(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 533 658**

(51) Int. CI.:

G06K 19/07 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **25.02.2009 E 09002629 (5)**

(97) Fecha y número de publicación de la concesión europea: **31.12.2014 EP 2224376**

(54) Título: **Alimentación eléctrica para una tarjeta chip**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.04.2015

(73) Titular/es:

VODAFONE HOLDING GMBH (100.0%)
MANNESMANNUFER 2
40213 DÜSSELDORF, DE

(72) Inventor/es:

HOEKSEL, SEBASTIAAN;
KORAICHI, NAJIB y
WATERS, PATRICK H.

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Alimentación eléctrica para una tarjeta chip

Campo técnico

La invención se refiere a los componentes de alimentación eléctrica de una tarjeta chip. Más específicamente, la invención se refiere a una tarjeta chip para insertar en un dispositivo anfitrión, comprendiendo la tarjeta chip un microcontrolador, incluyendo el microcontrolador un procesador y una unidad de memoria, y estando el microcontrolador conectado a un terminal de alimentación de la tarjeta chip para recibir energía de un primer medio de alimentación eléctrica del dispositivo anfitrión.

Antecedentes de la invención

Las tarjetas chip se usan a menudo en relación con dispositivos anfitriones para proporcionar cierta funcionalidad al dispositivo anfitrión. Un ejemplo de dicha tarjeta chip es una tarjeta de memoria que puede conectarse al dispositivo anfitrión para aumentar su espacio de memoria. Otro ejemplo es una denominada tarjeta SIM que se conecta a un dispositivo de comunicaciones móviles y proporciona una funcionalidad para identificar y autenticar al usuario del dispositivo de comunicaciones móviles en una red de comunicaciones móviles.

Una tarjeta chip comprende un microcontrolador que se alimenta normalmente con energía por medio de la fuente de alimentación del dispositivo anfitrión a través de una interfaz específica. De acuerdo con su especificación, la interfaz entre el dispositivo anfitrión y la tarjeta chip permite, normalmente, suministrar tensiones de valores definidos a la tarjeta chip. Por ejemplo, la especificación ISO 7816-3 comprende tres clases correspondientes a tensiones de alimentación de 5 V, 3 V y 1,8 V. Además, la corriente que puede suministrarse a la tarjeta chip está limitada, normalmente, a los valores predeterminados.

En particular, el microcontrolador de la tarjeta chip comprende al menos un procesador. El rendimiento o velocidad de cálculo del procesador, que depende especialmente de la frecuencia de reloj proporcionada al procesador, determina la corriente que va a suministrarse al procesador. Por esta razón, la limitación de la corriente que puede proporcionarse a través de la interfaz entre el dispositivo anfitrión y la tarjeta chip limita el rendimiento del procesador.

Además, el microcontrolador comprende, normalmente, unidades de memoria no volátil, tales como unidades EEPROM (memoria de solo lectura borrable eléctricamente) o unidades de memoria flash. Tal unidad de memoria puede borrarse y reprogramarse suministrando una tensión de programación a las celdas de memoria de la unidad de memoria. Sin embargo, la tensión de programación supera, normalmente, la tensión suministrada a la tarjeta chip por el dispositivo anfitrión. Por lo tanto, un conversor de CC a CC se integra normalmente en el microcontrolador, que proporciona la tensión de programación de las unidades de memoria. Tales conversores de CC a CC aumentan la complejidad del microcontrolador y pueden ser difíciles de implementar, cuando hay una gran diferencia entre la tensión de alimentación y la tensión de programación requerida de una unidad de memoria.

El documento US 2006/056216 A1 desvela un objeto portátil del tipo tarjeta inteligente que comprende un microcontrolador, una unidad de memoria adicional, un bus de comunicación interna y una trayectoria de alimentación eléctrica interna. El microcontrolador comprende, además, un regulador de tensión que recibe la tensión de alimentación primaria desde un teléfono móvil en el que la tarjeta 1 inteligente se ha insertado y genera, en base al mismo, una tensión de alimentación secundaria.

El documento US 5.267.211 desvela una tarjeta de memoria y un aparato electrónico que usa tal tarjeta de memoria. La tarjeta de memoria comprende una RAM, una batería, un conversor de tensión para elevar una tensión de la batería y para emitir la tensión elevada, y un circuito de conmutación para recibir una tensión de salida del conversor de tensión. Cuando se ha retirado la tarjeta de memoria del aparato electrónico o se ha apagado el aparato electrónico, no se suministra la tensión externa procedente de este aparato electrónico. A continuación, la unidad de conmutación suministra la tensión de salida del conversor de tensión elevando la tensión de la batería a la RAM como una tensión de reserva. Un monitor de tensión de la tarjeta de memoria supervisa la disponibilidad de la tensión alimentada externamente con el fin de poner el conversor de tensión en un modo de inhibición de funcionamiento cuando la tensión externa se suministra desde el aparato electrónico.

El documento US 2006/0250832 describe un sistema en una tarjeta de memoria para convertir una tensión de entrada de la tarjeta y para proporcionar una tensión adecuada para las necesidades de los componentes internos. El sistema comprende un módulo de conmutación para convertir la tensión de entrada, y el módulo de conmutación es capaz de proporcionar un nivel de tensión mayor y/o menor que la tensión de entrada.

Descripción de la invención

Un objeto de la presente invención es evitar los inconvenientes del estado de la técnica y permitir una alimentación eléctrica mejorada de los componentes de un microcontrolador de una tarjeta chip, tal como un procesador o una unidad de memoria.

El objeto se logra mediante una tarjeta chip de acuerdo con la reivindicación 1. Las realizaciones de la tarjeta chip se proporcionan en las reivindicaciones dependientes.

De acuerdo con un aspecto de la invención, se proporciona una tarjeta chip para insertar en un dispositivo anfitrión. La tarjeta chip comprende un microcontrolador que incluye un procesador y una unidad de memoria. El microcontrolador se conecta a un terminal de alimentación de la tarjeta chip para recibir energía de un primer medio de alimentación eléctrica del dispositivo anfitrión. Además, la tarjeta chip comprende un segundo medio de alimentación eléctrica, estando el segundo medio de alimentación eléctrica configurado para suministrar, al menos temporalmente, energía a un primer componente del microcontrolador.

La invención implica la idea de proporcionar un segundo medio de alimentación eléctrica, que está integrado en la tarjeta chip. El segundo medio de alimentación eléctrica es una fuente de energía adaptada para suministrar energía a, al menos, un componente del microcontrolador. La alimentación eléctrica por medio del segundo medio de alimentación eléctrica es independiente del primer medio de alimentación eléctrica del dispositivo anfitrión. En particular, la fuente de energía puede suministrar una tensión más alta y/o una corriente más alta al componente de lo que puede suministrarse a través del terminal de alimentación. Por medio del segundo medio de alimentación eléctrica puede lograrse una alimentación eléctrica adaptada del componente. En particular, el componente puede alimentarse por el segundo medio de alimentación eléctrica con una tensión que difiere de la tensión de alimentación externa proporcionada por el dispositivo anfitrión. Además, el segundo medio de alimentación eléctrica permite suministrar, al menos temporalmente, una alta corriente al componente independiente de la interfaz entre la tarjeta chip y el dispositivo anfitrión. Por lo tanto, pueden proporcionarse altas corrientes sin infringir los límites de corriente de la interfaz entre la tarjeta chip y el dispositivo anfitrión.

Mientras que el primer componente se alimenta con energía por el segundo medio de alimentación eléctrica, los componentes adicionales del microcontrolador pueden alimentarse, preferentemente, con energía a través del terminal de alimentación al mismo tiempo. Por lo tanto, los componentes específicos del microcontrolador pueden alimentarse con energía por el segundo medio de alimentación eléctrica y, al mismo tiempo, los componentes adicionales pueden hacerse funcionar en su modo de funcionamiento normal, en el que se alimentan con energía por la fuente de alimentación externa proporcionada por el dispositivo anfitrión. Esto también significa que no es necesaria una adaptación de estos componentes a una fuente de alimentación modificada. Además, cuando solo se suministra energía a los componentes específicos del microcontrolador, se ahorra energía del segundo medio de alimentación eléctrica.

Preferentemente, el primer componente está desconectado del terminal de alimentación, mientras que se alimenta con energía por el segundo medio de alimentación eléctrica. En particular, esto evita que haya dos fuentes de energía en el circuito de alimentación eléctrica del componente.

En una realización de la invención, el primer componente puede hacerse funcionar en un primer y en un segundo modo de funcionamiento, alimentándose el primer componente, en el primer modo de funcionamiento, con energía a través del terminal de alimentación y alimentándose el primer componente, en el segundo modo de funcionamiento, con energía por el segundo medio de alimentación eléctrica. Es una ventaja de esta realización que la alimentación eléctrica del componente pueda conmutarse temporalmente a una alimentación eléctrica por el segundo medio de alimentación eléctrica. En particular, esto ahorra de manera similar energía del segundo medio de alimentación eléctrica.

El primer componente puede ser un procesador principal y/o un coprocesador del microcontrolador. Cuando tal procesador se alimenta con energía por el segundo medio de alimentación eléctrica, puede suministrarse una corriente aumentada al procesador, lo que permite aumentar el rendimiento del procesador. En particular, el coprocesador puede ser un coprocesador criptográfico. Tales coprocesadores están integrados en el microcontrolador para ejecutar algoritmos criptográficos, que a menudo son muy complejos y requieren muchos ciclos de procesador. En consecuencia, es especialmente ventajoso para aumentar el rendimiento de un coprocesador criptográfico.

Con el fin de aumentar la velocidad de cálculo del procesador, el procesador puede hacerse funcionar, en el segundo modo de funcionamiento, a una frecuencia de reloj aumentada y/o a una tensión aumentada con respecto al primer modo de funcionamiento. Preferentemente, la tensión aumentada se corresponde con la tensión proporcionada por el segundo medio de alimentación eléctrica. Por lo tanto, no se requiere una conversión de tensión.

En una realización de la invención, el procesador se hace funcionar en el segundo modo de funcionamiento, cuando se determina que un procedimiento predeterminado se ejecuta en el procesador. Esto permite restringir el segundo modo de funcionamiento a unos procedimientos predeterminados, que pueden ser procedimientos especialmente complejos que requieren una alta potencia de cálculo. Por lo tanto, tales procedimientos pueden ejecutarse en poco tiempo, mientras que los procedimientos menos complejos se ejecutan en el primer modo de funcionamiento del procesador, ahorrando de este modo energía del segundo medio de alimentación eléctrica.

En una realización de la invención, al menos un procesador del microcontrolador se alimenta con energía exclusivamente por el segundo medio de alimentación eléctrica. Es una ventaja de esta realización que pueden suministrarse altas tensiones y/o altas corrientes al procesador para cada operación con independencia de la fuente de alimentación externa de la tarjeta chip por el dispositivo anfitrión. En particular, puede adaptarse el segundo medio de alimentación eléctrica para suministrar una primera tensión al procesador en su modo de funcionamiento normal, difiriendo la primera tensión de la tensión suministrada a la tarjeta chip por el dispositivo anfitrión. En particular, la primera tensión puede superar la tensión suministrada a la tarjeta chip por el primer medio de alimentación del dispositivo anfitrión. Preferentemente, en esta realización, el procesador es el coprocesador del microcontrolador que puede ejecutar, principalmente, procedimientos complejos, tales como por ejemplo cálculos criptográficos.

En una realización adicional de la invención, el primer componente electrónico es una unidad de memoria de un primer tipo, estando el segundo medio de alimentación eléctrica adaptado para proporcionar una tensión de programación para borrar y/o almacenar información en la unidad de memoria. Como se ha descrito anteriormente, la tensión de programación para las unidades de memoria, tales como la EEPROM y la memoria flash, supera normalmente la tensión de alimentación externa de la tarjeta chip. Por medio del segundo medio de alimentación eléctrica puede proporcionarse una tensión adaptada sin una conversión de tensión. Como alternativa, cuando se realiza una conversión de tensión, el segundo medio de alimentación eléctrica puede proporcionar una tensión que está más cerca de la tensión de programación que la tensión de alimentación externa, de tal manera que la diferencia de tensión requerida es menor. Esto simplifica la conversión de tensión.

En una realización de la invención, el microcontrolador comprende al menos dos unidades de memoria de tipos diferentes que tienen tensiones de programación diferentes, y el segundo medio de alimentación eléctrica está adaptado para proporcionar energía para borrar y/o almacenar información en las unidades de memoria. Preferentemente, en esta configuración, el segundo medio de alimentación eléctrica está adaptado para proporcionar una tensión correspondiente a la tensión de programación de una primera unidad de memoria de las unidades de memoria. Esto permite hacer funcionar las unidades de memoria, a la vez que no se requiere más que un conversor de CC a CC.

La primera unidad de memoria puede ser la que requiere la tensión de programación más baja. En este caso, la tensión de programación de la otra unidad de memoria puede generarse a partir de la tensión proporcionada por el segundo medio de alimentación eléctrica por medio de un conversor de CC a CC. Como alternativa, la primera unidad de memoria puede ser la que requiere la tensión de programación más alta. En este caso, la segunda unidad de memoria también puede hacerse funcionar usando la tensión más alta proporcionada por el segundo medio de alimentación eléctrica, o puede usarse un conversor de CC a CC para generar la tensión de programación más baja a partir de la tensión proporcionada por el segundo medio de alimentación eléctrica.

En una realización adicional de la invención, el segundo medio de alimentación eléctrica es una batería. En particular, el segundo medio de alimentación eléctrica puede ser una batería recargable y la batería puede cargarse suministrando energía a la batería a través del terminal de alimentación. Es una ventaja de esta realización que el segundo medio de alimentación eléctrica pueda recargarse por medio del medio de alimentación eléctrica del dispositivo anfitrión y que no tenga que sustituirse en caso de agotamiento.

De acuerdo con un aspecto adicional de la invención, se sugiere un dispositivo que comprende una tarjeta chip del tipo mencionado anteriormente y que comprende, además, un primer medio de alimentación eléctrica, estando el primer medio de alimentación eléctrica configurado para suministrar energía al terminal de alimentación de la tarjeta chip.

En una realización de la invención, la tarjeta chip es una tarjeta SIM. El dispositivo anfitrión puede ser un dispositivo de comunicaciones móviles, que puede usarse junto con la tarjeta SIM. La tarjeta SIM, tal como se usa en el presente documento, se refiere a una tarjeta chip usada en relación con un dispositivo de comunicaciones móviles que ofrece servicios de identificación y/o autenticación a una red de comunicaciones móviles. La tarjeta chip puede comprender una aplicación SIM de acuerdo con la norma GSM (SIM: módulo de identificación de abonado; GSM: sistema global para las comunicaciones móviles), una aplicación USIM de acuerdo con la norma UMTS (USIM: módulo de identidad de abonado universal; UMTS: sistema de telecomunicaciones móviles universal) o una aplicación correspondiente que proporciona funciones de autenticación y/o identificación en relación con una red de comunicaciones móviles.

Los aspectos de la invención mencionados anteriormente y otros también serán evidentes a partir de, y se aclararán con referencia a, las realizaciones descritas en lo sucesivo en el presente documento haciendo referencia a los dibujos.

Breve descripción de los dibujos

Se hará referencia a modo de ejemplo a los dibujos adjuntos en los que

Figura 1 muestra una representación esquemática de una tarjeta chip de acuerdo con la invención, que puede conectarse a un dispositivo anfitrión.

Descripción detallada de las realizaciones de la invención

La figura 1 representa esquemáticamente una tarjeta 101 chip que se proporciona para su uso en relación con un dispositivo 102 anfitrión de un usuario. La tarjeta 101 chip está configurada de acuerdo con un formato de tarjeta chip convencional y puede insertarse en una unidad 103 de lector de tarjetas del dispositivo 102 anfitrión configurada para recibir tarjetas 101 chip del formato convencional respectivo.

En una realización, el dispositivo 102 anfitrión está configurado como un dispositivo de comunicaciones móviles, que puede configurarse como un teléfono celular, una PDA (asistente personal digital) o similares. Por medio de un módulo de radio, que no se muestra en la figura 1, el dispositivo de comunicaciones móviles puede conectarse de manera inalámbrica a una red de comunicaciones móviles. Por ejemplo, la red de comunicaciones móviles puede ser una red GSM o una red UMTS. En esta realización, la tarjeta 101 chip puede usarse en relación con la utilización de un dispositivo 102 anfitrión en la red de comunicaciones móviles. En particular, la tarjeta 101 chip puede comprender una aplicación que proporciona servicios de identificación y autenticación de seguridad a la red de comunicaciones móviles. Si la red de comunicaciones móviles es una red GSM, la tarjeta 101 chip se configura como una tarjeta SIM de acuerdo con la norma GSM que comprende una aplicación SIM que proporciona los servicios de identificación y autenticación. Si la red de comunicaciones móviles es una red UMTS, la tarjeta 101 chip se configura como una UICC (tarjeta de circuito integrado universal) que comprende una aplicación USIM que proporciona los servicios de identificación y autenticación a la red de comunicaciones móviles. Sin embargo, la tarjeta 101 chip puede comprender otras aplicaciones correspondientes que proporcionan funciones de autenticación y/o identificación en relación con una red de comunicaciones móviles.

La tarjeta 101 chip comprende un microcontrolador 104 que está integrado en el cuerpo de la tarjeta 101 chip. El microcontrolador 104 está conectado a una interfaz 105 de contacto eléctrica que está dispuesta, preferentemente, en la superficie del cuerpo de la tarjeta 101 chip. La interfaz 105 de contacto comprende al menos dos elementos de contacto o almohadillas 106a,b de contacto para suministrar energía al microcontrolador 104. Un elemento 106a de contacto, que se denomina terminal de alimentación en lo sucesivo en el presente documento, puede alimentarse con una tensión de alimentación externa, y el otro elemento 106b de contacto puede ser un terminal de tierra.

Pueden proporcionarse elementos de contacto o almohadillas de contacto adicionales, que no se muestran en la figura 1, para intercambiar datos entre el microcontrolador 104 y el dispositivo 102 anfitrión y para recibir señales de control del dispositivo 102 anfitrión. En particular, la interfaz 105 de contacto eléctrica puede configurarse de acuerdo con la especificación ISO 7816-2. En esta realización, la interfaz 105 de contacto eléctrica comprende ocho elementos de contacto denominados normalmente C1 a C8. El elemento C1 de contacto, que se indica normalmente como Vcc, se usa para la alimentación eléctrica de la tarjeta 101 chip y, por lo tanto, se corresponde con el elemento 106a de contacto. El elemento C2 de contacto se usa para proporcionar una señal de reinicio al microcontrolador 104, y el elemento C3 de contacto se usa para proporcionar una señal de reloj al microcontrolador 104. El elemento C5 de contacto es el terminal de tierra y, por lo tanto, se corresponde con el elemento 106b de contacto. El elemento C7 de contacto es un terminal de entrada/salida para un intercambio de datos entre la tarjeta 101 chip y el dispositivo 102 anfitrión. Los elementos C4, C6 y C8 de contacto no se usan de acuerdo con la especificación ISO 7816.

Cuando la tarjeta 101 chip se inserta en la unidad 103 de lector de tarjetas del dispositivo 102 anfitrión, la interfaz 105 de contacto se pone en contacto con una interfaz de contacto correspondiente de la unidad 103 de lector de tarjetas, estableciendo de este modo una conexión de alimentación y una conexión de datos entre el dispositivo 102 anfitrión y la tarjeta 101 chip. Para proporcionar energía a la tarjeta 101 chip, el terminal 106a de alimentación se conecta a una unidad 107 de alimentación eléctrica del dispositivo 102 anfitrión a través de la unidad 103 de lector de tarjetas. La unidad 107 de alimentación eléctrica puede comprender una batería o puede tener, por ejemplo, una conexión a una red de energía. A través de la unidad 103 de lector de tarjetas, se suministra una tensión de alimentación que tiene un valor predeterminado al terminal 106a de alimentación. En una realización, la tensión de alimentación tiene un valor que se corresponde con una clase especificada en la especificación ISO 7816-3. De acuerdo con esta especificación, se proporcionan tres clases: la clase A proporciona una tensión de alimentación de 5 V, la clase B proporciona una tensión de alimentación de 3 V, y la clase C se corresponde con una tensión de alimentación de 1,8 V. La tolerancia de tensión permitida es de un 10% en cada clase. En realizaciones adicionales, el microcontrolador 104 se hace funcionar a otra tensión de alimentación, que puede ser especialmente una tensión más baja. Esto es especialmente ventajoso si la unidad 107 de alimentación eléctrica del dispositivo 102 anfitrión proporciona una tensión más baja, de manera que no se requiere una conversión de tensión para alimentar con energía el microcontrolador 104. De manera similar, la corriente de alimentación del microcontrolador 104 se recibe a través del terminal 106a de alimentación y está limitada a un valor predeterminado de acuerdo con la especificación de la tarjeta 101 chip o la especificación de la interfaz entre la tarjeta 101 chip y el dispositivo 102 anfitrión.

El microcontrolador 104 incluye un procesador 108 (CPU) primario o principal para ejecutar programas que controlan funciones de la tarjeta 101 chip. En diferentes realizaciones, el procesador 108 principal puede ser un procesador de 8 bits, 16 bits o 32 bits configurado de acuerdo con una arquitectura de procesador conocida para los expertos en la materia. El procesador 108 principal se hace funcionar usando un sistema operativo que permite ejecutar aplicaciones adicionales dedicadas a funcionalidades específicas de la tarjeta 101 chip.

Opcionalmente, el procesador 108 principal se complementa con un coprocesador 109, que está configurado para ejecutar operaciones predeterminadas en lugar del procesador 108 principal. En una realización, el coprocesador 109 es un coprocesador criptográfico que está configurado para ejecutar operaciones criptográficas, tales como la encriptación y la desencriptación de datos y procedimientos relacionados. En particular, el coprocesador 109 puede configurarse para ejecutar un algoritmo criptográfico simétrico, tal como, por ejemplo, DES, Triple-DES o AES (DES: norma de encriptación de datos; AES: norma de encriptación avanzada), o puede configurarse para ejecutar un algoritmo criptográfico asimétrico, tal como, por ejemplo, el algoritmo RSA o un algoritmo en base a una curva elíptica. De manera similar, es posible que la tarjeta 101 chip disponga de varios coprocesadores 109, que pueden ser un coprocesador 109 para algoritmos criptográficos simétricos y un coprocesador 109 para algoritmos criptográficos asimétricos.

Puede proporcionarse una frecuencia de reloj para el funcionamiento del procesador 108 principal o el coprocesador 109 al microcontrolador 104 por el dispositivo 102 anfitrión a través de la interfaz 105 de contacto. Si la interfaz 105 de contacto está configurada de acuerdo con la especificación ISO 7816-2, el elemento C5 de contacto se usa para suministrar una señal de reloj desde el dispositivo 102 anfitrión al microcontrolador 104. Sin embargo, en las realizaciones de la invención, la frecuencia de reloj para el procesador 108 principal y/o el coprocesador 109 puede diferir de manera permanente o temporal de la frecuencia de reloj suministrada externamente, en particular, el procesador 108 principal y/o el coprocesador pueden hacerse funcionar de manera permanente o temporal a una frecuencia de reloj más alta. Esto puede lograrse modificando de manera estática o dinámica el microcontrolador 104. Como alternativa, puede generarse una señal de reloj interno, que también puede modificarse de manera dinámica, que sustituye la señal de reloj externo de manera permanente o temporal. Además, el microcontrolador 104 comprende una memoria 110 volátil, que puede configurarse como una memoria de acceso aleatorio (RAM) y que se usa para almacenar y manipular datos durante la ejecución de las operaciones en el microcontrolador 104. Además, el microcontrolador 104 comprende una memoria no volátil. La memoria no volátil puede incluir una primera unidad 111 de memoria, que puede configurarse como una memoria de solo lectura (ROM). La primera unidad 111 de memoria incluye los datos que se almacenan en la misma en el momento de la fabricación de la tarjeta 101 chip, tales como las rutinas del sistema operativo de la tarjeta 101 chip.

Se proporciona una unidad 112 de memoria no volátil adicional, que permite leer y escribir datos. La unidad 112 de memoria puede usarse para almacenar datos, tales como, por ejemplo, las aplicaciones ejecutadas en el microcontrolador 104, y puede configurarse como una memoria de solo lectura borrable eléctricamente (EEPROM). Además, o como alternativa a la EEPROM 112, el microcontrolador 104 puede comprender una segunda unidad 113 de memoria no volátil que permite el acceso de lectura y escritura. Esta unidad 113 de memoria puede configurarse como una memoria flash (como siempre, debe entenderse que la EEPROM 112 es una EEPROM no flash). Tanto la EEPROM 112 como la memoria 113 flash comprenden una pluralidad de celdas de memoria que incluyen un elemento semiconductor. Las celdas pueden borrarse y reprogramarse eléctricamente aplicando una tensión de programación a las celdas. Normalmente, la tensión de programación es de aproximadamente 17 V para las celdas EEPROM y de 12 V para las celdas de memoria flash. Por lo tanto, cuando se hace funcionar la EEPROM 112 y/o la memoria 113 flash usando la fuente de alimentación externa de la tarjeta 101 chip que proporciona una tensión más baja, un conversor de CC a CC, tal como una bomba de carga o un conversor elevador, tiene que integrarse en el microcontrolador 104 con el fin de proporcionar la tensión de programación requerida.

Además del microcontrolador 104, la tarjeta 101 chip comprende una unidad 114 de alimentación eléctrica. Preferentemente, la unidad 114 de alimentación eléctrica está integrada en el cuerpo de la tarjeta 101 chip, junto con el microcontrolador 104 sin ampliar las dimensiones de la tarjeta 101 chip, que se determinan por el formato convencional respectivo. La unidad 114 de alimentación eléctrica puede ser una batería recargable que comprende una o más celdas de batería. La batería es lo suficientemente pequeña y delgada como para integrarse en el cuerpo de la tarjeta 101 chip. Por ejemplo, la unidad 114 de alimentación eléctrica puede ser una batería de láminas, una batería RHISS (RHISS: estado sólido de iones de hidrógeno recargable) o una batería de película delgada. En general, estos tipos de baterías y su integración en las tarjetas 101 chip se conocen por los expertos en la materia y, por lo tanto, no se describirán con mayor detalle en el presente documento.

En una realización de la invención, la unidad 114 de alimentación eléctrica se usa para suministrar energía al procesador 108 principal y/o al coprocesador 109, mientras que se hace funcionar el procesador 108; 109 pertinente con un rendimiento aumentado, es decir, con una velocidad de cálculo aumentada. En este caso, la unidad 114 de alimentación eléctrica interna está adaptada para proporcionar una mayor energía al procesador 108 principal y/o al coprocesador 109. Esto significa que la unidad 114 de alimentación eléctrica interna proporciona una corriente más alta y/o una tensión más alta que la proporcionada por el dispositivo 102 anfitrión a través del terminal 106a de alimentación.

El rendimiento del procesador 108 principal puede aumentarse temporalmente, cuando vayan a ejecutarse procedimientos predeterminados que requieran una velocidad de cálculo más alta y/o un tiempo de cálculo breve. Para este fin, el microcontrolador 104 puede hacerse funcionar en un modo de funcionamiento normal que proporciona un rendimiento normal y en un modo especial que proporciona un rendimiento aumentado. Como alternativa, pueden proporcionarse varios modos especiales, cada uno correspondiente a un modo de funcionamiento predeterminado que ofrece una velocidad de cálculo aumentada. Los diferentes modos de funcionamiento pueden controlarse mediante una unidad de control del microcontrolador 104, que puede ser una

aplicación independiente ejecutada en el procesador 108 principal. La unidad de control monitoriza los procedimientos ejecutados en el procesador 108 principal y activa un modo especial, cuando determina que va a ejecutarse una aplicación predeterminada o un procedimiento predeterminado dentro de una aplicación en el procesador 108 principal. Las aplicaciones o los procedimientos pertinentes, que están destinados a ejecutarse en un modo especial, pueden almacenarse en el microcontrolador 104 en una lista, a la que se accede por la unidad de control para identificar estas aplicaciones. Como alternativa, una aplicación que requiere una velocidad de cálculo aumentada comprende una unidad de control, que está configurada para activar el modo de funcionamiento especial, cuando se inicia la aplicación o cuando se inicia un procedimiento predeterminado dentro de la aplicación. Cuando se ha completado la aplicación o el procedimiento que va a ejecutarse en el modo especial, se desactiva el modo especial y se activa de nuevo el modo normal.

Además del procesador 108 principal, o como alternativa, el coprocesador 109 puede hacerse funcionar temporalmente en uno o más modos de funcionamiento especiales que proporcionan una velocidad de cálculo aumentada. Como para el procesador 108 principal, puede activarse el modo de funcionamiento especial cuando vayan a ejecutarse procedimientos predeterminados. Para este fin, puede asignarse una unidad de control al coprocesador 109, que está configurada para activar un modo de funcionamiento especial y que puede implementarse como una aplicación independiente ejecutada en el coprocesador 109 o en el procesador 108 principal. La unidad de control monitoriza de nuevo los procedimientos ejecutados en el coprocesador 109 y activa un modo especial, cuando determina que va a ejecutarse una aplicación predeterminada o un procedimiento predeterminado dentro de una aplicación en el coprocesador 109. Las aplicaciones o los procedimientos pertinentes, que están destinados a ejecutarse en un modo especial, pueden almacenarse en el microcontrolador 104 en una lista, que se usa por la unidad de control para identificar estas aplicaciones. Como alternativa, una aplicación que requiere una velocidad de cálculo aumentada comprende una unidad de control, que está configurada para activar el modo de funcionamiento especial del coprocesador 109, cuando se inicia la aplicación o cuando se inicia un procedimiento predeterminado dentro de la aplicación. Cuando se ha completado la aplicación o el procedimiento que va a ejecutarse en el modo especial, se desactiva el modo especial y se activa de nuevo el modo normal.

En el modo de funcionamiento normal, el procesador 108 principal y el coprocesador 109 se alimentan con energía a través del terminal 106a de alimentación, y se hacen funcionar a una frecuencia de reloj fija, que se proporciona por la señal de reloj externo, derivada de la frecuencia de reloj externo dentro del microcontrolador 104 o generada en el microcontrolador 104. Como alternativa, la frecuencia de reloj puede modificarse dinámicamente de una manera conocida para los expertos en la materia, con el fin de ahorrar energía. En particular, la frecuencia de reloj puede disminuirse cuando un procesador 108; 109 funciona a una baja carga. El procesador 108 principal y el coprocesador 109 pueden hacerse funcionar a la misma frecuencia de reloj o a frecuencias de reloj diferentes.

En un modo especial, el procesador 108 principal o el coprocesador 109 se alimenta con energía por la unidad 114 de alimentación eléctrica interna de la tarjeta 101 chip. La conexión de alimentación con el dispositivo 102 anfitrión a través del terminal 106a de alimentación se desconecta, preferentemente, cuando el procesador 108; 109 pertinente se alimenta con energía por la unidad 114 de alimentación eléctrica. En consecuencia, la activación de un modo especial comprende la conmutación de la alimentación eléctrica del procesador 108; 109 pertinente de una alimentación eléctrica a través del terminal 106a de alimentación a una alimentación eléctrica por la unidad 114 de alimentación eléctrica. Cuando se desactiva el modo especial, la alimentación eléctrica se conmuta de nuevo a una alimentación eléctrica a través del terminal 106a de alimentación.

La velocidad de cálculo puede incrementarse aumentando la frecuencia de reloj del procesador 108; 109 pertinente con respecto a la frecuencia de reloj fija o la frecuencia de reloj máxima usada en el modo de funcionamiento normal. La frecuencia de reloj aumentada puede generarse multiplicando la frecuencia de reloj provista de la señal de reloj externo, o puede generarse una señal de reloj adicional correspondiente a la frecuencia de reloj aumentada en el microcontrolador 104, que sustituye a la señal de reloj usada en el modo de funcionamiento normal. Por ejemplo, la frecuencia de reloj aumentada puede generarse usando un bucle de enganche de fase (PLL) o un oscilador RC interno del microcontrolador 104. Cuando se desactiva el modo especial, la frecuencia de reloj se conmuta de nuevo a la frecuencia de reloj usada en el modo de funcionamiento normal.

La tensión suministrada al procesador 108, 109 pertinente por la unidad 114 de alimentación eléctrica puede corresponderse con la tensión de alimentación proporcionada por el dispositivo 102 anfitrión. Esto significa que la unidad 114 de alimentación eléctrica puede configurarse de tal manera que proporciona una tensión correspondiente a una clase de tensión especificada, especialmente a la clase de tensión del dispositivo 102 anfitrión. En este caso, la unidad 114 de alimentación eléctrica garantiza que pueda suministrarse una corriente de alimentación al procesador 108; 109, que sea lo suficientemente alta para que el procesador 108; 109 funcione a la frecuencia de reloj aumentada.

Sin embargo, adicionalmente o como alternativa al aumento de la frecuencia de reloj, la velocidad de cálculo del procesador 108; 109 pertinente también puede aumentarse suministrando una tensión aumentada al procesador 108, 109. Esta técnica para aumentar el rendimiento de cálculo también se conoce como sobretensión. Preferentemente, la tensión aumentada se corresponde con la tensión proporcionada por la unidad 114 de alimentación eléctrica que, en consecuencia, supera la tensión de alimentación proporcionada por el dispositivo 102 anfitrión en esta realización.

Aunque, preferentemente, el procesador 108 principal solo se hace funcionar temporalmente en un modo especial, una realización de la invención prevé que el coprocesador 109 se haga funcionar exclusivamente de acuerdo con un modo especial descrito anteriormente. En esta realización, cuando el microcontrolador 104 está activado, el coprocesador 109 puede alimentarse permanentemente con energía por la unidad 114 de alimentación eléctrica interna de la tarjeta 101 chip. Preferentemente, en esta realización, no se proporciona una conexión de alimentación entre el coprocesador 109 y la fuente de alimentación externa o el terminal 106a de alimentación. En este caso, la unidad 114 de alimentación eléctrica está adaptada al coprocesador 109, de tal manera que se suministra una tensión de alimentación adecuada al coprocesador 109, que puede ser más alta que la tensión de alimentación proporcionada a la tarjeta 101 chip por el dispositivo 102 anfitrión. La frecuencia de reloj se ajusta de tal manera que se logra un alto rendimiento, especialmente una alta velocidad de cálculo del coprocesador 109. La frecuencia de reloj puede fijarse o puede modificarse dinámicamente de acuerdo con las técnicas de escalamiento de frecuencia conocidas con el fin de ahorrar energía. En particular, puede disminuirse la frecuencia de reloj cuando el coprocesador 109 se hace funcionar a baja carga. Cuando el coprocesador 109 se alimenta con energía exclusivamente por la unidad 114 de alimentación eléctrica, puede garantizarse que se proporciona una corriente lo suficientemente alta al coprocesador 109. Además, el coprocesador 109 puede hacerse funcionar a una tensión aumentada sin tener que transformar la tensión de alimentación externa.

En una realización adicional, la unidad 114 de alimentación eléctrica interna de la tarjeta 101 chip se usa para proporcionar la tensión de programación para el funcionamiento de la EEPROM 112 y/o la memoria 113 flash.

Cuando la tensión de programación se prevé solo para una unidad 112; 113 de memoria, la unidad 114 de alimentación eléctrica se adapta, preferentemente, para proporcionar una tensión que se corresponde con la tensión de programación de la unidad 112; 113 de memoria pertinente. En este caso, no es necesaria una transformación de tensión para proporcionar la tensión de programación de la unidad 112, 113 de memoria. Como alternativa, la unidad 114 de alimentación eléctrica puede proporcionar una tensión por debajo de la tensión de programación, pero preferentemente por encima de la tensión de alimentación externa de la tarjeta 101 chip. En esta realización, es necesaria una conversión de tensión, pero se disminuye la diferencia de tensión en comparación con una generación de la tensión de programación a partir de la tensión de alimentación externa, Por lo tanto, el conversor de CC a CC requerido puede dimensionarse más pequeño.

De manera similar, es posible proporcionar la tensión de programación para la EEPROM 112 y la memoria 113 flash por la unidad 114 de alimentación eléctrica. En esta realización, la unidad 114 de alimentación eléctrica se adapta, preferentemente, para proporcionar una tensión que se corresponde con la tensión de programación mínima de las tensiones de programación requeridas de las unidades 112; 113 de memoria, es decir, con la tensión de programación de la memoria 113 flash. Por lo tanto, la unidad 114 de alimentación eléctrica proporciona directamente la tensión de programación de la memoria 113 flash. Para la EEPROM 112, puede asignarse un conversor de CC a CC, en particular una bomba de carga o un conversor elevador, que transforma la tensión proporcionada por la unidad 114 de alimentación eléctrica en la tensión de programación más alta de la EEPROM 112.

Como alternativa, la unidad 114 de alimentación eléctrica está adaptada para proporcionar un tensión que se corresponde con la tensión de programación máxima requerida por las unidades 112; 113 de memoria, es decir, con la tensión de programación de la EEPROM 112. Por lo tanto, la unidad 114 de alimentación eléctrica proporciona directamente la tensión de programación de la EEPROM 112. La tensión proporcionada por la unidad 114 de alimentación eléctrica también puede usarse como tensión de programación para la otra unidad 113 de memoria, es decir, la memoria 113 flash. Sin embargo, la tensión de programación aumentada de la memoria 113 flash puede dar lugar a una corriente de programación aumentada que calienta la memoria 113 flash. Esto puede evitarse asignando un conversor de CC a CC a la memoria 113 flash, especialmente un conversor reductor, que transforma la tensión proporcionada por la unidad 114 de alimentación eléctrica en la tensión de programación más baja de la memoria 113 flash.

En otras realizaciones, la unidad 114 de alimentación eléctrica puede proporcionar un tensión que no se corresponde con la tensión de programación de una unidad 112; 113 de memoria, pero se encuentra preferentemente entre la tensión de alimentación externa de la tarjeta 101 chip y la tensión de programación máxima. Si la tensión se encuentra por debajo de la tensión de programación mínima, se asigna un conversor de CC a CC, especialmente un conversor elevador o una bomba de carga, a cada unidad 112; 113 de memoria, que transforma la tensión proporcionada por la unidad 114 de alimentación eléctrica en la tensión de programación de la unidad 112; 113 de memoria pertinente. Si la tensión se encuentra entre las tensiones de programación de las unidades 112, 113 de memoria, la tensión proporcionada por la unidad 114 de alimentación eléctrica puede usarse como tensión de programación para la unidad 112; 113 de memoria que requiere la tensión de programación más baja, es decir, la memoria 113 flash, y un conversor de CC a CC puede generar la tensión de programación para la otra unidad 112 de memoria, es decir, la EEPROM 112, a partir de la tensión proporcionada por la unidad 114 de alimentación eléctrica.

Preferentemente, puede cargarse la unidad 114 de alimentación eléctrica conectándola al terminal 106a de alimentación de la tarjeta 101 chip, mientras que la tarjeta 101 chip se alimenta con energía por el dispositivo 102 anfitrión. Preferentemente, la carga se controla por una unidad de gestión de energía del microcontrolador 104, que

puede comprender una aplicación correspondiente ejecutada en el procesador 108 principal o en otra unidad de cálculo del microcontrolador 104. Preferentemente, la unidad de gestión de energía dispone de un mecanismo para determinar el estado de carga de la unidad 114 de alimentación eléctrica. Si se determina que la capacidad de la unidad 114 de alimentación eléctrica está por debajo de un umbral predeterminado, se realiza la carga, cuando se determina que la tarjeta 101 chip se alimenta con energía por el dispositivo 102 anfitrión y, preferentemente, cuando el microcontrolador 104 funciona a baja carga. En este último caso, la corriente de alimentación del microcontrolador 108 es más baja, y se garantiza que la corriente suministrada a la tarjeta 101 chip no supere un umbral determinado debido a la corriente de carga. Si el coprocesador 109 se alimenta con energía exclusivamente por la unidad 114 de alimentación eléctrica, la carga puede realizarse, preferentemente, cuando el coprocesador 109, que se hace funcionar normalmente de manera intermitente, no ejecuta un cálculo.

Aunque la invención se ha ilustrado y descrito con detalle en los dibujos y la descripción anterior, tal ilustración y descripción deben considerarse ilustrativas o ejemplares y no restrictivas; la invención no se limita a las realizaciones desveladas.

En particular, la invención no se limita a los dispositivos 102 anfitriones configurados como dispositivos de comunicaciones móviles y a las tarjetas 101 chip configuradas como tarjetas SIM. Por el contrario, la invención puede implementarse en relación con dispositivos 102 anfitriones y tarjetas 101 chip arbitrarios.

Además, las diferentes realizaciones descritas anteriormente pueden combinarse. En consecuencia, puede usarse una unidad 114 de alimentación eléctrica para suministrar, al menos temporalmente, energía a un procesador 108; 109 y a una o más unidades 112, 113 de memoria. De manera similar, una tarjeta 101 chip puede estar equipada con varias unidades 114 de alimentación eléctrica, estando cada una adaptada para suministrar, al menos temporalmente, energía a uno o más componentes predeterminados del microcontrolador 104. Por ejemplo, puede proporcionarse una unidad 114 de alimentación eléctrica para suministrar energía al procesador 108 principal y/o al coprocesador 109, y puede proporcionarse una segunda unidad 114 de alimentación eléctrica para suministrar energía a una o más unidades 112, 113 de memoria. De manera similar, puede asignarse a cada unidad 112, 113 de memoria una unidad 114 de alimentación eléctrica de la tarjeta 101 chip que proporciona la tensión de programación para la unidad 112, 113 de memoria pertinente.

A partir de un estudio de los dibujos, la divulgación y las reivindicaciones adjuntas, pueden entenderse y realizarse por los expertos en la materia otras variantes de las realizaciones desveladas para poner en práctica la invención reivindicada.

En las reivindicaciones, la palabra "comprende" no excluye otros elementos o etapas, y el artículo indefinido "un" o "una" no excluye una pluralidad. Un único procesador u otra unidad pueden cumplir las funciones de varios elementos mencionados en las reivindicaciones. El mero hecho de que determinadas medidas se mencionen en reivindicaciones dependientes diferentes entre sí no indica que no pueda usarse de manera ventajosa una combinación de estas medidas.

Ningún signo de referencia en las reivindicaciones debe interpretarse como limitante del alcance.

REIVINDICACIONES

1. Una tarjeta (101) chip para insertar en un dispositivo (102) anfitrión, comprendiendo la tarjeta (101) chip un microcontrolador (104), incluyendo el microcontrolador (104) un procesador (108; 109) y una unidad (112; 113) de memoria y estando el microcontrolador (104) conectado a un terminal (106a) de alimentación de la tarjeta (101) chip para recibir energía de un primer medio (107) de alimentación eléctrica del dispositivo (102) anfitrión, **caracterizada porque** la tarjeta (101) chip comprende un segundo medio (114) de alimentación eléctrica, siendo el segundo medio (114) de alimentación eléctrica una fuente (114) de energía independiente del primer medio de alimentación eléctrica y estando el segundo medio (114) de alimentación eléctrica configurado para suministrar, al menos temporalmente, energía a un primer componente del microcontrolador (104), mientras que los componentes adicionales del microcontrolador (104) se alimentan con energía a través del terminal (106a) de alimentación.

2. La tarjeta (109) chip de acuerdo con la reivindicación 1, en la que el primer componente puede hacerse funcionar en un primer y en un segundo modo de funcionamiento, alimentándose el primer componente, en el primer modo de funcionamiento, con energía a través del terminal (106a) de alimentación y alimentándose el primer componente, en el segundo modo de funcionamiento, con energía a través del segundo medio (114) de alimentación eléctrica.

3. La tarjeta (101) chip de acuerdo con una de las reivindicaciones anteriores, en la que el primer componente electrónico es un procesador (108) principal y/o un coprocesador (109) del microcontrolador (104), especialmente un coprocesador criptográfico.

4. La tarjeta (101) chip de acuerdo con la reivindicación 3, en la que, en el segundo modo de funcionamiento, el procesador (108; 109) se hace funcionar a una frecuencia de reloj aumentada y/o a una tensión aumentada con respecto al primer modo de funcionamiento.

5. La tarjeta (101) chip de acuerdo con la reivindicación 4, en la que la tensión aumentada se corresponde con la tensión proporcionada por el segundo medio (114) de alimentación eléctrica.

6. La tarjeta (101) chip de acuerdo con una de las reivindicaciones 2 a 5, en la que el procesador (108; 109) se hace funcionar en el segundo modo de funcionamiento, cuando se determina que un procedimiento predeterminado se ejecuta en el procesador (108; 109).

7. La tarjeta (101) chip de acuerdo con una de las reivindicaciones anteriores, en la que al menos un procesador (108; 109) del microcontrolador (104) se alimenta con energía exclusivamente por el segundo medio (114) de alimentación eléctrica.

8. La tarjeta (101) chip de acuerdo con una de las reivindicaciones anteriores, en la que el primer componente electrónico es una unidad (112; 113) de memoria de un primer tipo, estando el segundo medio (114) de alimentación eléctrica adaptado para proporcionar una tensión de programación para borrar y/o almacenar información en la unidad (112; 113) de memoria.

9. La tarjeta (101) chip de acuerdo con una de las reivindicaciones anteriores, en la que el microcontrolador (104) comprende al menos dos unidades (112, 113) de memoria de tipos diferentes que tienen tensiones de programación diferentes, en la que el segundo medio (114) de alimentación eléctrica proporciona energía para borrar y/o almacenar información en las unidades de memoria.

10. La tarjeta (101) chip de acuerdo con la reivindicación 9, en la que el segundo medio (114) de alimentación eléctrica está adaptado para proporcionar una tensión correspondiente a la tensión de programación de una primera unidad (112; 113) de memoria de las unidades (112; 113) de memoria.

11. La tarjeta (101) chip de acuerdo con una de las reivindicaciones anteriores, en la que el segundo medio (114) de alimentación eléctrica es una batería recargable, y la batería puede cargarse suministrando energía a la batería a través del terminal (106a) de alimentación.

12. La tarjeta (101) chip de acuerdo con una de las reivindicaciones anteriores, en la que la tarjeta (101) chip es una tarjeta SIM.

13. Un dispositivo que comprende una tarjeta (101) chip de acuerdo con una de las reivindicaciones anteriores y que comprende, además, un primer medio (107) de alimentación eléctrica, estando el primer medio (107) de alimentación eléctrica configurado para suministrar energía al terminal (106a) de alimentación de la tarjeta (101) chip.

14. El dispositivo de acuerdo con la reivindicación 13, en el que el dispositivo (102) es un dispositivo de comunicaciones móviles y la tarjeta (101) chip es una tarjeta SIM.

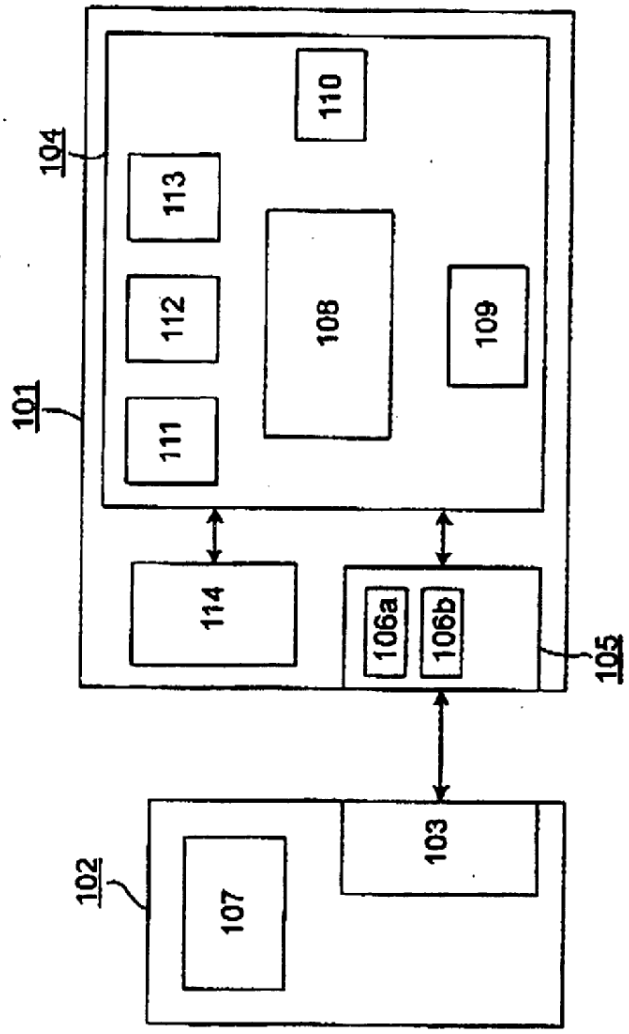

Fig. 1