(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 818 628**

(51) Int. CI.:

G06F 21/53 (2013.01)
G06F 9/455 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.06.2015 E 15173096 (7)**

(97) Fecha y número de publicación de la concesión europea: **26.08.2020 EP 3109788**

(54) Título: **Entorno de usuario basado en micronúcleo, arquitectura de red y motor interno seguro para impedir la pérdida de información**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.04.2021

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE

(72) Inventor/es:

PEYLO, CHRISTOPH;
SCHMIDT, AUBREY-DERRICK y
SEIFERT, JEAN-PIERRE

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Entorno de usuario basado en micronúcleo, arquitectura de red y motor interno seguro para impedir la pérdida de información

La invención se refiere a un entorno de usuario para el uso en una arquitectura de red y una arquitectura de red correspondiente y un motor interno seguro correspondiente.

La fuga de información, es decir, transferencia de información indeseada en sistemas realmente asegurados, es un problema clásico de la seguridad de información que solo se puede resolver hasta ahora de forma limitada. A este respecto, una de las fuentes principales para la transferencia de información indeseada es el usuario autorizado, que transfiere a un tercero no autorizado datos sensibles, confidenciales y/o clasificados de forma intencionada o no intencionada.

Las contramedidas conocidas por el estado de la técnica intervienen en el plano organizativo y técnico:

a) Organizativo:

- Las directivas o políticas definen el trato con la información, pero se vuelven inútiles o ineficaces debido al sencillo incumplimiento cuando el incumplimiento permanece desconocido.
- La clasificación representa igualmente un medio organizativo para la lucha contra la fuga de información, dado que los datos se clasifican en categorías conforme a su significado, para las cuales se definen diferentes grupos de autorización y pautas de comportamiento.
- Los mecanismos de control de accesos impiden el acceso físico a la información digna de protección.

b) Técnico

- Las arquitecturas de gestión de identidad y sistemas de control de accesos controlan y conceden el acceso a recursos limitados. La separación en dominios ayuda en este caso a hacer gestionables los controles de la información.
- La encriptación impide que terceros reciban acceso de forma no autorizada a los contenidos.
- Las plataformas informáticas fiables (Trusted Computing Plattform, TCP) intentan aportar las limitaciones del lado de hardware, en tanto que los componentes dignos de confianza controlan el acceso a operaciones sensibles. Las funciones principales de las TCP se pueden ver en la identificación de entornos (de hardware) y la protección de materiales criptográficos.

Sin embargo, una desventaja del estado de la técnica es que el uso y la funcionalidad de estas contramedidas organizativas y técnicas contra la fuga de información se pueden anular debido al comportamiento incorrecto del usuario.

Esto se destaca por estudios (2007) que ven los motivos principales en la fuga de información premeditada en “trabajadores indisciplinados” (77%) y “propósitos malintencionados” (23%) (véase la referencia [1]).

Los otros casos se refieren a interfaces de información de sistemas informáticos, que le ofrecen al usuario entre otros, gracias a una conectividad de USB, conectividad de web o conexión de correos electrónicos, la posibilidad de difundir información sensible.

Pero debido a la computarización creciente y movilidad correspondiente se debe observar la aparición multiplicada de acontecimientos de fuga de información fundamentados en la tecnología informática. Aumentan los ataques basados en firmware / controladores, así como el aprovechamiento de las debilidades de desbordamiento de búfer y conducen incluso en sistemas presuntamente protegidos a que se “ataque” la información.

Los sistemas operativos monolíticos (p. ej. Linux) presentan en el área de núcleo todos los componentes de sistema o funciones importantes y solo separan de ello las aplicaciones de usuario.

La desventaja de estos sistemas operativos es que, en el caso de ataque del plano de núcleo, p. ej. en un controlador en el modo privilegiado, esta arquitectura monolítica puede conducir a una toma del sistema global y se posibilita la exposición de información sensible.

El núcleo híbrido o también maco (p. ej. WIN 8, Mac OS X) intentan resolver este problema, en tanto que retiran partes del área de núcleo que no se deben funcionar de forma privilegiada. No obstante, a través de ataques basados en escalaciones de derechos es posible recibir un acceso completo a los sistemas atacados.

Un micronúcleo (p. ej. L4, véase la referencia [2]; QNX, véase la referencia [3]; o PikeOS, véase la referencia [4]) por el contrario solo posee funciones elementales en el área de núcleo, que se refieren en general a la gestión de memoria y proceso (virtual). Por consiguiente, la base de código atacable es muy pequeña y en el caso L4 está reducida a

aprox. 40.000 líneas de código.

Todos los otros componentes se realizan de forma separada o aislada en el modo de usuario, y no en el modo de núcleo.

Así, se pueden separar unos de otros p. ej. controladores, conexión a red, programas de usuario, memoria dividida, interfaces, aplicaciones o servicios del sistema. Los ataques se pueden propagar así difícilmente a otros componentes y comprometerlos.

Los dominios especiales, como por ejemplo operaciones criptográficas, se pueden aislar así tan fuertemente que los ataques sobre ellos se pueden dificultar mucho o casi excluir.

Por los documentos US2012/272240A1 y US2008/016313A1 se conocen otros entornos basados en micronúcleo.

En principio, la división de un sistema operativo de micronúcleo se puede implementar en caso de necesidad y según la finalidad de uso. Los micronúcleos, como el L4, ofrecen como base la posibilidad de permitir que otros sistemas operativos y componentes funcionen de forma virtualizada (tipo 1 virtualización). Esta virtualización ofrece una protección adicional dado que el micronúcleo actúa como capa de abstracción entre controlador / sistema operativo y hardware.

Adicionalmente, en un micronúcleo L4 es posible permitir que las aplicaciones de micronúcleo de poco peso funcionen de forma visualizada, las cuales pueden adoptar p. ej. tareas de gestión y control en el sistema.

Como modelo de acceso, en el micronúcleo L4 se usa el "Capability-based Access Control (control de accesos basado en la capacidad)", es decir, cada derecho de acceso se otorga en el sistema a través de “capacidades” o capabilities. Además, estas capacidades se establecen en el tiempo de compilación y no se pueden cambiar en el tiempo de ejecución. En este caso, una capacidad puede ser un derecho de acceso a un componente, un servicio, un recurso, etc., que también se puede ocupar con un protocolo de procesamiento propio. En este caso, este protocolo puede contener incluso chequeos de seguridad, para proteger servicios, componentes o recursos en peligro.

En el pasado, con frecuencia se han dejado de lados los micronúcleos, que también pueden gestionar varias instancias de sistemas operativos virtualizados, por motivos de rendimiento y recursos. No obstante, la TI moderna ofrece actualmente recursos suficientes para dotar incluso sistemas móviles con un micronúcleo en tal configuración.

La referencia [5] se refiere a un sistema y un procedimiento para el funcionamiento simultáneo de varios entornos de sistemas operativos en una plataforma de hardware. A este respecto se usa un micronúcleo que aloja varios sistemas operativos simultáneamente en un sistema.

La referencia [6] ofrece computación fiable con un micronúcleo.

La referencia [7] se refiere a un micronúcleo que está particionado en un espacio de direcciones de comunicación, un espacio de direcciones aumentado en seguridad y un espacio de direcciones de operación asegurado.

La referencia [8] se refiere a un aparato de comunicación móvil, que presenta un micronúcleo. Un núcleo L4 proporciona un dominio abierto, que puede usar el usuario para aplicaciones propias, y un dominio seguro separado, en el que se almacenan datos críticos para la seguridad.

Lista de referencias:

[1] - https://securelist.com/analysis/internal-threats-reports/36200/internaMt-threats-in-russia-in-2007-2008-summary-and-forecast/
[2] - L4 Mikrokern http://sigops.org/sosp/sospl3/papers/pl33-elphinstone.pdf
[3] - QNX http://www.qnx.de
[4] - PikeOS http://www.sysgo.com/products/pi- keos-rtos-and-virtualization-concept/
[5] - US 5,764,984 A
[6] - Setapa, S.; Isa, M.A.M.; Abdullah, N.; Manan, J.-L.A., "Trusted computing based microkernel," Computer Applications and Industrial Electronics (ICCAIE), 2010 International Conference on, 5-8 Dec. 2010
[7] - US 8,402,267 B1
[8] - SiMKo3 SMartphoneS; http://www.t-sys- tems.de/umn/t-systems-flyer-simko3-smartphones- aber-sicher-die-sichere-mobile-zukunft-hat-begon- nen-/1123256_1/blobBinary/Flyer-SiMKo3.pdf

La invención tiene el objetivo de proporcionar un entorno de red para el uso en una arquitectura de red, una arquitectura de red y un motor interno seguro para el uso en una arquitectura de red.

Este objetivo se consigue con los procedimientos o los dispositivos según las reivindicaciones independientes.

Las reivindicaciones dependientes se refieren a otros aspectos de la invención.

A este respecto, la invención parte de la idea fundamental de que mediante la separación lógica de todos los componentes críticos, tanto en el plano horizontal (aislamiento) como también en el plano vertical (virtualización), se minimiza la superficie de ataque en el sistema de usuario o el entorno de usuario o el *User Environment* (UE).

El micronúcleo como base de ejecución misma no está disponible desde fuera por su gama de funciones limitada e integración en el sistema.

Uno de los puntos clave de la invención es la elaboración de un entorno de usuario seguro o de un *User Environment* en base a una arquitectura de micronúcleo. El micronúcleo o el entorno en tiempo de ejecución correspondiente permiten la generación y gestión de dominios y/o aplicaciones de micronúcleo.

Se pueden implementar uno o varios dominios de usuario que le dan al usuario margen libre de manipulación, pero trabajan estrictamente separados de los otros dominios. Un área de trabajo segura implementa medidas que impidan la fuga de información, pero no el trabajo productivo. Una unidad de “expedidor” se ocupa de la comunicación exterior e impide la “fuga de información” vía interfaces de comunicación / canal lateral. Cada controlador crítico se realiza de forma aislada en un dominio, donde las interfaces correspondientes o servicios ofertados se definen e implementan de forma restrictiva, de modo que se impide una propagación de ataques de y hacia el controlador.

Las aplicaciones de micronúcleo de poco peso aportan una seguridad adicional en tanto que realizan chequeos de seguridad de otros dominios / componentes.

La invención se refiere a un entorno de usuario para el uso en una arquitectura de red, que comprende: un sistema operativo de micronúcleo, un entorno en tiempo de ejecución correspondiente y varios dispositivos, donde los varios dispositivos son dominios y/o aplicaciones de micronúcleo originados por virtualización. Los dispositivos están aislados unos de otros.

La virtualización de los dominios y/o aplicaciones de micronúcleo tiene lugar en el sistema operativo de micronúcleo.

El sistema operativo de micronúcleo y el entorno en tiempo de ejecución correspondiente forman la base de la presente invención. Preferentemente, el sistema operativo de micronúcleo y el entorno en tiempo de ejecución correspondiente se pueden transferir a cualquier arquitectura de a bordo / CPU.

Preferentemente, el micronúcleo usa las capacidades para distribuir derechos de acceso en el sistema (véase p. ej. http://en.wikipedia.org/wiki/Capability-based_security).

Preferentemente, en el dominio se pueden hacer funcionar de forma virtualizada un sistema operativo o partes de un sistema operativo. Preferentemente, las partes de un sistema operativo son sistemas adaptados a los requerimientos y funciones del dominio y/o del uso del entorno de usuario, que pueden asumir tareas dedicadas, preferentemente la facilitación de un área de trabajo segura o la gestión de controladores aislados.

Preferentemente, las aplicaciones de micronúcleo son programas, de forma especialmente preferida programas de poco peso, que están limitados en su gama de funciones, pero se tratan por el sistema operacional de micronúcleo igual que los dominios.

El entorno de usuario presenta un primer dispositivo que es apropiado para proporcionar al menos un servicio aislado y proporcionar acceso a al menos un servicio a otros dispositivos. El primer dispositivo puede ser un dominio o una aplicación de micronúcleo.

Preferentemente, el primer dispositivo proporciona acceso a los servicios a otros dispositivos, los cuales son necesarios para el procesamiento de datos.

Preferentemente, de forma especialmente preferida según el tamaño y complejidad, los servicios también se pueden proporcionar en forma de aplicaciones de micronúcleo a los otros dispositivos. Preferentemente, de forma especialmente preferida según la necesidad de seguridad y posibilidad, cada servicio puede aparecer por separado como instancia independiente o en una colección dentro de un dispositivo, es decir, de un dominio y/o una aplicación de micronúcleo.

El entorno de usuario presenta un segundo dispositivo que presenta un dominio que presenta un sistema operativo propio que es apropiado para ejecutar solo funciones y programas predefinidos en un modo de usuario.

Preferentemente, el sistema operativo propio del segundo dominio puede ser Windows, Linux o Android. Preferentemente, el sistema operativo está adaptado en tanto que en él solo se pueden ejecutar funciones y programas predefinidos en el modo de usuario. Preferentemente son posibles el procesamiento de documentos y la comunicación con el motor interno seguro y otros entornos de usuario. Preferentemente, el dominio de seguridad no se puede

comunicar de forma independiente con entidades externas, sino que depende para ello de un tercer dispositivo. Preferentemente se impide otra comunicación.

El entorno de usuario presenta un tercer dispositivo, donde el tercer dispositivo presenta un dominio que es apropiado para comunicar con un servidor de envío externo dedicado y recibir solicitudes de comunicación de uno o varios otros dominios del entorno de usuario y/o una o varias aplicaciones de micronúcleo, procesarlas a solicitudes de envío y transmitirlas al servidor de envío y recibir las respuestas a las solicitudes de envío del servidor de envío.

Preferentemente, el tercer dispositivo, también denominado expedidor, es el componente central para impedir la fuga de información a través de canales laterales en comunicación de internet externa a partir del dominio seguro. Preferentemente, el expedidor comunica para ello con el servidor de envío externo dedicado, que acepta y procesa las solicitudes de envío del expedidor.

Preferentemente, para aplicaciones y/o servicios permitidos solo es posible dirigirse al tercer dominio, es decir, el expedidor y enviar a través de estas solicitudes correspondientes al servidor de envío. Preferentemente, todas las otras rutas de comunicación están desactivadas, en tanto que a través de ellas no es posible una comunicación. Por consiguiente, se garantiza que solo esta ruta de comunicación se puede usar desde el aparato / el entorno de usuario.

En otras palabras, la propiedad del expedidor se limita en comparación a un túnel VPN, en tanto que el túnel VPN tiene el objetivo de proteger los datos transportados contra acceso no autorizado y opcionalmente también modificación desde fuera. El expedidor por el contrario asegura contra el acceso desde dentro, es decir, un aparato comprometido solo permite una comunicación limitada o incluso ninguna comunicación para el atacante.

El entorno de usuario presenta un cuarto dispositivo, que presenta un sistema cortafuegos, que es apropiado para impedir cualquier tipo de comunicación entrante o saliente del entorno de usuario aparte de la comunicación a través del expedidor. Preferentemente, el cuarto dispositivo se ocupa de que únicamente se permita la comunicación pretendida a través del expedidor.

Preferentemente, el cuarto dispositivo presenta una aplicación de microprocesador. Preferentemente, el cuarto dispositivo ejecuta chequeos de integridad iniciales y/o cíclicos de componentes importantes, en particular la verificación de sumas de comprobación, p. ej. SHA256. Preferentemente, componentes importantes son al menos uno de los siguientes: firmwares, servicios, operaciones, controladores, componentes de sistema u otras partes clasificadas como importantes. Preferentemente, la constatación de qué se considera como importante se deduce de la respectiva finalidad de uso de la solución.

El entorno de usuario presenta un quinto dispositivo, donde el quinto dispositivo presenta un dominio, que es apropiado para ejecutar de forma aislada cada controlador del entorno de usuario y poner a disposición los servicios y/o interfaces correspondientes del controlador a los otros componentes del entorno de usuario.

Preferentemente, en un dominio originado por virtualización se ejecutan de forma aislada los controladores. Preferentemente, a través de conexiones y servicios asegurados se ponen a disposición los componentes relevantes para ello.

Según una forma de realización de la invención, el entorno de usuario presenta un sexto dispositivo, que presenta un dominio que es apropiado para ejecutar de forma aislada operaciones criptográficas.

La ejecución aislada de la operación criptográfica eleva significativamente la seguridad, según la finalidad de uso. Preferentemente, las operaciones criptográficas, si no se ejecutan de forma aislada en el sexto dispositivo, se proporcionan junto con otras funciones.

Según una forma de realización de la invención, el entorno de usuario presenta un séptimo dispositivo, que presenta un dominio que presenta un sistema operativo propio, que es apropiado para ejecutar funciones y programas.

Preferentemente, para permitirles a los usuarios la posibilidad del uso no restrictivo del aparato, el séptimo dispositivo se puede ejecutar de forma aislada con un dominio abierto independiente. En este dominio, el usuario es capaz de realizar actividades sin limitaciones especiales, donde el acceso a las otras zonas está estrictamente limitado. Solo servicios mínimos, p. ej. para la comunicación de internet o el control, se ponen a disposición de forma fuertemente asegurada.

Según una forma de realización, las solicitudes de envío presentan al menos un ítem de una información siguiente:

- tamaño de la carga útil,
- instante de la transmisión,
- emisor de la comunicación,
- receptor de la comunicación,
- autor de la solicitud de comunicación al expedidor,

- firma criptográfica, preferentemente en base a una infraestructura de clave pública.

Según una forma de realización de la invención, el tercer dominio es apropiado para verificar la autorización de los dispositivos para la comunicación a través del tercer dominio.

Según una forma de realización de la invención, el tercer dominio es apropiado para conseguir acceso a una memoria de datos del motor interno a través de un modelo de control de accesos, donde el modelo de control de accesos es preferentemente al menos uno de los siguientes: modelo de control de accesos discrecional (Discretionary Access Control, DAC), modelo de control de acceso basado en roles (Role-based Access Control, RBAC) o modelo de control de acceso obligatorio (Mandatory Access Control, MAC).

Según una forma de realización de la invención, el tercer dominio es apropiado para comunicar con un tercer dominio de un segundo entorno de usuario a través de un servidor de comunicación del motor interno conectado con el servidor de envío.

Según una forma de realización de la invención, el tercer dominio es apropiado para acceder a un servidor web conectado con el servidor de envío.

La invención se refiere a una arquitectura de red, que comprende: al menos un entorno de usuario según cualquiera de las formas de realización anteriores, un motor interno seguro y un servidor de envío, donde el servidor de envío es apropiado para aceptar las solicitudes de envío y datos que llegan de al menos un entorno de usuario, seleccionarlos y transferirlos a los componentes del motor interno seguro y transferir los datos de los componentes del motor interno seguro a al menos un entorno de usuario, y donde el motor interno seguro presenta un servidor de acceso al motor interno, que está protegido por un dispositivo de protección y presenta una gestión de identidad y un sistema de control de accesos, que es apropiado para reglamentar el acceso a un motor interno seguro.

Preferentemente, el servidor de envío es parte del motor interno seguro.

Según una forma de realización preferida de la invención, el motor interno seguro comprende además una memoria de datos, que está configurada de manera que un tercer dispositivo de un entorno de usuario puede obtener acceso a la memoria de datos a través de un modelo de control de accesos, donde el modelo de control de accesos es preferentemente al menos uno de los siguientes: modelo de control de accesos discrecional (Discretionary Access Control, DAC), modelo de control de acceso basado en roles (Role--based Access Control, RBAC) o modelo de control de acceso obligatorio (Mandatory Access Control, MAC).

Según una forma de realización de la invención, la arquitectura de red presenta al menos un primer y un segundo entorno de usuario según una de las formas de realización anteriores.

Preferentemente, el motor interno seguro presenta un servidor de comunicación, que está conectado con el servidor de expendido y que está configurado de manera que un tercer dominio del primer entorno de usuario se puede comunicar con un tercer dominio del segundo entorno de usuario a través del servidor de comunicación.

La invención se refiere a un motor interno seguro para el uso en una arquitectura de red que comprende: un servidor de acceso al motor interno que presenta un sistema de control de accesos, que es apropiado para reglamentar el acceso al motor interno seguro, y un servidor de envío, que es apropiado para aceptar solicitudes de envío y datos que llegan de al menos un entorno de usuario según las formas de realización anteriores, seleccionarlos y transmitirlos a otros componentes del motor interno seguro y transmitir los datos de los otros componentes del motor interno seguro a al menos un entorno de usuario.

Preferentemente, el motor interno seguro (en inglés *Secure Backend*) puede presentar distintos componentes, pero que todos deben seguir una configuración técnica de seguridad.

Preferentemente, el servidor de acceso al motor interno seguro presenta una gestión de identidad.

Preferentemente, el servidor de acceso al motor interno se protege por un dispositivo de protección, donde el dispositivo de protección presenta de forma especialmente preferible al menos un cortafuegos y/o al menos un sistema de reconocimiento de intrusión (en inglés, Intrusion Detection System - IDS) y/o al menos un sistema de reconocimiento y prevención de intrusión (en inglés, Intrusion Detection and Prevention System).

Preferentemente, el sistema de control de accesos presenta un servidor de acceso a la red privada virtual (Virtual Private Network, VPN) o un sistema de acceso de propietario, que está configurado de modo que la comunicación con el motor interno seguro está encriptada de forma segura.

Preferentemente, el motor interno seguro presenta un servidor web de intranet, que es apropiado para la distribución de información interna dentro de la arquitectura de red. Preferentemente, el motor interno seguro presenta un servidor web de intranet, que solo es accesible a través de entornos de usuario autorizados. Preferentemente, el motor interno

seguro presenta un servidor web de intranet, que es apropiado para la distribución de información interna dentro de la arquitectura de red y que solo es accesible a través de entornos de usuario autorizados.

Preferentemente, el servidor de envío acepta consultas de comunicación del expedidor de servicio de terminal, es decir, del expedidor de entorno de usuario. Preferentemente, el servidor de envío es parte del servidor de acceso al motor interno. Preferentemente, el servidor de envío es parte de la infraestructura de un operador de red (de telefonía móvil). Preferentemente, una parte del servidor de envío es parte del servidor de acceso al motor interno y otra parte del servidor de envío es parte de la infraestructura de red de un operador de red (de telefonía móvil).

En general se debería garantizar que el motor interno seguro funcione en un entorno digno de confianza y se haga funcionar por personal digno de confianza.

Según una forma de realización preferida de la invención, el motor interno seguro comprende una memoria de datos, que está configurada de manera que un tercer dispositivo de un entorno de usuario puede obtener acceso a la memoria de datos a través de un modelo de control de accesos.

Preferentemente, la memoria de datos de motor interno puede presentar un sistema de gestión de documentos.

Preferentemente, la memoria de datos de motor interno puede presentar al menos uno de los siguientes: una base de datos, un servido de ficheros, servidor FTP, una memoria de red.

Preferentemente, la memoria de datos del motor interno puede servir como lugar de depósito central para la información. Preferentemente, a este respecto se implementa un modelo de control de accesos apropiado específico al caso.

Preferentemente, el modelo de control de accesos es al menos uno de los siguientes: modelo de control de accesos discrecional (Discretionary Access Control, DAC), modelo de control de acceso basado en roles (Role-based Access Control, RBAC) o modelo de control de acceso obligatorio (Mandatory Access Control, MAC).

Según una forma de realización de la invención, el motor interno seguro presenta un servidor de comunicación, que está conectado con el servidor de envío y que está configurado de manera que un tercer dominio de un primer entorno de usuario se puede comunicar según una de las formas de realización anteriores a través del servidor de comunicación con un tercer dominio de un segundo entorno de usuario según una de las formas de realización anteriores.

La invención aquí presentada interviene en estos problemas en el plano técnico, pero también ofrece medios auxiliares para resolver problemas basados en el papel. Así, por ejemplo, la información confidencial y/o clasificada no se debe memorizar / procesar siempre en ordenadores. Esta se imprime preferentemente. En el caso de impresión, en general existe el peligro de pérdida y copia de información confidencial. Cuando ahora ya no se imprime esta información, por ejemplo, y solo se pueden procesar, por ejemplo, de forma fuertemente asegurada en ordenadores, se resuelve el problema de las impresiones

Como base sirve un sistema operativo que sigue al enfoque de micronúcleo.

La invención se explica más en detalle a continuación mediante ejemplos y el dibujo. Muestran:
Figura 1 un diagrama esquemático de una forma de realización preferida de un entorno de red según la presente invención,
Figura 2 un diagrama esquemático de otra forma de realización preferida de un entorno de red según la presente invención,
Figura 3 un diagrama esquemático de otra forma de realización preferida de un entorno de red según la presente invención,
Fig. 4 un diagrama esquemático de una forma de realización preferida de un motor interno seguro según la presente invención, y
Fig. 5 un diagrama esquemático de una forma de realización preferida de una arquitectura de red según la presente invención.

La figura 1 muestra un diagrama esquemático de una forma de realización preferida de un entorno de red 100 según la presente invención. El entorno de usuario 100 presenta un sistema operativo de micronúcleo 101 y un entorno en tiempo de ejecución correspondiente (representado igualmente mediante la referencia 101). Además, el entorno de usuario 100 presenta varios dispositivos 110 a 150. Los dispositivos 110 a 150 están aislados entre sí, de modo que en principio no es posible una comunicación directa de los dispositivos 110 a 150 entre sí. Los varios dispositivos 110 a 150 son dominios y/o aplicaciones de micronúcleo que se originan por virtualización dentro del sistema operativo de micronúcleo 101. A este respecto, un primer dispositivo 110 es apropiado para proporcionar al menos un servicio aislado y proporcionar acceso a al menos un servicio a otros dispositivos 120 a 150. En el presente ejemplo, el al menos un servicio es necesario para el procesamiento de datos.

Un segundo dispositivo 120 presenta un dominio que presenta un sistema operativo que solo es apropiado para ejecutar funciones y programas predeterminados en un modo de usuario. En este caso se trata de un área de trabajo segura con un sistema operativo adecuado, en el que solo se pueden ejecutar funciones y programas definidos en el modo de usuario. Ante todo, son posibles el procesamiento de documentos y la comunicación con el motor interno seguro 200 descrito más abajo y otros entornos de usuario 100. No obstante, a este respecto se debe prestar atención que el segundo dispositivo 120 no se puede comunicar independientemente con entidades externas, sino que para ello depende del tercer dominio 130 descrito más abajo.

El entorno de usuario 100 también presenta un tercer dispositivo 130, que es apropiado para comunicar con un servidor de envío 201 externo dedicado y descrito más abajo y recibir las solicitudes de comunicación de uno o varios otros dominios y/o una o varias aplicaciones de micronúcleo. Estas solicitudes de comunicación se procesan formando solicitudes de envío y se le transmiten al servidor de envío. El tercer dispositivo 130 es apropiado igualmente para recibir las respuestas a las solicitudes de envío planteadas del servidor de envío y transmitirlas a los dominios y/o aplicaciones de micronúcleo correspondientes. En otras palabras, la comunicación segura de los otros dispositivos 110, 120, 140, 150 del entorno de usuario 100 funciona a través del tercer dispositivo 130.

El entorno de usuario 100 también presenta un cuarto dispositivo 140. El cuarto dispositivo 140 contiene un sistema cortafuegos, que es apropiado para impedir cualquier tipo de comunicación entrante o saliente del entorno de usuario 100 - a excepción de la comunicación a través del tercer dispositivo 130. Preferentemente, el cuarto dispositivo 140 también realiza chequeos de integridad iniciales y/o cíclicos de componentes importantes del entorno de usuario 100. Tales componentes importantes pueden ser entre otros firmwares, servicios, operaciones, controladores, componentes de sistema u otras partes clasificadas como importantes. A este respecto, la constatación de qué se considera como importante dentro del entorno de usuario 100 resulta de la respectiva finalidad de uso de la solución seguida con el entorno de usuario 100. Además, el cuarto dispositivo 140 también puede realizar la verificación de sumas de comprobación.

El entorno de usuario 100 presenta además un quinto dispositivo 150. A este respecto, el quinto dispositivo 150 presenta un dominio, que es apropiado para ejecutar de forma aislada cada controlador necesario del entorno de usuario 100 y poner a disposición los servicios y/o interfaces correspondientes del controlador a los otros componentes del entorno de usuario 100. Esta ejecución aislada de los respectivos controladores necesarios contribuye igualmente al concepto de seguridad global de la presente invención.

La figura 2 muestra un diagrama esquemático de otra forma de realización preferida de un entorno de red 100 según la presente invención. El entorno de usuario 100 según la figura 2 se diferencia a este respecto del entorno de usuario 100 según la figura 1 solo porque el entorno de usuario 100 según la figura 2 presenta otro dispositivo, el sexto dispositivo 160. Este dispositivo 160 está integrado en el entorno de usuario 100 en la misma medida que los entornos de usuario 110 a 150. El sexto entorno de usuario 160 es apropiado para ejecutar de forma aislada operaciones criptográficas. Esta ejecución aislada de la operación criptográfica aumenta significativamente, según la finalidad de uso, la seguridad de todo el entorno de usuario 100.

La figura 3 muestra un diagrama esquemático de otra forma de realización preferida de un entorno de red 100 según la presente invención. El entorno de usuario 100 según la figura 3 se diferencia a este respecto del entorno de usuario 100 según la figura 2 solo porque el entorno de usuario según la figura 3 presenta otro dispositivo, el séptimo dispositivo 170. El séptimo dispositivo 170 del entorno de usuario 100 presenta un dominio que presenta un sistema operativo propio, que es apropiado para ejecutar funciones y programas. El séptimo dispositivo 170 posibilita un uso abierto para el usuario, es decir, el usuario tiene la posibilidad del uso no restrictivo de aparato en el que funciona el entorno de usuario 100 y, por consiguiente, se ejecuta de forma asilada un dominio abierto independiente. En este dominio, el usuario es capaz de realizar actividades sin limitaciones especiales, donde el acceso desde el dominio abierto o el séptimo dispositivo 170 a los otros dispositivos 110 a 160 del entorno de usuario 100 está más estrictamente limitado o no es posible. Solo servicios mínimos, como p. ej. para el uso de la comunicación de internet o del control, se ponen a disposición de forma fuertemente asegurada.

La figura 4 muestra un diagrama esquemático de una forma de realización preferida de un motor interno seguro 200 según la presente invención. El motor interno seguro 200 presenta un servidor de acceso del motor interno y un servidor de envío. En la presente forma de realización, tanto el servidor de acceso del motor interno como también el servidor de envío están comprendidos por un servidor común 201. No obstante, se entiende que el servidor de acceso del motor interno también puede estar presente como el servidor de envío en respectivas unidades separadas. Así, por ejemplo, el servidor de envío es parte de la arquitectura de red de un operador de telefonía móvil. El servidor de acceso del motor interno presenta un sistema de control de accesos, que es apropiado para reglamentar el acceso al motor interno seguro. El servidor de envío es apropiado para aceptar las solicitudes de envío y datos que llegan del entorno de usuario 100, según se describe por ejemplo en las figuras 1 a 3, seleccionarlas y transmitirlas a otros componentes del motor interno seguro 200 y transmitir los datos o solicitudes correspondientes de los otros componentes del motor interno seguro 200 a este entorno de usuario 100. En otras palabras, la comunicación entre el entorno de usuario 100 y el motor interno seguro 200 funciona a través de este servidor de envío. En el presente ejemplo de realización, el servidor de acceso al motor interno presenta un dispositivo de protección, en cuestión un cortafuegos.

El motor interno seguro 200 presenta un servidor web de intranet 203, que es apropiado para la distribución de información interna dentro de la arquitectura de red. Este servidor web de intranet 203 es accesible a través de los entornos de usuario autorizados 100.

El motor interno seguro 200 presenta además un servidor de memoria de datos 202, que está configurado de manera que el tercer dispositivo 130 del entorno de usuario 100 puede obtener acceso a la memoria de datos / el servidor de memoria de datos 202 a través de un modelo de control de accesos.

El motor interno seguro 200 presenta además un servidor de mensajes instantáneos 204, es decir, un servidor de comunicación, a través del que un tercer dominio 130 de un primer entorno de usuario 100 se puede comunicar con un tercer dominio 130 de un segundo entorno de usuario 100. Para la misma finalidad, es decir, la comunicación de un entorno de usuario 100 con otro entorno de usuario 100, el motor interno seguro 200 presenta un servidor de correos electrónicos 205 según la presente invención.

La figura 5 muestra un diagrama esquemático de una forma de realización preferida de una arquitectura de red 1000 según la presente invención. La arquitectura de red 1000 presenta uno o varios entornos de usuario 100 según una forma de realización de la presente invención, que a través de una red de área amplia 300, p. ej. la internet, está o están conectado(s) con el motor interno seguro 200 según una realización de la presente invención. A modo de ejemplo, en la figura 5 está representado un motor interno seguro 200 según la forma de realización mostrada en la figura 4. No obstante, se entiende que cualquier otro motor interno seguro 200 es apropiado igualmente según la presente invención. A través de la arquitectura de red 1000 es posible que numerosos entornos de usuario 100 se puedan comunicar a través de conexión encriptada con el motor interno seguro 200, donde el motor interno seguro 200 es competente de forma centralizada para cualquier tipo de intercambio de información.

Aunque la invención se representa por medio de las figuras y la descripción correspondiente y está descrita de forma detallada, esta representación y esta descripción detallada se deben entender de forma ilustrativa y a modo de ejemplo y no como que limita la invención. Se entiende que los expertos en la materia pueden hacer cambios y modificaciones, sin abandonar el alcance de las reivindicaciones siguientes. En particular, la invención comprende igualmente formas de realización con cualquier tipo de combinación de características, que se mencionan o muestran anteriormente o a continuación, formando las distintas formas de realización.

La invención comprende igualmente características individuales en las figuras aun cuando allí no se muestran en relación con otras características y/o no se mencionan anteriormente o a continuación. Las alterativas descritas en las figuras y la descripción de formas de realización y alternativas individuales también pueden estar excluidas de sus características del objeto de la invención o de los objetos dados a conocer. La revelación comprende formas de realización, que comprende exclusivamente las características descritas en las reivindicaciones o en los ejemplos de realización, así como también aquellos que comprenden otras características adicionales.

REIVINDICACIONES

1. Entorno de usuario para el uso en una arquitectura de red, que comprende:

un sistema operativo de micronúcleo, un entorno en tiempo de ejecución correspondiente, y
varios dispositivos, donde los varios dispositivos son dominios y/o aplicaciones de micronúcleo originados por virtualización y los dispositivos están aislados entre sí,
donde un primer dispositivo está configurado para proporcionar al menos un servicio aislado y proporcionar acceso a al menos un servicio a otros dispositivos,
donde un segundo dispositivo presenta un dominio que presenta un sistema operativo propio que está configurado para ejecutar solo funciones y programas predefinidos en un modo de usuario,
donde un tercer dispositivo presenta un dominio que está configurado para comunicar con un servidor de envío externo dedicado y para recibir solicitudes de comunicación de uno o varios otros dominios del entorno de usuario y/o una o varias aplicaciones de micronúcleo, para procesar las solicitudes de envío y trasmitirlas al servidor de envío y recibir las respuestas a las solicitudes de envío del servidor de envío,
donde un cuarto dispositivo presenta un sistema cortafuegos, que está configurado para impedir cualquier tipo de comunicación entrante o saliente del entorno de usuario fuera de la comunicación a través del expedidor, y
donde un quinto dispositivo presenta un dominio, que está configurado para ejecutar de forma aislada cada controlador del entorno de usuario y poner a disposición los servicios y/o interfaces correspondientes del controlador a los otros componentes del entorno de usuario.

2. Entorno de usuario según la reivindicación 1, que comprende un sexto dispositivo que presenta un dominio, que está configurado para ejecutar de forma aislada operaciones criptográficas.

3. Entorno de usuario según la reivindicación 1 o 2, que comprende un séptimo dispositivo que presenta un dominio que presenta un sistema operativo propio, que está configurado para ejecutar funciones y programas.

4. Entorno de usuario según cualquiera de las reivindicaciones 1 a 3, donde el cuarto dispositivo está configurado para ejecutar chequeos de integridad iniciales y/o cíclicos de los dispositivos y/o componentes de los dispositivos.

5. Entorno de usuario según cualquiera de las reivindicaciones 1 a 4, donde las solicitudes de envío presentan al menos un ítem de la información siguiente:

- tamaño de la carga útil,
- instante de la transmisión,
- emisor de la comunicación,
- receptor de la comunicación,
- autor de la solicitud de comunicación al expedidor,
- firma criptográfica.

6. Entorno de usuario según cualquiera de las reivindicaciones 1 a 5, donde el tercer dominio está configurado para verificar la autorización de los dispositivos para la comunicación a través del tercer dominio.

7. Entorno de usuario según cualquiera de las reivindicaciones 1 a 6, donde el tercer dominio está configurado para conseguir acceso a una memoria de datos del motor interno a través de un modelo de control de accesos.

8. Entorno de usuario según cualquiera de las reivindicaciones 1 a 7, donde el tercer dominio está configurado para comunicar con un tercer dominio de un segundo entorno de usuario a través de un servidor de comunicación del motor interno conectado con el servidor de envío.

9. Entorno de usuario según cualquiera de las reivindicaciones 1 a 8, donde el tercer dominio está configurado para acceder a un servidor web conectado con el servidor de envío.

10. Arquitectura de red, que comprende:

al menos un entorno de usuario según cualquiera de las reivindicaciones anteriores, un motor interno seguro y un servidor de envío,
donde el servidor de envío está configurado para aceptar solicitudes de envío y datos que llegan del al menos un entorno de usuario, para seleccionarlos y transmitirlos a los componentes del motor interno seguro y transmitir los datos de los componentes del motor interno seguro a al menos un entorno de usuario, y
donde el motor interno seguro presenta un servidor de acceso al motor interno.

11. Arquitectura de red según la reivindicación 10, donde el servidor de envío es parte del motor interno seguro.

12. Arquitectura de red según la reivindicación 10 u 11, donde el motor interno seguro comprende además una memoria de datos, que está configurada de manera que un tercer dispositivo del entorno de red puede obtener acceso

a la memoria de datos a través de un modelo de control de accesos.

13. Arquitectura de red según cualquiera de las reivindicaciones 10 a 12, donde la arquitectura de red presenta al menos un primer y un segundo entorno de usuario según cualquiera de las reivindicaciones 1 a 9 y donde el motor interno seguro presenta un servidor de comunicación, que está conectado con el servidor de envío y está configurado de manera que un tercer dominio del primer entorno de usuario se pude comunicar con un tercer dominio del segundo entorno de usuario a través del servidor de comunicación.

14. Motor interno seguro para el uso en una arquitectura de red que comprende:

un servidor de acceso al motor interno, y
un servidor de envío, que está configurado para aceptar las solicitudes de envío y los datos que llegan de al menos un entorno de usuario según cualquiera de las reivindicaciones 1 a 9, seleccionarlos y transmitirlos a otros componentes del motor interno seguro y transmitir los datos de los otros componentes del motor interno seguro a al menos un entorno de usuario.

15. Motor interno seguro según la reivindicación 14, donde el motor interno seguro comprende una memoria de datos, que está configurada de manera que un tercer dispositivo de un entorno de usuario puede obtener acceso a la memoria de datos a través de un modelo de control de accesos, y/o donde el motor interno seguro presenta un servidor de comunicación, que está conectado con el servidor de envío y que está configurado de manera que un tercer dominio de un primer entorno de red según cualquiera de las reivindicaciones 1 a 9 se puede comunicar con un tercer dominio de un segundo entorno de usuario según cualquiera de las reivindicaciones 1 a 9 a través del servidor de comunicación.

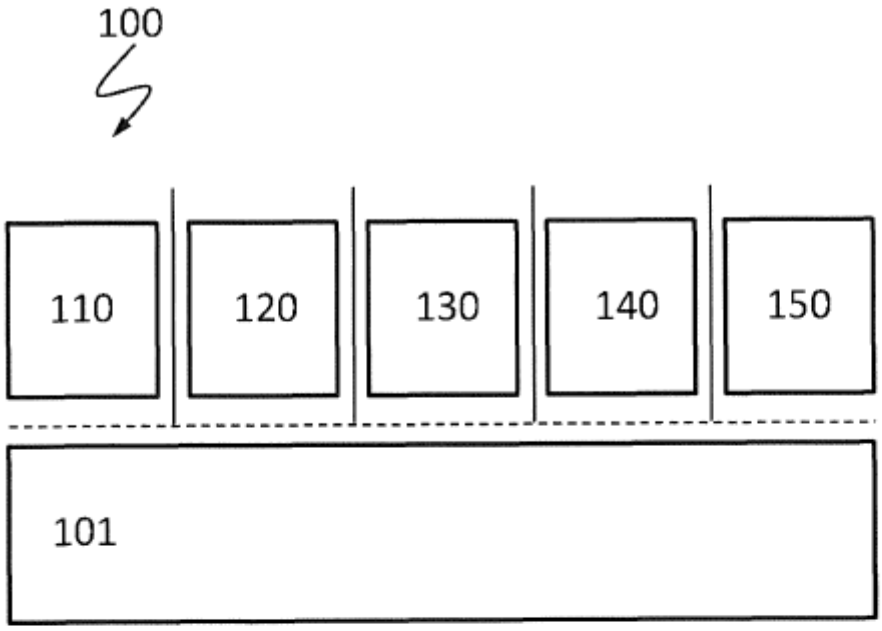

Fig. 1

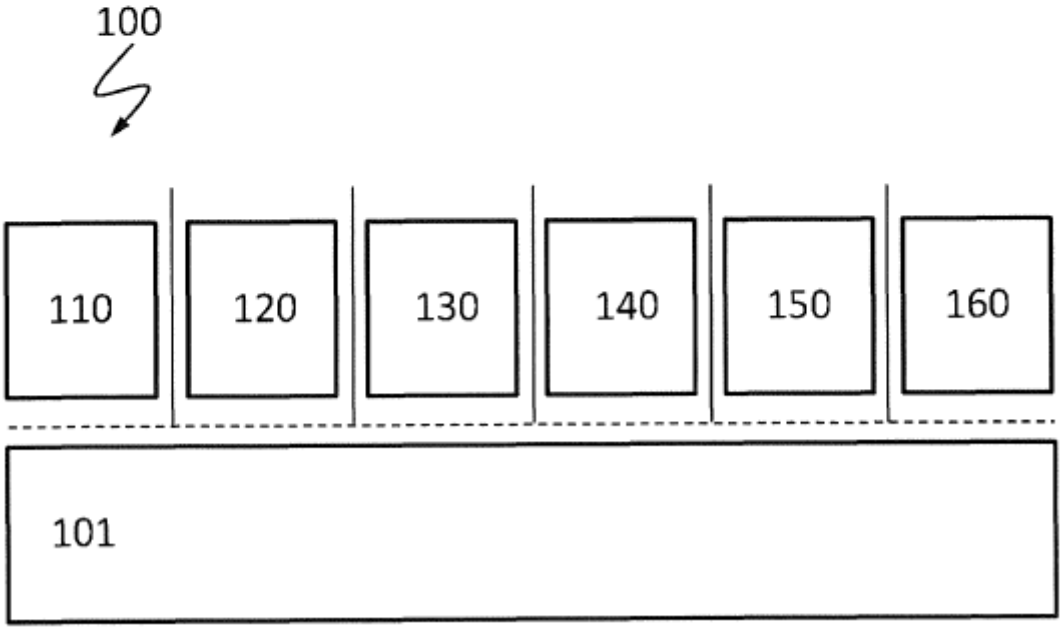

Fig. 2

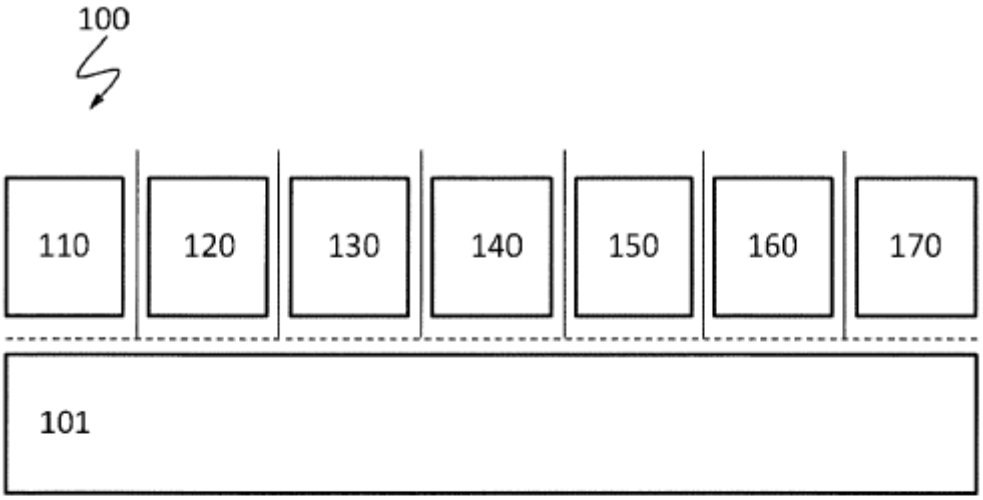

Fig. 3

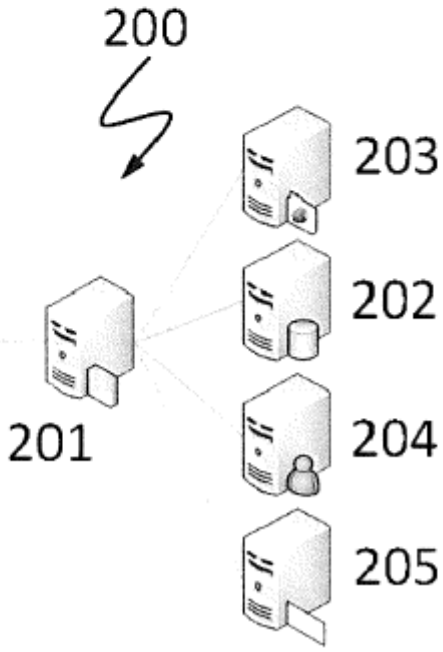

Fig. 4

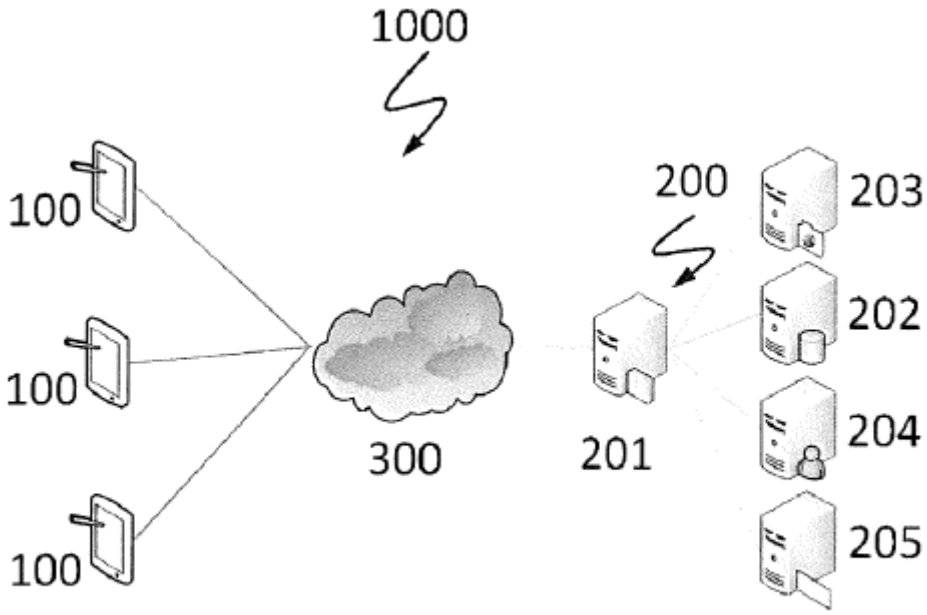

Fig. 5