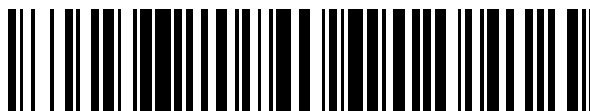


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 581 561**

51 Int. Cl.:

G06K 19/077 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **14.02.2006** **E 06710896 (9)**

97 Fecha y número de publicación de la concesión europea: **18.05.2016** **EP 1854053**

54 Título: **Una tarjeta inteligente y un procedimiento de operación de una tarjeta inteligente**

30 Prioridad:

17.02.2005 EP 05101208

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

06.09.2016

73 Titular/es:

**KONINKLIJKE PHILIPS N.V. (100.0%)
HIGH TECH CAMPUS 5
5656 AE EINDHOVEN, NL**

72 Inventor/es:

**MUSIAL, PAWEL y
SLIKKERVEER, PETER**

74 Agente/Representante:

ISERN JARA, Jorge

ES 2 581 561 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Una tarjeta inteligente y un procedimiento de operación de una tarjeta inteligente

5 CAMPO DE LA INVENCION

La invención se refiere a una tarjeta inteligente, así como a un procedimiento de operación de una tarjeta inteligente.

10 ANTECEDENTES DE LA INVENCION

Una tarjeta inteligente o tarjeta chip puede ser un criptoprocesador seguro pequeño incrustado en una tarjeta del tamaño de una tarjeta de crédito o en una tarjeta aún más pequeña, tal como una tarjeta SIM para teléfonos móviles. Una tarjeta inteligente no contiene usualmente una batería, sino que la energía se suministra mediante un lector/grabador de tarjetas, es decir, mediante un dispositivo de lectura y/o grabación para controlar la función de la tarjeta inteligente leyendo datos de la tarjeta inteligente o grabando datos en la tarjeta inteligente.

Un dispositivo de tarjeta inteligente se usa comúnmente en las áreas de finanzas, de acceso de seguridad y de transporte. Las tarjetas inteligentes contienen usualmente procesadores de alta seguridad que funcionan como medio de almacenamiento seguro de datos tales como los datos del titular de la tarjeta (por ejemplo, el nombre, el número de cuenta o el número de puntos de fidelidad acumulados). El acceso a estos datos solo es posible cuando se inserta la tarjeta en un terminal de lectura/grabación.

Es una tarea difícil permitir la integración de una función de interfaz de usuario directamente en tarjetas inteligentes. Por ejemplo, una pantalla puede estar integrada en una tarjeta inteligente para visualizar información a un usuario. O pueden incluirse botones en la tarjeta inteligente para permitir a un usuario introducir datos.

Las tarjetas inteligentes se diseñaron conscientemente sin una interfaz hombre-máquina que proporcionara la capacidad de interacción del usuario. La falta de soporte para la interacción del usuario se refleja en el diseño del hardware y en el diseño del software (sistema operativo) de las tarjetas inteligentes conocidas.

Esta elección consciente se ha visto impulsada por la falta de tecnología para pantallas delgadas y flexibles y por los requisitos estrictos de seguridad planteados por las tarjetas inteligentes. Hoy en día, como está disponible la tecnología para pantallas delgadas y flexibles, las normas y los procedimientos estrictos de seguridad hacen difícil la implementación de la interacción del usuario. Es difícil la introducción de la API (interfaz de programación de aplicaciones) conocida a partir de los dispositivos electrónicos del consumidor y de los dispositivos informáticos personales, ya que las normas de seguridad exigen que cada componente del sistema tenga que desarrollarse bajo la observación de procedimientos especiales, por ejemplo, con respecto a la seguridad y a la fiabilidad. Esto requiere, al desarrollar o cambiar cualquier componente del procesador de las tarjetas chip o cualquier componente de software, un largo procedimiento de certificación seguido de un largo proceso de aceptación de la industria.

En lo que sigue, en referencia a la Fig. 1, se describirá una tarjeta inteligente con la función de visualización integrada de acuerdo con la técnica anterior.

La tarjeta inteligente 100 comprende un sustrato de plástico 101 en el que se forma un circuito integrado, que proporciona la función de tarjeta inteligente.

En un dominio o procesador de seguridad 102 (un procesador de CI seguro) de la tarjeta inteligente 100, en el que se proporciona un alto nivel de seguridad, se dispone una unidad administradora de tarjetas 103 (que puede ser una unidad lógica, un procedimiento de software que se ejecuta cuando se recibe una Unidad de Datos de Protocolo de Aplicación, APDU) que se adapta para comunicarse con una pluralidad de unidades de aplicación 104, cada una de las cuales contiene datos y comandos necesarios para el servicio de diferentes aplicaciones. Se proporciona un sistema operativo 105 que contiene software para hacer funcionar la tarjeta inteligente 100. Además, se proporciona una pluralidad de unidades de accionamiento 106, que se usa cada una para accionar una unidad de hardware 107 asociada.

La tarjeta inteligente 100 está diseñada para comunicarse con un terminal de lectura y grabación de tarjetas inteligentes 108 como maestro. La comunicación entre el terminal 108 y la tarjeta inteligente 100 se realiza a través del intercambio de Unidades de Datos de Protocolo de Aplicación (APDU) de acuerdo con la norma ISO 7816. La unidad administradora de tarjetas 103 intercambia las APDUs con una particular de las unidades de aplicación 104 para llevar a cabo una correspondiente de las aplicaciones.

La estructura interna de la tarjeta inteligente 100 es similar a una arquitectura estándar (tal como un ordenador personal), que puede describirse, en el modelo por capas bien conocido. En cuanto a las unidades de hardware 107, estas unidades pueden incluir procesadores, memorias, periféricos y varios coprocesadores de cifrado/descifrado que funcionan directamente con accionadores de bajo nivel. Las unidades de accionamiento 106 forman parte de la Capa del Sistema Operativo (OSL). La OSL proporciona una abstracción de funciones en el hardware para

aplicaciones y proporciona funciones adicionales a menudo reutilizadas por las aplicaciones. El sistema operativo 105 es también responsable de la inicialización del chip durante el encendido.

En la parte superior del sistema operativo, pueden ejecutarse las aplicaciones específicas del proveedor que se muestran esquemáticamente en la Fig. 1 como unidades de aplicación 104. Como las tarjetas inteligentes como la tarjeta inteligente 100 se usan comúnmente con terminales como el terminal de lectura y grabación de tarjetas inteligentes 108, se despliega un maestro-esclavo como comportamiento de comunicación. Esto significa que el terminal 108 inicia la comunicación con la tarjeta inteligente 100 que envía Unidades de Datos de Protocolo de Aplicación (APDU) al procesador 102. El administrador de tarjetas 103 que usa el campo de dirección en la APDU puede reconocer a qué unidad de aplicación 104 debe enviarse. La aplicación dirigida, después de la recepción de esa información, ejecuta la acción solicitada y, a cambio, responde con estado/datos al terminal 108. Este esquema de comunicación requiere que, para las aplicaciones complejas, el terminal 108 y la tarjeta inteligente 100 tengan que almacenar el estado real de comunicación. Además de los componentes descritos y de su función, la tarjeta inteligente 100 comprende extensiones para permitir una función de interfaz de usuario de la tarjeta inteligente 100.

Para este propósito, en una porción de la tarjeta inteligente 100, que no se relaciona con el procesador 102 (dominio seguro), se proporcionan botones 112 y una pantalla 113. Con el fin de permitir a un usuario interactuar con la tarjeta inteligente 100 a través de la introducción de comandos mediante los botones 112 y a través de la producción de información en la pantalla 113, existe una conexión entre los botones 112, la pantalla 113 y una unidad de interfaz de botón/pantalla 111 dispuestas en el nivel de las unidades de hardware 107. Además, una unidad de accionamiento de botón/pantalla 110 se proporciona en el nivel de las unidades de accionamiento 106 para permitir a un usuario percibir visualmente los datos que se visualizan en la pantalla 113. En la tarjeta inteligente 100 mostrada en la Fig. 1, una función de visualización o interfaz de usuario se proporciona por la pantalla 113 y por los botones 112. Además, es necesaria una extensión o adaptación del sistema operativo 105, que se muestra esquemáticamente como extensión del sistema operativo 109 en la Fig. 1.

Mientras que los bloques estándar de la tarjeta inteligente 100 se muestran con líneas continuas, los bloques adicionales, que son necesarios para la función de entrada/salida, se marcan con líneas de puntos. Puede observarse que se han añadido la unidad de accionamiento de botón/pantalla 110, la unidad de interfaz de botón/pantalla 111, los botones 112 y la pantalla 113, así como la extensión del sistema operativo 109, y el sistema operativo 105 se han extendido con funciones para proporcionar la API de la función de visualización a las aplicaciones realizadas de acuerdo con las unidades de aplicación 104.

Sin embargo, la implementación de la tarjeta inteligente 100 de acuerdo con la Fig. 1 tiene algunos inconvenientes. En primer lugar, el sistema operativo 105 requiere la modificación en forma de extensión del sistema operativo 109. Esto causa costes de desarrollo y costes de certificación. Además, debido a las modificaciones que interfieren en el procesador 102 (el dominio seguro) de la tarjeta inteligente 100, se producen riesgos de seguridad potenciales.

En segundo lugar, además de adiciones a los accionadores del hardware, tiene que definirse un modo adicional de uso para la tarjeta inteligente 100, lo que difiere del modo nativo maestro-esclavo. Este modo adicional puede usarse cuando la tarjeta inteligente 100 se inicia fuera del terminal (el llamado "modo autónomo") para responder a un usuario que presione los botones 112 y para visualizar la información. Esto afecta a la arquitectura del sistema de la tarjeta inteligente 100 y trae una amenaza adicional para la seguridad, lo que requiere una cualificación adicional.

En tercer lugar, las unidades de aplicación 104 necesitan modificarse para incorporar una función de entrada/salida. Esto es difícil de lograr para los estándares establecidos y aceptados conocidos como EMV ("Europay, Mastercard, VISA", un estándar para aplicaciones de tarjetas financieras de crédito/débito) o CEPS ("Especificación de Monedero Electrónico Común", un estándar para las aplicaciones de monedero electrónico) y requeriría una reestandarización. En cuarto lugar, el dispositivo de tarjeta inteligente (chip) requiere tener adicionalmente una interfaz de hardware, en concreto la interfaz de botón/pantalla 111, para comunicarse con los botones 112/la pantalla 113 y con el accionador de botón/pantalla 110, respectivamente. No puede desearse dicha interfaz debido a las amenazas de seguridad.

El documento JP 2001-331771 divulga una tarjeta de CI con función de visualización automática, en la que se usa en común una línea de señal para una comunicación entre un lector/grabador y un microcontrolador como línea de señal para transferir datos a un accionador de pantalla desde el microcontrolador. De acuerdo con el documento JP 2001-331771, se proporciona una línea de reloj adicional (indicada como CLK2) entre la pantalla y el microcontrolador seguro, donde la línea de reloj adicional no se lleva a la parte externa. En otras palabras, de acuerdo con el documento JP 2001-331771, el microcontrolador controla la comunicación con la pantalla. Sin embargo, esto tiene la desventaja de que pueden producirse problemas de seguridad cuando se haga funcionar la tarjeta de CI. Además, en el documento JP 2001-331771, escribir en la pantalla solo es posible cuando la tarjeta está en un dispositivo de lectura/grabación.

El documento US 2003/0140221 divulga un soporte de datos portátil que tiene un procesador, una interfaz de tarjeta inteligente y un teclado que es parte integrante del soporte de datos, para una entrada de usuario.

El documento EP 1 004 980 divulga una tarjeta inteligente en la que puede introducirse el pin de un usuario directamente en la tarjeta inteligente cuando la tarjeta inteligente se presenta a un lector.

OBJETO Y SUMARIO DE LA INVENCION

Un objeto de la invención es operar una tarjeta inteligente de una manera segura.

Con el fin de lograr el objeto definido anteriormente, se proporcionan una tarjeta inteligente y un procedimiento de operación de una tarjeta inteligente de acuerdo con las reivindicaciones independientes.

De acuerdo con un modo de realización ejemplar de la invención, se proporciona una tarjeta inteligente que comprende un procesador. La tarjeta inteligente comprende además una interfaz de dispositivo de lectura/grabación diseñado para una comunicación entre el procesador y un dispositivo de lectura y/o grabación y una unidad de entrada y/o salida de usuario diseñada para iniciar una comunicación entre un usuario y el procesador a través de la interfaz de dispositivo de lectura y/o grabación

Además, de acuerdo con otro modo de realización ejemplar de la invención, se proporciona un procedimiento de funcionamiento de una tarjeta inteligente. El procedimiento comprende las etapas de hacer funcionar un procesador de la tarjeta inteligente, de permitir una comunicación entre el procesador y un dispositivo de lectura/grabación a través de una interfaz de dispositivo de lectura y/o grabación de la tarjeta inteligente y de iniciar, por medio de una unidad de entrada y/o salida de usuario, una comunicación entre un usuario y el procesador a través de la interfaz de dispositivo de lectura y/o grabación. Cabría destacar que las etapas mencionadas anteriormente no tienen que realizarse necesariamente en el orden dado.

El término "tarjeta inteligente" puede indicar particularmente una tarjeta chip del tipo de contacto o una tarjeta chip sin contacto, que puede comprender un procesador seguro para proporcionar una o más aplicaciones.

El término "procesador" indica particularmente una unidad de control o una unidad de administración de tarjetas inteligentes, como por ejemplo un microprocesador o una unidad de procesamiento central (CPU). Dicho procesador se fabricó quizás como un circuito integrado monolíticamente, por ejemplo producido con la tecnología de los semiconductores (particularmente en silicio).

El término "dispositivo de lectura/grabación" indica particularmente un dispositivo externo (con respecto a la tarjeta inteligente) para controlar la función de la tarjeta inteligente leyendo datos de la tarjeta inteligente y/o grabando datos en la tarjeta inteligente.

El término "unidad de entrada y/o salida de usuario" indica particularmente un dispositivo que puede proporcionarse al menos parcialmente en la tarjeta inteligente y que permite a un usuario interactuar con la tarjeta inteligente. Particularmente, dicha "unidad de entrada y/o salida de usuario" puede permitir a un usuario transmitir datos unidireccional o bidireccionalmente y/o recibir datos del procesador, que pueden relacionarse con una aplicación particular proporcionada por la tarjeta inteligente.

Una "interfaz" puede proporcionar particularmente una conexión o un acceso a un componente particular de un sistema de comunicación.

La tarjeta inteligente de acuerdo con la invención puede ser capaz de proporcionar una aplicación y el procesador de la tarjeta inteligente puede estar diseñado para hacerse funcionar para proporcionar la aplicación. El término "aplicación" indica cualquier función o servicio, que sea proporcionable por la tarjeta inteligente, en la que el procesador puede proporcionar los recursos computacionales para llevar a cabo dicha aplicación.

Los rasgos característicos de acuerdo con la invención tienen particularmente la ventaja de que se proporciona una tarjeta inteligente que, además de llevar a cabo opcionalmente al menos una aplicación particular, proporciona una interfaz de usuario (por ejemplo una pantalla y/o un teclado) que está conectada a un procesador a través de la misma ruta de señal que la que se usa para una conexión del procesador a un dispositivo de lectura y/o grabación para leer información de la tarjeta inteligente y/o para grabar información en la tarjeta inteligente. La comunicación entre un usuario por un lado (usando interactivamente la unidad de entrada/salida de usuario como interfaz de usuario) y el procesador por otro lado puede iniciarse mediante la interfaz de dispositivo de lectura y/o grabación. En otras palabras, la comunicación entre la interfaz de usuario y el procesador puede controlarse desde el lado del usuario, en lugar de desde el lado del procesador. Como consecuencia, desde el punto de vista del procesador (que puede situarse en una porción segura de la tarjeta inteligente), una comunicación con un terminal (maestro) de lectura/grabación puede realizarse de una manera similar o idéntica a una comunicación con la unidad (maestro) de entrada/salida de usuario. Por lo tanto, el procesador de la tarjeta inteligente de acuerdo con el modo de realización descrito de la invención puede actuar como esclavo en los canales de comunicación con el terminal de lectura y/o grabación y los canales de comunicación con la unidad (maestro) de entrada y/o salida de usuario. Por lo tanto, esta comunicación mantiene la porción segura que aloja el procesador sin cambios, proporcionando de esta manera un alto nivel de seguridad.

En contraste fundamental con conceptos conocidos (por ejemplo, de acuerdo con el documento JP 2001-331771), la tarjeta inteligente de acuerdo con el modo de realización ejemplar descrito de la invención no usa el procesador para controlar los medios de entrada/salida (por ejemplo el teclado o la pantalla). En su lugar, los medios de entrada/salida inician ellos mismos activamente la comunicación con el procesador, si se desea por un usuario. En otras palabras, los medios de entrada/salida de acuerdo con la invención funcionan como nodo maestro y las funciones del procesador como nodo esclavo en este canal de comunicación. Efectivamente, los medios de entrada/salida emulan un terminal o un dispositivo de lectura y/o grabación.

Como la comunicación entre el dispositivo de lectura y/o grabación por un lado y la tarjeta inteligente por otro lado se inicializa normalmente (por ejemplo en una aplicación de Bancomat) mediante el dispositivo de lectura y/o grabación, la tarjeta inteligente no reconoce esencialmente la diferencia entre una comunicación con un terminal de lectura y/o grabación o una comunicación con una interfaz de usuario (por ejemplo como un teclado o una pantalla). Esto tiene la ventaja de que todos los elementos de seguridad que (ya) se proporcionan para la comunicación entre la interfaz de lectura y/o grabación por un lado y la tarjeta inteligente por otro lado, son también utilizables para la comunicación entre la tarjeta inteligente (o más bien entre el procesador de la tarjeta inteligente) y la unidad de entrada y/o salida de usuario. Por lo tanto, puede prescindirse de una certificación costosa de la tarjeta inteligente modificada de acuerdo con la invención.

El sistema de acuerdo con la invención permite acoplar una o más unidades de entrada y/o salida de usuario, como un teclado o una pantalla, al procesador de una tarjeta inteligente de una manera sencilla pero muy eficiente. De acuerdo con la arquitectura descrita, el procesador está firmemente protegido contra manipulaciones, de modo que las aplicaciones críticas de seguridad (por ejemplo, tarjetas de crédito o monedero electrónico) pueden realizarse con fiabilidad con esta tarjeta inteligente. Adicionalmente, pueden realizarse por lo tanto aplicaciones de entrada y/o salida de usuario sin riesgos de seguridad. La invención permite acoplar una unidad de entrada y/o salida de usuario a un procesador sin el debilitamiento de sus mecanismos de seguridad. Como la provisión de una interfaz de usuario de acuerdo con la invención no requiere modificaciones en la mayor parte de las tarjetas inteligentes existentes, la tarjeta inteligente de acuerdo con la invención puede construirse con poco esfuerzo.

De acuerdo con un aspecto de la invención, una interfaz externa de una tarjeta inteligente, que proporciona normalmente comunicación entre una tarjeta inteligente y un terminal, se usa simultáneamente para la integración de componentes adicionales, como una pantalla o un teclado, en una tarjeta inteligente. Una comunicación entre las partes existentes situadas en el área segura y las partes nuevas, que pueden proporcionarse en el exterior del área segura, puede tener lugar a través de un externo que forme parte de la tarjeta inteligente, pero que se sitúe en el exterior del área segura.

Por lo tanto, pueden permanecer sin cambios partes grandes (por ejemplo una aplicación heredera de alta seguridad) de una tarjeta inteligente existente, ya que un protocolo de comunicación para una comunicación entre el procesador y la interfaz de usuario puede ser el mismo que el usado para la comunicación entre el procesador y el terminal.

De forma ventajosa, el sistema de acuerdo con la invención permite una integración rápida de, por ejemplo, la función de visualización en los sistemas de tarjetas inteligentes existentes sin afectar la seguridad total del sistema. Además, es posible la compatibilidad retroactiva con los sistemas existentes.

De acuerdo con un aspecto de la invención, se proporciona un procedimiento para la integración de la función de interacción del usuario en una tarjeta inteligente. Para este propósito, la interfaz externa de una tarjeta inteligente, que permite normalmente una comunicación de datos entre la tarjeta inteligente y un terminal de lectura/grabación, se usa para la conexión de componentes adicionales a la tarjeta inteligente.

De acuerdo con un aspecto de la invención, una unidad de accionamiento de pantalla puede tomar el papel de dispositivo maestro en comunicación, emulando un terminal ordinario de la norma ISO 7816. El controlador de pantalla de acuerdo con la invención puede comunicarse con el circuito integrado seguro (CI) o procesador de una forma estándar usando APDU de protocolo de nivel más alto (Unidades de Datos de Protocolo de Aplicación). Por lo tanto, el controlador de pantalla se considera, mediante el CI seguro, como un terminal ordinario. Por lo tanto, el sistema de acuerdo con la invención proporciona una forma muy segura de conectar la pantalla a un circuito integrado seguro, ya que no se requiere ninguna modificación del hardware del circuito integrado seguro ni del software (de bajo nivel) del circuito integrado seguro.

En contraste con el sistema de acuerdo con la invención, la tarjeta del CI de acuerdo con el documento JP 2001-331771 requiere una línea de reloj adicional desde el CI seguro hasta el controlador de pantalla. Además, es necesario un protocolo de propietario para la comunicación entre el CI seguro y el controlador de pantalla de acuerdo al documento JP 2001-331771. El sistema de acuerdo con el documento JP 2001-331771 se basa en la suposición de que, o bien el terminal o el CI seguro es un maestro en la comunicación y el controlador de pantalla es siempre un esclavo (es decir, no inicia la comunicación).

La tarjeta inteligente de acuerdo con la invención puede implementarse de acuerdo con una arquitectura en la que la comunicación entre el dispositivo de la interacción del usuario y el procesador es una arquitectura maestro-esclavo. En el marco de dicha comunicación, el dispositivo de interacción del usuario puede tomar el papel de maestro (es decir, puede iniciar una comunicación enviando un mensaje correspondiente al procesador) y el procesador puede tomar el papel de esclavo (es decir, puede enviar una respuesta al dispositivo de interacción del usuario solo en el caso de un mensaje enviado previamente desde el dispositivo de la interacción del usuario).

La tarjeta inteligente de acuerdo con la invención puede hacerse funcionar en un denominado "modo autónomo", es decir, puede hacerse funcionar también en ausencia de un terminal de lectura/grabación. En este modo autónomo, un usuario puede usar el dispositivo de interacción del usuario para comunicarse con el procesador independientemente de la presencia o ausencia de un terminal de lectura/grabación. Además, las herramientas de desarrollo estándar conocidas (SDE) pueden usarse para el desarrollo de aplicaciones.

Se menciona que la tarjeta inteligente de acuerdo con la invención puede incluir una o más unidades de entrada y/o salida de usuario y puede adaptarse para una comunicación entre el procesador y uno o más dispositivos de lectura y/o grabación.

Haciendo referencia a las reivindicaciones dependientes, se describirán a continuación modos de realización ejemplares adicionales de la invención. Estos modos de realización se aplican también al procedimiento de funcionamiento de una tarjeta inteligente.

La tarjeta inteligente puede estar diseñada de modo que un protocolo de comunicación para una comunicación entre un dispositivo de lectura y/o grabación y el procesador es igual a un protocolo de comunicación para una comunicación entre un usuario y el procesador. En otras palabras, los medios de entrada y/o salida pueden disponerse de manera que se comunican con el procesador esencialmente de la misma forma que lo hace el terminal. Esto permite construir el procesador de una manera muy simple, ya que implementar un único protocolo de comunicación es suficiente para comunicarse con un terminal de lectura y/o grabación por un lado y un usuario a través de una unidad de entrada y/o salida de usuario por otro lado.

La tarjeta inteligente puede comprender al menos un elemento de conexión por cable de conexión de un dispositivo de lectura y/o grabación con el procesador, en el que al menos una parte de al menos un elemento de conexión por cable puede formar una conexión (exclusivamente o no exclusivamente) de la unidad de entrada/salida de usuario con el procesador. De acuerdo con el modo de realización descrito, los mismos conductores o cables o contactos pueden usarse para conectar el dispositivo de lectura y/o grabación con el procesador, y para conectar la interfaz de usuario con el procesador. Tomando esta medida, es posible una construcción sencilla y con ahorro de espacio de la tarjeta inteligente debido a un uso sinérgico del cableado. Sin embargo, adicional o alternativamente a la provisión de un elemento de conexión por cable, también es posible la operación sin contacto entre el CI seguro y el controlador de pantalla inteligente de acuerdo con la invención.

La tarjeta inteligente puede estar diseñada de tal manera que puede realizarse una comunicación entre la unidad de entrada y/o salida de usuario y el procesador de acuerdo con la norma ISO 7816. Se hace particular referencia a este respecto a las partes de la norma ISO 7816 que se relacionan con la definición y el uso de Unidades de Datos de Protocolo de Aplicación (APDU). La serie o la norma ISO 7816 no sólo define las formas físicas de la tarjeta inteligente y las posiciones y las formas de sus conectores eléctricos, sino también los protocolos de comunicación y los voltajes de alimentación que van a aplicarse a esos conectores, una función y un formato de los comandos enviados a la tarjeta inteligente y de la respuesta devuelta por la tarjeta inteligente. La comunicación entre el dispositivo de lectura y/o grabación por un lado y el procesador por otro lado puede llevarse a cabo, de acuerdo con este modo de realización, de acuerdo con el mismo estándar industrial que la comunicación entre la unidad de entrada/salida de usuario por un lado y el procesador por el otro lado, que exige una arquitectura de comunicación simple.

Además, la tarjeta inteligente puede estar diseñada para una comunicación entre la unidad de entrada/salida de usuario y el procesador por medio de una transmisión de al menos una Unidad de Datos de Protocolo de Aplicación (APDU). Una Unidad de Datos de Protocolo de Aplicación puede definirse como una unidad de comunicación entre una tarjeta chip y un dispositivo de lectura/grabación de acuerdo con la norma ISO 7816. Existen APDUs de comandos, que transmiten comandos entre dos entidades, y APDUs de respuestas, que transmiten una respuesta a un comando. El esquema de comunicación se las APDUs se relaciona con el conocido modelo OSI ("Interconexión de Sistemas Abiertos") y, específicamente para las tarjetas inteligentes, el concepto de las APDUs se describe en la norma ISO 7816-4 a la que se hace referencia explícita en el presente documento.

La tarjeta inteligente puede dividirse en una porción de seguridad, en la que se proporciona una función de seguridad, y una porción restante, en la que la porción de seguridad incluye el procesador y en la que la porción restante incluye la unidad de entrada y/o salida de usuario. La porción de seguridad puede ser una porción de la tarjeta inteligente en la que se disponen los componentes de la tarjeta inteligente que contienen datos que son aspectos fundamentales de seguridad relativos. El procesador, de acuerdo con el modo de realización descrito, reside en esta porción de seguridad. Sin embargo, situando la unidad de entrada y/o salida en la porción restante

(que no tiene, o a un nivel más bajo, medidas de seguridad), el procesador se proporciona en un área segura y los medios de entrada y/o salida se proporcionan en un área menos segura. Tomando esta medida, se mejora la seguridad general, ya que el acceso de un usuario a través de la unidad de entrada y/o salida de usuario no influye en la seguridad dentro de la porción segura.

5 La unidad de entrada y/o salida de usuario pueden incluir al menos uno del grupo que consiste en una pantalla, un teclado, un botón, un medio de entrada y/o salida acústico y un sensor de identificación del usuario. En general, la unidad de entrada y/o salida del usuario puede incluir cualquier elemento que permita a un usuario humano influir en la función de la tarjeta inteligente o a informarse de una manera perceptible sobre dicha función. Particularmente, la

10 unidad de entrada y/o salida de usuario puede incluir medios que permitan a un usuario proporcionar datos o comandos o mensajes al procesador, para controlar por lo tanto la función de la(s) aplicación(es) que se ejecute(n) en la tarjeta inteligente. Por otro lado, esto incluye también proporcionar datos o mensajes o la información desde el procesador al usuario para informar al usuario sobre un estado de una aplicación que se ejecute en la tarjeta inteligente.

15 Por ejemplo, un usuario puede identificarse a sí mismo introduciendo una contraseña usando un teclado o un botón. O una tarjeta de pago o de crédito restante puede visualizarse a un usuario a través de una pantalla.

20 La unidad de entrada y/o salida de usuario pueden incluir cualquier tipo de medios de visualización adecuados. Por ejemplo, una pantalla flexible de acuerdo con la tecnología de Sistemas de Pantallas Flexibles Philips puede implementarse con una tarjeta inteligente. La interfaz de usuario puede consistir entonces en una pequeña pantalla y varios botones, que permiten una interacción simple basada en el menú del usuario con las aplicaciones que residen en la tarjeta inteligente.

25 Además, puede proporcionarse un teclado en la tarjeta inteligente a través del que un usuario puede introducir comandos o mensajes que vayan a enviarse al procesador. Un resultado similar puede lograrse proporcionando uno o más botones en la tarjeta inteligente. Particularmente, un teclado puede realizarse como una pluralidad de botones.

30 Es también posible que se proporcione un sensor acústico como un micrófono, en particular, un micrófono MEMS, en la tarjeta inteligente que permita a un usuario proporcionar la tarjeta inteligente con comandos acústicos como "¡visualizar mi crédito actual!" (si es necesario o se desea en el marco de un sistema de reconocimiento de voz). Además, puede proporcionarse una unidad de salida acústica, en particular un altavoz MEMS, en la tarjeta inteligente de modo que, por ejemplo, una voz humana producir información solicitada a un usuario de manera

35 audible, como "su crédito actual es de 100 €".

Además, la unidad de entrada y/o salida de usuario puede incluir un sensor de identificación del usuario, es decir, un sensor que permita que la tarjeta inteligente decida si un usuario está autorizado para acceder a la tarjeta inteligente o no. Dicho sensor de identificación puede ser un sensor de huella digital, un sensor de retina, un sensor de ADN, o similar.

40

La unidad de entrada y/o salida de usuario puede realizarse en el software y/o en el hardware. La función de entrada y/o salida de usuario de acuerdo con la invención puede realizarse por lo tanto mediante un programa informático, es decir, mediante el software, o usando uno o más circuitos de optimización electrónicos especiales, es decir, en el

45 hardware, o en forma híbrida, es decir, por medio de componentes de software y componentes de hardware.

En términos generales, la unidad de entrada y/o salida de usuario pueden comprender elementos que permitan a un usuario percibir datos, que se proporcionen por la tarjeta inteligente. Por otro lado, la unidad de entrada y/o salida de usuario puede incluir elementos que permitan a un usuario traducir comandos humanos en forma electrónica.

50

La tarjeta inteligente de acuerdo con la invención puede comprender además al menos una unidad de aplicación capaz de proporcionar los datos relativos a una aplicación correspondiente, pero incapaz de proporcionar los datos relativos a la aplicación correspondiente en un formato que sea producible (por ejemplo visualizable) por la unidad de entrada y/o salida de usuario (por ejemplo una pantalla). La tarjeta inteligente puede comprender además una

55 unidad de aplicación de interacción del usuario (que podría indicarse también como unidad de conversión de datos de aplicación) que sea al menos capaz de convertir los datos proporcionados por la unidad de aplicación en un formato que sea producible por la unidad de entrada y/o salida de usuario. Una comunicación entre la unidad de aplicación y la unidad de aplicación de interacción del usuario puede mediar por la unidad de entrada y/o salida de usuario, actuando entonces como espejo de datos. Este modo de realización permite extender una unidad de

60 aplicación ya existente, que puede situarse en la porción de seguridad pero que es incapaz de proporcionar los datos visualizables. La extensión es la unidad de aplicación de interacción del usuario (o unidad de conversión de datos de aplicación), que puede cumplir la función de convertir los datos proporcionados por la unidad de aplicación en un formato visualizable. También, la unidad de conversión de datos de aplicación puede proporcionarse en la porción segura. Además de la función de conversión, la unidad de aplicación de interacción del usuario puede

65 cumplir opcionalmente una o más funciones adicionales, es decir, no se limita a la conversión de datos en un formato visualizable.

La unidad de aplicación de interacción del usuario de la tarjeta inteligente puede adaptarse para tomar el papel de maestro en relación con una comunicación con la unidad de aplicación. En otras palabras, cuando la unidad de aplicación de interacción del usuario se comunica con la unidad de aplicación, entonces la unidad de aplicación de interacción del usuario puede controlar esta comunicación con la unidad de aplicación similar a un esclavo, y puede iniciar particularmente dicha comunicación.

Una comunicación entre la unidad de aplicación y la unidad de aplicación de interacción del usuario puede realizarse de forma ventajosa usando la unidad de entrada y/o salida de usuario, que puede situarse en el exterior de la porción segura. En otras palabras, la unidad de entrada y/o salida del usuario pueden funcionar como espejo enviando simplemente datos de la unidad de aplicación a la unidad de conversión de datos de aplicación, o viceversa.

La tarjeta inteligente puede adaptarse de manera que se cifra un mensaje transmitido entre la unidad de aplicación y la unidad de aplicación de interacción del usuario. Tomando esta medida, se obtiene un sistema de comunicación muy seguro, ya que, incluso cuando se media un mensaje a través de un área no segura, el cifrado garantiza que se mantiene un alto nivel de seguridad.

La unidad de entrada y/o salida de usuario que media un mensaje transmitido entre la unidad de aplicación y la unidad de aplicación de interacción del usuario puede ser incapaz de descifrar el mensaje. Como consecuencia, se mantiene un alto nivel de seguridad, ya que el medio de mediación carece de cualquier capacidad de descifrar mensajes mediados.

La unidad de aplicación puede contener un código que se relacione con una llamada "aplicación heredada". Este término indica particularmente una aplicación que se ha desarrollado antes de que estuviera disponible la función de visualización. Se considera que dichas aplicaciones están bien establecidas y estandarizadas (como EMV o CEPS), pero que no proporcionan la función de visualización. Dicho uso de la aplicación heredada se combina, de acuerdo con el modo de realización descrito, con una aplicación de pantalla, que puede situarse también en el área segura, como la aplicación heredada. Un controlador de pantalla inteligente de la unidad de entrada y/o salida de usuario puede considerarse como externo en el esquema de comunicación, que media entre la aplicación heredada y la aplicación de pantalla.

Por ejemplo, la aplicación de pantalla puede enviar datos (así como una petición para enviar datos a la aplicación heredada) al controlador de pantalla inteligente. El controlador de pantalla inteligente puede transmitir los datos como se solicite. La aplicación heredada puede responder de una forma usual, tal como comunicándose con un terminal. El controlador de pantalla inteligente puede enviar la respuesta a la aplicación de pantalla. Entonces, la aplicación de pantalla puede solicitar al controlador de pantalla inteligente visualizar los datos recibidos.

La unidad de aplicación y la unidad de aplicación de interacción del usuario (unidad de conversión de datos de aplicación) pueden situarse en la porción segura. De acuerdo con dicha disposición, los datos se transmiten desde la unidad de aplicación en el dominio seguro a través del controlador de pantalla inteligente situado en el dominio no seguro a la unidad de aplicación de interacción del usuario situada en la porción segura, o viceversa. Sin embargo, la unidad de entrada y/o salida de usuario solo refleja los datos desde una de las unidades descritas a la otra sin procesarlas, de modo que no se produce ningún problema de seguridad. El hecho es que pueden enviarse los datos de manera cifrada, y no se lleva a cabo ningún descifrado de los datos mediante el controlador de pantalla inteligente.

La comunicación entre la unidad de aplicación y la unidad de aplicación de interacción del usuario puede incluir la transmisión de al menos una Unidad de Datos de Protocolo de Aplicación (APDU). Por lo tanto, el protocolo de comunicación para esta función de espejo puede ser el mismo que para la comunicación entre la unidad de entrada y/o salida de usuario y el procesador o entre el dispositivo de lectura y/o grabación y el procesador.

Particularmente, la unidad de aplicación puede ser una unidad de aplicación heredada, es decir, una unidad de aplicación que solo proporciona la aplicación sin proporcionar una función de visualización sofisticada.

Las aplicaciones ejemplares de la tarjeta inteligente de acuerdo con la invención incluyen el uso como tarjeta de crédito, como una tarjeta SIM para un teléfono móvil, como una tarjeta de autorización para la televisión de pago, como una tarjeta de identificación y control de acceso, como un billete de transporte público, etc.

La tarjeta inteligente de acuerdo con la invención puede realizarse como tarjeta inteligente del tipo de contacto o como una tarjeta inteligente sin contacto. En una tarjeta inteligente del tipo de contacto, un chip de circuito integrado o de semiconductor que incluye el procesador puede reconocerse por los contactos conductores eléctricamente. En una tarjeta inteligente del tipo sin contacto, que puede indicarse también como tarjeta inteligente sin contacto, el chip puede comunicarse con el lector/grabador de tarjetas a través de la tecnología de inducción autoalimentada inalámbrica (particularmente intercambiando ondas electromagnéticas, por ejemplo en el dominio de alta frecuencia, entre el lector/grabador de tarjetas y la tarjeta inteligente). La tecnología de las tarjetas inteligentes sin contacto de

acuerdo con la invención puede realizarse o combinarse con la tecnología de RFID (identificación por radiofrecuencia).

A continuación, se describirá un modo de realización ejemplar del procedimiento de funcionamiento de una tarjeta inteligente. Este modo de realización se aplica también a la tarjeta inteligente de acuerdo con la invención.

La comunicación entre el usuario y el procesador a través de la interfaz de dispositivo de lectura y/o grabación puede iniciarse por medio de la unidad de entrada y/o salida de usuario que se dispone en la tarjeta inteligente. De acuerdo con este modo de realización, la unidad de entrada y/o salida de usuario se sitúa en la tarjeta inteligente.

Los aspectos definidos anteriormente y los aspectos adicionales de la invención son evidentes a partir de los ejemplos de modos de realización que van a describirse a continuación y se explican con referencia a estos ejemplos de modo de realización.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La invención se describirá con más detalle a continuación con referencia a ejemplos de modo realización, pero a la que la invención no está limitada.

La Fig.1 muestra una tarjeta inteligente de acuerdo con la técnica anterior,

La Fig. 2 muestra una tarjeta inteligente de acuerdo con otro modo de realización de la invención,

La Fig. 3 muestra una tarjeta inteligente de acuerdo con otro modo de realización de la invención,

La Fig. 4 muestra una parte de una tarjeta inteligente de acuerdo con un modo de realización ejemplar de la invención que ilustra una función de espejo de una unidad de entrada y/o salida de usuario.

DESCRIPCIÓN DE LOS MODOS DE REALIZACIÓN

La ilustración en el dibujo es esquemática. En diferentes dibujos, se proporcionan elementos similares o idénticos con los mismos signos de referencia.

En lo que sigue, en referencia a la Fig. 2, se describirá en detalle una tarjeta inteligente 200 de acuerdo con un modo de realización ejemplar de la invención. En cuanto a los componentes similares como se usan en la Fig. 1, se hace también referencia a la descripción anterior de la Fig. 1.

Los diversos componentes de la tarjeta inteligente 200 se proporcionan sobre y/o en un sustrato de plástico 201. El tamaño de la tarjeta inteligente 200 puede ser el de una tarjeta de crédito convencional. La tarjeta inteligente 200 mostrada en la Fig. 2 es capaz de proporcionar una pluralidad de aplicaciones (relacionándose cada una de las cuales con una particular de las unidades de aplicación 204). La tarjeta inteligente 200 comprende un microprocesador 202, que está diseñado para llevar a cabo cálculos y funciones de control en el marco del servicio de las diferentes aplicaciones.

Se proporciona un terminal de lectura y grabación de tarjetas 208 (indicado también como un lector/grabador de tarjetas) para leer la información almacenada o generada en la tarjeta inteligente 200 o para programar, o introducir, datos de entrada externamente en la tarjeta inteligente 200. Una interfaz de dispositivo de lectura y grabación 213 de la tarjeta inteligente 200 está diseñada para una comunicación bidireccional entre el dispositivo de lectura y grabación de tarjetas 208 y el microprocesador 202.

Además, se proporciona una unidad de entrada y salida de usuario 212 (unidad E/S) en la tarjeta inteligente. La unidad de entrada y salida de usuario 212 puede iniciar activamente una comunicación entre un usuario humano (no mostrado) y el microprocesador 202 a través de la interfaz de dispositivo de lectura y grabación de la tarjeta inteligente 213. Por lo tanto, en el marco de una comunicación entre la unidad de entrada y salida de usuario 212 por un lado y el microprocesador 202 por otro lado, la unidad de entrada y salida de usuario 212 juega el papel de maestro y el microprocesador 202 juega el papel de esclavo. Esta asignación de función es atípica, ya que, en el campo de la electrónica, es usualmente un microcontrolador el que juega el papel de maestro. Sin embargo, esta asignación de función tiene la ventaja fundamental de que mejora la seguridad de la transferencia de datos entre los diferentes componentes de la tarjeta inteligente 200.

La unidad de entrada y salida de usuario 212 comprende un controlador de pantalla inteligente 211 que se realiza, de acuerdo con el modo de realización descrito, en el hardware, y que coordina la comunicación entre el procesador 202 por un lado y el hardware de pantalla 210 y los botones 209 (como componentes adicionales de la unidad de entrada y salida de usuario 212) por otro lado.

Un usuario puede usar los botones 209 para introducir comandos que vayan a transportarse, a través del controlador de pantalla inteligente 211 y de la interfaz 213, al procesador 203 para el procesamiento adicional de los mismos en

el contexto de una de las aplicaciones asignadas a las unidades de aplicación 204. Por ejemplo, una aplicación puede ser una aplicación de tarjeta financiera de crédito/débito, o similar. Además, los datos relativos a una aplicación realizada por la tarjeta inteligente 200 pueden transmitirse desde el procesador 202 a través de la interfaz 213 y el controlador de pantalla inteligente 211 a un hardware de pantalla 210 que visualiza la información de audio y/o de vídeo correspondiente a un usuario humano.

Como puede verse en la Fig. 2, la tarjeta inteligente 200 se divide en una porción de seguridad o procesador 202 y una porción de no seguridad - restante -. El microprocesador 202 que incluye la pluralidad de unidades de aplicación 204 reside en la porción de seguridad. Además, se proporciona un sistema operativo 205, que puede comprender componentes de software para operar la tarjeta inteligente 200. Además, se proporcionan una pluralidad de unidades de accionamiento 206 y una pluralidad de unidades de hardware 207. Cada una de las unidades de hardware 207 puede incluir componentes como un subprocesador, una memoria, un periférico, o un subprocesador de cifrado/descifrado.

El protocolo de comunicación usado para una comunicación entre el terminal de lectura y grabación de tarjetas inteligentes 208 y el microprocesador 202 es igual a un protocolo de comunicación para una comunicación entre un usuario (no mostrado) que hace funcionar la unidad de entrada y salida de usuario 212 y el microprocesador 202. Ambos canales de comunicación se realizan mediante un intercambio de Unidades de Datos de Protocolo de Aplicación (APDU) y de acuerdo con la norma ISO industrial 7816.

La unidad de entrada y salida de usuario 212 incluye la pantalla 210 (que puede realizarse en base a la tecnología de Sistemas de Pantallas Flexibles de Philips) y los botones 209. De acuerdo con el modo de realización mostrado en la Fig. 2, la unidad de entrada y salida de usuario 212 se realiza como una unidad de hardware.

La tarjeta inteligente 200 es un dispositivo de alta velocidad, seguro y de bajo coste en el que el mundo de la alta seguridad de los dispositivos de tarjetas inteligentes y del software correspondiente permanece esencialmente sin cambios (y por lo tanto seguro e invulnerable a los ataques potenciales), pero dicha tarjeta inteligente ha incluido una posibilidad para la aplicación de tarjeta que permite la interacción del usuario a través de la infraestructura de seguridad existente. Aunque el modo de realización mostrado en la Fig. 2 se centra en una pantalla 210 y en los botones 209 conectados al hardware de la tarjeta inteligente 200, el sistema de acuerdo con la invención puede conectarse también a otros aparatos electrónicos en la tarjeta, como por ejemplo lectores de huellas dactilares, o similar.

En lo que sigue, se describirá la conexión del hardware/software de la función de visualización a través de interfaces físicas y lógicas existentes. La Fig. 2 muestra una extensión de un sistema de tarjeta inteligente con función de visualización. En la tarjeta inteligente 200, el sistema de procesador de tarjeta inteligente (hardware y software) permanece esencialmente sin cambios y por lo tanto sigue siendo seguro. En la Fig. 2, se añade la función de E/S como unidad de entrada y salida independiente de usuario 212 al lado del procesador o dominio seguro 202 de la tarjeta inteligente 200.

El controlador de pantalla inteligente 211 se comunica con las aplicaciones de tarjetas inteligentes (o más bien con el microprocesador 202) usando una interfaz 213 de la norma ISO 7816 e intercambiando las APDU con el microprocesador 202. La comunicación entre la unidad de entrada y salida de usuario 212 y el microprocesador 202 se realiza de la misma forma que la comunicación con el terminal de lectura y grabación de tarjetas inteligentes 208. A través de la interfaz 213, el controlador de pantalla inteligente 211 puede informar a una unidad de aplicación 204, por medio de un mensaje correspondiente, de que un botón 209 se ha presionado por un usuario y le pide a la unidad de aplicación respectiva los datos que deberían visualizarse en la pantalla 210. La seguridad del sistema no se ve afectada por la adición de la unidad de entrada y salida de usuario 212, ya que el único cambio reside en aplicaciones que necesitan entender el protocolo para accionar datos en la pantalla 210. No se requieren modificaciones en otros componentes del sistema.

El controlador de pantalla inteligente 211 puede realizarse en el hardware y el software, siendo ambas realizaciones conceptualmente iguales.

La tarjeta inteligente 200 muestra un modo de realización del controlador de pantalla inteligente 211 en el hardware. Esto requiere la implementación del bloque funcional en el controlador de pantalla y las conexiones de los contactos de la norma ISO 7816 con ese controlador. El modo de realización de la Fig. 2 es muy flexible, ya que la función de visualización solo depende de un desarrollador de aplicaciones. En dicho escenario, no se necesita ninguna interfaz de hardware adicional en el microprocesador 202.

En lo que sigue, en referencia a la Fig. 3, se describirá una tarjeta inteligente 300 de acuerdo con otro modo de realización ejemplar de la invención.

En el modo de realización mostrado en la Fig. 3, el controlador de pantalla inteligente 211 se realiza en software. Por lo tanto, el controlador de pantalla inteligente 211 de la unidad de entrada y salida de usuario 302 reside en un bloque de software 304 de la tarjeta inteligente 300. El controlador de pantalla inteligente 211 contiene además los

botones 209 y el hardware de pantalla 210. Una memoria intermedia de receptor/transmisor 303 (memoria intermedia RX/TX) y una unidad cortafuegos 301 residen también en el bloque de software 304.

Realizar el controlador de pantalla inteligente 211 en el software significa que existe una función para enviar y recibir las APDU al administrador de tarjetas 203 del microprocesador 202 en forma de software por medio de llamada de función, por ejemplo a través de la memoria intermedia de receptor/transmisor 303. El controlador de pantalla inteligente 211 se hace funcionar en base a los comandos de software también. Se ejecuta en una región cortafuegos del controlador de tarjeta, completamente separado del dominio seguro 202 (de forma similar a una emulación de Philips Mifare en procesadores de tarjetas inteligentes Philips). Acciona el hardware de pantalla 210 y los botones 209 a través de una interfaz dedicada, por ejemplo a través de una interfaz en serie. Ese modo de realización de Fig. 3 no necesita, o sólo un poco, certificación.

En lo que sigue, en referencia a la Fig. 4, se describirá una porción 400 de una tarjeta inteligente de acuerdo con otro modo de realización más de la invención en la que se implementa una función de espejo de datos del controlador de pantalla inteligente. La Fig. 4 ilustra un concepto para añadir la función de visualización a aplicaciones heredadas.

Como se ve en la Fig. 4, la porción 400 comprende una unidad de aplicación de pantalla 401 que reside en la porción de seguridad o procesador 202 y una unidad de aplicación heredada 402 que reside también en la porción de seguridad o en el procesador 202. Aparte de la unidad de aplicación de pantalla 401 y de la unidad de aplicación heredada 402, se proporcionan unidades de aplicación adicionales 204 en la porción de seguridad 202. Como se describirá en lo que sigue, una comunicación entre la unidad de aplicación de pantalla 401 y la unidad de aplicación heredada 402 se realiza a través de una pluralidad de canales de transmisión 403 a 407 y se media por el controlador de pantalla inteligente 211 que actúa como espejo de datos.

El modo de realización mostrado en la Fig. 4 soluciona el problema de visualizar información de aplicaciones heredadas bien establecidas y estandarizadas (como la que se incluye en la unidad de aplicación heredada 402), por ejemplo el monedero electrónico (CEPS, Geldkarte, Chipknip). En muchos casos, dichas aplicaciones ya existentes no están diseñadas para visualizar información, como una cantidad almacenada en el monedero electrónico, en una pantalla.

Una solución clara de este problema sería añadir una función de visualización de las unidades de aplicación. Sin embargo, este enfoque requeriría un esfuerzo de desarrollo importante, seguido de certificaciones y de un largo periodo de tiempo para lograr la aceptación industrial.

Otra posible solución podría ser una implementación de la función de emulación de terminal en el controlador de pantalla inteligente 211. Dicho terminal emulado sería capaz de leer datos requeridos (por ejemplo una cantidad del monedero electrónico) de la aplicación heredada, de formatearlos y de visualizarlos en la pantalla. Sin embargo, dicha solución tendría varias desventajas. Por ejemplo, el controlador de pantalla inteligente 211 tendría que implementar toda la función del terminal con protocolos para diferentes estándares de aplicaciones (por ejemplo Geldkarte para Alemania, Chipknip para los Países Bajos, o CEPS para las nuevas tarjetas). Eso daría como resultado un bloque complicado y caro de hardware y/o software.

Además, se cifra a menudo la comunicación con la unidad de aplicación heredada 402. Esta implementación requeriría, por lo tanto, claves de cifrado para almacenarse en el controlador de pantalla inteligente 211 durante un proceso de finalización de tarjeta (que es de alta intensidad de costes y complejo). Requeriría también la implementación de algoritmos criptográficos en el controlador de pantalla inteligente 211. Además, no habría posibilidad de personalización para la información visualizada en la tarjeta inteligente, ya que el controlador de pantalla inteligente 211 tendría que formatear el contenido de la pantalla.

La solución de acuerdo con la Fig. 4 es una implementación de la función de espejo para los paquetes de APDU en el controlador de pantalla inteligente 211 con una unidad de aplicación de pantalla independiente 401. Esta unidad de aplicación de pantalla 401 es capaz de recuperar la información necesaria para formatear un contenido de la pantalla usando un protocolo conocido de aplicación heredada estándar. Cualquier mensaje de comunicación transmitido entre la unidad de aplicación de pantalla 401 y la unidad de conversión de aplicación de pantalla 402 se refleja a través del controlador de pantalla inteligente 211 como se ilustra en la Fig. 4. En la Fig. 4, solo algunos de los componentes relevantes de una tarjeta inteligente se muestran como porción 400. Las flechas de comunicación 403 a 407 simbolizan el principio maestro-esclavo de intercambio de datos de los protocolos de la norma ISO 7816 para simplificar la imagen.

Los componentes de la aplicación se encapsulan en el dominio seguro 202 de un CI de tarjeta inteligente. En la implementación de la Fig. 4, existe una unidad de aplicación de pantalla 401 que es una aplicación especial diseñada para recuperar, interpretar y visualizar los datos de una o más unidades de aplicaciones heredadas dadas 401 a través del controlador de pantalla inteligente 211.

La comunicación funciona de la forma siguiente: La unidad de aplicación de pantalla 401 envía una solicitud al controlador de pantalla inteligente 211 al espejo (es decir, para enviar) mensajes de comunicación a la unidad de

aplicación heredada de destino 402. Junto con la solicitud, la unidad de aplicación de pantalla 401 envía una APDU encapsulada, que va a enviarse a la unidad de aplicación heredada 402, véase la primera flecha de transmisión 403.

5 Posteriormente, el controlador de pantalla inteligente 211 envía (es decir, refleja) la APDU solicitada a la unidad de aplicación heredada 401, véase la segunda flecha de transmisión 404.

10 La unidad de aplicación heredada 402 responde de una forma usual (al igual que en una comunicación con un terminal) transmitiendo datos/estado al controlador de pantalla inteligente 211, véase la tercera flecha de transmisión 405.

10 El controlador de pantalla inteligente 211 refleja de nuevo la respuesta de vuelta a la unidad de aplicación de pantalla 401, véase la cuarta flecha de transmisión 406.

15 Entonces, la unidad de aplicación de pantalla 401 puede proporcionar el contenido de la pantalla al controlador de pantalla inteligente 211, véase la quinta flecha de transmisión 407, en base a los datos recibidos de la unidad de aplicación heredada 402.

20 Una ventaja significativa de este procedimiento es la seguridad. Como el controlador de pantalla inteligente 211 no necesita interpretar los datos reflejados, los datos pueden cifrarse por medio de teclas criptográficas sin salir del dominio seguro 202. Esto significa que la unidad de aplicación de pantalla 401 puede, de una forma segura, obtener información de la unidad de aplicación heredada 402 (y viceversa) y extraer información que podría visualizarse en la pantalla y luego enviarla al controlador de pantalla inteligente 211. Así, la unidad de aplicación de pantalla 401 y la unidad de aplicación heredada 402, que forman parte ambas de un dominio seguro, puede comunicarse a través del controlador de pantalla inteligente 211, que está en el exterior del dominio seguro, de una manera segura.

25 Otro beneficio de esa solución es que un proveedor de servicios es capaz de personalizar la unidad de aplicación de pantalla 401 (es decir, por ejemplo, de cambiar la forma en que se visualizan los datos) y se mantiene independiente de la tarjeta o del sistema operativo usados. Dicha solución puede añadir incluso la identificación del usuario a través de, por ejemplo, el código PIN a la unidad de aplicación de pantalla 401 para asegurar el acceso a los datos personales en la unidad de aplicación heredada 402. La función de espejo puede implementarse fácilmente en el controlador de pantalla inteligente 211.

35 El sistema de acuerdo con la invención puede usarse en tarjetas inteligentes de múltiples componentes, especialmente en tarjetas inteligentes con una pantalla. La invención permite una rápida integración de la función de visualización en los sistemas de tarjetas inteligentes existentes sin afectar la seguridad total del sistema y proporciona una solución para la compatibilidad retroactiva. El sistema de acuerdo con la invención proporciona, a través del uso de las normas existentes como la norma ISO 7816, un alto grado de simplicidad en uso para clientes potenciales.

40 La tarjeta inteligente inventiva 200 puede usarse también para visualizar datos, que se reciben de la interfaz de dispositivo de lectura y/o grabación 213. En un modo de realización, dichos datos se transfieren directamente (sin usar el procesador 202) a la unidad de entrada y/o salida 212 a través de la interfaz de dispositivo de lectura y/o grabación 213. En este caso, la unidad de entrada y/o salida 212 actúa como esclavo. Sin embargo, el procesador 202 puede verse implicado en esta operación de visualización de datos también.

45 Cabría destacar que el término "que comprende" no excluye otros elementos ni etapas y que el uso del artículo indeterminado "uno" o "una" no excluye una pluralidad. Pueden combinarse también elementos descritos en asociación con diferentes modos de realización.

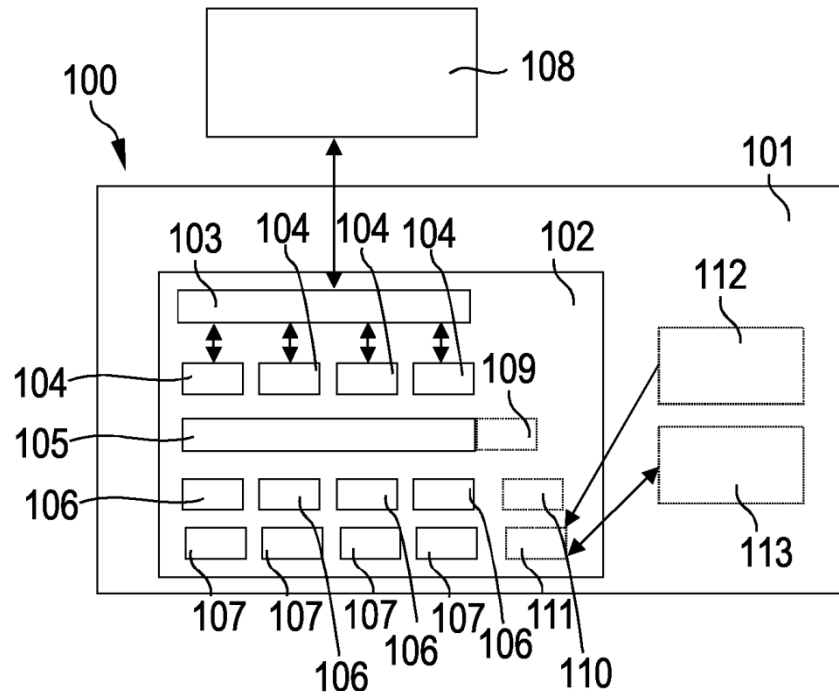
50 Cabría destacar también que los signos de referencia en las reivindicaciones no se considerarán limitativos del alcance de la invención.

REIVINDICACIONES

1. Una tarjeta inteligente (200), que comprende
 - 5 - un procesador (202) en una porción de seguridad de la tarjeta inteligente (200);
 - una interfaz de dispositivo de lectura/grabación (213) diseñada para una comunicación entre el procesador (202) y al menos un dispositivo externo de lectura/grabación (208); y
 - 10 - al menos una unidad de entrada y/o salida de usuario (212) para recibir al menos comandos del usuario y diseñada para iniciar una comunicación entre un usuario y el procesador (202),
 - caracterizada por que la comunicación entre un usuario y el procesador (202) es a través de la interfaz de dispositivo de lectura/grabación (213) y por que el protocolo de comunicación para la comunicación entre el
15 procesador y el dispositivo de lectura/grabación (208) es el mismo que el protocolo de comunicación para la comunicación entre la unidad de entrada/salida de usuario y el procesador.
2. La tarjeta inteligente (200) de acuerdo con la reivindicación 1, que está diseñada de manera que un protocolo de comunicación para una comunicación entre el procesador (202) y al menos un dispositivo de lectura/grabación (208)
20 es igual a un protocolo de comunicación para una comunicación entre al menos una unidad de entrada y/o salida de usuario (212) y el procesador (202).
3. La tarjeta inteligente (200) de acuerdo con la reivindicación 1, que está diseñada para una comunicación entre el procesador (202) y al menos una unidad de entrada y/o salida de usuario (212) de acuerdo con la norma ISO 7816.
25
4. La tarjeta inteligente (200) de acuerdo con la reivindicación 1, que está diseñada para una comunicación entre el procesador (202) y al menos una unidad de entrada y/o salida de usuario (212) por medio de una transmisión de al menos una Unidad de Datos de Protocolo de Aplicación.
5. La tarjeta inteligente (200) de acuerdo con la reivindicación 1, dividida en la porción de seguridad, en la que se proporciona una función de seguridad, y en una porción restante, en el que la porción restante incluye al menos parte de al menos una unidad de entrada y/o salida de usuario (212).
30
6. La tarjeta inteligente (200) de acuerdo con la reivindicación 1,
35 - que comprende una unidad de aplicación (402) que es capaz de proporcionar datos al procesador (202) que se relacionan con una aplicación correspondiente y que es incapaz de proporcionar los datos en un formato que sea producible por al menos una unidad de entrada/salida de usuario (212);
- y que comprende una unidad de aplicación de interacción del usuario (401) que es al menos capaz de convertir los datos proporcionados por la unidad de aplicación (402) en un formato que sea producible por al menos una unidad de entrada y/o salida de usuario (212).
40
7. La tarjeta inteligente (200) de acuerdo con la reivindicación 6, en la que la unidad de aplicación de interacción del usuario (401) se adapta para tomar el papel de maestro en relación con una comunicación con la unidad de aplicación (402).
45
8. La tarjeta inteligente (200) de acuerdo con la reivindicación 6, en la que una comunicación entre la unidad de aplicación (402) y la unidad de aplicación de interacción del usuario (401) se media por al menos una unidad de entrada/salida de usuario (212).
50
9. La tarjeta inteligente (200) de acuerdo con la reivindicación 8, que se adapta de tal manera que se cifra un mensaje transmitido entre la unidad de aplicación (402) y la unidad de aplicación de interacción del usuario (401).
10. La tarjeta inteligente (200) de acuerdo con la reivindicación 8, en la que una unidad de entrada y/o salida del usuario (212) que media un mensaje transmitido entre la unidad de aplicación (402) y la unidad de aplicación de interacción del usuario (401) es incapaz de descifrar el mensaje.
55
11. La tarjeta inteligente (200) de acuerdo con la reivindicación 5 y 6, en la que la unidad de aplicación (402) y la unidad de aplicación de interacción del usuario (401) se sitúan en la porción de seguridad.
60
12. La tarjeta inteligente de acuerdo con la reivindicación 6, en la que una comunicación entre la unidad de aplicación (402) y la unidad de aplicación de interacción del usuario (401) incluye la transmisión de al menos una Unidad de Datos de Protocolo de Aplicación.
65

13. Un procedimiento de operación de una tarjeta inteligente (200), en el que el procedimiento comprende las etapas de:

- 5 - operar un procesador (202) de la tarjeta inteligente (203);
- 10 - permitir una comunicación entre el procesador (202) y un dispositivo de lectura/grabación externo (208), a través de una interfaz de dispositivo de lectura/grabación (213) de la tarjeta inteligente (200);
- 10 - caracterizado por que el procedimiento comprende iniciar, por medio de una unidad de entrada y/o salida de usuario (212) que es al menos para recibir comandos del usuario, una comunicación entre un usuario y el procesador (202) a través de la interfaz de dispositivo de lectura/grabación (213), y por que el protocolo de comunicación para la comunicación entre el procesador y el dispositivo de lectura/grabación (208) es el mismo que el protocolo de comunicación para la comunicación entre la unidad de entrada y/o salida de usuario y el procesador.
- 15 14. El procedimiento de acuerdo con la reivindicación 13, en el que la comunicación entre el usuario y el procesador (202) a través de la interfaz de dispositivo de lectura/grabación (213) se inicia por medio de una unidad de entrada/salida de usuario (212) que se dispone en la tarjeta inteligente (200).



Estado de la técnica

FIG 1

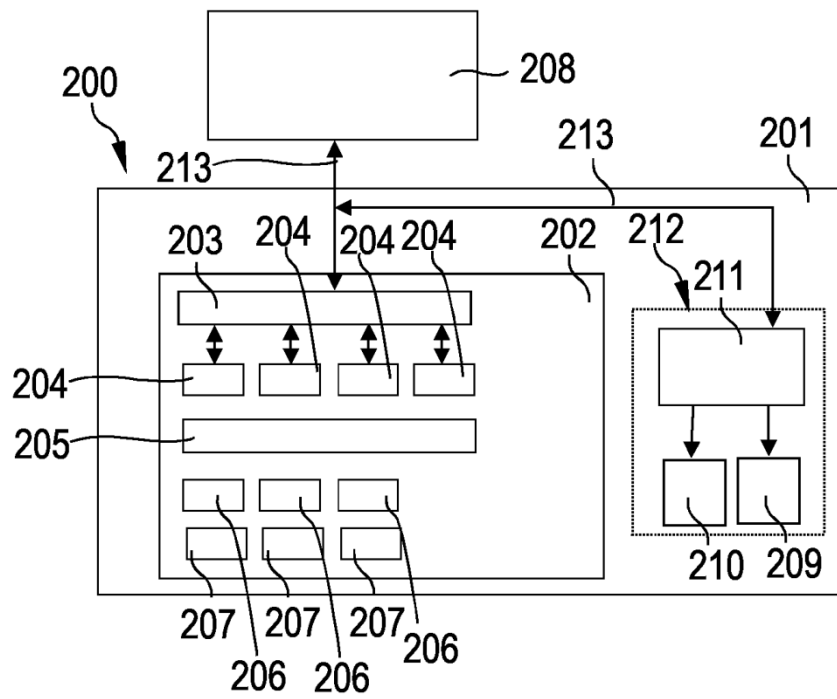


FIG 2

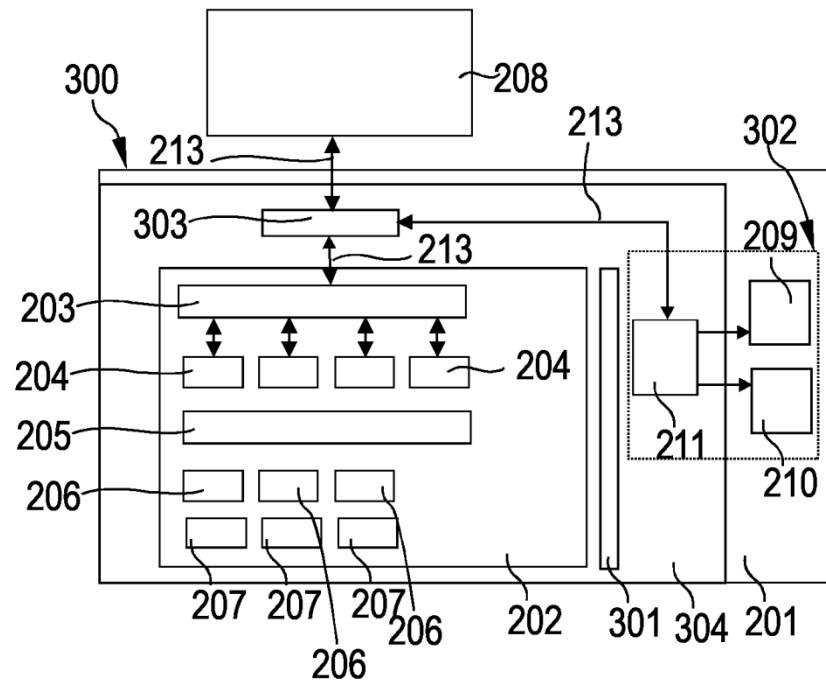


FIG 3

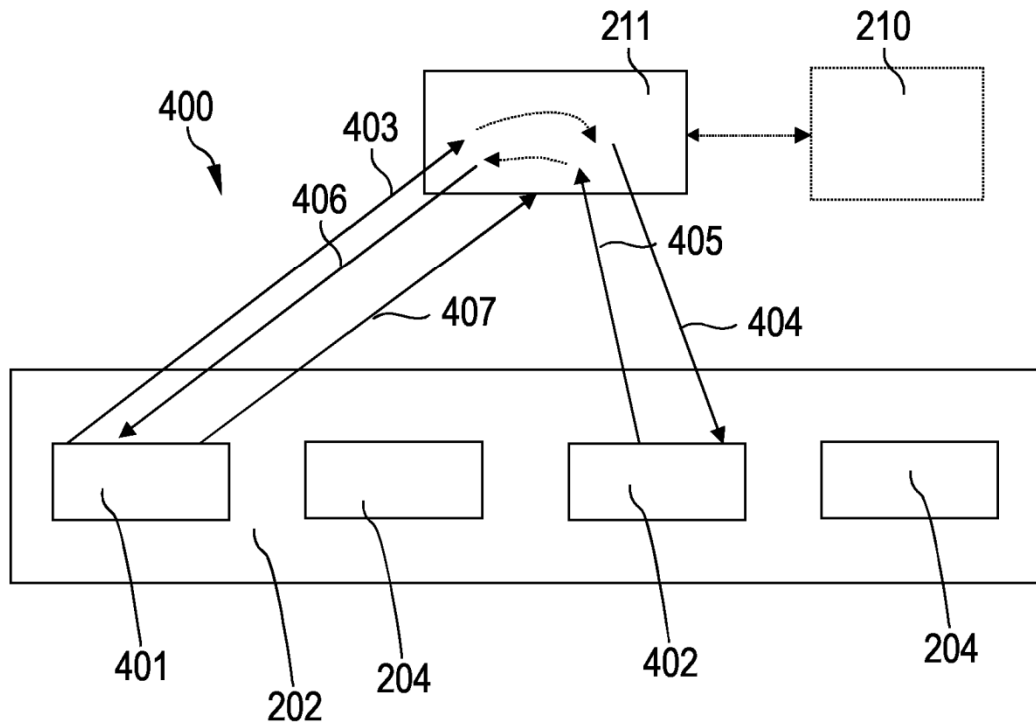


FIG 4