

Señora
Directora de la Dirección de Nuevas Creaciones
Superintendencia de Industria y Comercio
Ministerio de Comercio, Industria y Turismo
E. S. D.

Re.: Expediente No. NC2018/0008254

Solicitud de Patente PCT entrada en Fase Nacional, para: **“MÉTODO PARA EVITAR EL USO INDEBIDO DE PERMISOS DE ACCESO ELECTRÓNICOS, QUE PUEDEN GESTIONARSE EN DISPOSITIVOS ELECTRÓNICOS MÓVILES USANDO UNA APLICACIÓN DE MONEDERO Y QUE SE TRANSMITEN A LOS DISPOSITIVOS ELECTRÓNICOS MÓVILES MEDIANTE UN SERVIDOR, USANDO EN CADA CASO UN ENLACE PARA LA DESCARGA DEL PERMISO DE ACCESO”**

Solicitantes: **SKIDATA AG**

**SOLICITUD DE PROCEDIMIENTO ACELERADO DE PATENTES Y
MODIFICACIONES VOLUNTARIAS DEL PLIEGO REIVINDICATORIO**

Yo, **MARGARITA CASTELLANOS ABONDANO**, mayor de edad, identificada y domiciliada como aparece al pie de mi firma, obrando en mi calidad de apoderada de la sociedad solicitante del asunto citado en la referencia, en virtud del Artículo 46 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina que establece que *“La oficina nacional competente podrá requerir el informe de expertos o de organismos científicos o tecnológicos que se consideren idóneos, para que emitan opinión sobre la patentabilidad de la invención. Asimismo, cuando lo estime conveniente, podrá requerir informes de otras oficinas de propiedad industrial”*, me permito presentar una solicitud de reconocimiento de los resultados del examen de patentabilidad emitido por la Oficina Australiana de Patentes de No. de la solicitud australiana equivalente **2018204447**.

Para tal fin, adjunto los siguientes documentos:

- (i) Copia del examen de patentabilidad emitido el 06 de marzo de 2019 por la Oficina Australiana de Patentes y su correspondiente traducción al castellano
- (ii) Copia de la respuesta al examen de patentabilidad emitido el 06 de marzo de 2019 por la Oficina Australiana de Patentes y su correspondiente traducción al castellano

- (iii) Copia de la Aceptación de la patente por la Oficina Australiana de Patentes y su correspondiente traducción al castellano
- (iv) Copia de la Concesión de la patente por la Oficina Australiana de Patentes y su correspondiente traducción al castellano
- (v) Copia del Certificado de Concesión de la patente por la Oficina Australiana de Patentes y su correspondiente traducción al castellano
- (vi) Copia de la patente concedida, incluyendo todas las reivindicaciones determinadas como patentables otorgables por la Oficina Australiana de Patentes que profirió el examen de patentabilidad y su traducción al castellano
- (vii) Una tabla de correspondencias de las reivindicaciones que han sido determinadas como patentables u otorgables en la solicitud de la Oficina Australiana de Patentes

Adicionalmente, me permito poner de presente que el día de hoy se ha presentado como modificación voluntaria un nuevo pliego reivindicatorio que comprende dos reivindicaciones, el cual corresponde al pliego reivindicatorio concedido por la Oficina Australiana de Patentes. Específicamente, se pone de presente que las reivindicaciones 1 y 2 del nuevo pliego reivindicatorio presentado como modificación voluntaria, corresponde a aquel otorgado por la Oficina Australiana de Patentes así:

Reivindicaciones pliego reivindicatorio modificado en Colombia	Reivindicaciones concedidas por la Oficina Australiana de Patentes
1	1
2	2

Se anexa al presente memorial copia de la discusión que evidencia la radicación de las modificaciones voluntarias, así como copia del pliego reivindicatorio modificado.

Anexos

- (i) Tabla de correspondencias de las reivindicaciones que han sido determinadas como patentables u otorgables en la solicitud de la Oficina Australiana de Patentes
- (ii) Copia del examen de patentabilidad emitido el 06 de marzo de 2019 por la Oficina Australiana de Patentes y su correspondiente traducción al castellano

- (iii) Copia de la respuesta al examen de patentabilidad emitido el 06 de marzo de 2019 por la Oficina Australiana de Patentes y su correspondiente traducción al castellano
- (iv) Copia de la Aceptación de la patente por la Oficina Australiana de Patentes y su correspondiente traducción al castellano
- (v) Copia de la Concesión de la patente por la Oficina Australiana de Patentes y su correspondiente traducción al castellano
- (vi) Copia del Certificado de Concesión de la patente por la Oficina Australiana de Patentes y su correspondiente traducción al castellano
- (vii) Copia de la patente concedida, incluyendo todas las reivindicaciones determinadas como patentables otorgables por la Oficina Australiana de Patentes que profirió el examen de patentabilidad y su traducción al castellano
- (viii) Copia de la discusión que evidencia la radicación de las modificaciones voluntarias
- (ix) Nuevo pliego reivindicatorio del expediente No. NC2018/0008254 que comprende dos reivindicaciones

Señora Directora,



Margarita Castellanos Abondano

C.C. No. **39.779.654** de Bogotá

T.P.A. No. **70.819** del C.S.J.

Calle 117 No. 5A-35 - Bogotá, D.C.

Teléfono: 7560770

Bogotá, D.C.

MCA/dpg

P4904

(i) Tabla de correspondencias de las reivindicaciones que han sido determinadas como patentables u otorgables en la solicitud de la Oficina Australiana de Patentes

	TABLA DE CORRESPONDENCIA DE REIVINDICACIONES	
	Reivindicaciones concedidas por la Oficina Australiana de Patentes	Reivindicaciones pliego reivindicatorio modificado en Colombia
Reivindicación 1 y 2	No contiene los números de referencia de cada una de las partes del envase del medicamento.	Se modificó de manera que ahora incluye las características de la anterior reivindicación 2. A fin de darle claridad a las reivindicaciones, incluye los números de referencia de cada uno de los elementos que hacen parte del método reivindicado
Reivindicación 2		Han sido incluidas las características técnicas en la nueva reivindicación 1
Reivindicación 3		Ha sido renumerada como la nueva reivindicación 2



Patents



Trade Marks



Designs



Plant Breeder's Rights

Delivering a world leading IP system

www.ipaustralia.gov.au

ABN: 38 113 072 755

6 March 2019

Examination report No. 1 for standard patent application

Spruson & Ferguson

GPO Box 3898
Sydney NSW 2001
Australia

Your reference	P309471
Application number	2018204447
Applicant name	SKIDATA AG
Earliest priority date	07 August 2017

Final date for acceptance:	6 March 2020
Date of this report:	6 March 2019
Examination request date:	23 August 2018

Dear Spruson & Ferguson,

Your application has been examined under [section 45 of the Patents Act 1990](#). I consider that this application does not meet the requirements of the Act because there are issues with the application that are explained in the report details.

You have **12 months** from the date of this report to overcome all my objection(s) otherwise this application will lapse.

You will also need to pay any annual continuation fees that apply. Your next continuation fee is due on **20 June 2022**.

NOTE: There is a current postponement of acceptance in place. If you overcome all other objections before the expiration of that postponement, the Commissioner will only accept the application at that time if you have filed a clear and unambiguous statement requesting the withdrawal of that postponement. Otherwise, a further adverse report will be issued.

Details of this patent application can be viewed on [AusPat](#), our Australian patent search database.

Yours sincerely,

Yogita Chapre
Section: ELEC 2 – ELECTRONICS & COMMUNICATIONS
Phone: (612) 6222 3638

Report details

Basis of the report

In examining this application I have considered:

- the specification as filed

Summary of novelty, inventive step and patentable subject matter

	<i>Satisfy requirements?</i>	<i>Claim numbers</i>
Novelty/inventive step	Yes	NONE
	No	1-3
Patentable subject matter	Yes	1-3
	No	NONE

Detailed objections on issues that have been identified

Documents cited or considered relevant

D1 : US 20160350547 A1 (LOUGHLIN-MCHUGH Eleanor Simone Frederika et al.) 01 December 2016 ^[1]
Category: **X** Claims: 1-3

^[1] Cited in EP 3442249

Special categories of cited documents:

X: The claimed invention cannot be considered novel under [subsection 7\(1\)](#) in light of the document and/or cannot be considered to involve an inventive step under [subsection 7\(2\)](#) of the Act in light of the common general knowledge considered together with the document.

Novelty and inventive step

1 **Claim 1** is not novel and therefore lack an inventive step in light of the prior art document **D1**.

As per **independent claim 1, D1** discloses A method for preventing the misuse of electronic access permissions (D1: Para[0104]), which can be managed in mobile electronic devices using a wallet application (D1: Para[0052]) and which are transmitted to the mobile electronic devices (D1: Para[0050]) by a server (D1: Figure 2), in each case using a link (D1: Para[0049]) for downloading the access permission, wherein an electronic access permission is purchased by means of an interaction with a server (D1: Para[0082]), wherein during the purchase of the electronic access permission by a purchaser, a password or authentication data and a mobile electronic device (D1: Para[0057]), to which the electronic access permission is transmitted by the server via a link for downloading the access permission, are specified (D1: Para[0082]), wherein when activating the link for downloading the purchased access permission a unique ID of the mobile electronic device is transmitted to the server, which is associated with an ID of the purchased access permission (D1: Para[0075]; Figure 2), wherein the electronic access

permission is only transferred from the mobile electronic device to another mobile electronic device (D1: Para[0084]) after the password specified by the purchaser of the access permission or the authentication data (D1: Para[0062], [0090]) specified by the purchaser of the access permission is first entered by means of an interaction with the server (D1: Para[0085]; Figure 3), wherein upon successful transfer the access permission ID is associated with the ID of the other mobile electronic device in the server (D1: Para[0092]; Figure 3) and the access permission stored on the first mobile electronic device is marked by the server as invalid (D1: Para[0103]).

Furthermore, I have considered each of the **appended claims 2-3**. Each of these claims is not considered to make any patentable contribution over the teachings of the above cited document D1. The relevant features of these claims are either disclosed in the above cited document D1 or are common general knowledge in the art/mere design choices and which therefore cannot contribute to providing novelty or an inventive step. For example, the features of **dependent claim 3** merely add *"wherein if an access permission is to be transferred from one mobile electronic device to another mobile electronic device, i.e. if the access permission ID has already been associated with a unique ID of a mobile electronic device, then on the basis of the number of the completed associations between the access permission ID and unique IDs of mobile electronic devices, it is verified how often the access permission has already been transferred, wherein if the number of completed transfers has reached a predefined threshold value, no further transfer is possible"*, which are matters of common general knowledge.

END OF REPORT

6 de marzo de 2019

INFORME DE EXAMEN No. 1 PARA SOLICITUD ESTANDAR DE PATENTE

Spruson & Ferguson
GPO Box 3898
Sydney NSW 2001
Australia

Su referencia: P309471
Número de la solicitud: 2018204447
Nombre del solicitante: SKIDATA AG

Fecha fina para aceptación: 6 de marzo de 2020
Fecha de este informe: 6 de marzo de 2019
Fecha de petición del examen: 23 de agosto de 2019

Estimados Spruson & Ferguson,

Su solicitud ha sido evaluada bajo la sección 45 del Acta de Patentes de 1990. Yo considero que esta solicitud no cumple con los requerimientos del Acta debido a que hay inconvenientes con la solicitud que se explican en los detalles del informe.

Usted tiene 12 meses desde la fecha de este informe para superar todas mis objeciones, de lo contrario la solicitud caerá en abandono.

Usted también necesitará pagar cualquier tasa anual de continuación que aplique. Su siguiente tasa de continuación vence el 20 de junio de 2022.

NOTA: Existe un actual aplazamiento de aceptación e en curso. Si usted supera todas las otras objeciones antes de la expiración de dicho aplazamiento (postergamiento), el Comisionado solo aceptará la solicitud en ese momento si usted ha presentado de manera clara y no ambigua una declaración solicitando la desestimación de dicho aplazamiento. De lo contrario, se emitirá otro informe adverso.

Los detalles de esa solicitud de patente se pueden ver en AusPat, nuestra base de datos de patentes australiana.

Cordialmente,

Yogita Chapre

Sección: ELEC 2 – ELECTRONICS & COMMUNICATIONS

Teléfono: (612) 6222 3638

Su referencia: P309471
Número de la solicitud: 2018204447

Detalles del Informe

Bases del informe

Al examinar esta solicitud, he considerado:

-La descripción como se presentó

Resumen de novedad, nivel inventivo y patentabilidad de la materia a proteger

	¿Satisface los requerimientos?	Número de reivindicaciones
Novedad/ nivel inventivo	Si	Ninguna
	No	1-3
Patentabilidad	Si	Ninguna
	No	1-3

Objeciones detalladas sobre los problemas que se han identificado

Documentos citados o considerados relevantes

D1: US 20160350547 A1 (LOUGHLIN-MCHUGH Eleanor Simone Frederika *et al.*)
01 de diciembre de 2016

Categoría: **X** Reivindicaciones: 1-3

Categorías especiales de los documentos citados:

X: La invención reivindicada no puede ser considerada novedosa bajo la subsección 7(1) a la luz del documento y/o no puede ser considerada que involucre actividad inventiva bajo la subsección 7(2) del Acta a la luz del conocimiento general considerado en conjunto con el documento.

Novedad y nivel inventivo

- 1 La reivindicación 1 no es novedosa y por lo tanto carece de nivel inventivo a la luz del arte previo del documento D1.

Según **la reivindicación independiente 1, D1** discute un método para prevenir el uso indebido de permisos de acceso electrónico (D1: Párrafo[0104]), que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero (D1: Párrafo[0052]) y que se transmiten a los dispositivos electrónicos móviles (D1: Párrafo[0050]) mediante un servidor (D1: Figura 2), usando en cada caso un enlace (D1: Párrafo[0049]) para la descarga del permiso de acceso en donde durante la compra del permiso de acceso electrónico por un comprador, una contraseña o datos de autenticación y un dispositivo electrónico móvil (D1: Párrafo[0057]), al que se transmite el permiso de acceso electrónico mediante el servidor a través de un enlace para la descarga del permiso de acceso se especifica (D1: Para[0082]), en donde cuando se activa el enlace para descargar el permiso de acceso comprado se transmite un ID único del dispositivo electrónico móvil al servidor, que está asociado con un ID del permiso de acceso comprado (D1: Párrafo[0075]; Figura 2), en donde el permiso de acceso electrónico se transfiere únicamente desde el dispositivo electrónico móvil a otro dispositivo electrónico móvil (D1: Párrafo [0084]) después de la contraseña especificada por el comprador del permiso de acceso o los datos de autenticación (D1: Párrafo[0062], [0090]) especificados por el comprador del permiso de acceso se introducen primero por

medio de una interacción con el servidor (D1: Párrafo[0085]; Figura 3), en donde tras una transferencia satisfactoria el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil en el servidor (D1: Párrafo[0092]; Figure 3) y el permiso de acceso almacenado en el primer dispositivo electrónico móvil se marca por el servidor como inválido (D1: Párrafo[0103]).

Además, he considerado cada una de las **reivindicaciones dependientes 2-3**. No se considera que cada una de estas reivindicaciones haga una contribución patentable sobre las enseñanzas del documento D1 mencionado anteriormente. Las características relevantes de estas reivindicaciones se describen en el documento D1 citado anteriormente o son de conocimiento general común para la persona versada en la materia / solamente elecciones de diseño y que, por lo tanto, no pueden contribuir a proporcionar novedad o nivel inventivo. Por ejemplo, las características técnicas de la **reivindicación dependiente 3** solamente adiciona que *“en donde si un permiso de acceso debe transferirse desde un dispositivo electrónico móvil (3) a otro dispositivo electrónico móvil (4), es decir si el ID de permiso de acceso ya se ha asociado con un ID único de un dispositivo electrónico móvil (3), entonces sobre la base del número de las asociaciones completadas entre el ID de permiso de acceso e ID únicos de dispositivos electrónicos móviles, se verifica con qué frecuencia ya se ha transferido el permiso de acceso, en el que si el número de transferencias completadas ha alcanzado un valor umbral predefinido, no es posible ninguna transferencia adicional”*, que corresponde a materia de conocimiento general.

FIN DEL INFORME

Commissioner of Patents
P O Box 200
Woden ACT 2606

SPRUSON & FERGUSON
Sydney NSW
Speed Dial 509
(CCN 3710000177)

5 July, 2019

Our Ref : P309471:GPT:FGC
Telephone Contact: Francis Carreon

Dear Commissioner

Australian Patent Application No. 2018204447

SKIDATA AG

Method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission

Response to Examiner's Report / Withdrawal of Postponement of Acceptance

The Examiner's Report dated 6 March 2019 is acknowledged.

The Applicant seeks leave of the Commissioner under Section 104 to amend the application in accordance with the attached Statement of Proposed Amendments.

The Applicant withdraws the request for postponement of acceptance.

The Applicant has amended independent claim 1 to include the features of previous claim 2 and submits that reference document D1 does not describe or suggest the additional features in amended independent claim 1.

The Applicant submits that the following features of amended independent claim 1 are not disclosed in reference document D1:

- after transferring the link for downloading the access permission to the mobile electronic device, the wallet application which is installed on the mobile device activates the link and in order to download the acquired access permission, transmits a unique ID of the mobile electronic device to the server, wherein in the server it is verified whether an ID of the acquired access permission is associated with the transmitted unique ID of the mobile electronic device, wherein if this is not the case, the access permission ID and the unique ID of the mobile electronic device are associated with each other and the electronic access permission is then downloaded;
- if the electronic access is to be transmitted from one mobile electronic device to another mobile electronic device, after initiation of the process by the owner of the mobile electronic device with whose unique ID the access permission ID is associated, the wallet application of the mobile electronic device, with whose unique ID the access permission ID is associated, transmits the link for downloading the access permission to the other mobile electronic device, wherein the wallet application of the other mobile electronic device activates the link and transmits a unique ID of the other mobile electronic device to the server, whereupon a check is made in the server as to whether an association exists between the ID of the access permission to be transferred with a unique ID of another mobile electronic device, wherein if this is the case, a link is sent by the server to the other mobile electronic device, the execution of which link by the wallet application leads to an input screen for either the password specified by the purchaser of

the access permission or for the authentication data specified by the purchaser of the access permission, wherein if the password is valid or the authentication data are valid, the access permission ID is associated with the ID of the other mobile electronic device in the server and the electronic access permission is downloaded to the other mobile electronic device.

These features are not considered general knowledge of a person skilled in the art and cannot be derived from any prior art document cited without involving an inventive step.

That is, a person skilled in the art would not be led as a matter of course to the invention as claimed when considering the prior art in light of the common general knowledge at the priority date.

Favourable reconsideration of the application is therefore requested.

Yours faithfully

SPRUSON & FERGUSON

A handwritten signature in black ink, appearing to read 'Guy Tucker', written in a cursive style.

Guy Tucker

Registered Patent Attorney

AUSTRALIA

Patents Act 1990

Statement of Proposed Amendments - Section 104

Application No: 2018204447

Our Ref: P309471:GPT:FGC
(CCN 3710000177)

Applicant : SKIDATA AG

1.	Description pages:	Delete pages 2 and 3 as currently on file and substitute new pages 2, 3, 3a and 3b provided herewith in duplicate.
2.	Claims pages:	Delete the claims as currently on file and substitute new claims 1-2 provided herewith in duplicate.

5 July 2019

SKIDATA AG



Registered Patent Attorney

[0004] It is an object of the present invention to substantially overcome, or at least ameliorate, one or more disadvantages of existing arrangements.

[0004a] In one aspect of the present invention, there is provided a method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission, wherein an electronic access permission is purchased by means of an interaction with the server, wherein during the purchase of the electronic access permission by a purchaser, a password or authentication data and a mobile electronic device, to which the electronic access permission is transmitted by the server via the link for downloading the access permission, are specified, wherein when activating the link for downloading the purchased access permission a unique ID of the mobile electronic device is transmitted to the server, which is associated with an ID of the purchased access permission, wherein the electronic access permission is only transferred from the mobile electronic device to another mobile electronic device after the password specified by the purchaser of the access permission or the authentication data specified by the purchaser of the access permission is first entered by means of an interaction with the server, wherein upon successful transfer the access permission ID is associated with the ID of the other mobile electronic device in the server and the access permission stored on the first mobile electronic device is marked by the server as invalid, wherein after transferring the link for downloading the access permission to the mobile electronic device, the wallet application which is installed on the mobile device activates the link and in order to download the acquired access permission, transmits a unique ID of the mobile electronic device to the server, wherein in the server it is verified whether an ID of the acquired access permission is associated with the transmitted unique ID of the mobile electronic device, wherein if this is not the case, the access permission ID and the unique ID of the mobile electronic device are associated with each other and the electronic access permission is then downloaded, and wherein if the electronic access is to be transmitted from one mobile electronic device to another mobile electronic device, after initiation of the process by the owner of the mobile electronic device with whose unique ID the access permission ID is associated, the wallet application of the mobile electronic device, with whose unique ID the access permission ID is associated, transmits the link for downloading the access permission to the other mobile electronic device, wherein the wallet application of the other mobile electronic device activates the link and transmits a unique ID of the other mobile

electronic device to the server, whereupon a check is made in the server as to whether an association exists between the ID of the access permission to be transferred with a unique ID of another mobile electronic device, wherein if this is the case, a link is sent by the server to the other mobile electronic device, the execution of which link by the wallet application leads to an input screen for either the password specified by the purchaser of the access permission or for the authentication data specified by the purchaser of the access permission, wherein if the password is valid or the authentication data are valid, the access permission ID is associated with the ID of the other mobile electronic device in the server and the electronic access permission is downloaded to the other mobile electronic device.

[0005] Consequently, a method is proposed for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission, wherein in said method an electronic access permission is purchased by means of an interaction with a server, wherein during the purchase of the electronic access permission by a buyer, a password or authentication data and a mobile electronic device are specified, wherein the electronic access permission is transmitted from the server to the mobile electronic device by means of a link for downloading the access permission.

[0006] According to the present disclosure, in implementing the link for downloading the purchased access permission a unique ID of the mobile electronic device is transmitted to the server, which is associated with an ID of the acquired access permission, wherein a transmission of the electronic access permission from the first mobile electronic device to another mobile electronic device takes place only after the input of the password specified by the purchaser of the access permission, and/or input of the authentication data specified by the buyer of the access permission by means of an interaction with the server, wherein on completion of the transfer the access permission ID is associated with the ID of the other mobile electronic device in the server, and the server marks the access permission stored on the first mobile electronic device as invalid.

[0007] In the context of one design of the present disclosure, after the transmission of the link for downloading the access permission to the mobile electronic device, a wallet application installed on the mobile device activates the link and in order to download the acquired access permission a unique ID of the mobile electronic device is transmitted to the server, wherein it is verified in the server whether an ID of the acquired access permission is

associated with the transmitted unique ID of the mobile electronic device, wherein if this is not the case, the access permission ID and the unique ID of the mobile electronic device are associated with each other and the electronic access permission is then downloaded.

[0008] In the event that the electronic access permission is to be transferred from one mobile electronic device to another mobile electronic device, the wallet application of the mobile electronic device, whose unique ID is associated with the access permission ID, transmits a link for downloading the access permission to the other mobile electronic device, wherein the wallet application of the other mobile electronic device activates the link and transmits a unique ID of the other mobile electronic device to the server.

[0009] According to the present disclosure, it is verified in the server whether an association of the access permission ID with a unique ID of another mobile electronic device exists, wherein if this is the case, the server sends a link to the other mobile electronic device, the activation of which by the wallet application leads to an input screen for either the password specified by the purchaser of the access permission or for the authentication data specified by the purchaser of the access permission, wherein if the password is valid or the authentication data are valid, the access permission ID is associated with the ID of the other mobile electronic device in the server and the electronic access permission is downloaded to the other mobile electronic device.

[0010] Then, the access permission stored on the first mobile electronic device is marked by the server as invalid, preferably by means of a push message to the wallet application, wherein the association of the ID of the first mobile electronic device with the electronic access permission is deleted and the corresponding data are stored on the server.

[0011] The design according to the present disclosure provides a method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission, the activation of which ensures that an access permission can only be transferred to another mobile electronic device if this is a mobile electronic device of an authorized person.

[0012] In the context of an extension of the present disclosure, if an access permission is to be transferred from one mobile electronic device to another mobile electronic device, i.e. if the access permission ID has already been associated with a unique ID of a mobile electronic device, then on the basis of the number of the completed associations from the access permission ID to unique IDs of mobile electronic devices it is verified how often the access permission has already been transferred, wherein if the number of completed transfers has reached a predefined threshold value, no further transfer is possible.

CLAIMS

1. A method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission, wherein an electronic access permission is purchased by means of an interaction with the server, wherein during the purchase of the electronic access permission by a purchaser, a password or authentication data and a mobile electronic device, to which the electronic access permission is transmitted by the server via the link for downloading the access permission, are specified, wherein when activating the link for downloading the purchased access permission a unique ID of the mobile electronic device is transmitted to the server, which is associated with an ID of the purchased access permission, wherein the electronic access permission is only transferred from the mobile electronic device to another mobile electronic device after the password specified by the purchaser of the access permission or the authentication data specified by the purchaser of the access permission is first entered by means of an interaction with the server, wherein upon successful transfer the access permission ID is associated with the ID of the other mobile electronic device in the server and the access permission stored on the first mobile electronic device is marked by the server as invalid, wherein after transferring the link for downloading the access permission to the mobile electronic device, the wallet application which is installed on the mobile device activates the link and in order to download the acquired access permission, transmits a unique ID of the mobile electronic device to the server, wherein in the server it is verified whether an ID of the acquired access permission is associated with the transmitted unique ID of the mobile electronic device, wherein if this is not the case, the access permission ID and the unique ID of the mobile electronic device are associated with each other and the electronic access permission is then downloaded, and wherein if the electronic access is to be transmitted from one mobile electronic device to another mobile electronic device, after initiation of the process by the owner of the mobile electronic device with whose unique ID the access permission ID is associated, the wallet application of the mobile electronic device, with whose unique ID the access permission ID is associated, transmits the link for downloading the access permission to the other mobile electronic device, wherein the wallet application of the other mobile electronic device activates the link and transmits a unique ID of the other mobile electronic device to the server, whereupon a check is made in the server as to whether an association exists between the ID of the access permission to be transferred with a unique ID of

another mobile electronic device, wherein if this is the case, a link is sent by the server to the other mobile electronic device, the execution of which link by the wallet application leads to an input screen for either the password specified by the purchaser of the access permission or for the authentication data specified by the purchaser of the access permission, wherein if the password is valid or the authentication data are valid, the access permission ID is associated with the ID of the other mobile electronic device in the server and the electronic access permission is downloaded to the other mobile electronic device.

2. A method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application, and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission, according to Claim 1, wherein if an access permission is to be transferred from one mobile electronic device to another mobile electronic device, i.e. if the access permission ID has already been associated with a unique ID of a mobile electronic device, then on the basis of the number of the completed associations between the access permission ID and unique IDs of mobile electronic devices, it is verified how often the access permission has already been transferred, wherein if the number of completed transfers has reached a predefined threshold value, no further transfer is possible.

SKIDATA AG

Patent Attorneys for the Applicant/Nominated Person

SPRUSON & FERGUSON

[0004] It is an object of the present invention to substantially overcome, or at least ameliorate, one or more disadvantages of existing arrangements.

[0004a] In one aspect of the present invention, there is provided a method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission, wherein an electronic access permission is purchased by means of an interaction with the server, wherein during the purchase of the electronic access permission by a purchaser, a password or authentication data and a mobile electronic device, to which the electronic access permission is transmitted by the server via the link for downloading the access permission, are specified, wherein when activating the link for downloading the purchased access permission a unique ID of the mobile electronic device is transmitted to the server, which is associated with an ID of the purchased access permission, wherein the electronic access permission is only transferred from the mobile electronic device to another mobile electronic device after the password specified by the purchaser of the access permission or the authentication data specified by the purchaser of the access permission is first entered by means of an interaction with the server, wherein upon successful transfer the access permission ID is associated with the ID of the other mobile electronic device in the server and the access permission stored on the first mobile electronic device is marked by the server as invalid, wherein after transferring the link for downloading the access permission to the mobile electronic device, the wallet application which is installed on the mobile device activates the link and in order to download the acquired access permission, transmits a unique ID of the mobile electronic device to the server, wherein in the server it is verified whether an ID of the acquired access permission is associated with the transmitted unique ID of the mobile electronic device, wherein if this is not the case, the access permission ID and the unique ID of the mobile electronic device are associated with each other and the electronic access permission is then downloaded, and wherein if the electronic access is to be transmitted from one mobile electronic device to another mobile electronic device, after initiation of the process by the owner of the mobile electronic device with whose unique ID the access permission ID is associated, the wallet application of the mobile electronic device, with whose unique ID the access permission ID is associated, transmits the link for downloading the access permission to the other mobile electronic device, wherein the wallet application of the other mobile electronic device activates the link and transmits a unique ID of the other mobile

electronic device to the server, whereupon a check is made in the server as to whether an association exists between the ID of the access permission to be transferred with a unique ID of another mobile electronic device, wherein if this is the case, a link is sent by the server to the other mobile electronic device, the execution of which link by the wallet application leads to an input screen for either the password specified by the purchaser of the access permission or for the authentication data specified by the purchaser of the access permission, wherein if the password is valid or the authentication data are valid, the access permission ID is associated with the ID of the other mobile electronic device in the server and the electronic access permission is downloaded to the other mobile electronic device.

[0005] Consequently, a method is proposed for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission, wherein in said method an electronic access permission is purchased by means of an interaction with a server, wherein during the purchase of the electronic access permission by a buyer, a password or authentication data and a mobile electronic device are specified, wherein the electronic access permission is transmitted from the server to the mobile electronic device by means of a link for downloading the access permission.

[0006] According to the ~~present disclosure~~invention, in implementing the link for downloading the purchased access permission a unique ID of the mobile electronic device is transmitted to the server, which is associated with an ID of the acquired access permission, wherein a transmission of the electronic access permission from the first mobile electronic device to another mobile electronic device takes place only after the input of the password specified by the purchaser of the access permission, and/or input of the authentication data specified by the buyer of the access permission by means of an interaction with the server, wherein on completion of the transfer the access permission ID is associated with the ID of the other mobile electronic device in the server, and the server marks the access permission stored on the first mobile electronic device as invalid.

[0007] In the context of one design of the ~~present disclosure~~invention, after the transmission of the link for downloading the access permission to the mobile electronic device, a wallet application installed on the mobile device activates the link and in order to download the acquired access permission a unique ID of the mobile electronic device is transmitted to the server, wherein it is verified in the server whether an ID of the acquired access permission is

associated with the transmitted unique ID of the mobile electronic device, wherein if this is not the case, the access permission ID and the unique ID of the mobile electronic device are associated with each other and the electronic access permission is then downloaded.

[0008] In the event that the electronic access permission is to be transferred from one mobile electronic device to another mobile electronic device, the wallet application of the mobile electronic device, whose unique ID is associated with the access permission ID, transmits a link for downloading the access permission to the other mobile electronic device, wherein the wallet application of the other mobile electronic device activates the link and transmits a unique ID of the other mobile electronic device to the server.

[0009] According to the ~~present disclosure~~~~invention~~, it is verified in the server whether an association of the access permission ID with a unique ID of another mobile electronic device exists, wherein if this is the case, the server sends a link to the other mobile electronic device, the activation of which by the wallet application leads to an input screen for either the password specified by the purchaser of the access permission or for the authentication data specified by the purchaser of the access permission, wherein if the password is valid or the authentication data are valid, the access permission ID is associated with the ID of the other mobile electronic device in the server and the electronic access permission is downloaded to the other mobile electronic device.

[0010] Then, the access permission stored on the first mobile electronic device is marked by the server as invalid, preferably by means of a push message to the wallet application, wherein the association of the ID of the first mobile electronic device with the electronic access permission is deleted and the corresponding data are stored on the server.

[0011] The design according to the ~~present disclosure~~~~invention~~ provides a method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission, the activation of which ensures that an access permission can only be transferred to another mobile electronic device if this is a mobile electronic device of an authorized person.

[0012] In the context of an extension of the ~~present disclosure~~invention, if an access permission is to be transferred from one mobile electronic device to another mobile electronic device, i.e. if the access permission ID has already been associated with a unique ID of a mobile electronic device, then on the basis of the number of the completed associations from the access permission ID to unique IDs of mobile electronic devices it is verified how often the access permission has already been transferred, wherein if the number of completed transfers has reached a predefined threshold value, no further transfer is possible.

CLAIMS

1. A method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission, wherein an electronic access permission is purchased by means of an interaction with athe server, wherein during the purchase of the electronic access permission by a purchaser, a password or authentication data and a mobile electronic device, to which the electronic access permission is transmitted by the server via thea link for downloading the access permission, are specified, wherein when activating the link for downloading the purchased access permission a unique ID of the mobile electronic device is transmitted to the server, which is associated with an ID of the purchased access permission, wherein the electronic access permission is only transferred from the mobile electronic device to another mobile electronic device after the password specified by the purchaser of the access permission or the authentication data specified by the purchaser of the access permission is first entered by means of an interaction with the server, wherein upon successful transfer the access permission ID is associated with the ID of the other mobile electronic device in the server and the access permission stored on the first mobile electronic device is marked by the server as invalid₁

~~2. A method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission, according to Claim 1,~~ wherein after transferring the link for downloading the access permission to the mobile electronic device, athe wallet application which is installed on the mobile device activates the link and in order to download the acquired access permission, transmits a unique ID of the mobile electronic device to the server, wherein in the server it is verified whether an ID of the acquired access permission is associated with the transmitted unique ID of the mobile electronic device, wherein if this is not the case, the access permission ID and the unique ID of the mobile electronic device are associated with each other and the electronic access permission is then downloaded, and wherein if ~~an-the~~ athe electronic access is to be transmitted from one mobile electronic device to another mobile electronic device, after initiation of the process by the owner of the mobile electronic device with whose unique ID the access permission ID is associated, the wallet application of the mobile electronic device, with whose unique ID the access permission

ID is associated, transmits ~~the~~ link for downloading the access permission to the other mobile electronic device, wherein the wallet application of the other mobile electronic device activates the link and transmits a unique ID of the other mobile electronic device to the server, whereupon a check is made in the server as to whether an association exists between the ID of the access permission to be transferred with a unique ID of another mobile electronic device, wherein if this is the case, a link is sent by the server to the other mobile electronic device, the execution of which link by the wallet application leads to an input screen for either the password specified by the purchaser of the access permission or for the authentication data specified by the purchaser of the access permission, wherein if the password is valid or the authentication data are valid, the access permission ID is associated with the ID of the other mobile electronic device in the server and the electronic access permission is downloaded to the other mobile electronic device.

~~23~~. A method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application, and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission, according to Claim 1 ~~or Claim 2~~, wherein if an access permission is to be transferred from one mobile electronic device to another mobile electronic device, i.e. if the access permission ID has already been associated with a unique ID of a mobile electronic device, then on the basis of the number of the completed associations between the access permission ID and unique IDs of mobile electronic devices, it is verified how often the access permission has already been transferred, wherein if the number of completed transfers has reached a predefined threshold value, no further transfer is possible.

SKIDATA AG

Patent Attorneys for the Applicant/Nominated Person

SPRUSON & FERGUSON

Comisionado de Patentes

PO Box 200

Woden ACt 2606

SPRUSON & FERGUSON

Sydney NSW

Speed Dial 509

(CCN 3710000177)

5 Julio, 2019

Nuestra ref : P309471:GPT:FGC

Contacto telefónico: Francis Carreon

Estimado Comisionado,

Solicitud de Patente Australiana No. 2018204447

SKIDATA AG

Método para prevenir el uso indebido de permisos de acceso electrónico que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso

Respuesta al Informe del Examinador (Retirada de aplazamiento de aceptación)

Se reconoce el informe del examinador de fecha 6 de marzo de 2019.

El Solicitante solicita el permiso del Comisionado bajo la Sección 104 para enmendar la solicitud de acuerdo con la Declaración de Enmiendas Propuestas adjunta.

El Solicitante retira la solicitud de aplazamiento de aceptación.

El Solicitante ha modificado la reivindicación independiente 1 incluyendo las características que estaban previamente en la reivindicación 2 e indica que el documento de referencia D1 no describe o sugiere las características adicionales en la reivindicación independiente 1 modificada.

El Solicitante muestra que las siguientes características de la reivindicación independiente 1 modificada no están discutidas en el documento de referencia D1:

- después de transferir el enlace para descargar el permiso de acceso al dispositivo electrónico móvil, la aplicación de monedero que se instala en el dispositivo móvil activa el enlace y para descargar el permiso de acceso adquirido, transmite un ID único del dispositivo electrónico móvil al servidor, en el que en el servidor verifica si un ID del permiso de acceso adquirido está asociado con el ID único transmitido del dispositivo electrónico móvil, en el que si este no es el caso, el ID de permiso de acceso y el ID único del dispositivo electrónico móvil se asocian entre sí y el permiso de acceso electrónico se descarga a continuación;
- si el acceso electrónico debe transmitirse desde un dispositivo electrónico móvil a otro dispositivo electrónico móvil, después de la iniciación del proceso por el propietario del dispositivo electrónico móvil con cuyo ID único está asociado el ID de permiso de acceso, la aplicación de monedero del dispositivo electrónico móvil, con cuyo ID único está asociado el ID de permiso de acceso, transmite el enlace para la descarga del permiso de acceso al otro dispositivo electrónico móvil, en el que la aplicación de

monedero del otro dispositivo electrónico móvil activa el enlace y transmite un ID único del otro dispositivo electrónico móvil al servidor, tras lo cual se hace una comprobación en el servidor en cuanto a si existe una asociación entre el ID del permiso de acceso a transferir con un ID único de otro dispositivo electrónico móvil, en el que si este es el caso, se envía un enlace mediante el servidor al otro dispositivo electrónico móvil, cuya ejecución de enlace por la aplicación de monedero conduce a una pantalla de entrada para o bien la contraseña especificada por el comprador del permiso de acceso o bien para los datos de autenticación especificados por el comprador del permiso de acceso, en el que si la contraseña es válida o los datos de autenticación son válidos, el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil (4) en el servidor y el permiso de acceso electrónico se descarga al otro dispositivo electrónico móvil.

Estas características no están consideradas dentro del conocimiento general de una persona versada en la materia y no pueden ser derivadas de ningún documento de arte previo contado sin necesariamente requerir actividad inventiva.

Esto es, una persona normalmente versada en la materia no sería conducida de forma natural a la invención como se reivindica cuando se considera la técnica anterior a la luz del conocimiento general a la fecha de prioridad.

Por lo tanto, se solicita una reconsideración favorable de la solicitud.

Cordialmente,

SPRUSON & FERGUSON

Guy Tucker

Abogado registrado de Patentes

AUSTRALIA

Acta de Patente 1990

Declaración de modificaciones propuestas- Sección 104

Solicitud No: 2018204447

Nuestra ref.: P309471:GPT:FGC

(CCN 3710000177)

Solicitante: SKIDATA AG

1.	Páginas de la descripción:	Borrar las páginas 2 y 3 como actualmente se encuentran en el archivo y sustituirlas por las páginas nuevas 2, 3, 3a y 3b provistas aquí en duplicado
2.	Páginas de las reivindicaciones:	Borrar las reivindicaciones como actualmente se encuentran en el archivo y sustituirlas por las nuevas reivindicaciones 1-2 provistas aquí en duplicado

5 de julio de 2019

SKIDATA AG

Abogado registrado de Patentes

Es un objeto de la presente invención superar sustancialmente, o al menos aminorar, una o más desventajas de los arreglos ya existentes.

En un aspecto de la presente invención, se provee un método para prevenir el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso, caracterizado por que un permiso de acceso electrónico se compra por medio de una interacción con un servidor, en el que durante la compra del permiso de acceso electrónico por un comprador, se especifican una contraseña o datos de autenticación y un dispositivo electrónico móvil, al que se transmite el permiso de acceso electrónico mediante el servidor a través de un enlace para la descarga del permiso de acceso, en el que cuando se activa el enlace para descargar el permiso de acceso comprado transmite un ID único del dispositivo electrónico móvil al servidor, que está asociado con un ID del permiso de acceso comprado, en el que el permiso de acceso electrónico se transfiere únicamente desde el dispositivo electrónico móvil a otro dispositivo electrónico móvil después de la contraseña especificada por el comprador del permiso de acceso o los datos de autenticación especificados por el comprador del permiso de acceso se introducen primero por medio de una interacción con el servidor, en el que tras una transferencia satisfactoria el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil en el servidor y el permiso de acceso almacenado en el primer dispositivo electrónico móvil se marca por el servidor como inválido, caracterizado por que después de transferir el enlace para descargar el permiso de acceso al dispositivo electrónico móvil, la aplicación de monedero que se instala en el dispositivo móvil activa el enlace y para descargar el permiso de acceso adquirido, transmite un ID único del dispositivo electrónico móvil al servidor, en el que en el servidor verifica si un ID del permiso de acceso adquirido está asociado con el ID único transmitido del dispositivo electrónico móvil, en el que si este no es el caso, el ID de permiso de acceso y el ID único del dispositivo electrónico móvil se asocian entre sí y el permiso de acceso electrónico se descarga a continuación, y en el que si el acceso electrónico debe transmitirse desde un dispositivo electrónico móvil a otro dispositivo electrónico móvil, después de la iniciación del proceso por el propietario del dispositivo electrónico móvil con cuyo ID único está asociado el ID de permiso

de acceso, la aplicación de monedero del dispositivo electrónico móvil, con cuyo ID único está asociado el ID de permiso de acceso, transmite el enlace para la descarga del permiso de acceso al otro dispositivo electrónico móvil, en el que la aplicación de monedero del otro dispositivo electrónico móvil activa el enlace y transmite un ID único del otro dispositivo electrónico móvil al servidor, tras lo cual se hace una comprobación en el servidor en cuanto a si existe una asociación entre el ID del permiso de acceso a transferir con un ID único de otro dispositivo electrónico móvil, en el que si este es el caso, se envía un enlace mediante el servidor al otro dispositivo electrónico móvil, cuya ejecución de enlace por la aplicación de monedero conduce a una pantalla de entrada para o bien la contraseña especificada por el comprador del permiso de acceso o bien para los datos de autenticación especificados por el comprador del permiso de acceso, en el que si la contraseña es válida o los datos de autenticación son válidos, el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil en el servidor y el permiso de acceso electrónico se descarga al otro dispositivo electrónico móvil.

En consecuencia, se propone un método para evitar el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso, en el que en dicho método se compra un permiso de acceso electrónico por medio de una interacción con un servidor, en el que durante la compra del permiso de acceso electrónico por un comprador, se especifican una contraseña o datos de autenticación y un dispositivo electrónico móvil, en el que el permiso de acceso electrónico se transmite desde el servidor al dispositivo electrónico móvil por medio de un enlace para la descarga del permiso de acceso.

De acuerdo con la invención, en la implementación del enlace para descargar el permiso de acceso comprado se transmite un ID único del dispositivo electrónico móvil al servidor, que se asocia con un ID del permiso de acceso adquirido, en el que una transmisión del permiso de acceso electrónico desde el primer dispositivo electrónico móvil a otro dispositivo electrónico móvil se produce únicamente después de la entrada de la contraseña especificada por el comprador del permiso de acceso, y/o entrada de los datos de autenticación especificados por el comprador del permiso de acceso por medio de una interacción con el servidor, en el que al

finalizar la transferencia el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil en el servidor, y el servidor marca el permiso de acceso almacenado en el primer dispositivo electrónico móvil como inválido.

En el contexto de un diseño de la invención, después de la transmisión del enlace para descargar el permiso de acceso al dispositivo electrónico móvil, una aplicación de monedero instalada en el dispositivo móvil activa el enlace y para descargar el permiso de acceso adquirido se transmite un ID único del dispositivo electrónico móvil al servidor, en el que se verifica en el servidor si un ID del permiso de acceso adquirido está asociado con el ID único transmitido del dispositivo electrónico móvil, en el que si este no es el caso, el ID de permiso de acceso y el ID único del dispositivo electrónico móvil se asocian entre sí y el permiso de acceso electrónico se descarga a continuación.

En el caso que el permiso de acceso electrónico deba transferirse desde un dispositivo electrónico móvil a otro dispositivo electrónico móvil, la aplicación de monedero del dispositivo electrónico móvil, cuyo ID único está asociado con el ID de permiso de acceso, transmite un enlace para la descarga del permiso de acceso al otro dispositivo electrónico móvil, en el que la aplicación de monedero del otro dispositivo electrónico móvil activa el enlace y transmite un ID único del otro dispositivo electrónico móvil al servidor.

De acuerdo con la invención, se verifica en el servidor si existe una asociación del ID de permiso de acceso con un ID único de otro dispositivo electrónico móvil, en el que si este es el caso, el servidor envía un enlace al otro dispositivo electrónico móvil, cuya activación por la aplicación de monedero conduce a una pantalla de entrada para o bien la contraseña especificada por el comprador del permiso de acceso o bien para los datos de autenticación especificados por el comprador del permiso de acceso, en el que si la contraseña es válida o los datos de autenticación son válidos, el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil en el servidor y el permiso de acceso electrónico se descarga al otro dispositivo electrónico móvil.

A continuación, el permiso de acceso almacenado en el primer dispositivo electrónico móvil se marca por el servidor como inválido, preferentemente por medio de un mensaje por proposición a la aplicación de monedero, en el que se elimina la asociación del ID del primer dispositivo electrónico móvil con el permiso de acceso electrónico y los datos correspondientes se almacenan en el servidor.

El diseño de acuerdo con la invención proporciona un método para evitar el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso, cuya activación garantiza que un permiso de acceso puede transferirse únicamente a otro dispositivo electrónico móvil si este es un dispositivo electrónico móvil de una persona autorizada.

En el contexto de una extensión de la invención, si un permiso de acceso debe transferirse desde un dispositivo electrónico móvil a otro dispositivo electrónico móvil, es decir si el ID de permiso de acceso ya se ha asociado con un ID único de un dispositivo electrónico móvil, entonces sobre la base del número de las asociaciones completadas desde el ID de permiso de acceso a ID únicos de dispositivos electrónicos móviles se verifica con qué frecuencia ya se ha transferido el permiso de acceso, en el que si el número de transferencias completadas ha alcanzado un valor umbral predefinido, no es posible ninguna transferencia adicional.

REIVINDICACIONES

1. Un método para evitar el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso, caracterizado por que un permiso de acceso electrónico se compra por medio de una interacción con un servidor, en el que durante la compra del permiso de acceso electrónico por un comprador, se especifican una contraseña o datos de autenticación y un dispositivo electrónico móvil, al que se transmite el permiso de acceso electrónico mediante el servidor a través de un enlace para la descarga del permiso de acceso, en el que cuando se activa el enlace para descargar el permiso de acceso comprado transmite un ID único del dispositivo electrónico móvil al servidor, que está asociado con un ID del permiso de acceso comprado, en el que el permiso de acceso electrónico se transfiere únicamente desde el dispositivo electrónico móvil a otro dispositivo electrónico móvil después de la contraseña especificada por el comprador del permiso de acceso o los datos de autenticación especificados por el comprador del permiso de acceso se introducen primero por medio de una interacción con el servidor, en el que tras una transferencia satisfactoria el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil en el servidor y el permiso de acceso almacenado en el primer dispositivo electrónico móvil se marca por el servidor como inválido, caracterizado por que después de transferir el enlace para descargar el permiso de acceso al dispositivo electrónico móvil, la aplicación de monedero que se instala en el dispositivo móvil activa el enlace y para descargar el permiso de acceso adquirido, transmite un ID único del dispositivo electrónico móvil al servidor, en el que en el servidor verifica si un ID del permiso de acceso adquirido está asociado con el ID único transmitido del dispositivo electrónico móvil, en el que si este no es el caso, el ID de permiso de acceso y el ID único del dispositivo electrónico móvil se asocian entre sí y el permiso de acceso electrónico se descarga a continuación, y en el que si el acceso electrónico debe transmitirse desde un dispositivo electrónico móvil a otro dispositivo electrónico móvil, después de la iniciación del proceso por el propietario del dispositivo electrónico móvil con cuyo ID único está asociado el ID de permiso de acceso, la aplicación de monedero del dispositivo electrónico móvil, con cuyo ID único está asociado el ID de permiso de acceso, transmite el enlace

para la descarga del permiso de acceso al otro dispositivo electrónico móvil, en el que la aplicación de monedero del otro dispositivo electrónico móvil activa el enlace y transmite un ID único del otro dispositivo electrónico móvil al servidor, tras lo cual se hace una comprobación en el servidor en cuanto a si existe una asociación entre el ID del permiso de acceso a transferir con un ID único de otro dispositivo electrónico móvil, en el que si este es el caso, se envía un enlace mediante el servidor al otro dispositivo electrónico móvil, cuya ejecución de enlace por la aplicación de monedero conduce a una pantalla de entrada para o bien la contraseña especificada por el comprador del permiso de acceso o bien para los datos de autenticación especificados por el comprador del permiso de acceso, en el que si la contraseña es válida o los datos de autenticación son válidos, el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil (4) en el servidor y el permiso de acceso electrónico se descarga al otro dispositivo electrónico móvil.

2. Un método para evitar el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero, y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso, de acuerdo con la reivindicación 1, caracterizado por que si un permiso de acceso debe transferirse desde un dispositivo electrónico móvil a otro dispositivo electrónico móvil, es decir si el ID de permiso de acceso ya se ha asociado con un ID único de un dispositivo electrónico móvil, entonces sobre la base del número de las asociaciones completadas entre el ID de permiso de acceso e ID únicos de dispositivos electrónicos móviles, se verifica con qué frecuencia ya se ha transferido el permiso de acceso, en el que si el número de transferencias completadas ha alcanzado un valor umbral predefinido, no es posible ninguna transferencia adicional.

SKIDATA AG

Abogados de patentes para el solicitante / persona nominada

SPRUSON & FERGUSON

Es un objeto de la presente invención superar sustancialmente, o al menos aminorar, una o más desventajas de los arreglos ya existentes.

En un aspecto de la presente invención, se provee un método para prevenir el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso, caracterizado por que un permiso de acceso electrónico se compra por medio de una interacción con un servidor, en el que durante la compra del permiso de acceso electrónico por un comprador, se especifican una contraseña o datos de autenticación y un dispositivo electrónico móvil, al que se transmite el permiso de acceso electrónico mediante el servidor a través de un enlace para la descarga del permiso de acceso, en el que cuando se activa el enlace para descargar el permiso de acceso comprado transmite un ID único del dispositivo electrónico móvil al servidor, que está asociado con un ID del permiso de acceso comprado, en el que el permiso de acceso electrónico se transfiere únicamente desde el dispositivo electrónico móvil a otro dispositivo electrónico móvil después de la contraseña especificada por el comprador del permiso de acceso o los datos de autenticación especificados por el comprador del permiso de acceso se introducen primero por medio de una interacción con el servidor, en el que tras una transferencia satisfactoria el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil en el servidor y el permiso de acceso almacenado en el primer dispositivo electrónico móvil se marca por el servidor como inválido, caracterizado por que después de transferir el enlace para descargar el permiso de acceso al dispositivo electrónico móvil, la aplicación de monedero que se instala en el dispositivo móvil activa el enlace y para descargar el permiso de acceso adquirido, transmite un ID único del dispositivo electrónico móvil al servidor, en el que en el servidor verifica si un ID del permiso de acceso adquirido está asociado con el ID único transmitido del dispositivo electrónico móvil, en el que si este no es el caso, el ID de permiso de acceso y el ID único del dispositivo electrónico móvil se asocian entre sí y el permiso de acceso electrónico se descarga a continuación, y en el que si el acceso electrónico debe transmitirse desde un dispositivo electrónico móvil a otro dispositivo electrónico móvil, después de la iniciación del proceso por el propietario del dispositivo electrónico móvil con cuyo ID único está asociado el ID de permiso

de acceso, la aplicación de monedero del dispositivo electrónico móvil, con cuyo ID único está asociado el ID de permiso de acceso, transmite el enlace para la descarga del permiso de acceso al otro dispositivo electrónico móvil, en el que la aplicación de monedero del otro dispositivo electrónico móvil activa el enlace y transmite un ID único del otro dispositivo electrónico móvil al servidor, tras lo cual se hace una comprobación en el servidor en cuanto a si existe una asociación entre el ID del permiso de acceso a transferir con un ID único de otro dispositivo electrónico móvil, en el que si este es el caso, se envía un enlace mediante el servidor al otro dispositivo electrónico móvil, cuya ejecución de enlace por la aplicación de monedero conduce a una pantalla de entrada para o bien la contraseña especificada por el comprador del permiso de acceso o bien para los datos de autenticación especificados por el comprador del permiso de acceso, en el que si la contraseña es válida o los datos de autenticación son válidos, el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil en el servidor y el permiso de acceso electrónico se descarga al otro dispositivo electrónico móvil.

En consecuencia, se propone un método para evitar el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso, en el que en dicho método se compra un permiso de acceso electrónico por medio de una interacción con un servidor, en el que durante la compra del permiso de acceso electrónico por un comprador, se especifican una contraseña o datos de autenticación y un dispositivo electrónico móvil, en el que el permiso de acceso electrónico se transmite desde el servidor al dispositivo electrónico móvil por medio de un enlace para la descarga del permiso de acceso.

De acuerdo con la invención presente divulgación, en la implementación del enlace para descargar el permiso de acceso comprado se transmite un ID único del dispositivo electrónico móvil al servidor, que se asocia con un ID del permiso de acceso adquirido, en el que una transmisión del permiso de acceso electrónico desde el primer dispositivo electrónico móvil a otro dispositivo electrónico móvil se produce únicamente después de la entrada de la contraseña especificada por el

comprador del permiso de acceso, y/o entrada de los datos de autenticación especificados por el comprador del permiso de acceso por medio de una interacción con el servidor, en el que al finalizar la transferencia el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil en el servidor, y el servidor marca el permiso de acceso almacenado en el primer dispositivo electrónico móvil como inválido.

En el contexto de un diseño de la ~~invención~~presente divulgación, después de la transmisión del enlace para descargar el permiso de acceso al dispositivo electrónico móvil, una aplicación de monedero instalada en el dispositivo móvil activa el enlace y para descargar el permiso de acceso adquirido se transmite un ID único del dispositivo electrónico móvil al servidor, en el que se verifica en el servidor si un ID del permiso de acceso adquirido está asociado con el ID único transmitido del dispositivo electrónico móvil, en el que si este no es el caso, el ID de permiso de acceso y el ID único del dispositivo electrónico móvil se asocian entre sí y el permiso de acceso electrónico se descarga a continuación.

En el caso que el permiso de acceso electrónico deba transferirse desde un dispositivo electrónico móvil a otro dispositivo electrónico móvil, la aplicación de monedero del dispositivo electrónico móvil, cuyo ID único está asociado con el ID de permiso de acceso, transmite un enlace para la descarga del permiso de acceso al otro dispositivo electrónico móvil, en el que la aplicación de monedero del otro dispositivo electrónico móvil activa el enlace y transmite un ID único del otro dispositivo electrónico móvil al servidor.

De acuerdo con la ~~invención~~presente divulgación, se verifica en el servidor si existe una asociación del ID de permiso de acceso con un ID único de otro dispositivo electrónico móvil, en el que si este es el caso, el servidor envía un enlace al otro dispositivo electrónico móvil, cuya activación por la aplicación de monedero conduce a una pantalla de entrada para o bien la contraseña especificada por el comprador del permiso de acceso o bien para los datos de autenticación especificados por el comprador del permiso de acceso, en el que si la contraseña es válida o los datos de autenticación son válidos, el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil en el servidor y el permiso de acceso electrónico se descarga al otro dispositivo electrónico móvil.

A continuación, el permiso de acceso almacenado en el primer dispositivo electrónico móvil se marca por el servidor como inválido, preferentemente por medio

de un mensaje por proposición a la aplicación de monedero, en el que se elimina la asociación del ID del primer dispositivo electrónico móvil con el permiso de acceso electrónico y los datos correspondientes se almacenan en el servidor.

El diseño de acuerdo con la ~~invención~~ presente divulgación proporciona un método para evitar el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso, cuya activación garantiza que un permiso de acceso puede transferirse únicamente a otro dispositivo electrónico móvil si este es un dispositivo electrónico móvil de una persona autorizada.

En el contexto de una extensión de la ~~invención~~ presente invención, si un permiso de acceso debe transferirse desde un dispositivo electrónico móvil a otro dispositivo electrónico móvil, es decir si el ID de permiso de acceso ya se ha asociado con un ID único de un dispositivo electrónico móvil, entonces sobre la base del número de las asociaciones completadas desde el ID de permiso de acceso a ID únicos de dispositivos electrónicos móviles se verifica con qué frecuencia ya se ha transferido el permiso de acceso, en el que si el número de transferencias completadas ha alcanzado un valor umbral predefinido, no es posible ninguna transferencia adicional.

REIVINDICACIONES

1. Un método para evitar el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso, caracterizado por que un permiso de acceso electrónico se compra por medio de una interacción con un servidor, en el que durante se especifican la compra del permiso de acceso electrónico por un comprador, se especifican una contraseña o datos de autenticación y un dispositivo electrónico móvil, al que se transmite el permiso de acceso electrónico mediante el servidor a través de un enlace para la descarga del permiso de acceso, en el que cuando se activa el enlace para descargar el permiso de acceso comprado se transmite un ID único del dispositivo electrónico móvil al servidor, que está asociado con un ID del permiso de acceso comprado, en el que el permiso de acceso electrónico se transfiere únicamente desde el dispositivo electrónico móvil a otro dispositivo electrónico móvil después de la contraseña especificada por el comprador del permiso de acceso o los datos de autenticación especificados por el comprador del permiso de acceso se introducen primero por medio de una interacción con el servidor, en el que tras una transferencia satisfactoria el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil en el servidor y el permiso de acceso almacenado en el primer dispositivo electrónico móvil se marca por el servidor como inválido.

~~2. Un método para evitar el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso, de acuerdo con la reivindicación 1,~~ caracterizado por que después de transferir el enlace para descargar el permiso de acceso al dispositivo electrónico móvil, la ~~una~~ aplicación de monedero que se instala en el dispositivo móvil activa el enlace y para descargar el permiso de acceso adquirido, transmite un ID único del dispositivo electrónico móvil al servidor, en el que en el servidor ~~se~~ verifica si un ID del permiso de acceso adquirido está asociado con el ID único transmitido del dispositivo electrónico móvil, en el que si este no es el caso, el ID de permiso de

acceso y el ID único del dispositivo electrónico móvil se asocian entre sí y el permiso de acceso electrónico se descarga a continuación, y en el que si el ~~un~~ acceso electrónico debe transmitirse desde un dispositivo electrónico móvil a otro dispositivo electrónico móvil, después de la iniciación del proceso por el propietario del dispositivo electrónico móvil con cuyo ID único está asociado el ID de permiso de acceso, la aplicación de monedero del dispositivo electrónico móvil, con cuyo ID único está asociado el ID de permiso de acceso, transmite el ~~un~~ enlace para la descarga del permiso de acceso al otro dispositivo electrónico móvil, en el que la aplicación de monedero del otro dispositivo electrónico móvil activa el enlace y transmite un ID único del otro dispositivo electrónico móvil al servidor, tras lo cual se hace una comprobación en el servidor en cuanto a si existe una asociación entre el ID del permiso de acceso a transferir con un ID único de otro dispositivo electrónico móvil, en el que si este es el caso, se envía un enlace mediante el servidor al otro dispositivo electrónico móvil, cuya ejecución de enlace por la aplicación de monedero conduce a una pantalla de entrada para o bien la contraseña especificada por el comprador del permiso de acceso o bien para los datos de autenticación especificados por el comprador del permiso de acceso, en el que si la contraseña es válida o los datos de autenticación son válidos, el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil en el servidor y el permiso de acceso electrónico se descarga al otro dispositivo electrónico móvil.

23. Un método para evitar el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero, y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso, de acuerdo con la reivindicación 1 ~~o la reivindicación 2~~, caracterizado por que si un permiso de acceso debe transferirse desde un dispositivo electrónico móvil a otro dispositivo electrónico móvil, es decir si el ID de permiso de acceso ya se ha asociado con un ID único de un dispositivo electrónico móvil, entonces sobre la base del número de las asociaciones completadas entre el ID de permiso de acceso e ID únicos de dispositivos electrónicos móviles, se verifica con qué frecuencia ya se ha transferido el permiso de acceso, en el que si el número de transferencias completadas ha alcanzado un valor umbral predefinido, no es posible ninguna transferencia adicional.

SKIDATA AG

Abogados de patentes para el solicitante / persona nominada

SPRUSON & FERGUSON



Australian Government
IP Australia

17 July 2019



Delivering a world leading IP system

Phone: 1300 651 010
International: +61 2 6283 2999

www.ipaustralia.gov.au

ABN: 38 113 072 755

Notice of acceptance for patent application

Spruson & Ferguson

GPO Box 3898
Sydney NSW 2001
Australia

Your reference	P309471
Application number	2018204447
Applicant name	SKIDATA AG

Dear Spruson & Ferguson,

This patent application was accepted on 12 July 2019. The accepted specification incorporates the following amendments:

S104 amendments up to and including item number: 2

The total number of claims at acceptance has been reported as: 2

Notice of the acceptance will appear in the Australian Official Journal of Patents on 1 August 2019.

Please review the acceptance details attached to this letter to ensure that they are correct. If you wish to amend any details prior to the grant please do so within 3 months of the advertisement of acceptance.

An Invitation to Pay (ITP) the acceptance fee will be issued to you. This fee will include an additional component if the number of claims exceeds 20.

Details of this patent application can be viewed on AusPat, our Australian patent search database.

Yours sincerely,

IP Australia

Acceptance summary

Standard patent details

Patent number:	2018204447
Title:	Method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission
Your reference:	P309471
Number of claims at acceptance:	2

Applicant and inventor details

Applicant name(s) and address(es) (as it will appear on certificate/s) :

SKIDATA AG of Untersbergstr. 40 5083 Grödig/Salzburg Austria

Inventor name(s): MALMBORG, Anders
JAYAPRAKASH, Vijayanthi Mala

Agent details

Agent Name Spruson & Ferguson

Address for correspondence: GPO Box 3898
Sydney NSW 2001
Australia

Address for legal service: GPO Box 3898
Sydney NSW 2001
Australia

Prior art details

Prior art documents:
US 20160350547 A1

Priority details

Number	Date	Country
17185122.3	7 August 2017	EP

International classification

H04L 9/32 (2006.01)

Relevant dates

Acceptance date:	12 July 2019
Acceptance to be advertised:	1 August 2019
Complete filing date:	20 June 2018
OPI date:	21 February 2019
Continuation fee due date:	20 June 2022
Date of patent:	20 June 2018
Expiry date:	20 June 2038
National phase entry date:	Not Applicable

17 de Julio de 2019

AVISO DE ACEPTACIÓN DE LA SOLICITUD DE PATENTE

Spruson & Ferguson
GPO Box 3898
Sydney NSW 2001
Australia

Su referencia: P309471
Número de la solicitud: 2018204447
Nombre del solicitante: SKIDATA AG

Estimados Spruson & Ferguson,

Esta solicitud de patente fue aceptada el 12 de julio de 2019. La descripción aceptada incorpora las siguientes modificaciones:

Modificaciones S104 hasta e incluyendo el número de ítem: 2

El total de números de reivindicaciones aceptadas como habían sido informadas: 2

La notificación de Aceptación aparecerá en la Revista de Patentes Oficial Australiana el 0 de agosto de 2019.

Por favor revise los detalles de la aceptación adjuntas a esta carta para asegurar que están correctos. Si usted desea modificar algún detalle antes de la concesión,

por favor realizarlo dentro de los 3 meses siguientes a esta notificación de aceptación.

Una invitación a pagar(ITP) la tasa de aceptación será notificada a usted. Esta tasa incluirá un componente adicional si el número de reivindicaciones excede las 20.

Los detalles de esa solicitud de patente se pueden ver en AusPat, nuestra base de datos de patentes australiana.

Cordialmente,

IP Australia

RESUMEN DE ACEPTACIÓN

Detalles estándares de la patente

Número de la patente: 2018204447

Título: Método para prevenir el uso indebido de permisos de acceso electrónico que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso.

Su referencia: P309471

Número de reivindicaciones aceptadas: 2

Detalles del solicitante y del inventor

Nombre(s) del Solicitante(s) y dirección (es) *(como aparecerá en el certificado)*:

SKIDATA AG of Untersbergstr. 40 5083 Grödig/Salzburg Austria

Nombre(s) del Inventor(es): MALMBORG, Anders
JAYAPRAKASH, Vijayanthi Mala

Detalles del agente

Nombre del Agente: Spruson & Ferguson

Dirección para correspondencia: GPO Box 3898

Sydney NSW 2001
Australia

Detalles del arte previo

Número	Fecha	País
17185122.3	7 Agosto 2017	EP

Clasificación Internacional

H04L 9/32 (2006.01)

Su referencia: P309471

Número de solicitud: 2018204447

Datos relevantes

Fecha de aceptación:	12 de Julio de 2019
Aceptación para ser anunciada:	1 de Agosto de 2019
Fecha de presentación completa:	20 de Junio de 2018
Fecha OPI:	21 de Febrero de 2019
Fecha de vencimiento de la tasa de continuación:	20 de Junio de 2022
Fecha de la patente:	20 de Junio 2018
Fecha de expiración:	20 de Junio de 2038
Fecha de entrada en fase nacional:	No aplica



Australian Government
IP Australia

14 November 2019



Delivering a world leading IP system

Phone: 1300 651 010
International: +61 2 6283 2999

www.ipaustralia.gov.au

ABN: 38 113 072 755

Notice of grant for patent

Spruson & Ferguson

GPO Box 3898
Sydney NSW 2001
Australia

Your reference	P309471
Patent number	2018204447
Patentee name	SKIDATA AG

Dear Spruson & Ferguson,

A patent has been granted in respect of this application. The grant date is 14 November 2019 and the Certificate of Grant is enclosed.

The term of this standard patent is 20 years from the date of the patent (20 June 2018).

The first renewal fee payment, being for the 4th year anniversary is due on 20 June 2022.

To maintain this patent, you have to pay annual renewal fees. The fee can be paid up to 6 months after the due date provided it is accompanied by the required late payment fee. Please note that this patent will cease if renewal fees are not paid.

Details of this patent can be viewed on [AusPat](#), our Australian patent search database.

Yours sincerely,

IP Australia

14 de Noviembre de 2019

AVISO DE CONCESIÓN DE LA SOLICITUD DE PATENTE

Spruson & Ferguson
GPO Box 3898
Sydney NSW 2001
Australia

Su referencia: P309471
Número de la solicitud: 2018204447
Nombre del solicitante: SKIDATA AG

Estimados Spruson & Ferguson,

Una patente ha sido concedida con respecto a esta solicitud. La fecha de concesión es 14 de noviembre de 2019 y el certificado de concesión se adjunta.

El término de esta patente estándar es 20 años a partir de la fecha de la patente (20 de junio 2018).

El primer pago de la tasa de renovación, correspondiente al cuarto año es el 20 de junio de 2022.

Para mantener esta patente, usted debe pagar tasas de renovación anuales. La tasa puede ser pagada hasta 6 meses después de la fecha de vencimiento siempre que

esté acompañada de la tarifa de pago atrasado requerida. Por favor note que esta patente cesará si las tasas de renovación no son pagadas.

Los detalles de esa solicitud de patente se pueden ver en AusPat, nuestra base de datos de patentes australianas.

Cordialmente,

IP Australia



Australian Government

IP Australia

CERTIFICATE OF GRANT STANDARD PATENT

Patent number: 2018204447

The Commissioner of Patents has granted the above patent on 14 November 2019, and certifies that the below particulars have been registered in the Register of Patents.

Name and address of patentee(s):

SKIDATA AG of Untersbergstr. 40 5083 Grödig/Salzburg Austria

Title of invention:

Method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission

Name of inventor(s):

MALMBORG, Anders and JAYAPRAKASH, Vaijayanthi Mala

Term of Patent:

Twenty years from 20 June 2018

Priority details:

Number
17185122.3

Date
7 August 2017

Filed with
EP



Dated this 14th day of November 2019

Commissioner of Patents

PATENTS ACT 1990

The Australian Patents Register is the official record and should be referred to for the full details pertaining to this IP Right.

CERTIFICADO DE CONCESIÓN DE UNA PATENTE ESTÁNDAR

Número de patente: 2018224447

El Comisionado de Patentes ha otorgado la anterior patente el 14 de noviembre de 2019, y certifica que los siguientes datos han sido registrados en el Registro de Patentes.

Nombre y dirección del Titular(es):

SKIDATA AG of Untersbergstr. 40 5083 Grödig/Salzburg Austria

Título de la invención:

Método para prevenir el uso indebido de permisos de acceso electrónico que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso

Nombre del inventor(es):

MALMBORG, Anders y JAYAPRAKASH, Vaijayanthi Mala

Término de la patente:

20 años desde el 20 de junio de 2018

Detalles de la prioridad:

Número
17185122.3

Fecha
7 de agosto de 2017

Presentado con
EP

Fechado este día 14 de noviembre de 2019

Comisionado de Patentes



Australian Government

IP Australia

CERTIFICATE OF GRANT STANDARD PATENT

Patent number: 2018204447

The Commissioner of Patents has granted the above patent on 14 November 2019, and certifies that the below particulars have been registered in the Register of Patents.

Name and address of patentee(s):

SKIDATA AG of Untersbergstr. 40 5083 Grödig/Salzburg Austria

Title of invention:

Method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission

Name of inventor(s):

MALMBORG, Anders and JAYAPRAKASH, Vaijayanthi Mala

Term of Patent:

Twenty years from 20 June 2018

Priority details:

Number
17185122.3

Date
7 August 2017

Filed with
EP



Dated this 14th day of November 2019

Commissioner of Patents

PATENTS ACT 1990

The Australian Patents Register is the official record and should be referred to for the full details pertaining to this IP Right.

(12) STANDARD PATENT
(19) AUSTRALIAN PATENT OFFICE

(11) Application No. **AU 2018204447 B2**

(54) Title
Method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission

(51) International Patent Classification(s)
H04L 9/32 (2006.01)

(21) Application No: **2018204447** (22) Date of Filing: **2018.06.20**

(30) Priority Data

(31) Number	(32) Date	(33) Country
17185122.3	2017.08.07	EP

(43) Publication Date: **2019.02.21**

(43) Publication Journal Date: **2019.02.21**

(44) Accepted Journal Date: **2019.08.01**

(71) Applicant(s)
SKIDATA AG

(72) Inventor(s)
MALMBORG, Anders; JAYAPRAKASH, Vijayanthi Mala

(74) Agent / Attorney
Spruson & Ferguson, GPO Box 3898, Sydney, NSW, 2001, AU

(56) Related Art
US 20160350547 A1

METHOD FOR PREVENTING THE MISUSE OF ELECTRONIC ACCESS PERMISSIONS, WHICH CAN BE MANAGED IN MOBILE ELECTRONIC DEVICES USING A WALLET APPLICATION AND WHICH ARE TRANSMITTED TO THE MOBILE ELECTRONIC DEVICES BY A SERVER, IN EACH CASE USING A LINK FOR DOWNLOAD

ABSTRACT

In the context of the method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission, an electronic access permission is purchased by means of an interaction with a server (2), wherein during the purchase of the electronic access permission by the purchaser (1) a password or authentication data and a mobile electronic device, to which the electronic access permission is transmitted by the server (1) via a link for downloading the access permission, are specified, wherein when activating the link for downloading the purchased access permission a unique ID of the mobile electronic device (3), which is associated with an ID of the purchased access permission, is transmitted to the server (2), wherein the electronic access permission is only transferred from the mobile electronic device (3) to another mobile electronic device (4) after the password specified by the purchaser of the access permission or the authentication data specified by the purchaser of the access permission is first entered by means of an interaction with the server (2), wherein upon successful transfer the access permission ID is associated with the ID of the other mobile electronic device (4) in the server (2) and the access permission stored on the first mobile electronic device (3) is marked by the server (2) as invalid.

METHOD FOR PREVENTING THE MISUSE OF ELECTRONIC ACCESS PERMISSIONS, WHICH CAN BE MANAGED IN MOBILE ELECTRONIC DEVICES USING A WALLET APPLICATION AND WHICH ARE TRANSMITTED TO THE MOBILE ELECTRONIC DEVICES BY A SERVER, IN EACH CASE USING A LINK FOR DOWNLOAD

Field

[0001] The present invention relates to a method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission.

Background

[0002] From the prior art it is known to store and manage electronic access permissions, for example by means of so-called wallet applications on mobile electronic devices, such as smartphones and tablets. In this case it is possible, for example, by means of the IOS "Wallet" app, to forward electronic access permissions to other mobile electronic devices. This increases the convenience for the user, in the case where an authorized person would like to use a new mobile electronic device; on the other hand, this technique can allow personal electronic access permissions to be "borrowed", thereby allowing a misuse of these access permissions.

Summary of Invention

[0003] A need of the present invention is to specify a method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission, the use of which excludes the possibility of misuse of the access permission while at the same time ensuring the facility for transmitting the electronic access permission to another mobile electronic device of an authorized person.

[0004] It is an object of the present invention to substantially overcome, or at least ameliorate, one or more disadvantages of existing arrangements.

[0004a] In one aspect of the present invention, there is provided a method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission, wherein an electronic access permission is purchased by means of an interaction with the server, wherein during the purchase of the electronic access permission by a purchaser, a password or authentication data and a mobile electronic device, to which the electronic access permission is transmitted by the server via the link for downloading the access permission, are specified, wherein when activating the link for downloading the purchased access permission a unique ID of the mobile electronic device is transmitted to the server, which is associated with an ID of the purchased access permission, wherein the electronic access permission is only transferred from the mobile electronic device to another mobile electronic device after the password specified by the purchaser of the access permission or the authentication data specified by the purchaser of the access permission is first entered by means of an interaction with the server, wherein upon successful transfer the access permission ID is associated with the ID of the other mobile electronic device in the server and the access permission stored on the first mobile electronic device is marked by the server as invalid, wherein after transferring the link for downloading the access permission to the mobile electronic device, the wallet application which is installed on the mobile device activates the link and in order to download the acquired access permission, transmits a unique ID of the mobile electronic device to the server, wherein in the server it is verified whether an ID of the acquired access permission is associated with the transmitted unique ID of the mobile electronic device, wherein if this is not the case, the access permission ID and the unique ID of the mobile electronic device are associated with each other and the electronic access permission is then downloaded, and wherein if the electronic access is to be transmitted from one mobile electronic device to another mobile electronic device, after initiation of the process by the owner of the mobile electronic device with whose unique ID the access permission ID is associated, the wallet application of the mobile electronic device, with whose unique ID the access permission ID is associated, transmits the link for downloading the access permission to the other mobile electronic device, wherein the wallet application of the other mobile electronic device activates the link and transmits a unique ID of the other mobile

electronic device to the server, whereupon a check is made in the server as to whether an association exists between the ID of the access permission to be transferred with a unique ID of another mobile electronic device, wherein if this is the case, a link is sent by the server to the other mobile electronic device, the execution of which link by the wallet application leads to an input screen for either the password specified by the purchaser of the access permission or for the authentication data specified by the purchaser of the access permission, wherein if the password is valid or the authentication data are valid, the access permission ID is associated with the ID of the other mobile electronic device in the server and the electronic access permission is downloaded to the other mobile electronic device.

[0005] Consequently, a method is proposed for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission, wherein in said method an electronic access permission is purchased by means of an interaction with a server, wherein during the purchase of the electronic access permission by a buyer, a password or authentication data and a mobile electronic device are specified, wherein the electronic access permission is transmitted from the server to the mobile electronic device by means of a link for downloading the access permission.

[0006] According to the present disclosure, in implementing the link for downloading the purchased access permission a unique ID of the mobile electronic device is transmitted to the server, which is associated with an ID of the acquired access permission, wherein a transmission of the electronic access permission from the first mobile electronic device to another mobile electronic device takes place only after the input of the password specified by the purchaser of the access permission, and/or input of the authentication data specified by the buyer of the access permission by means of an interaction with the server, wherein on completion of the transfer the access permission ID is associated with the ID of the other mobile electronic device in the server, and the server marks the access permission stored on the first mobile electronic device as invalid.

[0007] In the context of one design of the present disclosure, after the transmission of the link for downloading the access permission to the mobile electronic device, a wallet application installed on the mobile device activates the link and in order to download the acquired access permission a unique ID of the mobile electronic device is transmitted to the server, wherein it is verified in the server whether an ID of the acquired access permission is

associated with the transmitted unique ID of the mobile electronic device, wherein if this is not the case, the access permission ID and the unique ID of the mobile electronic device are associated with each other and the electronic access permission is then downloaded.

[0008] In the event that the electronic access permission is to be transferred from one mobile electronic device to another mobile electronic device, the wallet application of the mobile electronic device, whose unique ID is associated with the access permission ID, transmits a link for downloading the access permission to the other mobile electronic device, wherein the wallet application of the other mobile electronic device activates the link and transmits a unique ID of the other mobile electronic device to the server.

[0009] According to the present disclosure, it is verified in the server whether an association of the access permission ID with a unique ID of another mobile electronic device exists, wherein if this is the case, the server sends a link to the other mobile electronic device, the activation of which by the wallet application leads to an input screen for either the password specified by the purchaser of the access permission or for the authentication data specified by the purchaser of the access permission, wherein if the password is valid or the authentication data are valid, the access permission ID is associated with the ID of the other mobile electronic device in the server and the electronic access permission is downloaded to the other mobile electronic device.

[0010] Then, the access permission stored on the first mobile electronic device is marked by the server as invalid, preferably by means of a push message to the wallet application, wherein the association of the ID of the first mobile electronic device with the electronic access permission is deleted and the corresponding data are stored on the server.

[0011] The design according to the present disclosure provides a method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission, the activation of which ensures that an access permission can only be transferred to another mobile electronic device if this is a mobile electronic device of an authorized person.

[0012] In the context of an extension of the present disclosure, if an access permission is to be transferred from one mobile electronic device to another mobile electronic device, i.e. if the access permission ID has already been associated with a unique ID of a mobile electronic device, then on the basis of the number of the completed associations from the access permission ID to unique IDs of mobile electronic devices it is verified how often the access permission has already been transferred, wherein if the number of completed transfers has reached a predefined threshold value, no further transfer is possible.

Brief Description of the Drawings

[0013] In the following, an example of the invention is described in greater detail on the basis of the attached figure, which shows a sequence diagram to illustrate the main features of the method according to the invention.

Detailed Description

[0014] Referring to the attached figure, at the start of the method an electronic access permission is purchased by a buyer 1 by means of an interaction with a server 2 (step 1), wherein when the electronic access permission is purchased by the buyer a password or authentication data is specified. Then (step 2), the electronic access permission is transferred from the server 1 to a mobile electronic device 3 specified during the purchase of the access permission, by means of a link for downloading the access permission, wherein a wallet application installed on the mobile device 3 activates the link and in order to download the acquired access permission, a unique ID of the mobile electronic device is transmitted to the server 2 (step 3), wherein it is verified in the server 2 whether an ID of the acquired access permission is associated with the transmitted unique ID of the mobile electronic device 3, wherein if this is not the case, the access permission ID and the unique ID of the mobile electronic device 3 are associated with each other (step 4) and the electronic access permission is then downloaded.

[0015] If the electronic access permission is to be transferred from one mobile electronic device 3 to another mobile electronic device 4, i.e., if the access permission ID has already been associated with a unique ID of a mobile electronic device 3, then after initiation of the process by the owner of the mobile electronic device 3 (step 5) with whose unique ID the access permission ID is associated, the wallet application of the mobile electronic device 3, with whose unique ID the access permission ID is associated, transmits a link for downloading the access permission to the other mobile electronic device 4 (step 6), wherein the wallet application of the other mobile electronic device 4 activates the link (step 7) and transmits a unique ID of the other mobile electronic device 4 to the server 2.

[0016] It is then verified in the server 2 whether an association of the access permission ID with a unique ID of another mobile electronic device exists, wherein if this is the case, the server 2 sends a link to the other mobile electronic device 4 (step 8), the activation of which by the wallet

application leads to an input screen for entering either the password specified by the purchaser of the access permission or for the authentication data specified by the purchaser of the access permission (step 9), wherein if the password is valid or the authentication data is valid, the access permission ID is associated with the ID of the other mobile electronic device 4 in the server 2 and the electronic access permission is downloaded to the other mobile electronic device 4.

[0017] The access permission stored on the first mobile electronic device 3 is then marked by the server 2 as invalid (step 11), preferably by means of a push message to the wallet application.

CLAIMS

1. A method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission, wherein an electronic access permission is purchased by means of an interaction with the server, wherein during the purchase of the electronic access permission by a purchaser, a password or authentication data and a mobile electronic device, to which the electronic access permission is transmitted by the server via the link for downloading the access permission, are specified, wherein when activating the link for downloading the purchased access permission a unique ID of the mobile electronic device is transmitted to the server, which is associated with an ID of the purchased access permission, wherein the electronic access permission is only transferred from the mobile electronic device to another mobile electronic device after the password specified by the purchaser of the access permission or the authentication data specified by the purchaser of the access permission is first entered by means of an interaction with the server, wherein upon successful transfer the access permission ID is associated with the ID of the other mobile electronic device in the server and the access permission stored on the first mobile electronic device is marked by the server as invalid, wherein after transferring the link for downloading the access permission to the mobile electronic device, the wallet application which is installed on the mobile device activates the link and in order to download the acquired access permission, transmits a unique ID of the mobile electronic device to the server, wherein in the server it is verified whether an ID of the acquired access permission is associated with the transmitted unique ID of the mobile electronic device, wherein if this is not the case, the access permission ID and the unique ID of the mobile electronic device are associated with each other and the electronic access permission is then downloaded, and wherein if the electronic access is to be transmitted from one mobile electronic device to another mobile electronic device, after initiation of the process by the owner of the mobile electronic device with whose unique ID the access permission ID is associated, the wallet application of the mobile electronic device, with whose unique ID the access permission ID is associated, transmits the link for downloading the access permission to the other mobile electronic device, wherein the wallet application of the other mobile electronic device activates the link and transmits a unique ID of the other mobile electronic device to the server, whereupon a check is made in the server as to whether an association exists between the ID of the access permission to be transferred with a unique ID of

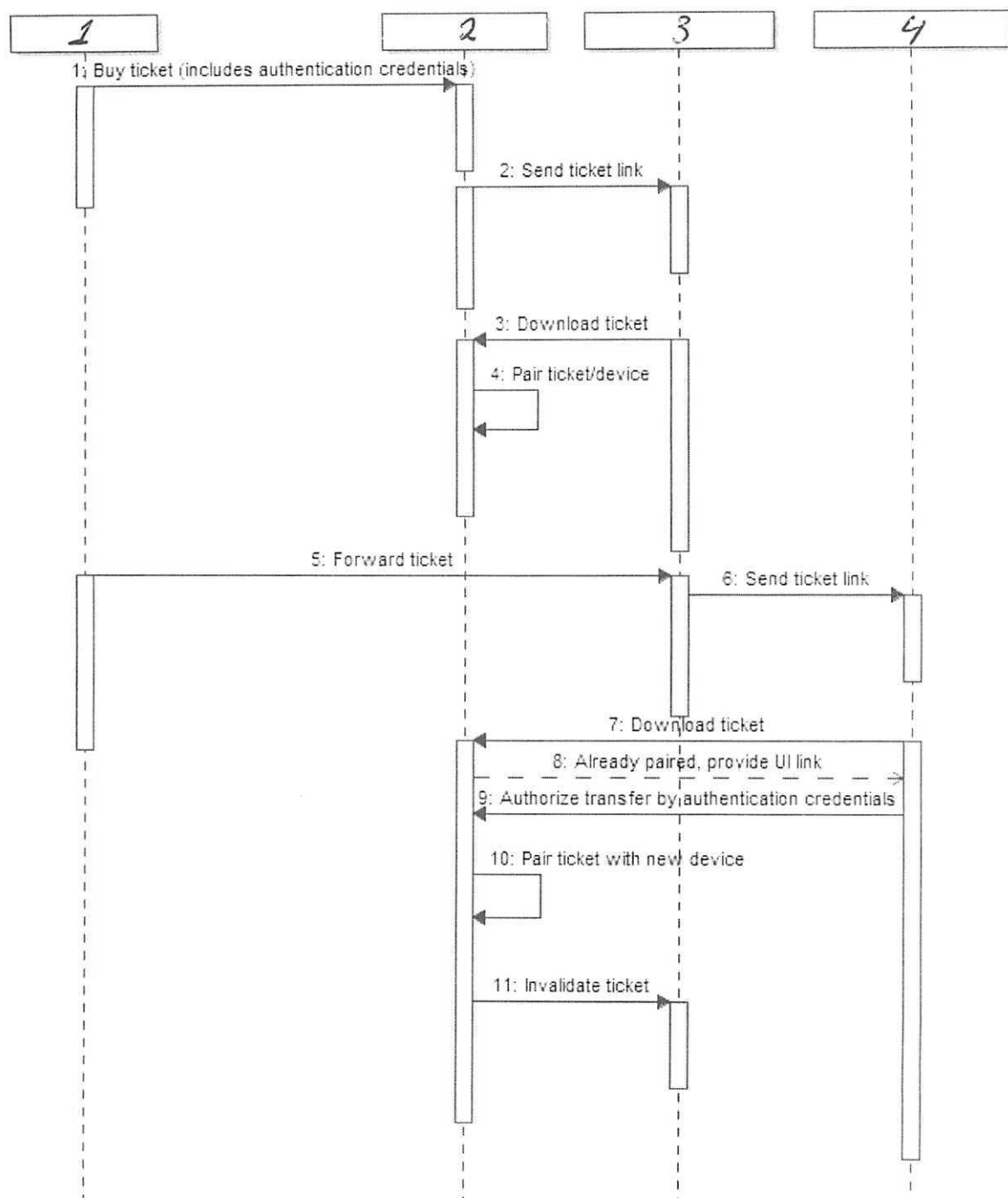
another mobile electronic device, wherein if this is the case, a link is sent by the server to the other mobile electronic device, the execution of which link by the wallet application leads to an input screen for either the password specified by the purchaser of the access permission or for the authentication data specified by the purchaser of the access permission, wherein if the password is valid or the authentication data are valid, the access permission ID is associated with the ID of the other mobile electronic device in the server and the electronic access permission is downloaded to the other mobile electronic device.

2. A method for preventing the misuse of electronic access permissions, which can be managed in mobile electronic devices using a wallet application, and which are transmitted to the mobile electronic devices by a server, in each case using a link for downloading the access permission, according to Claim 1, wherein if an access permission is to be transferred from one mobile electronic device to another mobile electronic device, i.e. if the access permission ID has already been associated with a unique ID of a mobile electronic device, then on the basis of the number of the completed associations between the access permission ID and unique IDs of mobile electronic devices, it is verified how often the access permission has already been transferred, wherein if the number of completed transfers has reached a predefined threshold value, no further transfer is possible.

SKIDATA AG

Patent Attorneys for the Applicant/Nominated Person

SPRUSON & FERGUSON



CERTIFICADO DE CONCESIÓN DE UNA PATENTE ESTÁNDAR

Número de patente: 2018224447

El Comisionado de Patentes ha otorgado la anterior patente el 14 de noviembre de 2019, y certifica que los siguientes datos han sido registrados en el Registro de Patentes.

Nombre y dirección del Titular(es):

SKIDATA AG of Untersbergstr. 40 5083 Grödig/Salzburg Austria

Título de la invención:

Método para prevenir el uso indebido de permisos de acceso electrónico que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso

Nombre del inventor(es):

MALMBORG, Anders y JAYAPRAKASH, Vijayanthi Mala

Término de la patente:

20 años desde el 20 de junio de 2018

Detalles de la prioridad:

Número

Fecha

Presentado con

17185122.3

7 de agosto de 2017

EP

Fechado este día 14 de noviembre de 2019

Comisionado de Patentes

(12) PATENTE ESTÁNDAR

(11) Solicitud No. AU 2018204447 B2

(19) OFICINA DE PATENTES AUSTRALIANA

(54) Título

Método para prevenir el uso indebido de permisos de acceso electrónico que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso

(51) Clasificación (es) Internacional de Patentes

H04L 9/32 (2006.01)

(21) Solicitud No. 2018204447

(22) Fecha de presentación: 2018.06.20

(30) Datos de prioridad

**(31) Número
17185122.3**

**(32) Fecha
2017.08.07**

**(33) País
EP**

(43) Fecha de publicación: 2019.02.21

(43) Fecha de publicación en revista: 2019.02.21

(44) Fecha de aceptación en revista: 2019.08.01

(71) Solicitante (s)

SKIDATA AG

(72) Inventor (es)

MALMBORG, Anders y JAYAPRAKASH, Vaijayanthi Mala

(74) Agente /Abogado

Spruson & Ferguson, GPO Box 3898, Sydney, NSW, 2001, AU

(56) Arte previo relacionado

US 20160350547 A1

MÉTODO PARA EVITAR EL USO INDEBIDO DE PERMISOS DE ACCESO ELECTRÓNICOS, QUE PUEDEN GESTIONARSE EN DISPOSITIVOS ELECTRÓNICOS MÓVILES USANDO UNA APLICACIÓN DE MONEDERO Y QUE SE TRANSMITEN A LOS DISPOSITIVOS ELECTRÓNICOS MÓVILES MEDIANTE UN SERVIDOR, USANDO EN CADA CASO UN ENLACE PARA LA DESCARGA DEL PERMISO DE ACCESO

RESUMEN

En el contexto del método para evitar el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso, se compra un permiso de acceso electrónico por medio de una interacción con un servidor (2), en el que durante la compra del permiso de acceso electrónico por el comprador (1) se especifican una contraseña o datos de autenticación y un dispositivo electrónico móvil, al que se transmite el permiso de acceso electrónico mediante el servidor (1) a través de un enlace para la descarga del permiso de acceso, en el que cuando se activa el enlace para descargar el permiso de acceso comprado se transmite un ID único del dispositivo electrónico móvil (3), que está asociado con un ID del permiso de acceso comprado, al servidor (2), en el que el permiso de acceso electrónico se transfiere únicamente desde el dispositivo electrónico móvil (3) a otro dispositivo electrónico móvil (4) después de la contraseña especificada por el comprador del permiso de acceso o los datos de autenticación especificados por el comprador del permiso de acceso se introducen primero por medio de una interacción con el servidor (2), en el que tras una transferencia satisfactoria se asocia el ID de permiso de acceso con el ID del otro dispositivo electrónico móvil (4) en el servidor (2) y el permiso de acceso almacenado en el primer dispositivo electrónico móvil (3) se marca por el servidor (2) como inválido.

La presente invención se refiere a un método para evitar el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso, de acuerdo con el preámbulo de la reivindicación 1.

Antecedentes

De la técnica anterior se conoce almacenar y gestionar permisos de acceso electrónicos, por ejemplo, por medio de las así llamadas aplicaciones de monedero en dispositivos electrónicos móviles, tal como teléfonos inteligentes y tabletas. En este caso es posible reenviar, por ejemplo, por medio de la aplicación de IOS "Wallet", permisos de acceso electrónicos a otros dispositivos electrónicos móviles. Esto aumenta la comodidad del usuario, en el caso en el que una persona autorizada quisiera usar un dispositivo electrónico móvil nuevo; por otra parte, esta técnica puede permitir que se "presten" permisos de acceso electrónicos personales, permitiendo de este modo un uso indebido de estos permisos de acceso.

Resumen de la invención

El objeto de la presente invención es especificar un método para evitar el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso, cuyo uso excluye la posibilidad de uso indebido del permiso de acceso mientras al mismo tiempo garantiza la facilidad para la transmisión del permiso de acceso electrónico a otro dispositivo electrónico móvil de una persona autorizada.

Este objeto se consigue mediante las características de la reivindicación 1. Configuraciones adicionales de acuerdo con la invención y ventajas son evidentes a partir de las reivindicaciones dependientes.

Es un objeto de la presente invención superar sustancialmente, o al menos aminorar, una o más desventajas de los arreglos ya existentes.

En un aspecto de la presente invención, se provee un método para prevenir el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso, caracterizado por que un permiso de acceso electrónico se compra por medio de una interacción con un servidor, en el que durante la compra del permiso de acceso electrónico por un comprador, se especifican una contraseña o datos de autenticación y un dispositivo electrónico móvil, al que se transmite el permiso de acceso electrónico mediante el servidor a través de un enlace para la descarga del permiso de acceso, en el que cuando se activa el enlace para descargar el permiso de acceso comprado transmite un ID único del dispositivo electrónico móvil al servidor, que está asociado con un ID del permiso de acceso comprado, en el que el permiso de acceso electrónico se transfiere únicamente desde el dispositivo electrónico móvil a otro dispositivo electrónico móvil después de la contraseña especificada por el comprador del permiso de acceso o los datos de autenticación especificados por el comprador del permiso de acceso se introducen primero por medio de una interacción con el servidor, en el que tras una transferencia satisfactoria el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil en el servidor y el permiso de acceso almacenado en el primer dispositivo electrónico móvil se marca por el servidor como inválido, caracterizado por que después de transferir el enlace para descargar el permiso de acceso al dispositivo electrónico móvil, la aplicación de monedero que se instala en el dispositivo móvil activa el enlace y para descargar el permiso de acceso adquirido, transmite un ID único del dispositivo electrónico móvil al servidor, en el que en el servidor verifica si un ID del permiso de acceso adquirido está asociado con el ID único transmitido del dispositivo electrónico móvil, en el que si este no es el caso, el ID de permiso de acceso y el ID único del dispositivo electrónico móvil se asocian entre sí y el permiso de acceso electrónico se descarga a continuación, y en el que si el acceso electrónico debe transmitirse desde un dispositivo electrónico móvil a otro dispositivo electrónico móvil, después de la iniciación del proceso por el propietario del dispositivo electrónico móvil con cuyo ID único está asociado el ID de permiso de acceso, la aplicación de monedero del dispositivo electrónico móvil, con cuyo ID

único está asociado el ID de permiso de acceso, transmite el enlace para la descarga del permiso de acceso al otro dispositivo electrónico móvil, en el que la aplicación de monedero del otro dispositivo electrónico móvil activa el enlace y transmite un ID único del otro dispositivo electrónico móvil al servidor, tras lo cual se hace una comprobación en el servidor en cuanto a si existe una asociación entre el ID del permiso de acceso a transferir con un ID único de otro dispositivo electrónico móvil, en el que si este es el caso, se envía un enlace mediante el servidor al otro dispositivo electrónico móvil, cuya ejecución de enlace por la aplicación de monedero conduce a una pantalla de entrada para o bien la contraseña especificada por el comprador del permiso de acceso o bien para los datos de autenticación especificados por el comprador del permiso de acceso, en el que si la contraseña es válida o los datos de autenticación son válidos, el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil en el servidor y el permiso de acceso electrónico se descarga al otro dispositivo electrónico móvil.

En consecuencia, se propone un método para evitar el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso, en el que en dicho método se compra un permiso de acceso electrónico por medio de una interacción con un servidor, en el que durante la compra del permiso de acceso electrónico por un comprador, se especifican una contraseña o datos de autenticación y un dispositivo electrónico móvil, en el que el permiso de acceso electrónico se transmite desde el servidor al dispositivo electrónico móvil por medio de un enlace para la descarga del permiso de acceso.

De acuerdo con la presente divulgación, en la implementación del enlace para descargar el permiso de acceso comprado se transmite un ID único del dispositivo electrónico móvil al servidor, que se asocia con un ID del permiso de acceso adquirido, en el que una transmisión del permiso de acceso electrónico desde el primer dispositivo electrónico móvil a otro dispositivo electrónico móvil se produce únicamente después de la entrada de la contraseña especificada por el comprador del permiso de acceso, y/o entrada de los datos de autenticación especificados por el comprador del permiso de acceso por medio de una interacción con el servidor, en el que al finalizar la transferencia el ID de permiso de acceso se

asocia con el ID del otro dispositivo electrónico móvil en el servidor, y el servidor marca el permiso de acceso almacenado en el primer dispositivo electrónico móvil como inválido.

En el contexto de un diseño de la presente divulgación, después de la transmisión del enlace para descargar el permiso de acceso al dispositivo electrónico móvil, una aplicación de monedero instalada en el dispositivo móvil activa el enlace y para descargar el permiso de acceso adquirido se transmite un ID único del dispositivo electrónico móvil al servidor, en el que se verifica en el servidor si un ID del permiso de acceso adquirido está asociado con el ID único transmitido del dispositivo electrónico móvil, en el que si este no es el caso, el ID de permiso de acceso y el ID único del dispositivo electrónico móvil se asocian entre sí y el permiso de acceso electrónico se descarga a continuación.

En el caso que el permiso de acceso electrónico deba transferirse desde un dispositivo electrónico móvil a otro dispositivo electrónico móvil, la aplicación de monedero del dispositivo electrónico móvil, cuyo ID único está asociado con el ID de permiso de acceso, transmite un enlace para la descarga del permiso de acceso al otro dispositivo electrónico móvil, en el que la aplicación de monedero del otro dispositivo electrónico móvil activa el enlace y transmite un ID único del otro dispositivo electrónico móvil al servidor.

De acuerdo con la presente divulgación, se verifica en el servidor si existe una asociación del ID de permiso de acceso con un ID único de otro dispositivo electrónico móvil, en el que si este es el caso, el servidor envía un enlace al otro dispositivo electrónico móvil, cuya activación por la aplicación de monedero conduce a una pantalla de entrada para o bien la contraseña especificada por el comprador del permiso de acceso o bien para los datos de autenticación especificados por el comprador del permiso de acceso, en el que si la contraseña es válida o los datos de autenticación son válidos, el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil en el servidor y el permiso de acceso electrónico se descarga al otro dispositivo electrónico móvil.

A continuación, el permiso de acceso almacenado en el primer dispositivo electrónico móvil se marca por el servidor como inválido, preferentemente por medio de un mensaje por proposición a la aplicación de monedero, en el que se elimina la asociación del ID del primer dispositivo electrónico móvil con el permiso de acceso electrónico y los datos correspondientes se almacenan en el servidor.

El diseño de acuerdo con la presente divulgación proporciona un método para evitar el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso, cuya activación garantiza que un permiso de acceso puede transferirse únicamente a otro dispositivo electrónico móvil si este es un dispositivo electrónico móvil de una persona autorizada.

En el contexto de una extensión de la presente invención, si un permiso de acceso debe transferirse desde un dispositivo electrónico móvil a otro dispositivo electrónico móvil, es decir si el ID de permiso de acceso ya se ha asociado con un ID único de un dispositivo electrónico móvil, entonces sobre la base del número de las asociaciones completadas desde el ID de permiso de acceso a ID únicos de dispositivos electrónicos móviles se verifica con qué frecuencia ya se ha transferido el permiso de acceso, en el que si el número de transferencias completadas ha alcanzado un valor umbral predefinido, no es posible ninguna transferencia adicional.

Descripción breve de las figuras

A continuación, se describe un ejemplo de la invención en mayor detalle sobre la base de la figura adjunta, que muestra un diagrama de secuencia para ilustrar las principales características del método de acuerdo con la invención.

Descripción detallada

Haciendo referencia a la figura adjunta, en el inicio del método un permiso de acceso electrónico se compra por un comprador 1 por medio de una interacción con un servidor 2 (etapa 1), en el que cuando el permiso de acceso electrónico se compra por el comprador se especifica una contraseña o datos de autenticación. A continuación (etapa 2), el permiso de acceso electrónico se transfiere desde el servidor 1 a un dispositivo electrónico móvil 3 especificado durante la compra del permiso de acceso, por medio de un enlace para la descarga del permiso de acceso, en el que una aplicación de monedero instalada en el dispositivo móvil 3 activa el enlace y para descargar el permiso de acceso adquirido, se transmite un ID único del dispositivo electrónico móvil al servidor 2 (etapa 3), en el que se verifica en el

servidor 2 si un ID del permiso de acceso adquirido está asociado con el ID único transmitido del dispositivo electrónico móvil 3, en el que si este no es el caso, el ID de permiso de acceso y el ID único del dispositivo electrónico móvil 3 se asocian entre sí (etapa 4) y el permiso de acceso electrónico se descarga a continuación.

Si el permiso de acceso electrónico debe transferirse desde un dispositivo electrónico móvil 3 a otro dispositivo electrónico móvil 4, es decir, si el ID de permiso de acceso ya se ha asociado con un ID único de un dispositivo electrónico móvil 3, entonces después de la iniciación del proceso por el propietario del dispositivo electrónico móvil 3 (etapa 5) con cuyo ID único está asociado el ID de permiso de acceso, la aplicación de monedero del dispositivo electrónico móvil 3, con cuyo ID único está asociado el ID de permiso de acceso, transmite un enlace para la descarga del permiso de acceso al otro dispositivo electrónico móvil 4 (etapa 6), en el que la aplicación de monedero del otro dispositivo electrónico móvil 4 activa el enlace (etapa 7) y transmite un ID único del otro dispositivo electrónico móvil 4 al servidor 2.

Se verifica a continuación en el servidor 2 si existe una asociación del ID de permiso de acceso con un ID único de otro dispositivo electrónico móvil, en el que si este es el caso, el servidor 2 envía un enlace al otro dispositivo electrónico móvil 4 (etapa 8), cuya activación por la aplicación de monedero conduce a una pantalla de entrada para introducir o bien la contraseña especificada por el comprador del permiso de acceso o bien para los datos de autenticación especificados por el comprador del permiso de acceso (etapa 9), en el que si la contraseña es válida o los datos de autenticación son válidos, el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil 4 en el servidor 2 y el permiso de acceso electrónico se descarga al otro dispositivo electrónico móvil 4.

El permiso de acceso almacenado en el primer dispositivo electrónico móvil 3 se marca a continuación por el servidor 2 como inválido (etapa 11), preferentemente por medio de un mensaje por proposición a la aplicación de monedero.

REIVINDICACIONES

1. Un método para evitar el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso, caracterizado por que un permiso de acceso electrónico se compra por medio de una interacción con un servidor, en el que durante la compra del permiso de acceso electrónico por un comprador, se especifican una contraseña o datos de autenticación y un dispositivo electrónico móvil, al que se transmite el permiso de acceso electrónico mediante el servidor a través de un enlace para la descarga del permiso de acceso, en el que cuando se activa el enlace para descargar el permiso de acceso comprado transmite un ID único del dispositivo electrónico móvil al servidor, que está asociado con un ID del permiso de acceso comprado, en el que el permiso de acceso electrónico se transfiere únicamente desde el dispositivo electrónico móvil a otro dispositivo electrónico móvil después de la contraseña especificada por el comprador del permiso de acceso o los datos de autenticación especificados por el comprador del permiso de acceso se introducen primero por medio de una interacción con el servidor, en el que tras una transferencia

satisfactoria el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil en el servidor y el permiso de acceso almacenado en el primer dispositivo electrónico móvil se marca por el servidor como inválido, caracterizado por que después de transferir el enlace para descargar el permiso de acceso al dispositivo electrónico móvil, la aplicación de monedero que se instala en el dispositivo móvil activa el enlace y para descargar el permiso de acceso adquirido, transmite un ID único del dispositivo electrónico móvil al servidor, en el que en el servidor verifica si un ID del permiso de acceso adquirido está asociado con el ID único transmitido del dispositivo electrónico móvil, en el que si este no es el caso, el ID de permiso de acceso y el ID único del dispositivo electrónico móvil se asocian entre sí y el permiso de acceso electrónico se descarga a continuación, y en el que si el acceso electrónico debe transmitirse desde un dispositivo electrónico móvil a otro dispositivo electrónico móvil, después de la iniciación del proceso por el propietario del dispositivo electrónico móvil con cuyo ID único está asociado el ID de permiso de acceso, la aplicación de monedero del dispositivo electrónico móvil, con cuyo ID único está asociado el ID de permiso de acceso, transmite el enlace para la descarga del permiso de acceso al otro dispositivo electrónico móvil, en el que la aplicación de monedero del otro dispositivo electrónico móvil activa el enlace y transmite un ID único del otro dispositivo electrónico móvil al servidor, tras lo cual se hace una comprobación en el servidor en cuanto a si existe una asociación entre el ID del permiso de acceso a transferir con un ID único de otro dispositivo electrónico móvil, en el que si este es el caso, se envía un enlace mediante el servidor al otro dispositivo electrónico móvil, cuya ejecución de enlace por la aplicación de monedero conduce a una pantalla de entrada para o bien la contraseña especificada por el comprador del permiso de acceso o bien para los datos de autenticación especificados por el comprador del permiso de acceso, en el que si la contraseña es válida o los datos de autenticación son válidos, el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil (4) en el servidor y el permiso de acceso electrónico se descarga al otro dispositivo electrónico móvil.

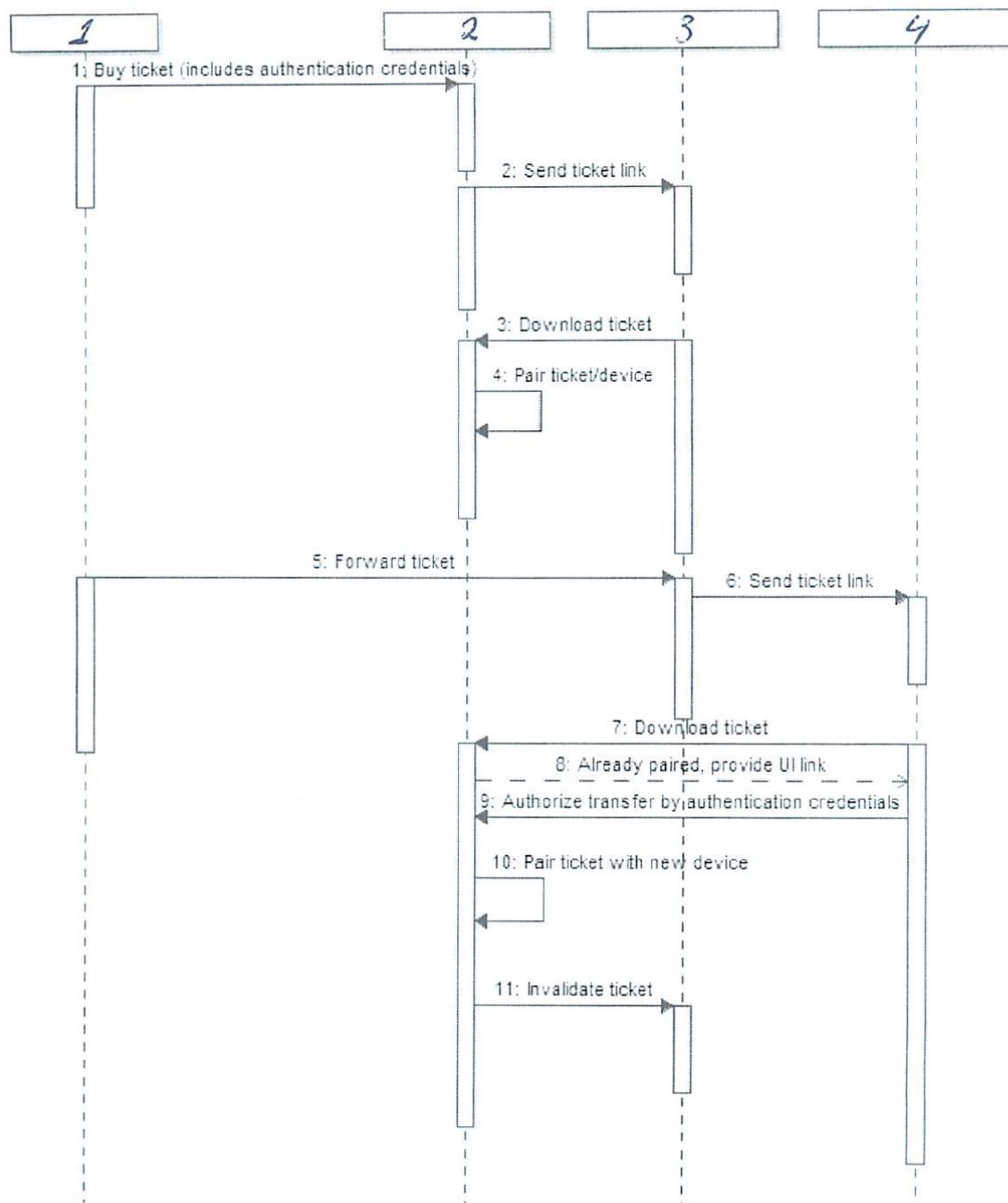
2. Un método para evitar el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero, y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de

acceso, de acuerdo con la reivindicación 1, caracterizado por que si un permiso de acceso debe transferirse desde un dispositivo electrónico móvil a otro dispositivo electrónico móvil, es decir si el ID de permiso de acceso ya se ha asociado con un ID único de un dispositivo electrónico móvil, entonces sobre la base del número de las asociaciones completadas entre el ID de permiso de acceso e ID únicos de dispositivos electrónicos móviles, se verifica con qué frecuencia ya se ha transferido el permiso de acceso, en el que si el número de transferencias completadas ha alcanzado un valor umbral predefinido, no es posible ninguna transferencia adicional.

SKIDATA AG

Abogados de patentes para el solicitante / persona nominada

SPRUSON & FERGUSON





SIC - 1.9.0.20814 - SRVWINEXTRA02

BANDEJA DE ENTRADA >

NC2020/0005368 - NC Modificación a las reivindicaciones - Discutir el asunto

[Salir](#)

Información

[NC2020/0005368](#)NC Modificación a
las reivindicacionesSolicitado en Patente
NC2018/0008254

Presentada

Solicitud de PI
relacionada[NC2018/0008254](#)Patente de Invención
NacionalMÉTODO PARA
EVITAR EL USO
INDEBIDO DE
PERMISOS DE
ACCESO
ELECTRÓNICOS,
QUE PUEDEN
GESTIONARSE EN
DISPOSITIVOS
ELECTRÓNICOS
MÓVILES USANDO
UNA APLICACIÓN
DE MONEDERO Y
QUE SE
TRANSMITEN A
LOS DISPOSITIVOS
ELECTRÓNICOS

Discusión

Título	Presentación solicitud modificación de reivindicaciones
Fecha de creación	29 abr. 2020
Estado	Cerrado

Mensajes

castellanosyconuevascreaciones - 29 abr. 2020

La solicitud de modificación de reivindicaciones ha sido presentada

[Cerrar](#)

MÓVILES
MEDIANTE UN
SERVIDOR,
USANDO EN CADA
CASO UN ENLACE
PARA LA
DESCARGA DEL
PERMISO DE
ACCESO

Publicado sin
pago

Cra 13 No. 27-00 pisos 1, 3, 4, 5, 6, 7 y 10 PBX: (571)5870000 . Call center: (571)5920400 Línea gratuita nacional 018000-910165
www.sic.gov.co . e-mail: contactenos@sic.gov.co . Bogotá D.C. - Colombia.

Política de privacidad | Política editorial | Créditos | Webmaster: contactenos@sic.gov.co ::: Todos los derechos reservados 2008 - 2020

REIVINDICACIONES

1. Un método para evitar el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso, caracterizado por que un permiso de acceso electrónico se compra por medio de una interacción con un servidor (2), en el que durante la compra del permiso de acceso electrónico por un comprador (1), se especifican una contraseña o datos de autenticación y un dispositivo electrónico móvil, al que se transmite el permiso de acceso electrónico mediante el servidor (1) a través de un enlace para la descarga del permiso de acceso, en el que cuando se activa el enlace para descargar el permiso de acceso comprado transmite un ID único del dispositivo electrónico móvil (3) al servidor (2), que está asociado con un ID del permiso de acceso comprado, en el que el permiso de acceso electrónico se transfiere únicamente desde el dispositivo electrónico móvil (3) a otro dispositivo electrónico móvil (4) después de la contraseña especificada por el comprador del permiso de acceso o los datos de autenticación especificados por el comprador del permiso de acceso se introducen primero por medio de una interacción con el servidor (2), en el que tras una transferencia satisfactoria el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil (4) en el servidor (2) y el permiso de acceso almacenado en el primer dispositivo electrónico móvil (3) se marca por el servidor (2) como inválido, caracterizado por que después de transferir el enlace para descargar el permiso de acceso al dispositivo electrónico móvil (3), la aplicación de monedero que se instala en el dispositivo móvil (3) activa el enlace y para descargar el permiso de acceso adquirido, transmite un ID único del dispositivo electrónico móvil al servidor (2), en el que en el servidor (2) verifica si un ID del permiso de acceso adquirido está asociado con el ID único transmitido del dispositivo electrónico móvil (3), en el que si este no es el caso, el ID de permiso de acceso y el ID único del dispositivo electrónico móvil (3) se asocian entre sí y el permiso de acceso electrónico se descarga a continuación, y en el que si el acceso electrónico debe transmitirse desde un dispositivo electrónico móvil (3) a otro dispositivo electrónico móvil (4), después de la iniciación del proceso por el propietario del dispositivo electrónico móvil (3) con cuyo ID único está asociado el ID de permiso de acceso, la aplicación de monedero del dispositivo electrónico móvil (3), con cuyo ID único está asociado el ID de permiso de acceso, transmite el enlace

para la descarga del permiso de acceso al otro dispositivo electrónico móvil (4), en el que la aplicación de monedero del otro dispositivo electrónico móvil (4) activa el enlace y transmite un ID único del otro dispositivo electrónico móvil (4) al servidor (2), tras lo cual se hace una comprobación en el servidor (2) en cuanto a si existe una asociación entre el ID del permiso de acceso a transferir con un ID único de otro dispositivo electrónico móvil, en el que si este es el caso, se envía un enlace mediante el servidor (2) al otro dispositivo electrónico móvil (4), cuya ejecución de enlace por la aplicación de monedero conduce a una pantalla de entrada para o bien la contraseña especificada por el comprador del permiso de acceso o bien para los datos de autenticación especificados por el comprador del permiso de acceso, en el que si la contraseña es válida o los datos de autenticación son válidos, el ID de permiso de acceso se asocia con el ID del otro dispositivo electrónico móvil (4) en el servidor (2) y el permiso de acceso electrónico se descarga al otro dispositivo electrónico móvil (4).

2. Un método para evitar el uso indebido de permisos de acceso electrónicos, que pueden gestionarse en dispositivos electrónicos móviles usando una aplicación de monedero, y que se transmiten a los dispositivos electrónicos móviles mediante un servidor, usando en cada caso un enlace para la descarga del permiso de acceso, de acuerdo con la reivindicación 1, caracterizado por que si un permiso de acceso debe transferirse desde un dispositivo electrónico móvil (3) a otro dispositivo electrónico móvil (4), es decir si el ID de permiso de acceso ya se ha asociado con un ID único de un dispositivo electrónico móvil (3), entonces sobre la base del número de las asociaciones completadas entre el ID de permiso de acceso e ID únicos de dispositivos electrónicos móviles, se verifica con qué frecuencia ya se ha transferido el permiso de acceso, en el que si el número de transferencias completadas ha alcanzado un valor umbral predefinido, no es posible ninguna transferencia adicional.