada vez que se genere una contraseña.

En ocasiones la contraseña dinámica del primer esquema criptográfico puede ser incompatible con el dispositivo del segundo esquema criptográfico, y el código para generar una contraseña dinámica puede comprender código para generar contraseñas dinámicas repetidamente hasta que se halle una contraseña dinámica que sea compatible con el segundo esquema criptográfico.

Esta incompatibilidad puede ser causada por ceros añadidos que aparecen en ciertas contraseñas dinámicas del primer esquema criptográfico, que pueden ser incompatibles con el dispositivo del segundo esquema criptográfico.

Alternativamente la incompatibilidad puede producirse por un dígito de comprobación generado automáticamente por dicho dispositivo que sea incompatible con ciertas contraseñas dinámicas del primer esquema criptográfico.

De acuerdo con otro aspecto de la presente invención, se proporciona un método de generación de datos de criptograma intermedio que corresponden a un criptograma de acuerdo con un primer esquema criptográfico, siendo adecuados los datos para la visualización en un dispositivo diseñado para un segundo, diferente esquema criptográfico, comprendiendo el método: la generación de una contraseña dinámica de acuerdo con el primer esquema criptográfico; y la generación de datos de criptograma intermedio correspondientes a dicha contraseña dinámica, siendo adecuados dichos datos de criptograma intermedio para producir la salida hacia dicho dispositivo de modo que, cuando dicho dispositivo procesa dichos datos de criptograma intermedio de acuerdo con el segundo esquema criptográfico, dicho dispositivo produce la salida de dicha contraseña dinámica.

La invención proporciona adicionalmente códigos de control del procesador para implementar los métodos descritos anteriormente, por ejemplo en un sistema de ordenador de propósito general o en un procesador de señal digital (PSP) o en un circuito integrado dedicado, por ejemplo una tarjeta inteligente. El código puede proporcionarse sobre un portador tal como un disco, CD o DVD ROM, memoria programada tal como memoria solo de lectura (Firmware) o en un portador de datos tal como un portador de señal óptica o eléctrica. El código (y/o datos) para implementar realizaciones de la invención puede comprender un código fuente, objeto o ejecutable en un lenguaje de programación convencional (interpretado o compilado) tal como C, o un código ensamblador. Los métodos anteriormente descritos pueden implementarse también, por ejemplo, en una FPGA (matriz de puertas programable en campo) o en un ASIC (circuito integrado de aplicación específica). De ese modo el código puede comprender también códigos para el ajuste o control de un ASIC o FPGA, o códigos para un lenguaje de descripción de hardware tal como Verilog (marca registrada), VHDL (lenguaje de descripción de hardware de circuitos integrados de muy alta velocidad), o código RTL o SystemC. Normalmente se describe hardware dedicado usando un código tal como RTL (código a nivel de transferencia de registros) o, en un nivel más alto, usando un lenguaje tal como C. Como un experto en la materia apreciará dichos códigos y/o datos pueden distribuirse entre una pluralidad de componentes conectados en comunicación entre sí.

Las características de los aspectos y realizaciones de la invención descritos anteriormente pueden combinarse en cualquier permutación.

Las realizaciones de estos y otros aspectos de la invención se describirán ahora en detalle con referencia a los dibujos adjuntos, en los que:

La Figura 3 muestra un diagrama de flujo de un método de acuerdo con una realización de la invención.

La Figura 4 muestra un diagrama de bloques de un dispositivo de acuerdo con una realización de la invención.

Se describirá primero el Programa de Autenticación por Chip de MasterCard.

Tarjetas de Chip y PIN

Las tarjetas de "Chip y PIN" siguen normas técnicas más formalmente conocidas como EMV, por Europay, MasterCard y Visa. Están ampliamente adoptadas en muchos países en todo el mundo, dado que ofrecen potentes

características de seguridad permitiendo a los emisores de las tarjetas controlar varias formas de fraude.

Se usa un chip embebido en cada tarjeta EMV para autorizar las transacciones. La autorización se basa en un criptograma calculado usando una única clave para la tarjeta, junto con detalles de la transacción. La clave está embebida dentro del chip durante el proceso de emisión, y se mantiene una copia de seguridad por el banco emisor. El chip también mantiene un valor de contador, conocido como el Contador de Transacción de Aplicación (ATC, del inglés "Application Transaction Counter"), que se incluye en el cálculo de criptograma y se incrementa con cada transacción, como una defensa contra ataques por reproducción. Finalmente, el poseedor de la tarjeta suministra un PIN, que el chip verifica contra un valor de referencia almacenado, antes de permitir que se calcule el criptograma.

Tras la recepción de la transacción, el emisor es capaz de recalcular el criptograma usando su copia de la clave de la tarjeta. Dado que nadie más tiene la clave, debe originar un criptograma válido con la tarjeta, y la verificación del PIN y la tarjeta demuestra que la tarjeta está aún en posesión del poseedor original de la tarjeta.

Visión general del CAP

Una clase especial de transacciones es conocida como transacciones de "tarjeta no presente" (CNP del inglés "Card Not Present"). Estas incluyen pedidos por correo, pedidos telefónicos y transacciones de comercio electrónico basadas en la web. En estos casos, el pago es autorizado por el banco emisor basándose simplemente en los detalles visibles de la tarjeta tales como el número de tarjeta y la fecha de caducidad. Dado que estos valores son estáticos por naturaleza y fácilmente copiados, las transacciones CNP son un objetivo atractivo para el fraude.

MasterCard, junto con un cierto número de otras organizaciones en la industria de las tarjetas, ha desarrollado una norma para permitir que la seguridad de las tarjetas chip y PIN se mejore en escenarios CNP. Este esquema es denominado Programa de Autenticación del Chip (CAP, del inglés "Chip Authentication Program"). CAP requiere que cada poseedor de tarjeta esté provisto con un lector de tarjetas pequeño, portátil. Al insertar su tarjeta en el lector, e introduciendo su PIN, el poseedor de la tarjeta puede generar una OTP basada en la clave y al ATC en la tarjeta. El emisor puede verificar la OTP mediante el recálculo de criptograma basado en los mismos datos de entrada y clave.

Obsérvese que el lector de tarjeta no es personal para el poseedor de la tarjeta en ninguna manera, y no se realizan operaciones críticas de seguridad.

Cálculo de la OTP de CAP en EMV

Las tarjetas con chip de Chip y PIN fueron diseñadas para su uso en terminales de pago de puntos de venta y cajeros automáticos, no específicamente para la generación de contraseñas de un uso. Los lectores CAP simulan los terminales de pago EMV en su interacción con la tarjeta, y el lector es responsable entonces de tomar el criptograma de pago producido por la tarjeta y convertirlo en una contraseña de un uso.

El procesamiento llevado a cabo por el lector CAP se especifica en detalle en [Chip Authentication Program Function Architecture], pero en resumen comprende las siguientes etapas:

1. Recogida de los datos de entrada del criptograma
2. Extracción de los datos de la OTP
3. Conversión al sistema decimal

Cada etapa se explica con detalle adicional a continuación.

Recogida de los datos de entrada del criptograma

Las dos principales entradas al proceso de cálculo del criptograma son la clave de la tarjeta y el ATC. Sin embargo, con EMV, hay un cierto número de otros parámetros que se usan como entradas dentro de la validación del criptograma. Estos son específicos para las tarjetas de pago, y no tienen equivalentes en otros tipos de identificadores. Para reproducir el criptograma, el servidor de validación debe usar valores idénticos para estos parámetros.

En un escenario CAP típico, la mayor parte de estos parámetros son o bien fijos en valor cuando se emite la tarjeta, o pueden predecirse por el servidor de validación. Sin embargo, un pequeño número de los parámetros puede cambiar durante el ciclo de vida de la tarjeta, de acuerdo con cómo se use la tarjeta. Por ejemplo, esto incluye parámetros que limitan el número o cantidad de las transacciones que la tarjeta autorizará fuera de línea. Dado que el servidor de validación no puede predecir estos valores, deben transmitirse desde la tarjeta al servidor, embebidas en la contraseña de un uso en sí.

Extracción de los datos de la OTP

Para ser tan amigable para el usuario como sea posible, la contraseña de un uso producida debería ser tan corta

como sea posible, mientras se mantiene un nivel razonable de seguridad. Dado que los datos de entrada del criptograma EMV, combinados con el criptograma en sí, son de lejos demasiado largos para incluirse en la contraseña de un uso en su totalidad, estos se comprimen.

El proceso de compresión se define por un campo específico de CAP en la tarjeta, conocido como Mapa de bits Propietario del Emisor (IPB, del inglés "Issuer Proprietary Bitmap"), pero el proceso en sí se lleva a cabo por el lector de la tarjeta. El IPB define qué bits del ATC, criptograma y otros datos de entrada EMV se usarán en la contraseña de un uso, los otros bits se descartan.

Normalmente, se incluye un pequeño número de los bits ATC, para ayudar con la sincronización de los valores del contador entre servidor y tarjeta, junto con al menos 16 bits del criptograma, y finalmente esas entradas del criptograma adicionales que no pueden predecirse por el servidor. En algunos casos, en los que la aplicación de la tarjeta se usa solamente para CAP y no para pagos, puede ser que todas las entradas adicionales puedan predecirse por el servidor y de ese modo la OTP se basa en el ATC y criptograma en solitario.

Conversión al sistema decimal

Finalmente, la salida binaria desde el proceso de compresión se convierte a decimal para visualización al usuario en la pantalla del lector. Son posibles un cierto número de esquemas de conversión decimal, pero CAP define un único esquema basado en la interpretación simple de la salida del proceso de truncado como la representación binaria de un único entero. Se ignoran los ceros iniciales, y de ese modo la longitud final de la OTP puede variar.

A continuación se describirán las Normas de Autenticación Abierta (OATH).

Visión general

La iniciativa para autenticación abierta (OATH) es un cuerpo de coordinación de la industria que busca promover la normalización del mercado de la autenticación basada en un identificador. OATH ha publicado una "arquitectura de referencia" que describe una visión de un marco de autenticación general, y está promocionando un cierto número de normas para las diversas interfaces y componentes dentro de este sistema.

La más interesante de esta aplicación es "HOTP: An HMAC-based one-time-password algorithm", que está siendo normalizada por el IETF como RFC4226 [HOTP: An HMAC-Based One-Time Password Algorithm, http:/www.ietf.org/rfc/rfc4226.txt, diciembre de 2005].

Cálculo HOTP

Como con CAP, el algoritmo HOTP se basa en una primitiva criptográfica subyacente, en este caso HMAC-SHA1. Las entradas de este algoritmo definidas en HOTP son una clave del identificador y un contador muy similares a las entradas básicas a un cálculo del criptograma EMV tal como se usa por CAP.

El proceso de cálculo HOTP es como sigue:

1. Cálculo HMAC, basándose en la clave de identificador y contador. El contador se incrementa entonces automáticamente.
2. "Truncado dinámico" del resultado para dar un valor de 31 bits.
3. Conversión adicional del valor truncado, para dar la OTP.

Aunque los paralelismos con el cálculo de la OTP de CAP son claros, es importante observar que los detalles de cada etapa son completamente diferentes. Cada etapa se describe y contrasta con el equivalente CAP a continuación.

Cálculo HMAC

El cálculo HMAC usado es tal como se especifica en [HMAC: Keyed Hashing for Message Authentication, RFC2104, http://www.ietf.org/rfc/rfc2104.txt, febrero de 1997], usando SHA1 como el algoritmo de cifrado subyacente [US Secure Hash Algorithm 1 (SHA1), RFC3174, http://www.ietf.org/rfc3174.txt, septiembre de 2001]. La clave requerida por HMAC-SHA1 tiene normalmente 20 bytes de longitud, y [HOTP] especifica que se use un contador de 8 bytes como el único dato de entrada HMAC.

El resultado es un valor binario de 20 bytes, comparado con el criptograma de 8 bytes usado por CAP. En ambos casos, un objetivo principal es que no debería ser factible recuperar información acerca de la clave a partir de las OTP resultantes. Esta es la razón por la que, en ambos casos, se emplea un algoritmo criptográfico de alguna clase.

Truncado dinámico

El proceso de truncado definido por [HOTP] reduce la salida HMAC de 20 bytes a una cadena de 31 bits.

En primer lugar, los últimos 4 bits del último byte de la salida HMAC se consideran como un entero n en el intervalo 0-15. A continuación, se usan los bytes *n*, *n*+1,…, *n*+3 como la salida del truncado (con el bit inicial ignorado).

Se resaltan las diferencias con el esquema de compresión usado por CAP:

El IPB de CAP siempre selecciona bits desde la misma posición en el criptograma EMV para su uso en la OTP. En OATH, la posición de los bits varía, determinados por los últimos 4 bits en la salida HMAC, y de ahí el término "dinámico".

La edición actual de [HOTP] no proporciona mecanismos para información de sincronización de contador embebida en la OTP resultante, mientras que el IPB de CAP puede especificar un número arbitrario de bits ATC para inclusión en la OTP.

El IPB de CAP puede especificar un número de otros elementos de datos, específicos de EMV para su inclusión en la OTP. Dicha facilidad no es relevante para HOTP.

Conversión a decimal

La conversión a decimal HOTP consiste en la interpretación de la salida de 31 bits desde el proceso de truncado dinámico como la representación binaria de un entero, y a continuación la reducción de ese módulo entero 10^d, en la que *d* es el número de dígitos deseados en la OTP resultante. Por el contrario con CAP, si el resultado tiene menos de *d* dígitos se insertan ceros iniciales para dar una longitud *d* de la OTP total.

Obsérvese también que este proceso de conversión decimal realiza realmente un truncado adicional, en el sentido de que la salida tiene un contenido de información más pequeño que la entrada. En CAP, no se pierde información durante la conversión a decimal.

Se describirá a continuación la generación de las OTP de OATH usando un lector CAP. La Figura 3 muestra un ejemplo de un método para conseguir esto.

Se describirá un medio para generar OTP compatibles con OATH usando una norma, un lector CAP no modificado, mediante la producción de una tarjeta de chip OATH especial para usar dentro del selector. Esto permite a una organización que desee desplegar OATH el desplegar tarjetas de chip de bajo coste en lugar de los identificadores de coste más alto, aprovechando la infraestructura de lectores de tarjetas CAP desplegada para usar estas tarjetas de chip con los servidores de validación OATH existentes, comerciales.

Claramente el lector de chips OATH reproduce la interfaz de tarjeta EMV, o al menos aquellas partes de la interfaz EMV que se usan por el lector CAP. En caso contrario, el lector rechazaría la tarjeta.

La llamada a la función de tarjeta crítica es la llamada GENERATE_AC que se usa para generar el criptograma en sí. Obsérvese que esto no es suficiente para reemplazar simplemente la implementación de esta función en la tarjeta con una función que genere un valor de cifrado HOTP, tal como se usa en el cálculo de las OTP OATH. Esto es debido a que el proceso de compresión y conversión a decimal del criptograma para dar las OTP se lleva a cabo en el lector, y es totalmente diferente entre CAP y OATH.

La tarjeta de chip OATH implementa por lo tanto la siguiente secuencia de operaciones:

1. Generar el valor de cifrado HOTP (301), basándose en la clave de la tarjeta y el contador, e incrementar el contador (302).
2. Truncar y convertir a decimal el valor de cifrado (303) para producir la OTP en sí.
3. Convertir la OTP de vuelta al formato binario (304), usando un proceso que es el inverso del proceso de conversión adicional empleado por un lector CAP.
4. Rellenar los datos binarios resultantes (305) en una forma que es la inversa del proceso de compresión empleado por un lector CAP (tal como se define por el valor IPB en la tarjeta).

Se denomina el resultado un criptograma intermedio. La tarjeta de chip OATH pasa este criptograma intermedio al lector CAP, como si fuese un criptograma EMV normal.

El lector CAP comprimirá y convertirá entonces a decimal los datos, invirtiendo efectivamente las etapas 4 y 3 anteriores, y de ese modo el resultado final mostrado sobre la pantalla del lector será la OTP OATH, tal como se ha calculado por la tarjeta OATH en la etapa 2 anterior. La Figura 4 muestra un diagrama de bloques de un ejemplo de un dispositivo para una tarjeta de chip OATH compatible con lectores CAP.

Casos especiales

Surgen un cierto número de casos especiales, que se consideran como sigue.

Ceros iniciales

Durante la conversión a decimal, tanto CAP como HOTP pueden dar como resultado un resultado decimal que comience con "0". CAP especifica que dichos ceros iniciales se eliminen (y de ese modo la OTP resultante puede variar en longitud), mientras que HOTP especifica que se incluirán en la OTP (que por lo tanto tiene longitud fija).

Obsérvese que en CAP, el proceso de conversión a decimal que incluye el truncado de los ceros iniciales tiene lugar en el lector. Por ello no es posible forzar a un lector CAP a visualizar una OTP HOTP que incluyen ceros iniciales, independientemente del método usado en la tarjeta de sí. Se presentan tres posibles soluciones a este problema:

1. La primera solución posible es simple, pero insatisfactoria: dar instrucciones a los usuarios para insertar ceros adicionales por delante de la OTP visualizada cuando esté por debajo de la longitud esperada.
2. La segunda posible es hacer que la aplicación de autenticación o el servidor de validación inserten automáticamente cualquier cero inicial faltante antes de la validación de la OTP. Esto proporciona una mejor experiencia de usuario, pero frustra el objetivo original de implementar OATH usando lectores CAP sin ningún cambio en la infraestructura de validación.
3. El tercer enfoque es que la tarjeta de chip OATH identifique dichos casos, y cuando suceden, descartar automáticamente la OTP (en la etapa 2 anterior), y generar una nueva OTP basada en el valor de contador incrementado.

Dado que el dígito inicial es efectivamente aleatorio, una secuencia larga de contraseñas comenzando todas con cero es altamente improbable. Más aún, dado que el servidor de validación en cualquier caso acepta un intervalo de valores de contador para evitar problemas de sincronización, la omisión ocasional de la contraseña debido a que comienza con un cero no provoca que la validación falle, y no es notado por el usuario. Finalmente, aunque esta técnica reduce el número de salidas HOTP posibles en aproximadamente el 10%, una longitud mínima de 6 dígitos da al menos 1 millón de OTP posibles y de ese modo la seguridad global ofrecida es aun completamente aceptable.

Dígitos de sincronización del contador

En la actualidad HOTP no especifica ningún medio de inclusión de dígitos de sincronización del contador en la OTP, mientras que CAP ofrece un esquema flexible, configurado usando el IPB embebido en la tarjeta. Suprimiendo simplemente los dígitos de sincronización CAP con un valor IPB apropiado, se puede conseguir compatibilidad.

Considérese la posibilidad de que una versión futura de HOTP pueda incluir un medio de inclusión de información de sincronización del contador en la OTP. Es altamente probable que el algoritmo elegido no sea compatible con el usado por CAP, dado que no hay analogía para el IPB de CAP en HOTP. Se remarca que la compatibilidad puede obtenerse aún, continuando la supresión de la información de sincronización CAP usando el IPB y pasando los datos de sincronización HOTP desde la tarjeta al lector en el criptograma intermedio, junto con el resto de la OTP.

Considérese ahora el escenario en el que el lector CAP incluye un dígito de comprobación obligatoria u otros datos de sincronización, pero que HOTP no lo hace. En este caso, el lector recibirá el criptograma desde la tarjeta, y recibirá también adicionalmente el valor ATC, a partir del que extraerá los datos de sincronización, combinando los dos para dar la OTP visualizada. En este caso, se puede mantener aún la compatibilidad, mediante el uso de una lógica de tarjeta adicional. La tarjeta debería calcular la OTP de HOTP, y separarla en dos partes la que el lector extraerá de criptograma intermedio, y la que el lector extraerá desde el ATC. La tarjeta proporciona entonces un criptograma intermedio y un ATC alternativo al lector, sabiendo que el lector combinará éstos para reconstruir la OTP original. La observación clave es que el lector no tiene forma de saber que el valor en el ATC alternativo no es el mismo que el valor de contador usado para calcular la OTP.

Finalmente, obsérvese que el escenario en el que tanto HOTP como CAP implementan esquemas de sincronización, pero de modo diferente, puede manejarse mediante una combinación de las técnicas anteriores.

Dígitos de comprobación

Los dígitos de comprobación se usan a veces para detectar errores en los datos, en particular errores producidos por la transcripción humana. En la actualidad, ni CAP ni HOTP incluyen un mecanismo de dígito de comprobación para las OTP creadas, pero es posible que esto pueda cambiar en el futuro. Si un lector CAP estándar fuera requerido para soportar un dígito de comprobación HOTP, esto se podría conseguir embebiendo simplemente el dígito de comprobación en el criptograma intermedio que se pasa al lector, de modo similar a la técnica usada para pasar datos de sincronización explicada anteriormente.

Alternativamente, supóngase que el lector CAP fuese a incluir un dígito de comprobación en las OTP, que HOTP no

especifica. Esto crearía un problema más significativo, dado que la tarjeta no tendría medios de suprimir dicho dígito de comprobación. Las únicas soluciones son modificar la aplicación o infraestructura de validación para aceptar las OTP de HOTP con dígitos de comprobación CAP añadidos, o hacer que la tarjeta personalizada genere repetidamente unas OTP hasta que (por fortuna) se encuentre una OTP correcta con un dígito de comprobación y un criptograma intermedio apropiado (que no incluya el dígito de comprobación, dado que se añadirá por el lector) calculado.

Este último enfoque incrementaría grandemente el tiempo de cálculo de la tarjeta, dado que han de ser calculadas un gran número de OTP antes de que se encuentre un valor adecuado. El contador de tarjetas se incrementaría mucho más rápido que lo normal, y puede ser necesario en consecuencia ajustar la tolerancia en el servidor de validación. Aunque el incremento requerido en el contador de tarjetas es impredecible, es probable que se pueda aún encontrar un equilibrio apropiado de los parámetros del sistema (longitud de la OTP, tolerancia del servidor de validación) que ofrezca seguridad y fiabilidad aceptables siempre que la cantidad de información de comprobación de error insertada por lector de tarjeta no sea demasiado grande.

Obsérvese que esta última técnica es una repetición de la técnica usada para manejar los ceros iniciales en la OTP basada en HOTP. En general: si la OTP de HOTP es incompatible con el lector de tarjetas por cualquier razón (en los ejemplos anteriores, debido a un cero inicial o un dígito de comprobación), es siempre posible que la tarjeta simplemente incremente el valor de contador de la tarjeta hasta que se encuentre una OTP compatible. La aplicabilidad de esta técnica en la práctica depende del número y distribución de las OTP compatibles y los parámetros del servidor de validación.

Se ha descrito el escenario específico de un lector de tarjetas CAP que use una tarjeta especial para conseguir compatibilidad con OATH, y alternativas en relación a la sincronización del contador y dígitos de comprobación. Se realizarán ahora algunas posibles aplicaciones adicionales:

pueden proporcionarse tarjetas para su uso con lectores diseñados para cualquier sistema basado en las OTP en un motor criptográfico separado de la interfaz de usuario, no solamente el CAP. Sin embargo, CAP es el sistema más probable para conseguir un alto volumen de despliegue en los próximos pocos años. Las tarjetas pueden proporcionarse para su uso en cualquier sistema de OTP, no solamente OATH. En los ejemplos incluyen RSA SecureID, VASCO DigiPass, Secure Computing y ActivIdentity. Se podrían proporcionar tarjetas para autenticación en respuesta a desafíos. Las tarjetas pueden proporcionarse para "firmas cortas", en las que el identificador produce una OTP basada en datos de mensaje introducidos por el usuario (tanto incluyendo aún el valor del contador, como no). Posibles aplicaciones incluyen aquellas en las que el lector CAP es sustituido por un teléfono móvil (es decir un teléfono móvil con un lector de tarjetas que tenga suficiente compatibilidad CAP para trabajar con las tarjetas). Otras aplicaciones incluyen aquellas en las que se inserta una tarjeta OATH en un lector de tarjetas que se conecta al PC del usuario. Aplicaciones adicionales incluyen aquellas en las que la OTP se comunica verbalmente a través del teléfono, en lugar de la Internet, o por correo, o por fax, o a través de una red interior.

Sin ninguna duda se les ocurrirán a los expertos en la materia muchas otras alternativas efectivas. Se entenderá que la invención no está limitada a las realizaciones descritas y que engloba las modificaciones evidentes para los expertos en la materia incluidas dentro del espíritu y alcance de las reivindicaciones adjuntas al presente documento.

REIVINDICACIONES

1. Un aparato para la generación de datos de criptograma intermedio correspondientes a una contraseña dinámica para un primer esquema criptográfico, siendo adecuados los datos de criptograma intermedio para su visualización usando un dispositivo compatible con CAP diseñado para un segundo esquema criptográfico para la generación de una contraseña, en donde dicho segundo esquema criptográfico es un esquema del Programa de Autenticación por Chip (CAP), comprendiendo el aparato:

una interfaz de comunicaciones para la comunicación con dicho dispositivo compatible con CAP; y
un procesador acoplado a una memoria, almacenando la memoria un código de control del procesador para controlar el procesador con lo que dicho procesador está configurado para:

generar una contraseña dinámica de acuerdo con el primer esquema criptográfico; y
generar datos de criptograma intermedio a partir de dicha contraseña dinámica mediante
la conversión de la contraseña en datos binarios usando un proceso que es el inverso del proceso de conversión a decimal empleado por un dispositivo compatible con CAP y
rellenar los datos binarios de una manera que es la inversa del proceso de compresión empleado por el dispositivo compatible con CAP,
con lo que los datos de criptograma intermedio son adecuados para producir la salida hacia dicho dispositivo de modo que, cuando dicho dispositivo procesa dichos datos de criptograma intermedio de acuerdo con el segundo esquema criptográfico para generar una contraseña, dicho dispositivo produce la salida de dicha contraseña dinámica generada mediante el primer esquema criptográfico.

2. Un aparato de acuerdo con la reivindicación 1, en el que la contraseña dinámica comprende una contraseña de un solo uso.

3. Un aparato de acuerdo con las reivindicaciones 1 o 2, en el que el primer esquema criptográfico comprende un esquema de Autenticación Abierta, RSA SecureID o Vasco Digipass.

4. Un aparato de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en el que el rellenado de dichos datos binarios incluye la inserción de bits de acuerdo con un Mapa de bits Propietario del Emisor del CAP.

5. Un aparato de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en el que el rellenado de dichos datos binarios inversos incluye la incorporación de los datos del dígito de comprobación correspondientes a uno o más dígitos de comprobación.

6. Un aparato de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en el que una parte de las contraseñas dinámicas posibles en el primer esquema criptográfico no puede visualizarse usando dicho dispositivo, y en el que la generación de una contraseña dinámica comprende la generación repetidamente de contraseñas dinámicas hasta que se halla una contraseña dinámica que pueda visualizarse usando dicho dispositivo compatible con CAP.

7. Un aparato de acuerdo con la reivindicación 6, en el que dicha parte de contraseñas dinámicas posibles comprende contraseñas dinámicas que tienen ceros iniciales.

8. Un aparato de acuerdo con la reivindicación 6, en el que la generación de contraseñas dinámicas comprende adicionalmente la determinación del dígito de comprobación generado por dicho dispositivo.

9. Un aparato de acuerdo con una cualquiera de las reivindicaciones 1 a 8, en el que dicho dispositivo está configurado para procesar datos de sincronización además de dichos datos de criptograma intermedio, y en el que la generación de los datos de criptograma intermedio comprende adicionalmente la generación de datos de sincronización para producir la salida hacia dicho dispositivo de modo que, cuando dicho dispositivo compatible con CAP procesa dichos datos de sincronización y dichos datos de criptograma intermedio de acuerdo con el segundo esquema criptográfico, dicho dispositivo compatible con CAP genera datos adecuados para la visualización de dicha contraseña dinámica.

10. Un aparato de acuerdo con la reivindicación 11, en el que dichos datos de sincronización comprenden un Contador de Transacción de la Aplicación (ATC).

11. Un método de generación de datos de criptograma intermedio correspondientes a una contraseña dinámica para un primer esquema criptográfico, siendo adecuados los datos de criptograma intermedio para producir una visualización de dicha contraseña en un dispositivo compatible con CAP diseñado para un segundo esquema criptográfico para la generación de una contraseña, en donde dicho segundo esquema criptográfico es un esquema del Programa de Autenticación por Chip (CAP) comprendiendo el método:

la generación de una contraseña dinámica de acuerdo con el primer esquema criptográfico; y
generación de datos de criptograma intermedio a partir de dicha contraseña dinámica mediante

la conversión de la contraseña en datos binarios usando un proceso que es el inverso del proceso de conversión a decimal empleado por un dispositivo compatible con CAP y
el rellenado de los datos binarios de una manera que es la inversa del proceso de compresión empleado por un dispositivo compatible con CAP,
en el que dichos datos de criptograma intermedio son adecuados para producir la salida hacia dicho dispositivo de modo que, cuando dicho dispositivo procesa dichos datos de criptograma intermedio de acuerdo con el segundo esquema criptográfico para generar una contraseña, dicho dispositivo produce la salida de dicha contraseña dinámica generada mediante dicho primer esquema criptográfico.

12. Un método de acuerdo con la reivindicación 11, en el que la generación de la contraseña dinámica comprende la generación de un criptograma HMAC-SHA1.

13. Un medio legible por ordenador que lleva el código de control del procesador para controlar un procesador para, cuando se ejecuta, llevar a cabo el método de la reivindicación 11 o de la reivindicación 12.

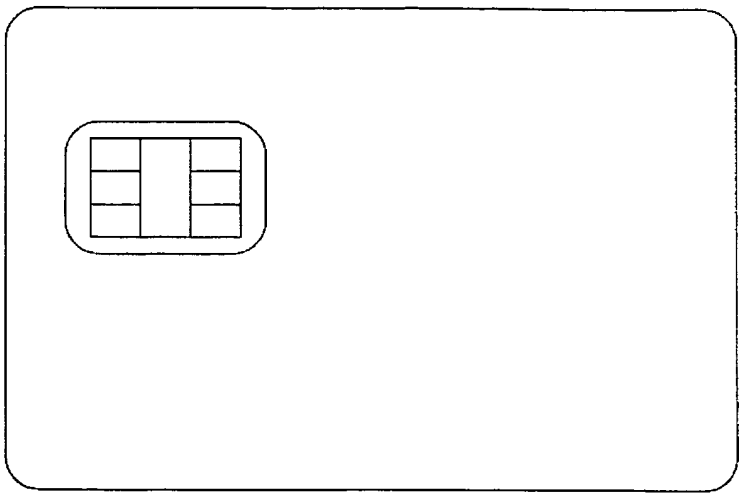

Figura 1

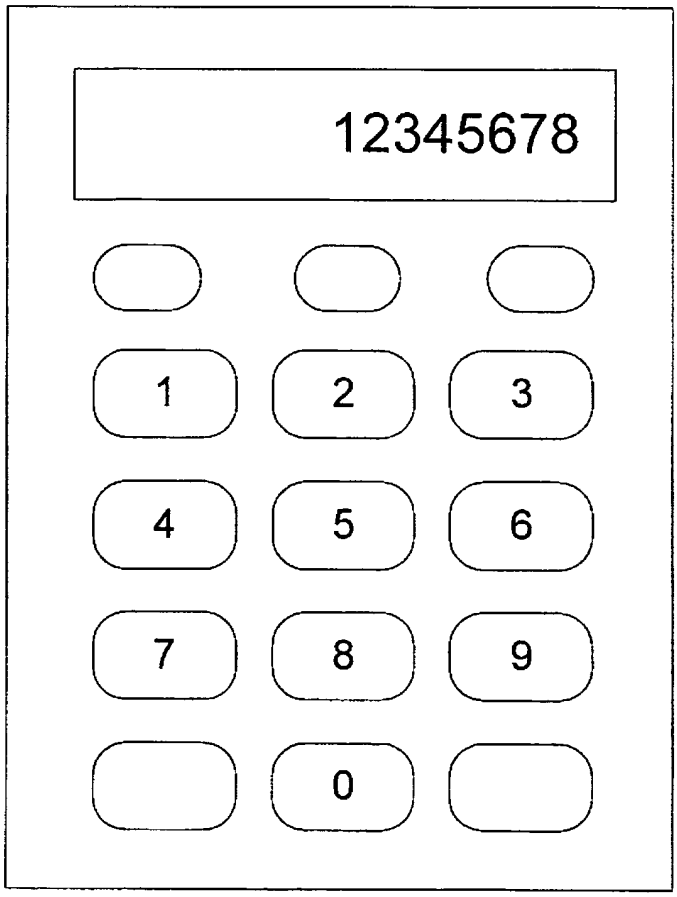

Figura 2

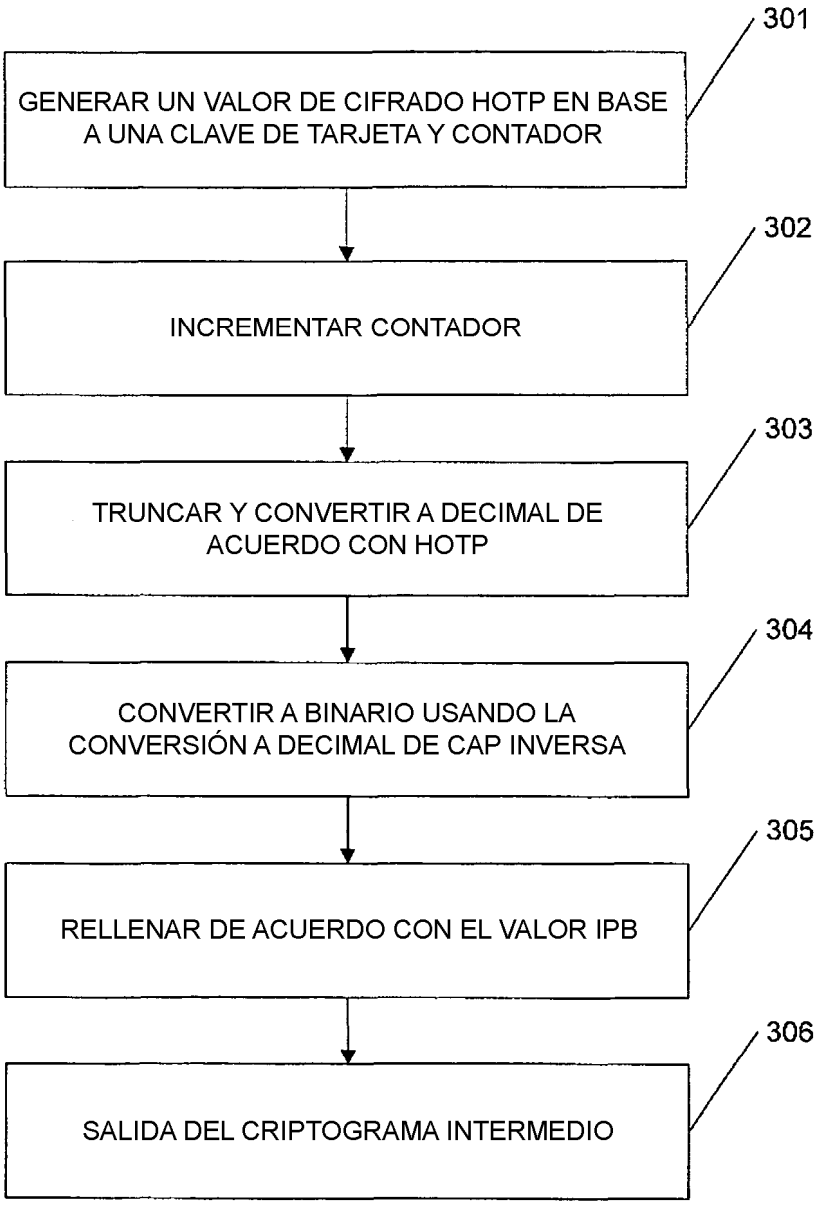
301
GENERAR UN VALOR DE CIFRADO HOTP EN BASE A UNA CLAVE DE TARJETA Y CONTADOR
302
INCREMENTAR CONTADOR
303
TRUNCAR Y CONVERTIR A DECIMAL DE ACUERDO CON HOTP
304
CONVERTIR A BINARIO USANDO LA CONVERSIÓN A DECIMAL DE CAP INVERSA
305
RELLENAR DE ACUERDO CON EL VALOR IPB
306
SALIDA DEL CRIPTOGRAMA INTERMEDIO

Figura 3

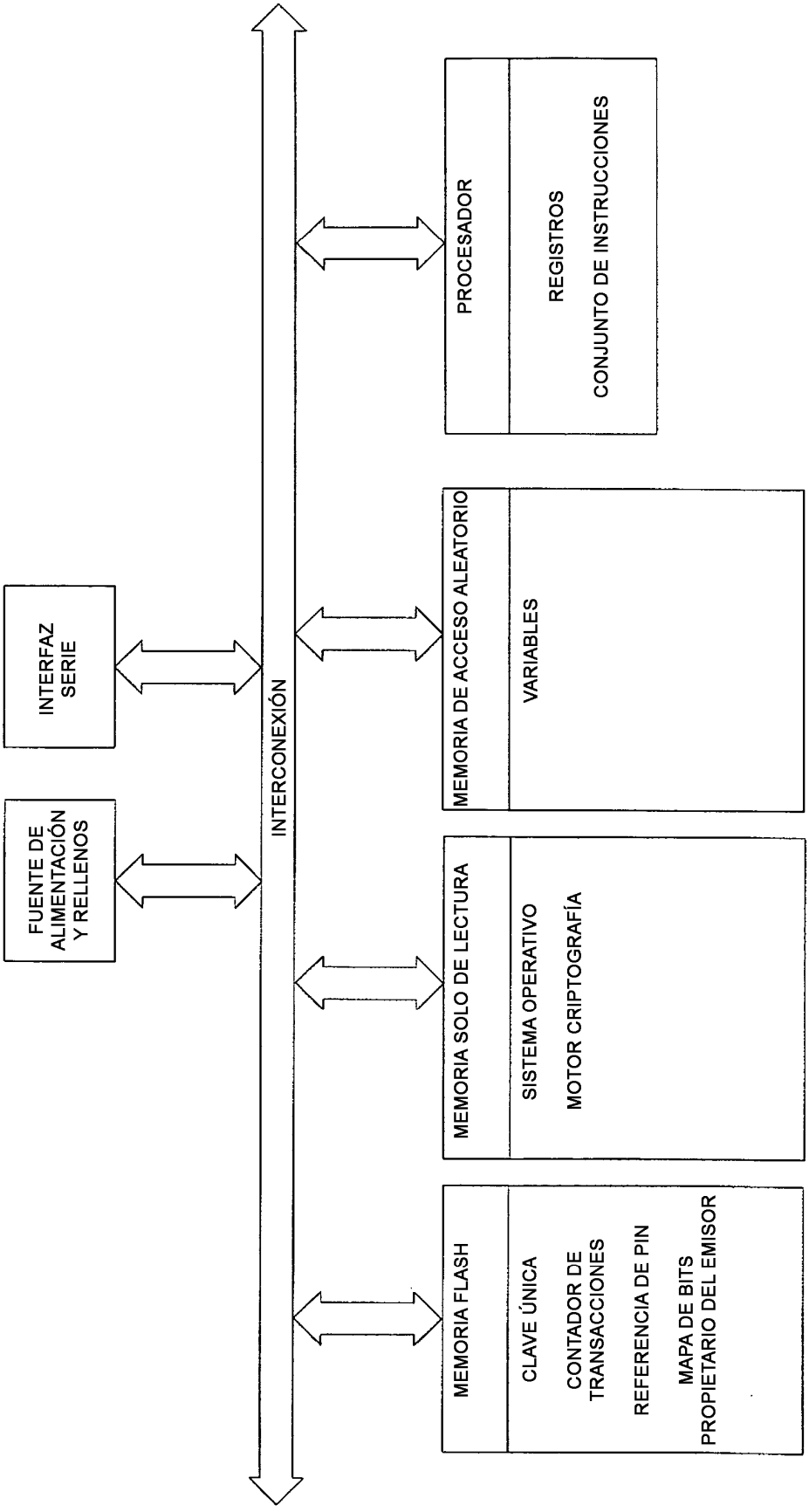
INTERFAZ SERIE
FUENTE DE ALIMENTACIÓN Y RELLENOS
INTERCONEXIÓN
PROCESADOR
REGISTROS
CONJUNTO DE INSTRUCCIONES
MEMORIA DE ACCESO ALEATORIO
VARIABLES
MEMORIA SOLO DE LECTURA
SISTEMA OPERATIVO
MOTOR CRIPTOGRAFÍA
MEMORIA FLASH
CLAVE ÚNICA
CONTADOR DE TRANSACCIONES
REFERENCIA DE PIN
MAPA DE BITS PROPIETARIO DEL EMISOR

Figura 4