Fecha de Realización de la Opinión Escrita: 20.02.2023

Declaración:

Novedad (Art. 6.1 LP 24/2015)	Reivindicaciones Reivindicaciones	1-17	**SI** **NO**
Actividad Inventiva (Art. 8.1 LP 24/2015)	Reivindicaciones Reivindicaciones	1-17	**SI** **NO**
Aplicación Industrial (Art. 9 LP 24/2015)	Reivindicaciones Reivindicaciones	1-17	**SI** **NO**

Base de la Opinión. -

La presente opinión se ha realizado sobre la base de la solicitud de patente con los documentos recibidos en fecha 21/12/2022.
.

1. Documentos considerados. -

A continuación, se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	CN 113657889 A (ZHEJIANG WEIRONG ELECTRONIC CO LTD)	16.11.2021
D02	CN 113347616 A (SHENZHEN HUASHU CLOUD COMPUTING TECH CO LTD)	03.09.2021
D03	CN 201622584U U (SHANGHAI KINGTRUST INFORMATION TECHNOLOGIES CO LMT)	03.11.2010

2. Declaración motivada según el artículo 26.5 del Reglamento de ejecución de la Ley 24/2015, de 24 de Julio, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración.

El documento D01 presenta un monedero electrónico que comprende un microcontrolador para enviar y recibir comandos de control, calcular parámetros y ejecutar programas; un chip de cifrado; un módulo de red; un módulo NFC para lectura y escritura de dispositivos NFC; un módulo Bluetooth; un módulo de posicionamiento y un módulo de memoria. El dispositivo permite la lectura y escritura de tarjetas IC a través de NFC; simular señales de tarjetas IC y de llaves, reemplazando las llaves de cerraduras de puertas y automóviles.
La carcasa del dispositivo incluye un componente de cifrado con un chip de cifrado y está provista de pantalla táctil, batería, cámara frontal y cámara trasera.
La lectura y escritura de tarjetas IC, principalmente a través de NFC, adopta un método de autorización jerárquico que se implementa a través del módulo de autorización. La autorización general es principalmente para tarjetas IC ordinarias y la autorización especial para tarjetas con información confidencial, como tarjetas de identificación, tarjetas bancarias, etc… El método de autorización utiliza contraseñas y reconocimiento facial, la autorización especial utiliza además la autorización del chip de cifrado interrumpiéndose conexión a red y el usuario debe ingresar el código PIN preestablecido.
Con referencia a la Figura 19, también utiliza un programa de seguridad a través de la cámara trasera que obtiene la imagen de la cara del usuario y compara esta imagen con la imagen de cara preestablecida.
La comunicación encriptada entre el servidor y la billetera electrónica puede usar los métodos de clave pública y clave privada existentes.
Los titulares del dispositivo deben realizar el registro de usuario en el que se requiere autenticación de información y se establecen los permisos y condiciones de utilización del monedero electrónico.

El documento D02, con referencia a la figura 1 del documento, presenta un sistema de monedero hardware de moneda digital tipo tarjeta. El sistema comprende un chip de control principal (11), un chip criptográfico (12), un chip de memoria (13), un módulo de visualización (14) y un módulo de comunicación NFC (15). El chip de control principal (11) se usa para administrar cada módulo y conectarlo a una estructura unificada de modo que el dispositivo inteligente (2) que participa en la transacción puede acceder a cada módulo a través del protocolo NFC del módulo de comunicación NFC (15). El chip criptográfico (12) es responsable de la gestión de claves, la generación de claves públicas y la operación de firma digital de datos. El módulo de comunicación NFC (15) se utiliza para comunicar la tarjeta de monedero hardware (1) con el dispositivo inteligente (2) que participa en la transacción.

La reivindicación 1ª se refiere a un dispositivo para encriptación de claves privadas / semillas de monederos de criptoactivos y almacenamiento en tarjetas NFC que comprende:
-un primer microcontrolador con un primer microprocesador con sistema operativo, memoria de almacenamiento de firmware, e interfaces con el resto de elementos del dispositivo,
-un elemento seguro del hardware que comprende un segundo microcontrolador con un segundo microprocesador y firmware separado físicamente del primer microcontrolador para las funciones de generación de criptogramas y gestión de cualquier dato sensible del proceso.
-un lector/escritor de tarjetas NFC.
-una pantalla.
-un teclado.
-unos lectores de variables biométricas.
-una fuente de alimentación.
donde el elemento seguro del hardware comprende una memoria segura separada de la memoria de funcionamiento general, para almacenar datos de máxima seguridad.

No aparece en el documento más cercano del estado de la técnica D01 las características de incluir en el monedero electrónico dos microcontroladores uno de ellos dedicado al encriptado/desencriptado así como un lector de variables biométricas.

El método de la reivindicación independiente 4ª para el encriptado/desencriptado de las claves/semillas sigue un procedimiento que tampoco se ha descrito en el estado de la técnica.

De igual forma, no se han encontrado en el estado de la técnica sugerencias que guíen de manera sencilla e inmediata al experto en la materia hacia la consecución del objeto técnico de las reivindicaciones 1ª y 4ª.

Consideramos en consecuencia, que las reivindicaciones 1ª- 17ª son nuevas y tienen actividad inventiva (Artículos 6,8 LP).