(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 601 084**

(51) Int. CI.:

G06Q 20/34 (2012.01)
G07F 7/10 (2006.01)
G07F 7/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.03.2010 PCT/EP2010/053608**

(87) Fecha y número de publicación internacional: **18.11.2010 WO10130489**

(96) Fecha de presentación y número de la solicitud europea: **19.03.2010 E 10712917 (3)**

(97) Fecha y número de publicación de la concesión europea: **17.08.2016 EP 2430582**

(54) Título: **Clave electrónica para autentificación**

(30) Prioridad:

13.05.2009 DE 102009021011

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.02.2017

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Wittelsbacherplatz 2
80333 München, DE

(72) Inventor/es:

FALK, RAINER y
FRIES, STEFFEN

(74) Agente/Representante:

LOZANO GANDIA, José

CLAVE ELECTRÓNICA PARA AUTENTIFICACIÓN

DESCRIPCIÓN

La invención se refiere a una clave electrónica para autentificar un usuario, así como a un procedimiento y a un sistema para autentificar un usuario con una clave electrónica y un aparato lector.

Los procedimientos de autentificación para servicios críticos para la seguridad deben sustituirse a menudo a lo largo del tiempo por procedimientos nuevos, mejores. Un ejemplo de ello es la tarjeta EC, en la que en su versión inicial se utilizan informaciones de una banda magnética existente y un PIN (Personal Identification Number, número de identificación personal) para permitir el acceso a una cuenta asociada. No obstante, últimamente suceden cada vez con más frecuencia los llamados ataques skimming (robo de información in situ), en los que mediante aparatos antepuestos en los cajeros automáticos se copia la tarjeta y se piratea el PIN mediante medidas técnicas adecuadas. El contenido de la banda magnética se copia entonces sobre una nueva tarjeta, con lo que es posible un acceso no autorizado a la cuenta. Ciertamente los datos de la banda magnética están usualmente codificados o dotados de una suma de comprobación criptográfica, con lo que las informaciones no pueden leerse sin conocer la clave central. Desde luego un atacante no necesita esta clave central cuando él ha copiado la banda magnética completa y posee el PIN.

Por ello últimamente apoyan las tarjetas EC más modernas una smartcard (tarjeta inteligente) integrada, que no puede copiarse tan sencillamente como una banda magnética. La misma ofrece una seguridad claramente superior a la del procedimiento basado en banda magnética. No obstante, para asegurar la compatibilidad "hacia atrás" con sistemas ya existentes, sigue apoyándose el procedimiento basado en banda magnética, para que no tengan que sustituirse simultáneamente todos los cajeros automáticos.

El cajero automático o bien lector de tarjetas comprueba la existencia de un smartcard-chip (chip de tarjeta inteligente) sometido a un contacto mediante una conexión galvánica con los contactos de la tarjeta de chip existentes sobre la tarjeta. Un chip de tarjeta inteligente existente puede detectarse por ejemplo cuando el mismo transmite al aplicar la tensión de alimentación un mensaje ATR (Answer to Reset, respuesta a la reinicialización). Cuando se detecta un chip de tarjeta inteligente, se utiliza el procedimiento de autentificación basado en tarjeta inteligente en lugar del procedimiento de autentificación basado en tarjeta magnética. No obstante, si no se detecta ningún chip de tarjeta inteligente, se utiliza el procedimiento de autentificación existente basado en banda magnética.

Entonces es problemático que la banda magnética de tarjetas que apoyan tanto el procedimiento de autentificación basado en banda magnética como también el basado en tarjeta inteligente, sigue siendo fácil de copiar. Una tarjeta copiada es aceptada entonces por cajeros automáticos, que realmente apoyarían tanto procedimientos de autentificación basados en banda magnética como también el procedimiento de autentificación basado en tarjeta inteligente. Tales ataques se denominan también ataques “bidding-down” (de puja a la baja).

Los ataques bidding-down se conocen por protocolos de seguridad para autentificar acuerdos de clave. Dentro de un protocolo de autentificación se apoyan varias variantes, que tienen distinta fuerza. Al principio intercambian ambos interlocutores de comunicación informaciones sobre las respectivas variantes apoyadas. Se elige la más fuerte de ambas variantes apoyadas y se utiliza en la secuencia del protocolo. No obstante, puesto que el intercambio de información inicial aún no está protegido criptográficamente frente a manipulación, puede manipular un atacante la información intercambiada tal que se elija un procedimiento débil, aún cuando ambos interlocutores de comunicación también apoyarían procedimientos fuertes. Para ello aparenta el mismo que un interlocutor de la comunicación sólo apoya esta variante débil. Como contramedida comprueban algunos protocolos en un momento posterior, cuando se ha realizado la autentificación y el acuerdo de claves, la integridad de las informaciones inicialmente intercambiadas a posteriori. Para ello se calculan sumas de prueba, se transmiten y se comprueban.

En consecuencia, la presente invención tiene como objetivo básico indicar una clave electrónica que apoye varios procedimientos de autentificación y con la que se impidan los antes citados ataques bidding-down.

En el marco de la invención se logra este objetivo mediante una clave electrónica, un procedimiento y un sistema con las características de las reivindicaciones 1, 5 y 7. Ventajosos perfeccionamientos de la invención se indican en las reivindicaciones dependientes.

La clave electrónica correspondiente a la invención (security token, token de seguridad) para autentificar un usuario apoya al menos dos procedimientos de autentificación, estando memorizada para cada procedimiento de autentificación una información de seguridad separada. La correspondiente información de seguridad puede leerse mediante al menos una interfaz. La información de seguridad para un primer procedimiento de autentificación presenta una información sobre el apoyo a al menos otro procedimiento de autentificación.

Una clave electrónica incluye, sin limitación con respecto a la generalidad, este concepto de security token, que para autentificar un usuario memoriza al menos una información de seguridad. Al respecto puede tratarse de una información de identificación o de una clave criptográfica para autentificar un usuario. La clave electrónica puede realizarse en distintos factores de forma, por ejemplo como tarjeta de chip, como lápiz USB o como tarjeta de

memoria. Además dispone la clave electrónica de distintas interfaces, que por ejemplo están configuradas como interfaz para tarjetas de chip, interfaz USB, interfaz para tarjetas de memoria (SD-Card, MMC-Card) o como una interfaz inalámbrica. La interfaz puede también estar disponible en forma de una banda magnética o como Machine Readable Zone (zona legible por máquina).

La invención reivindicada se refiere en consecuencia a una clave electrónica (security token), que apoya al menos dos procedimientos de autentificación de distinta clase. Una información de seguridad asociada en cada caso al correspondiente procedimiento de autentificación está memorizada separadamente en la clave electrónica y puede leerse mediante distintas interfaces de la clave electrónica. Como parte de la información de seguridad del primer procedimiento de autentificación, se incluye una información sobre el apoyo al segundo procedimiento de autentificación. Así está codificada por ejemplo sobre la banda magnética de una tarjeta EC la existencia de un chip de tarjeta inteligente sobre la tarjeta. Esta información está codificada por ejemplo con una clave de sistema del banco emisor, con lo que la información sobre la existencia del chip de tarjeta inteligente queda igualmente asegurada.

Ventajosamente se detecta así mediante un aparato lector de tarjetas qué procedimientos de autentificación apoya la clave electrónica. Cuando en base a esta información detecta el aparato lector que la clave electrónica apoya un segundo procedimiento de autentificación más fuerte, pero que este procedimiento de autentificación no ha sido reconocido por el aparato lector de tarjetas, entonces se rechaza por ejemplo la clave electrónica.

En una variante ventajosa de la presente invención está archivada la información sobre el apoyo a otro procedimiento de autentificación en un servidor. En este servidor puede consultarse la información mediante el aparato lector de tarjetas.

El procedimiento correspondiente a la invención para autentificar un usuario con un aparato lector y una clave electrónica incluye las siguientes etapas, que ejecuta el aparato lector: Se averiguan los primeros procedimientos de autentificación apoyados por la clave electrónica. Se elige un procedimiento de autentificación según una directiva (policy) que puede predeterminarse a partir de los primeros procedimientos de autentificación apoyados. Se lee una información de seguridad para el procedimiento de autentificación elegido. En base a la información de seguridad leída se averiguan segundos procedimientos de autentificación apoyados. El procedimiento de autentificación elegido se comprueba en base a los segundos procedimientos de autentificación apoyados según una directiva de comprobación (policy) que puede predeterminarse, con lo que cuando el resultado de la comprobación es conforme con las directivas de comprobación, prosigue la autentificación con el procedimiento de autentificación elegido y cuando el resultado de la comprobación no es conforme con las directivas de comprobación, se impide la autentificación con el procedimiento de autentificación elegido.

El sistema correspondiente a la invención para autentificar un usuario presenta una clave electrónica con medios para realizar al menos dos procedimientos de autentificación, en la que para cada procedimiento de autentificación está memorizada una información de seguridad separada, que puede leerse en cada caso mediante al menos una interfaz y en la que la información de seguridad para un primer procedimiento de autentificación presenta una información sobre el apoyo a al menos otro procedimiento de autentificación. Además presenta el sistema un aparato lector con medios para determinar otros procedimientos de autentificación apoyados en base a la información de seguridad leída y medios para comprobar un procedimiento de autentificación elegido en base a los otros procedimientos de autentificación apoyados según una directiva de comprobación que puede predeterminarse, con lo que para un resultado de la comprobación conforme con las directivas de comprobación, prosigue la autentificación con el procedimiento de autentificación elegido y cuando el resultado de la comprobación no es conforme con las directivas de comprobación, se interrumpe la autentificación con el procedimiento de autentificación elegido.

La presente invención se describirá a continuación más en detalle con ejemplos de ejecución en base a los dibujos. Se muestra en

figura 1 una representación esquemática de un sistema para la autentificación con una clave electrónica (ST) y tres aparatos lectores de tarjetas (STR1, STR2, STR3);
figura 2 una representación esquemática de informaciones memorizadas sobre una banda magnética según el estado de la técnica y según la presente invención;
figura 3 un diagrama secuencial del procedimiento correspondiente a la invención.

La figura 1 muestra una clave electrónica ST que apoya un procedimiento de autentificación basado en banda magnética y uno basado en tarjetas de chip. Con el chip de tarjeta inteligente se comunica mediante las superficies de contacto de la cara superior de la tarjeta. Además se representan en la figura 1 tres aparatos lectores de tarjetas STR1, STR2 y STR3. El primer aparato lector de tarjetas SRT1 apoya sólo el procedimiento de autentificación basado en banda magnética y por el contrario el segundo aparato lector de tarjetas STR2 apoya tanto el procedimiento de autentificación basado en tarjetas inteligentes como también el procedimiento basado en banda magnética. El tercer aparato lector de tarjetas STR3 está unido mediante una red de comunicación no representada con un sistema back-end (de respaldo) BE. Mediante esta conexión puede recibir el aparato lector de tarjetas STR3 informaciones en base a los datos de identificación leídos mediante la clave electrónica ST a través del sistema

back-end BE. También el aparato lector de tarjetas STR3 apoya tanto el procedimiento de autentificación basado en banda magnética como también el basado en tarjetas inteligentes.

Mediante la invención se mantiene con continuidad la seguridad del procedimiento de autentificación de mayor valor basado en tarjeta inteligente, ya que no es posible un ataque bidding-down sobre el procedimiento de autentificación más débil basado en tarjetas magnéticas. Con ello ya no puede engañarse a un aparato lector de tarjetas que apoya también una variante de autentificación fuerte (como por ejemplo STR2 y STR3) para utilizar la variante de autentificación más débil de una clave electrónica que también apoya la variante fuerte.

Incluso cuando tanto la clave electrónica ST como también el aparato lector STR2 apoyen una autentificación utilizando la banda magnética, queda garantizado mediante la invención que un atacante bidding-down no puede utilizar este procedimiento de autentificación más débil en el caso de que tanto la clave electrónica ST como también el aparato lector de tarjetas STR2 y/o STR3 apoyen el procedimiento de autentificación de más valor. El procedimiento de autentificación débil se sigue utilizando sólo cuando en la realidad la clave electrónica ST o el aparato lector de tarjetas STR1 sólo apoyen la variante de autentificación más débil.

En consecuencia se apoya la seguridad de una clave electrónica (security token) que apoya varias alternativas de procedimientos de autentificación y aumenta la seguridad de un procedimiento de autentificación que utiliza esta clave electrónica. No es suficiente comprometer una de estas variantes, sino que deben reproducirse varias o bien en general todas las variantes apoyadas sobre una clave electrónica reproducida (clonada). Esto aumenta el coste de un ataque con éxito y con ello también la seguridad frente al mismo.

Como aplicación pueden considerarse todos los procedimientos en los que tiene lugar una migración de una tecnología de autentificación débil a otra tecnología de autentificación más fuerte.

La figura 2 muestra en una representación esquemática una información memorizada sobre una banda magnética. Según el estado de la técnica 201 se memoriza una información sobre la tarjeta CI (Card Information, información de tarjeta), como por ejemplo finalidad de aplicación, emisor, número de cuenta, nombre del titular de la tarjeta. Para proteger frente a errores de lectura, está prevista una suma de comprobación LRC (Longitudinal Redundancy Check, comprobación de redundancia longitudinal).

Según la presente invención se proporcionan informaciones adicionales 202. Así se prevé una información sobre otros procedimientos de autentificación apoyados AV. Esta información sobre otros procedimientos de autentificación apoyados se protege de manera opcional mediante una suma de comprobación criptográfica CKS separada, que por ejemplo está configurada como Message Authentication Code (código de autentificación del mensaje). La suma de comprobación criptográfica se calcula por ejemplo mediante los campos CI y AV.

Según un perfeccionamiento de la presente invención, pueden ligarse autorizaciones y/o servicios a la fuerza de la autentificación elegida. Esto hace posible por ejemplo que se unan nuevos servicios a los procedimientos de autentificación más fuertes, para evitar en este caso un abuso con tarjetas más antiguas.

La figura 3 muestra un diagrama secuencial de un ejemplo de ejecución del procedimiento correspondiente a la invención para autentificar un usuario con un aparato lector y una clave electrónica. Una vez que se ha introducido 301 la clave electrónica, aquí una tarjeta EC, en el aparato lector de tarjetas, aquí un cajero automático, se reconoce 302 primeramente la tarjeta EC como tal mediante el cajero automático. A continuación averigua el cajero automático a partir de la tarjeta EC introducida las variantes de autentificación 303 efectivamente apoyadas.

En este ejemplo de ejecución se comprueba en particular la existencia de un chip de tarjeta inteligente. Esto puede realizarse con distinta complejidad, por ejemplo detectando una superficie de contacto para un chip en la posición prevista para ello. Esto se detecta por ejemplo en que existe una unión galvánica y en consecuencia puede fluir una corriente. Otra posibilidad adicional es la detección de la existencia de una comunicación de chip de tarjeta inteligente, por ejemplo en forma de un aviso ATR (Answer to Reset). Además existe una posibilidad de leer una información de identificación de chip de tarjeta inteligente, por ejemplo un número de serie del aviso ATR y comparar la misma con una información de comprobación memorizada en la banda magnética. Una tal suma de comprobación se archiva por ejemplo sobre la banda magnética y se evalúa, o se calcula y se evalúa mediante una información combinada, que en parte está memorizada en la banda magnética y en parte sobre el chip.

En la siguiente etapa 304 se elige una variante de autentificación según una directiva (policy) definida. Por lo general esto significa que cuando hay varias alternativas de autentificación se elige la más segura o más fuerte criptográficamente. A continuación se lee 305 la información de seguridad asociada a través de la interfaz asociada. En base a la información de seguridad se determinan 306 finalmente las variantes de autentificación apoyadas por la clave electrónica.

Finalmente se comprueba en la etapa 307, en base a una directiva de comprobación, el procedimiento de autentificación elegido en la etapa 304 y el procedimiento de autentificación apoyado determinado en la etapa 306 a partir de la información de seguridad. Si el resultado de la prueba no es conforme con las directivas de comprobación 308, se interrumpe el procedimiento para autentificar un usuario y aparece por ejemplo un aviso de falta. Éste es por ejemplo el caso cuando se ha elegido un procedimiento de autentificación basado en banda

magnética, resultando claro en base a la información de seguridad y a la directiva de comprobación que tanto el aparato lector como también la clave electrónica proporcionarían un procedimiento basado en tarjeta inteligente.

Pero si el resultado de la comprobación en la etapa 307 es conforme con la directiva de comprobación, prosigue el procedimiento de autentificación con el procedimiento de autentificación elegido. El procedimiento termina en la etapa 310.

REIVINDICACIONES

1. Clave electrónica para autentificar un usuario,
en la que la autentificación puede realizarse en cada caso mediante al menos dos procedimientos de autentificación y en la que para cada respectivo procedimiento de autentificación está memorizada separadamente una información de seguridad, que puede leerse en cada caso a través de al menos una interfaz, estando configuradas diferentes las interfaces, de las que al menos hay dos,
caracterizada porque la información de seguridad sobre un primer procedimiento de autentificación presenta una información sobre el apoyo a al menos otro procedimiento de autentificación.

2. Clave electrónica según la reivindicación 1,
en la que la interfaz, de las que al menos hay una, está configurada como tarjeta de chip que funciona con contacto, tarjeta de chip sin contacto o banda magnética.

3. Clave electrónica según la reivindicación 1 ó 2,
en la que la integridad de la información sobre el apoyo a al menos otro procedimiento de autentificación está protegida mediante una suma de comprobación criptográfica.

4. Clave electrónica según una de las reivindicaciones 1 a 3,
en la que la información sobre el apoyo de otro procedimiento de autentificación puede obtenerse de un servidor.

5. Procedimiento para autentificar un usuario con un aparato lector y una clave electrónica según una de las reivindicaciones 1 a 4,
en el que el aparato lector ejecuta las siguientes etapas:
   - averiguación de primeros procedimientos de autentificación apoyados por la clave electrónica, en base a una primera interfaz del aparato lector
   - elección de un procedimiento de autentificación según una directiva que puede predeterminarse a partir de los primeros procedimientos de autentificación apoyados, en base a una segunda interfaz del aparato lector, diferenciándose la primera y la segunda interfaz
   - lectura de una información de seguridad para el procedimiento de autentificación elegido,
   - en base a la información de seguridad, averiguación de segundos procedimientos de autentificación apoyados,
   - comprobación del procedimiento de autentificación elegido en base a los segundos procedimientos de autentificación apoyados según una directiva de comprobación que puede predeterminarse, tal que
   - cuando un resultado de la comprobación es conforme con las directivas de comprobación, prosigue la autentificación con el procedimiento de autentificación elegido,
   - cuando el resultado de la comprobación no es conforme con las directivas de comprobación, se impide la autentificación con el procedimiento de autentificación elegido.

6. Procedimiento según la reivindicación 5, en el que se impide la autentificación con la clave electrónica.

7. Sistema para autentificar un usuario, que presenta
   - una clave electrónica con medios para realizar al menos dos procedimientos de autentificación, en la que para cada procedimiento de autentificación está memorizada una información de seguridad separada, que puede leerse en cada caso mediante al menos una interfaz y en la que están configuradas de manera diferente al menos dos interfaces y en la que la información de seguridad sobre un primer procedimiento de autentificación presenta una información sobre el apoyo a al menos otro procedimiento de autentificación,
   - un aparato lector con medios para determinar otros procedimientos de autentificación apoyados en base a la información de seguridad leída y para comprobar un procedimiento de autentificación elegido en base a los otros procedimientos de autentificación apoyados según una directiva de comprobación que puede predeterminarse, con lo que
   - para un resultado de la comprobación conforme con las directivas de comprobación, prosigue la autentificación con el procedimiento de autentificación elegido,
   - cuando el resultado de la comprobación no es conforme con las directivas de comprobación, se interrumpe la autentificación con el procedimiento de autentificación elegido.

FIG 1

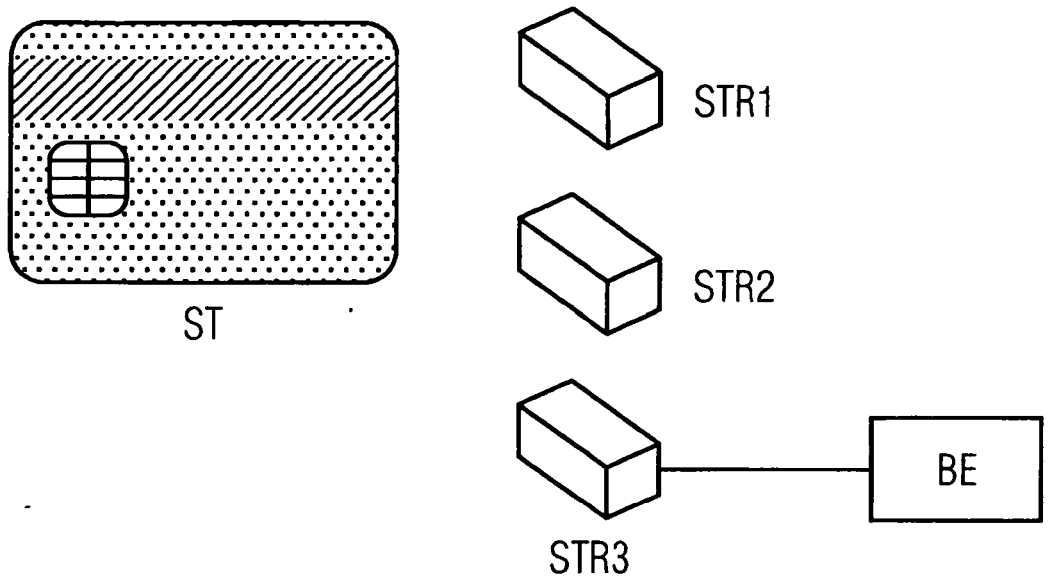

FIG 2

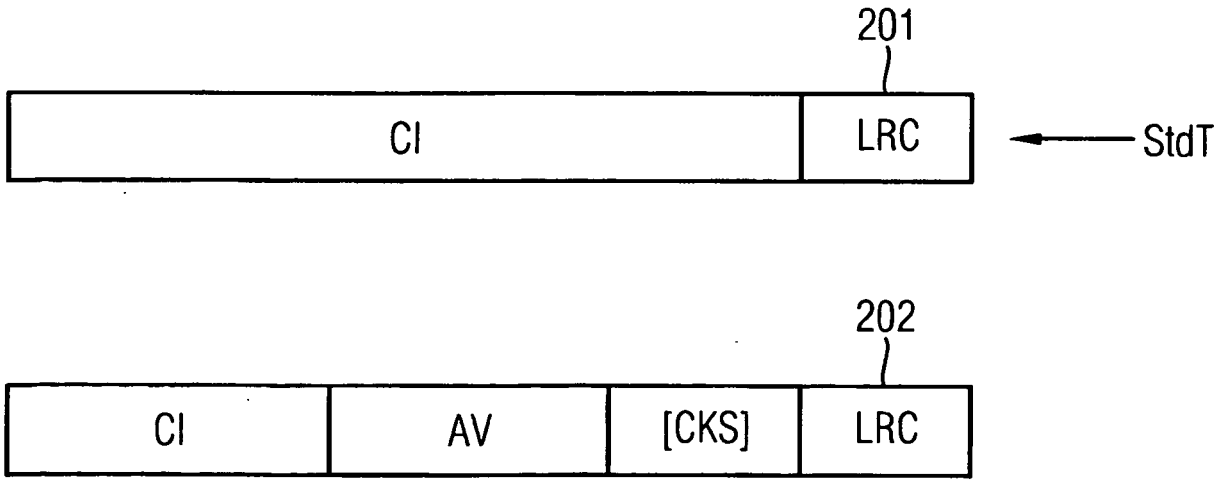

FIG 3