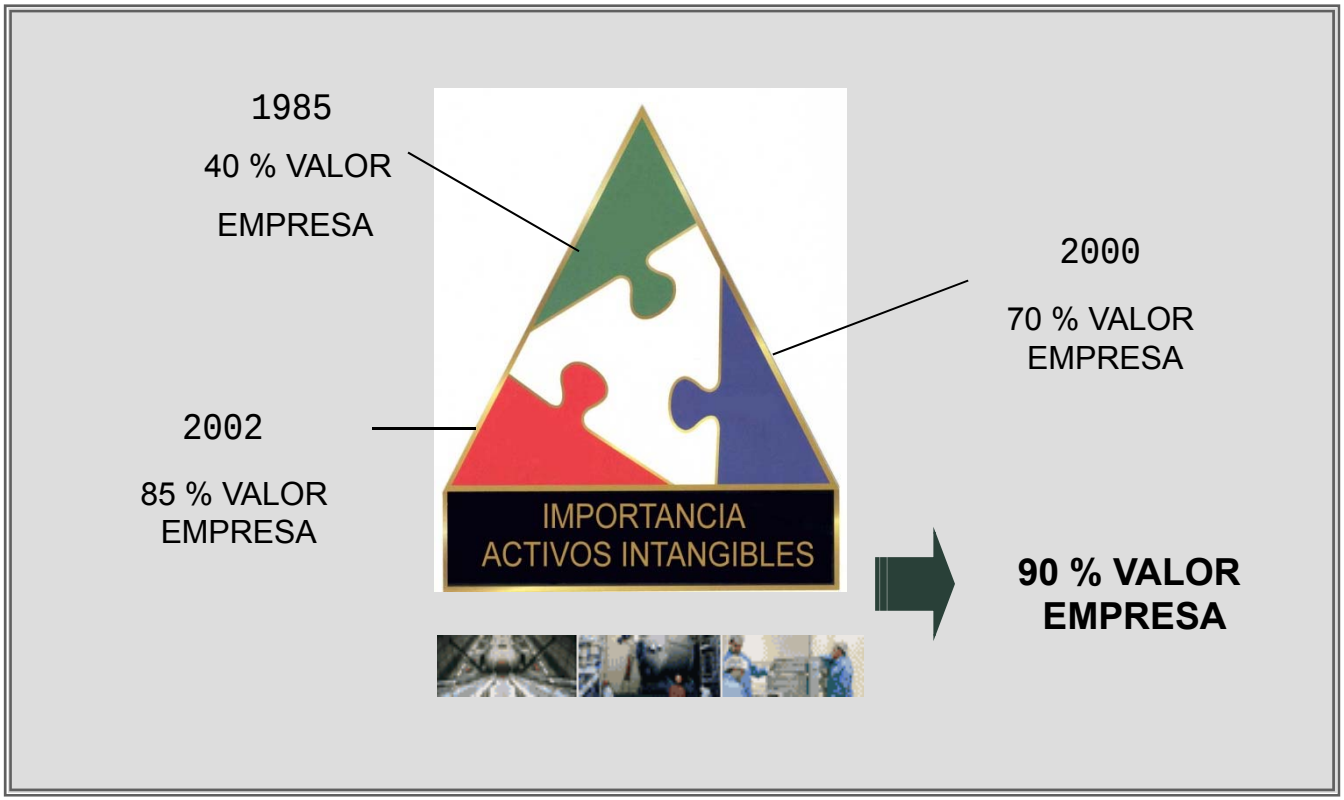
Clarke, Modet & Cº
FUNDADA EN 1879

CEL abogados

PROPIEDAD INDUSTRIAL E INTELECTUAL 4.0

EVOLUCIÓN DE LA IMPORTANCIA DE LOS ACTIVOS INTANGIBLES DE PROPIEDAD INDUSTRIAL E INTELECTUAL



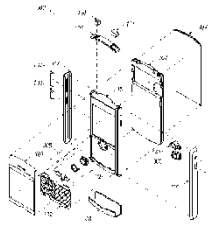
P. Intelectual ≠ P. industrial

PROPIEDAD INDUSTRIAL

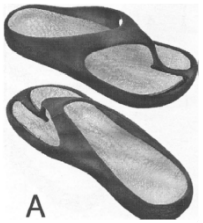
MODALIDADES INVENTIVAS | SIGNOS DISTINTIVOS | DISEÑOS INDUSTRIALES | NOMBRES DOMINIO | VARIEDADES VEGETALES | SEMICONDUCTORES

Patentes

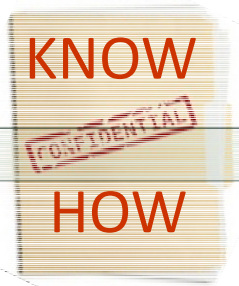
M. utilidad



Clarke, Modet & Cº
FUNDADA EN 1879



SOFTWARE QUE CUMPLA UNA FUNCIÓN TÉCNICA



SECRETOS INDUSTRIALES

OBRAS LITERARIAS | O. ARTÍSTICAS | O. CIENTÍFICAS | SOFTWARE

PROPIEDAD INTELECTUAL

CREACIONES ORIGINALES

ESTRATEGIAS PARA LA PROTECCIÓN DE LA PROPIEDAD INDUSTRIAL

QUE PROTEGER

- VENTAJA COMPETITIVA

CÓMO PROTEGERLO

- MODOS DE PROTECCIÓN:
  - PATENTES
  - DISEÑOS INDUSTRIALES
  - MARCAS
  - SECRETO INDUSTRIAL

DONDE PROTEGERLO

- PRINCIPIO TERRITORIALIDAD CONOCIMIENTO SISTEMAS
- PROTECCIÓN NACIONALES/ REGIONALES

SOCIEDAD DE LA INFORMACIÓN

CONOCIMIENTO

-GLOBALIZACIÓN

-ERA DIGITAL

-INDUSTRIA 4.0

-INTERNET DE LAS COSAS

-CONECTIVIDAD TOTAL

-INTELIGENCIA TECNOLÓGICA

-VELOCIDAD DE CAMBIO

EL ANTEPROYECTO DE LEY ESPAÑOLA DE SECRETOS INDUSTRIALES.

¿CUÁL ES EL MARCO DEL ANTEPROYECTO DE LEY DE SECRETOS EMPRESARIALES?

Se transpone al ordenamiento jurídico interno español la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016 la cual a su vez recoge los criterios del acuerdo internacional comúnmente, denominados «ADPIC». (Aspectos de los derechos de propiedad intelectual relacionados con el comercio. - Ronda Uruguay de 1994).

¿CUÁLES SON LOS REQUISITOS PARA QUE UNA INFORMACIÓN SEA PROTEGIDA COMO SECRETO EMPRESARIAL?

- Que sea **SECRETA**, en el sentido de que no sea generalmente conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza el tipo de información en cuestión.
- Que tenga un **VALOR COMERCIAL** por ser secreta
- Que haya sido objeto de **MEDIDAS RAZONABLES** (técnicas, jurídicas y organizativas), en las circunstancias del caso, para mantenerla secreta.

¿CUÁLES SON LAS VENTAJAS DEL SECRETO EMPRESARIAL?

1.- No está sujeto a límites temporales.

2.- No entraña costes de registro.

3.- Tienen un efecto inmediato.

¿CUÁLES SON LAS DESVENTAJAS DEL SECRETO EMPRESARIAL?

1.- La legitimidad de la ingeniería inversa.

- Si el secreto se plasma en un producto innovador, éste podrá ser inspeccionado, diseccionado y analizado (a través de la denominada "ingeniería inversa") por terceros que podrán descubrir el secreto y, por consiguiente, utilizarlo.
- De hecho, la protección por secreto empresarial de una invención no confiere el derecho exclusivo de impedir a terceros utilizarla de manera comercial.
- Únicamente las patentes y los modelos de utilidad dan tal tipo de protección.

2.- La extinción por su divulgación.

- Una vez que el secreto se divulga, todo el mundo puede tener acceso al mismo y utilizarlo.

¿COMO QUEDARÁ LA NORMATIVA TRAS LA PROMULGACIÓN DE LA PROYECTADA LEY DE SECRETOS EMPRESARIALES?

- Está ley tiene el carácter de especial y, en consecuencia, será de aplicación preferente.

- Como ley especial, se incorporará a la Ley de competencia desleal por remisión del artículo 13 de esta que queda redactado como sigue:

  "Artículo 13. Violación de secretos.

  Se considera desleal la violación de secretos empresariales, que se regirá por lo dispuesto en la legislación sobre protección de los secretos empresariales."

- En el ámbito penal, no hay modificación de los ya existentes artículos 278 a 280 del Código Penal.

- En el ámbito procesal civil, se establece:

  - ✓ La competencia de los Juzgados de lo Mercantil.

  - ✓ Regula el tratamiento, dentro del proceso de la información, que pueda constituir secreto empresarial.

  - ✓ Regula las diligencias para la preparación del ejercicio de acciones de defensa de los secretos empresariales.

  - ✓ Se establece también un régimen especial para las medidas cautelares.

¿PUEDE HABER CONFLICTO ENTRE LA PROYECTADA LEY DE SECRETOS EMPRESARIALES Y LOS DERECHOS DE LOS TRABAJADORES?

La protección del secreto empresarial suele tener fricciones con la **movilidad de los trabajadores** y los **pactos de no competencia post contractuales**.

En este sentido, el artículo 1. Punto 3 del anteproyecto dispone que:

> *"La protección de los secretos empresariales no (…) podrá restringir la movilidad de los trabajadores; en particular, no podrá servir de base para justificar limitaciones del uso por parte de estos de experiencia y competencias adquiridas honestamente durante el normal transcurso de su carrera profesional (…)"*

En España la **libertad de trabajo** está consagrada en el artículo 35 de la CE.

Una vez extinguido el contrato, el ex empleado recobra su plena libertad de trabajo.

Sin embargo, el **artículo 21.2 ET** autoriza a suscribir **pactos de no competencia post contractual** que deben cumplir como requisitos para su validez:

- El pago de una compensación económica adecuada.
- La fijación de una duración máxima.
- Existencia de un interés industrial o comercial del empresario o empleador.

Estos pactos no bloquean la libertad de trabajo del ex trabajador, sino que, en caso de incumplimiento, facultan al antiguo empresario para reclamar, la cantidad pagada en compensación por el pacto y una indemnización por daños y perjuicios en caso de acreditar debidamente haberlos sufrido.

En otro orden de cosas, **el punto más difícil es diferenciar el secreto empresarial del uso por parte del trabajador de la experiencia y competencias adquiridas honestamente durante el normal transcurso de su carrera profesional.**

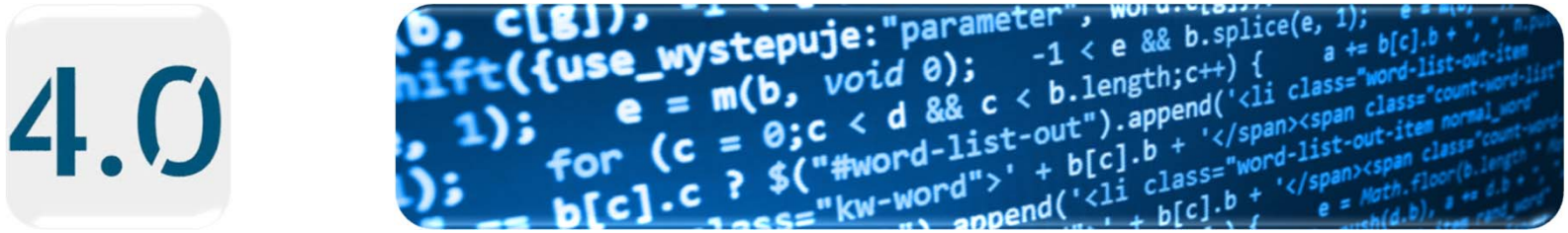
La **Sentencia de la Audiencia Provincial de Barcelona de 18 marzo de 2015** distingue entre lo que son habilidades, capacidades y experiencia profesional de un sujeto y lo que es secreto empresarial.

Al efecto, establece: *"Es preciso distinguir entre secreto empresarial y todas aquellas informaciones que forman parte de las habilidades, capacidades y experiencia profesional de un sujeto. Pertenecen, por el contrario, al ámbito del secreto y no al de la formación o capacitación profesional, los conocimientos que se adquieren como consecuencia del desempeño de un puesto de responsabilidad y confianza y aquellos que no es posible retener en la memoria."*

Es decir, que es secreta una información:

- **Que solo sea accesible a personas que ejerzan un puesto de responsabilidad y confianza.**
- **Que no pueda ser retenida en la memoria** (si puede ser retenida en la memoria tal información puede ser considerada habilidades, capacidades y experiencia profesional del trabajador).

LAS TECNOLOGÍAS EN LA INDUSTRIA 4.0 Y EL CONTRATO DE LICENCIA.



TITULARES DE LOS INTANGIBLES EN LA INDUSTRIA 4.0 E INDUSTRIA CONECTADA.

La Industria 4.0 supone la **transformación tecnológica** de las empresas tanto en la organización y producción de las factorías como en la gestión de la relación con el cliente.

Las tecnologías -y por tanto, los intangibles- se convierten **elementos indispensables para el funcionamiento** de la Industria 4.0.

No obstante, lo usual es que estas tecnologías -que los intangibles- no sean creadas por la Industria 4.0 sino **por compañías especializadas en la creación y desarrollo de las mismas.**

Por este motivo, lo usual es que sean estas compañías -y no la Industria 4.0- las **titulares** de los intangibles.

POSICIÓN DOMINANTE DE LAS EMPRESAS QUE CREAN LOS INTANGIBLES SOBRE EL EMPRESARIO 4.0 Y EL CONTRATO DE LICENCIA.

De este modo, vemos como las compañías especializadas en la creación y desarrollo de tecnologías pasan a adquirir una **posición dominante sobre el empresario 4.0**.

La Industria 4.0 tiene una gran **dependencia tecnológica**. Habida cuenta que la incorporación de intangibles en la Industria 4.0 se articula mediante un **CONTRATO DE LICENCIA**, se hace indispensable su análisis detenido antes de aplicar un intangible a la Industria 4.0.

Una vez aplicado, esta Industria, normalmente, pasa a **depender** del licenciante en los términos pactados en el contrato licencia- que suele ser un contrato de adhesión-.

¿LAS LICENCIAS DE USO DE INTANGIBLES QUE SON ESENCIALES PARA LA INDUSTRIA 4.0 PUEDEN SER REVOCADAS POR SUS TITULARES?

Toda licencia puede ser REVOCADA, pero no arbitrariamente.

La infracción por el licenciado del contrato de licencia puede conllevar su revocación. Pero no toda infracción del contrato de licencia debe dar derecho a la revocación. Las infracciones que deben dar derecho a la revocación tienen que ser **SUSTANCIALES y NO SUBSANABLES.**

Es esencial que en el contrato de licencia se establezca exactamente **cuáles son las infracciones esenciales** que pueden dar lugar a la revocación.

Es igualmente necesario el establecer en el contrato un **mecanismo de notificación** de la posible infracción por parte del licenciante y un **plazo a favor del licenciado para subsanar** la presunta infracción.

Se ha de regular en la licencia que, incluso en casos de revocación procedente, la misma no puede ser inmediata sino que el licenciado ha de disfrutar de un **periodo de transición** para sustituir el intangible licenciado por otro de prestaciones equivalentes.

¿PUEDEN LAS LICENCIAS SER INDEFINIDAS?

Existe un gran equívoco en relación a los contratos de duración indefinida.

Los contratos de duración indefinida **NO SON PERPETUOS.**

Los contratos de duración indefinida son **RESOLUBLES** siempre que se den una serie de condiciones, entre las que son de destacar:

- Exista justa causa.
- Se dé un preaviso razonable que permita a la otra parte reorganizarse.
- No se provoque en la otra parte un daño o perjuicio desproporcionado.

La **RESOLUCIÓN** de los contratos indefinidos es una figura jurídica **distinta de la REVOCACIÓN** ya que:

- No exige incumplimiento contractual de ninguna de las partes.
- Es una simple consecuencia de la no perpetuidad de las relaciones jurídicas.
- Al no haber ninguna parte infractora la resolución ha de realizarse con el menor perjuicio para todas las partes.

En casos de licencias de duración indefinida hay que regular detalladamente el procedimiento a seguir en caso de resolución, especialmente el plazo de preaviso y el proceso a seguir en el periodo de sustitución de la licencia que se extingue por la nueva licencia.

¿ES LA INDUSTRIA 4.0 FRÁGIL POR SU DEPENDENCIA DE LAS LICENCIAS DE USO DE INTANGIBLES TITULARIDAD DE TERCEROS?

Efectivamente, la Industria 4.0 es una industria frágil desde la perspectiva jurídica en la medida que dependa de licencias de terceros.

Algunas de las FRAGILIDADES más relevantes son:

- La sustitución de una licencia puede ser costosa y laboriosa, exigiendo a veces la modificación de otros intangibles conexos a aquél cuya licencia se extingue. El costo de sustitución puede llevar a aceptar nuevos precios que objetivamente son abusivos.

- Las MEJORAS realizadas en los intangibles por el licenciado pueden pasar a ser titularidad del licenciante si no se ha pactado claramente en el contrato de licencia su destino y titularidad.

- Si las mejoras realizadas en los intangibles por el licenciado pasan a ser titularidad del licenciante el licenciado pierde la ventaja competitiva que tales mejoras hayan podido significar. El licenciante al pasar a ser titular de tales mejoras podría licenciarlas a terceros incluso a competidores.

- El licenciante al finalizar el contrato puede haber obtenido a través de los programas licenciados información relativa a la empresa licenciada que afecte a su know how o a su secreto industrial.

- Puede ocurrir que en el mercado no exista un intangible equivalente al licenciado, en cuyo caso, estaríamos en una situación muy complicada.

¿CÓMO MINORAR ESTA FRAGILIDAD? MEDIDAS PREVENTIVAS.

Para minorar la fragilidad es aconsejable tomar medidas preventivas, tales como:

- En los contratos de duración definida:
  - Tener con la debida antelación localizada en el mercado una **opción alternativa** al intangible cuya licencia se vaya a extinguir.
  - **Negociar con suficiente anticipación** con el nuevo licenciante un contrato de licencia antes de que llegue la fecha de extinción de la licencia en curso.
  - Regular con el nuevo licenciante de forma detallada la **colaboración a prestar en el proceso de transición.**

- En los contratos de duración indefinida:

  - Establecer un **amplio periodo de preaviso** que permita localizar en el mercado una opción alternativa al intangible cuya licencia se vaya a extinguir y permita negociar con el nuevo licenciante un contrato de licencia satisfactorio.

  - Regular con el licenciante de forma detallada la **colaboración** a prestar al nuevo licenciante y a la empresa en el pro**ceso de transición**.

- En ambos casos:
  - Tener presupuestado el **coste de sustitución** del intangible cuya licencia se extingue por el nuevo intangible.
  - Cerciorarse de que el nuevo intangible es **equivalente** al intangible cuya licencia se vaya a extinguir y de su **compatibilidad** con los demás intangibles conexos que use la compañía.
  - Regular con ambos licenciantes de forma detallada la **colaboración** a prestar en el **proceso de transición** y la coordinación entre ellos.
  - Obtener del licenciante saliente un **certificado** acreditativo de que todos los **datos** relativos a la empresa licenciada que puedan obrar en su poder han sido **borrados** y que la **documentación** que se haya podido entregar durante el periodo de licencia ha sido **destruida**.

- Obtener del licenciante saliente una declaración formal de que las **mejoras** introducidas en el intangible durante el periodo de duración de la licencia quedan **titularidad de la empresa licenciada** y de que:

  - El licenciante saliente se obliga a **no licenciar tales mejoras** a terceros.

  - El **empresario**, cuya licencia se extingue, puede **hacer uso** de tales mejoras e incorporarlas, si así o precisa, al nuevo intangible que sustituya al anterior.

INDUSTRIA 4.0

- Qué es?

Cuarta revolución industrial.
Basada en la transformación digital de la industria integrando y digitalizando todos los procesos industriales.

- Qué tecnologías incluye?

Big data
Ciberseguridad
Realidad Aumentada
Simulación
IoT
Nube
Interconectividad
mpresión 3D
Robótica
Etc...

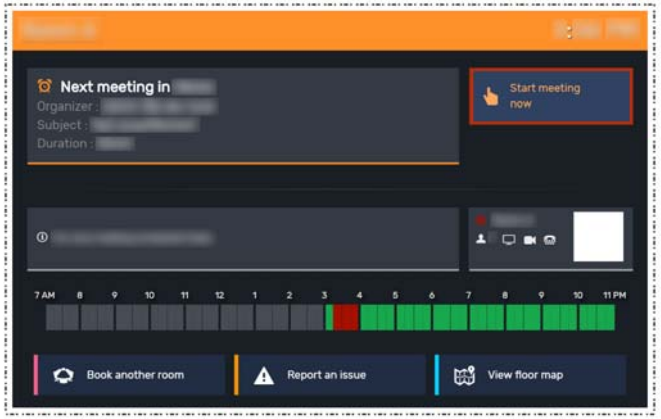
} SOFTWARE

FORMAS DE PROTECCIÓN

- Propiedad Intelectual.
    - Derechos de autor (incluyendo software).
    - Protección sui generis de las bases de datos.
- Secreto comercial.
- Propiedad Industrial.
    - Diseño Industrial.
    - Marca.
    - **Patententes.**

FORMAS DE PROTECCIÓN

- Diseño Industrial
  - Novedad
  - Carácter Singular
- Por ejemplo, dispositivos o interfaces.



EU design **004127868-0003**

EU design **003465657-0001**

Source: https://euipo.europa.eu/eSearch/

PROTECCIÓN MEDIANTE PATENTE

- Definición de Patente?
- Derecho a impedir que terceros exploten la invención sin el consentimiento del titular.
- Temporalidad: 20 años desde la fecha de presentación.
- Requisitos básicos:
    - Novedad
    - Actividad inventiva
    - Aplicabilidad industrial

PROTECCIÓN POR PATENTE EN I 4.0

- 3 tipos fundamentales de creaciones:
  - Dispositivos
  - Procedimientos
  - Software

PROTECCIÓN POR PATENTE EN I 4.0

- Software

- Exclusiones de patentabilidad:

  Article 52(2) EPC:

(2) The following in particular shall not be regarded as inventions within the meaning of paragraph 1:
(a) discoveries, scientific theories and ***mathematical methods****;*
(b) aesthetic creations;
(c) schemes, rules and methods for performing mental acts, playing games or doing business, and ***programs for computers****;*
(d) ***presentations of information****.*

- Quedan excluidas por considerarse no-técnicas.

PROTECCIÓN POR PATENTE EN I 4.0

- MÉTODOS MATEMÁTICOS.
  - Excluidos de protección como tales.

  Sin embargo, ...

  - Lo que importa para una invención es si es técnica o no y si proporciona un efecto técnico.

  Por tanto, ...

  - Las aplicaciones técnicas de un método matemático son patentables, aunque requieran, incluyan o se basen (exclusivamente) en el método matemático.
  - Por ejemplo, un dispositivo u objeto producido de acuerdo con un método matemáticos o un procedimiento industrial basado en un método matemático.

PROTECCIÓN POR PATENTE EN I 4.0

- PRESENTACIÓN DE LA INFORMACIÓN.

  - Incluye el cotenido y su forma de presentación.

  - No patentable como tal → Se podría incluir dentro de una reivindicación técnica.

  - **<u>Patentable si proporiona un efecto técnico (es decir, si ayuda a llevar a cabo una tarea técnica)</u>**.

    - Si se basa en preferencias de los usuarios: no se considera técnico.

    En cambio sí podrían ser técnicas y, por tanto, patentables:

    - Estado interno que prevalece en un sistema.
    - Presentaciones de información que facilitan la interacción humano-máquina. Debe ser objetiva la facilitación, no una cuestión de preferencia.
    - Presentación de información que produce un efecto en la fisiología humana.
    - Interfaces de usuario → por ejemplo, cuando facilitan técnicamente el input, se suelen considerar técnicos.
    - Procesado de datos o formato de datos: si permiten un procesado más eficioente, un almacenado de datos más eficiente, un incremento de la seguriad...

PROTECCIÓN POR PATENTE EN I 4.0

- INVENCIONES IMPLEMENTADAS POR ORDENADOR:
  - DEFINICIÓN: implican el uso de un ordenador, red informática u otro aparato programable y donde una o más características (de la invención) se llevan a cabo total o parcialmente por medio de un programa de ordenador
  - Carácter técnico + efecto técnico adicional.
  - Qué es patentable?

    Procedimiento que lleva a cabo el programa de ordenador cuando se ejecuta.

    Las reivindicaciones deben incluir o referirse al procedimiento llevado a cabo por el programa de ordenador.

    Las reivindicaciones, preferentemente, no deberían incluir código fuente (program listings).

PROTECCIÓN POR PATENTE EN I 4.0

- INVENCIONES IMPLEMENTADAS POR ORDENADOR:

  - Descripción:

    Describir el procedimiento llevado a cabo por el programa de ordenador.

    Se puede incluir código fuente (program listings), pero no puede ser la única descripción o explicación de la invención.

    Escrita sustancialmente en “lenguaje normal”.

    Puede incluir diagramas de flujo (figuras) para ayudar a la compresnsión de la invención.

OBJETIVO: que la invención sea entendida por un experto en la materia que no sea un especialista en un lengaje informático específico, pero que tenga habilidades generales de programación.

PROTECCIÓN POR PATENTE EN I 4.0

Todas las etapas del método/procedimiento pueden llevarse a cabo completamente mediante funciones genéricas de procesamiento de datos:

(i) Method claim (claim 1)

A computer-implemented method comprising steps A, B, ...

A method carried out by a computer comprising steps A, B, ...

(ii) Apparatus/device/system claim (claim 2) (comprising means for carrying out [the steps of] the method of claim 1 / means to carry out steps A, B, .../ a processor adapted to/configured to perform [the steps of] the method of claim 1.)

(iii) Computer program [product] claim (claim 3) (comprising instructions which, when the program is executed by a computer, cause the computer to carry out [the steps of] the method of claim 1/ steps A, B, ...)

(iv) Computer-readable [storage] medium/data carrier claim (claim 4) (comprising instructions which, when executed by a computer, cause the computer to carry out [the steps of] the method of claim 1 / steps A, B, .../ having stored thereon the computer program [product] of claim 3)

PROTECCIÓN POR PATENTE EN I 4.0

No todas las etapas del método/procedimiento pueden llevarse a cabo completamente mediante funciones genéricas de procesamiento de datos:

- Se necesitan medios técnicos adicionales.
- Las reivindicaciones DEBEN incluir los medios técnicos requeridos.
- Las reivindicaciones DEBEN reflejar claramente por qué medios técnicos se lleva a cabo cada etapa y las interacciones entre dichos medios técnicos.

1. A method of determining oxygen saturation in blood in a **pulse oximeter**, comprising:
– receiving in an **electromagnetic detector** first and second electromagnetic radiation signals from a blood-perfused tissue portion corresponding to two different wavelengths of light;
– normalising said electromagnetic signals according to steps A, B and C to provide normalised electromagnetic signals;
– determining oxygen saturation based on said normalised electromagnetic signals according to steps D and E.

2. A pulse oximeter having an electromagnetic detector and means adapted to execute the steps of the method of claim 1.

3. A computer program [product] comprising instructions to cause the device of claim 2 to execute the steps of the method of claim 1.

4. A computer-readable medium having stored thereon the computer program of claim 3.

EJEMPLO: CIBERSEGURIDAD

(19) Europäisches Patentamt / European Patent Office / Office européen des brevets

(11) EP 2 925 036 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent: **01.11.2017 Bulletin 2017/44**

(51) Int Cl.: ***H04W 12/06*** *(2009.01)* ***H04L 29/06*** *(2006.01)* ***H04W 4/22*** *(2009.01)* ***H04W 12/04*** *(2009.01)*

(21) Application number: **15161068.0**

(22) Date of filing: **26.03.2015**

(54) **APPARATUS AND METHOD FOR AUTHENTICATION IN WIRELESS COMMUNICATION SYSTEM**

VORRICHTUNG UND VERFAHREN ZUR AUTHENTIFIZIERUNG IN EINEM DRAHTLOSEN KOMMUNIKATIONSSYSTEM

APPAREIL ET PROCÉDÉ D'AUTHENTIFICATION DANS UN SYSTÈME DE COMMUNICATION SANS FIL

(84) Designated Contracting States: **AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR**

(30) Priority: **26.03.2014 KR 20140035355**

(43) Date of publication of application: **30.09.2015 Bulletin 2015/40**

(73) Proprietor: **Samsung Electronics Co., Ltd.**
Suwon-si, Gyeonggi-do, 443-742 (KR)

(72) Inventors:
- **Lee, Duckey**
  Seoul (KR)
- **Kang, Bo-Gyeong**
  Seoul (KR)
- **Son, Jung-Je**
  Gyeonggi-do (KR)

(74) Representative: **Nederlandsch Octrooibureau**
P.O. Box 29720
2502 LS The Hague (NL)

(56) References cited:
EP-A1- 2 503 754

- **"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 12)", 3GPP DRAFT; 33102-C00, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , 10 March 2014 (2014-03-10), XP050837214, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_74_Taipei/SA#63/specs/ [retrieved on 2014-03-10]**

1. A method carried out by a server (208) in a communication system, comprising:

receiving, from a user equipment (200), information regarding an identifier of the user equipment (200) for an access to a network; and
if an authentication key corresponding to the identifier is not detected in a storage device (320) of the server (208), determining another authentication key among a plurality of authentication keys based on a policy; and
transmitting, to the user equipment (200), a token comprising information for indicating a type of the another authentication key, wherein the plurality of authentication keys comprises: a first authentication key shared among at least another user equipment, the user equipment (200), and the server (208); and
a second authentication key shared between the user equipment (200) and another server.

5. A method carried out by a network node (204, 206) in a communication system, comprising:

receiving, from a user equipment (200), information regarding an identifier of the user equipment (200) for an access to a network;

transmitting, to a server (208), the information regarding the identifier;
if a response for the information regarding the identifier is not received from the server (208), determining an authentication key among a plurality of authentication keys based on a policy;
transmitting, to the user equipment (200), a token comprising information for indicating a type of the authentication key; and
receiving, from the user equipment (200), a message indicating whether an authentication for accessing a network is successful in response to transmission of the token,
wherein the plurality of authentication keys comprises:

a first authentication key shared among at least another user equipment, the user equipment (200), and the network node (204, 206); and
a second authentication key shared between the user equipment (200) and another server.

EJEMPLO: CIBERSEGURIDAD

9. A method carried out by a user equipment (200) in a communication system, comprising:

transmitting (801), to a network node (204, 206), information regarding an identifier of the user equipment for an access to a network;
receiving (803), from the network node (204, 206), a first token comprising information for indicating a type of an authentication key, the authentication key determined among a plurality of authentication keys comprising

a first authentication key shared among at least another user equipment, the user equipment, a server for the authentication, and the network node; and
a second authentication key shared between the user equipment and another server;

if the type of the authentication key indicates the first authentication key or the second authentication key, determining (809, 811) whether the authentication key is usable according to a preset authentication use policy,
if the authentication key is usable, generating (817) a second token based on the authentication key corresponding to the type of the authentication key;
determining (821) whether an authentication for accessing the network is successful or not based according to whether the first token corresponds to second token; and
transmitting a message indicating whether the authentication is successful or not.

15. An apparatus for authentication, the apparatus comprises:

at least one transceiver; and
at least one processor operatively coupled to the at least one transceiver,
wherein the at least one processor is configured to implement a method of one among claims 1 to 14.

Problema técnico:
autentificación de un dispositivo para acceder a una red.

Solución:
procedimiento/método de autentificación.

Source: https://worldwide.espacenet.com/advancedSearch?locale=en_EP

EJEMPLO: NUBE

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 058 703 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
04.04.2018 Bulletin 2018/14

(21) Application number: **14790926.1**

(22) Date of filing: **13.10.2014**

(51) Int Cl.:
H04L 12/24 *(2006.01)* ***H04L 12/801*** *(2013.01)*
H04L 12/911 *(2013.01)* ***H04L 29/08*** *(2006.01)*

(86) International application number:
PCT/US2014/060209

(87) International publication number:
WO 2015/057534 (23.04.2015 Gazette 2015/16)

(54) **OPTIMIZING DATA TRANSFERS IN CLOUD COMPUTING PLATFORMS**

OPTIMIERUNG VON DATENÜBERTRAGUNGEN IN CLOUD-COMPUTING-PLATTFORMEN

OPTIMISATION DE TRANSFERTS DE DONNÉES SUR DES PLATEFORMES INFORMATIQUES EN NUAGE

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **17.10.2013 US 201314056630**

(43) Date of publication of application:
24.08.2016 Bulletin 2016/34

(73) Proprietor: **Microsoft Technology Licensing, LLC**
Redmond, WA 98052 (US)

(72) Inventors:
- **TANG, Jun**
  Redmond, Washington 98052-6399 (US)
- **PEELEN, Nicolaas Deodorus**
  Redmond, Washington 98052-6399 (US)
- **WANG, Hui**
  Redmond, Washington 98052-6399 (US)
- **ZHU, Xiaoting**
  Redmond, Washington 98052-6399 (US)
- **ZHAO, Tao**
  Redmond, Washington 98052-6399 (US)

(74) Representative: **Grünecker Patent- und Rechtsanwälte**
PartG mbB
Leopoldstraße 4
80802 München (DE)

(56) References cited:
WO-A2-2007/127401 **US-A1- 2008 219 158**
US-A1- 2011 196 971 **US-A1- 2013 003 543**

1. A system (200) for performing a method for optimizing data transfers, the system comprising:

a data transfer optimization server (230) configured for:

initiating a data transfer session, wherein initiating the data transfer session comprises analyzing transfer parameters that impact maximum throughput for one or more data-source devices;
calculating an optimum number of concurrent network calls that are used to transfer data for the data transfer session based on the transfer parameters;
allocating at least a portion of the optimum number of concurrent network calls to execute the data transfer session;
monitoring the transfer parameters for changes in the transfer parameters;
updating the optimum number of concurrent network calls for the data transfer session based on a triggering event associated with the data transfer session, wherein updating the optimum number of concurrent network call comprises recalculating the optimum number of concurrent network calls based on the transfer parameters at or after the triggering event; and
executing the data transfer session with the recalculated optimum number of concurrent network calls to optimize data transferred during the data transfer session;

characterized in that

said allocating at least a portion of the optimum number of concurrent network calls comprises:

determining the size of each individual file to be transferred from the one or more data-source devices; and
assigning a number of concurrent network calls to each individual file in proportion to the size of the individual file, wherein the number of concurrent network calls is assigned from the optimum number of concurrent network calls; and

in that the triggering event is a predefined period, wherein expiration of the predefined period triggers analyzing the transfer parameters for updating the optimum number of concurrent network calls based on the transfer parameters.

Source: https://worldwide.espacenet.com/advancedSearch?locale=en_EP

EJEMPLO: NUBE

1. A system (200) for performing a method for optimizing data transfers, the system comprising:

a data transfer optimization server (230) configured for:

initiating a data transfer session, wherein initiating the data transfer session comprises analyzing transfer parameters that impact maximum throughput for one or more data-source devices;
calculating an optimum number of concurrent network calls that are used to transfer data for the data transfer session based on the transfer parameters;
allocating at least a portion of the optimum number of concurrent network calls to execute the data transfer session;
monitoring the transfer parameters for changes in the transfer parameters;
updating the optimum number of concurrent network calls for the data transfer session based on a triggering event associated with the data transfer session, wherein updating the optimum number of concurrent network call comprises recalculating the optimum number of concurrent network calls based on the transfer parameters at or after the triggering event; and
executing the data transfer session with the recalculated optimum number of concurrent network calls to optimize data transferred during the data transfer session;

characterized in that

said allocating at least a portion of the optimum number of concurrent network calls comprises:

determining the size of each individual file to be transferred from the one or more data-source devices; and
assigning a number of concurrent network calls to each individual file in proportion to the size of the individual file, wherein the number of concurrent network calls is assigned from the optimum number of concurrent network calls; and

in that the triggering event is a predefined period, wherein expiration of the predefined period triggers analyzing the transfer parameters for updating the optimum number of concurrent network calls based on the transfer parameters.

8. One or more computer-readable media storing computer-useable instructions that, when used by one or more computing devices, causes the one or more computing devices to perform a method for optimizing data transfers, the method comprising:

12. A method for optimizing data transfer between private enterprise systems and cloud computing platforms, the method comprising:

Source: https://worldwide.espacenet.com/advancedSearch?locale=en_EP

- Problema técnico: transferencia de datos eficiente y efectiva, sobretodo desde sistemas locales a la nube.

- Solución: un procedimiento o método que se materializa en forma de programa de ordenador.

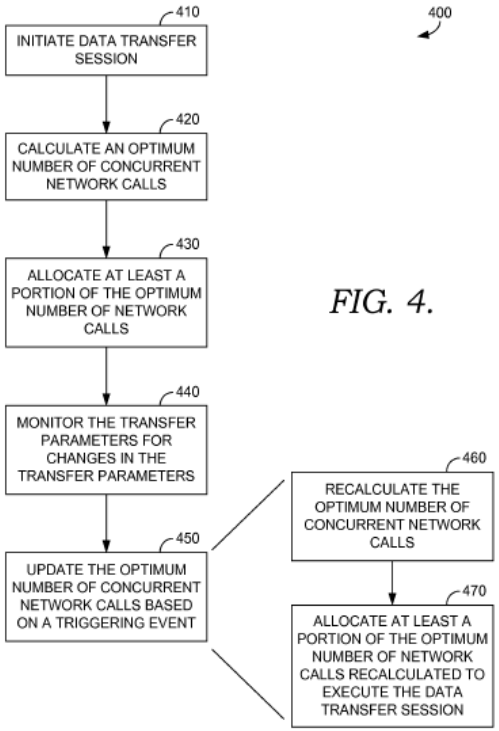


FIG. 4.

EJEMPLO: SEGURIDAD EN LA NUBE

(19) Europäisches Patentamt / European Patent Office / Office européen des brevets

(11) EP 2 913 956 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
04.01.2017 Bulletin 2017/01

(21) Application number: **12888666.0**

(22) Date of filing: **22.11.2012**

(51) Int Cl.:
H04L 12/24 *(2006.01)* ***G06F 21/31*** *(2013.01)*
G06F 9/455 *(2006.01)* ***H04L 29/06*** *(2006.01)*
H04L 9/30 *(2006.01)* ***H04L 9/32*** *(2006.01)*

(86) International application number:
PCT/CN2012/085008

(87) International publication number:
WO 2014/079009 (30.05.2014 Gazette 2014/22)

(54) **MANAGEMENT CONTROL METHOD AND DEVICE FOR VIRTUAL MACHINES**

VERWALTUNGSSTEUERUNGSVERFAHREN UND -VORRICHTUNG FÜR VIRTUELLE MASCHINEN

PROCÉDÉ ET APPAREIL DE COMMANDE DE LA GESTION POUR MACHINES VIRTUELLES

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(43) Date of publication of application:
02.09.2015 Bulletin 2015/36

(73) Proprietor: **Huawei Technologies Co., Ltd.**
Longgang District
Shenzhen, Guangdong 518129 (CN)

(72) Inventors:
- **YE, Sihai**
  Shenzhen
  Guangdong 518129 (CN)
- **SHI, Xun**
  Shenzhen
  Guangdong 518129 (CN)

(74) Representative: **Goddar, Heinz J.**
Boehmert & Boehmert
Anwaltspartnerschaft mbB
Patentanwälte Rechtsanwälte
Pettenkoferstrasse 20-22
80336 München (DE)

(56) References cited:
WO-A1-2011/116459 **WO-A1-2012/148324**
WO-A2-2011/141579 **CN-A- 101 188 624**
CN-A- 102 202 046 **CN-A- 102 291 452**

1. A management control method for a virtual machine, the method being carried out by a security control platform and comprising:

receiving (101), a virtual machine starting request message that is from user equipment and forwarded by a management platform, wherein the virtual machine starting request message comprises an identifier of a virtual machine that needs to be enabled and user information;
invoking (102) a third-party trusted platform to generate data encrypted by using a key of the third-party trusted platform;
sending the encrypted data to the user equipment by using the management platform, so that the user equipment decrypts the encrypted data by using a private key provided by the third-party trusted platform for the authorized user, and returns decrypted data to the security control platform; and
if it is determined that the decrypted data is the same as the data before encryption, determining that the virtual machine starting request message is initiated by the user equipment according to the instruction of the authorized user; and

performing (103) authentication on the user information, and based on successful authentication, invoking the third-party trusted platform to decapsulate the virtual machine that needs to be enabled.

8. A security control platform, comprising:

a receiving module (51), configured to receive a virtual machine starting request message that is from user equipment and forwarded by a management platform, wherein the virtual machine starting request message comprises an identifier of a virtual machine that needs to be enabled and user information;
a determining module (52), configured to: on the basis that the receiving module (51) receives the virtual machine starting request message that is from the user equipment, invoke a third-party trusted platform to generate data encrypted by using a key of the third-party trusted platform; send the encrypted data to the user equipment by using the management platform, so that the user equipment decrypts the encrypted data by using a private key provided by the third-party trusted platform for the authorized user, and returns decrypted data to the security control platform; and if it is determined that the decrypted data is the same as the data before encryption,

determine that the virtual machine starting request message is initiated by the user equipment according to the instruction of the authorized user; and
a decapsulating module, configured to: on the basis that the determining module determines that the virtual machine starting request message is initiated by the user equipment according to the instruction of the authorized user, after the user information is authenticated successfully, invoke the third-party trusted platform to decapsulate the virtual machine that needs to be enabled.

EJEMPLO: SEGURIDAD EN LA NUBE

1. A management control method for a virtual machine, the method being carried out by a security control platform and comprising:

receiving (101), a virtual machine starting request message that is from user equipment and forwarded by a management platform, wherein the virtual machine starting request message comprises an identifier of a virtual machine that needs to be enabled and user information;
invoking (102) a third-party trusted platform to generate data encrypted by using a key of the third-party trusted platform;
sending the encrypted data to the user equipment by using the management platform, so that the user equipment decrypts the encrypted data by using a private key provided by the third-party trusted platform for the authorized user, and returns decrypted data to the security control platform; and
if it is determined that the decrypted data is the same as the data before encryption, determining that the virtual machine starting request message is initiated by the user equipment according to the instruction of the authorized user; and

performing (103) authentication on the user information, and based on successful authentication, invoking the third-party trusted platform to decapsulate the virtual machine that needs to be enabled.

8. A security control platform, comprising:

a receiving module (51), configured to receive a virtual machine starting request message that is from user equipment and forwarded by a management platform, wherein the virtual machine starting request message comprises an identifier of a virtual machine that needs to be enabled and user information;
a determining module (52), configured to: on the basis that the receiving module (51) receives the virtual machine starting request message that is from the user equipment, invoke a third-party trusted platform to generate data encrypted by using a key of the third-party trusted platform; send the encrypted data to the user equipment by using the management platform, so that the user equipment decrypts the encrypted data by using a private key provided by the third-party trusted platform for the authorized user, and returns decrypted data to the security control platform; and if it is determined that the decrypted data is the same as the data before encryption,

determine that the virtual machine starting request message is initiated by the user equipment according to the instruction of the authorized user; and
a decapsulating module, configured to: on the basis that the determining module determines that the virtual machine starting request message is initiated by the user equipment according to the instruction of the authorized user, after the user information is authenticated successfully, invoke the third-party trusted platform to decapsulate the virtual machine that needs to be enabled.

- Problema técnico: seguridad de la computación en la nube
- Solución: procedimiento/método a llevar a cabo por una plataforma de control de la seguridad.

EJEMPLO: INTERFAZ

(19) Europäisches Patentamt / European Patent Office / Office européen des brevets

(11) EP 2 930 613 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent: **11.01.2017 Bulletin 2017/02**

(51) Int Cl.: ***H04L 29/06*** *(2006.01)* ***H04L 29/08*** *(2006.01)* ***G06F 3/0481*** *(2013.01)* ***G06F 9/44*** *(2006.01)*

(21) Application number: **15000999.1**

(22) Date of filing: **08.04.2015**

(54) **DYNAMIC USER INTERFACE LAYOUT ALGORITHM**

DYNAMISCHER BENUTZERSCHNITTSTELLENLAYOUTALGORITHMUS

ALGORITHME DE DISPOSITION D'UNE INTERFACE UTILISATEUR DYNAMIQUE

(84) Designated Contracting States: **AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR**

(30) Priority: **09.04.2014 US 201414249089**

(43) Date of publication of application: **14.10.2015 Bulletin 2015/42**

(73) Proprietor: **SAP SE**
69190 Walldorf (DE)

(72) Inventor: **Peters, Johan Christiaan**
69190 Walldorf (DE)

(74) Representative: **Müller-Boré & Partner Patentanwälte PartG mbB**
Friedenheimer Brücke 21
80639 München (DE)

(56) References cited:
WO-A1-01/09835 **US-A1- 2012 054 602**
US-B1- 6 785 866

Printed by Jouve, 75001 PARIS (FR)

EP 2 930 613 B1

1. A computer-implemented method (300) comprising:

dividing (302) an available vertical space associated with a graphical user interface, GUI (142), into a plurality of allowed vertical space allocations based on a priority of a plurality of data display fields (402, 404, 406);
calculating (304), by a computer, slack (408) following each data display field expanding to fill an allowed vertical space allocation associated with the data display fields;
allocating (306) the slack among the plurality of data display fields (402, 404, 406);
re-calculating (308), by a computer, slack following allocation of slack among the plurality of data display fields; and
finalizing (312) display of the plurality of data display elements in the GUI,

characterized in that
the calculated slack is either positive or negative, and **in that**
the method further comprises:

determining (310) whether the plurality of data display elements need to be resized based on the re-calculated slack (408),
resizing, for calculated positive slack, each data display field from highest priority to lowest priority to expand into a vertical space including its current size, remaining allowed vertical space allocation, and determined slack, and
resizing, for calculated negative slack, each data display field from low-est priority to highest priority to shrink into a vertical space including its current size minus the determined slack.

4. A non-transitory, computer-readable medium storing computer-readable instructions executable by a computer and operable to:

7. A system (100), comprising:

a memory (148);
at least one hardware processor (144) interoperably coupled with the memory and configured to:

Source: https://worldwide.espacenet.com/advancedSearch?locale=en_EP

EJEMPLO: INTERFAZ

(19) Europäisches Patentamt / European Patent Office / Office européen des brevets

(11) EP 2 930 613 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
11.01.2017 Bulletin 2017/02

(51) Int Cl.:
H04L 29/06 *(2006.01)* ***G06F 3/0481*** *(2013.01)*
H04L 29/08 *(2006.01)* ***G06F 9/44*** *(2006.01)*

(21) Application number: **15000999.1**

(22) Date of filing: **08.04.2015**

(54) **DYNAMIC USER INTERFACE LAYOUT ALGORITHM**
DYNAMISCHER BENUTZERSCHNITTSTELLENLAYOUTALGORITHMUS
ALGORITHME DE DISPOSITION D'UNE INTERFACE UTILISATEUR DYNAMIQUE

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **09.04.2014 US 201414249089**

(43) Date of publication of application:
14.10.2015 Bulletin 2015/42

(73) Proprietor: **SAP SE**
69190 Walldorf (DE)

(72) Inventor: **Peters, Johan Christiaan**
69190 Walldorf (DE)

(74) Representative: **Müller-Boré & Partner**
Patentanwälte PartG mbB
Friedenheimer Brücke 21
80639 München (DE)

(56) References cited:
WO-A1-01/09835 US-A1- 2012 054 602
US-B1- 6 785 866

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Printed by Jouve, 75001 PARIS (FR)

EP 2 930 613 B1

[0055] In some implementations, the following software code can be used to perform the above-described

```
UI5VerticalLayout.prototype.setSize =
function(size) {
        var content = this.UI5.getContent();
      var totalPrio = this.getPrio().weighted;
        var ns;
        var height = 0;
       var slack = 0;
        var y;
        var yPad = 7;
        // calculate the available space for
each element, proportional to its importance.
      // than have each element resize to the
largest size that fist into this space
       // and calculate slack
        content.forEach(function(o,i) {
          y = Math.max(0, slack) + size[1] *
o.data("template").getPrio().weighted /
totalPrio;
     ns = o.data("template").setSize([size[0],
y]);
          o.size = ns; // store size on UI5
object since not available
          slack = y - ns[1];
          height += ns[1];
        });
       // sort by priority from high to low
       content.sort(function(a,b) {
          return
b.data("template").getPrio().weighted -
a.data("template") .getPrio().weighted;
        });
        // add remaining slack to all objects
        slack = size[1] - height;
        height = 0;
        (slack >= 0 ? content:
content.reverse()).forEach(function(o,i)
        { // if slack > start with
        heighest prio elements, if slack < 0
start with lowest prio elements
       y = o.size[1] + slack; // give element
its own space + available slack
     ns = o.data("template").setSize([size[0],
y]); // compute new height of element
        o.size = ns; // store as new attribute
size on UI5 object since not available in UI5
          slack += (o.size [1] - ns[1]); //
calculate remaining slack - slack - difference
          between old and new size of element
          height += ns[1]; // add height of
element to total height
        });
        slack = size [1] - height;
        content.forEach(function(o,i) {
          var hidecontent =
lgGetAttr(o.data("template").struc,"format.hi
decontent", true);
         if ((slack < 0 || o.size[1] <= 0) &&
hidecontent) {
            slack += o.size[1];
            height -= o.size[1];
            o.setVisible (false);


   } else {
     o.setVisible(true);
   }
 });
this.UI5.setWidth(size[0] + "px");
return [seize[0], height];
};
```

EJEMPLO: INTERFAZ

1. A computer-implemented method (300) comprising

dividing (302) an available vertical space associated with a graphical user interface, GUI (142) into a plurality of allowed vertical space allocations based on a priority of a plurality of data display fields (402, 404, 406);
calculating (304), by a computer, slack (408) following each data display field expanding to fill an allowed vertical space allocation associated with the data display fields;
allocating (306) the slack among the plurality of data display fields (402, 404, 406);
re-calculating (308), by a computer, slack following allocation of slack among the plurality of data display fields; and
finalizing (312) display of the plurality of data display elements in the GUI,

characterized in that
the calculated slack is either positive or negative, and **in that**
the method further comprises:

determining (310) whether the plurality of data display elements need to be resized based on the re-calculated slack (408),
resizing, for calculated positive slack, each data display field from highest priority to lowest priority to expand into a vertical space including its current size, remaining allowed vertical space allocation, and determined slack, and
resizing, for calculated negative slack, each data display field from low-est priority to highest priority to shrink into a vertical space including its current size minus the determined slack.

4. A non-transitory, computer-readable medium storing computer-readable instructions executable by a computer and operable to:

7. A system (100), comprising:

a memory (148);
at least one hardware processor (144) interoperably coupled with the memory and configured to:

Problema técnico: disposición de la información en pantallas de diferentes tamaños.

Solución: procedimiento/método para la generación de interfaz.

Se incluge código fuente en la descripción.

Clarke, Modet & Cº

FUNDADA EN 1879

CEL abogados

Para más información, duda o cuestión pueden dirigirse a:

José Mª del Valle/Dámaso Gallardo
Avda. Diagonal 403, 4º 4ª
08008 BARCELONA
CLARKE MODET & Co.
Tel. 93 217 38 00

Cristina Fernández
Consell de Cent, 413-415, 4ª planta
08009 BARCELONA
CEL ABOGADOS ASOCIADOS S.L.P
Tel. 93 265 90 09
Fax. 93 265 80 88

www.clarkemodet.com