

[Sello de la Oficina de Patentes Europea]

Certificado

Los documentos adjuntos coinciden con la versión considerada como presentada originalmente de la solicitud de patente europea especificada en la página siguiente

Nº. de solicitud

17185122.3/ EP 17185122

El código de organización y número de su solicitud de prioridad a utilizar para la presentación en el extranjero bajo la convención de París es EP 17185122

El presidente de la Oficina Europea
de Patentes
p.o.

[Firma]

V.Joseph

Nº. de solicitud: 17185122.3

Fecha de presentación: 07/08/2017

Solicitante:

SKIDATA AG
Untersbergstrasse 40
5083 Grödig/Salzburg/Austria

Título de la invención:

(En el caso de no indicar el título de la invención, o en el caso de que la solicitud no se presentara en una lengua no oficial de la OEP véase la descripción con referencia al título original.)

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

Prioridad(es) reivindicada(s)
País/Fecha/Nº de expediente

Países contratantes designados en la fecha de presentación:

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

Bescheinigung

Die angehefteten
Unterlagen stimmen mit der
als ursprünglich eingereicht
geltenden Fassung der auf
dem nächsten Blatt
bezeichneten europäischen
Patentanmeldung überein.

Certificate

The attached documents are
exact copies of the text in
which the European patent
application described on the
following page is deemed to
have been filed.

Attestation

Les documents joints à la
présente attestation sont
conformes au texte,
considéré comme
initialement déposé, de la
demande de brevet
européen qui est spécifiée à
la page suivante.

Patentanmeldung Nr.

Patent application No.

Demande de brevet n°

17185122.3 / EP17185122

The organisation code and number of your priority application, to be used for filing abroad under the Paris Convention, is EP17185122.

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.



V. Joseph

Anmeldung Nr:
Application no.: 17185122.3
Demande no :

Anmeldetag:
Date of filing: 07.08.17
Date de dépôt :

Anmelder / Applicant(s) / Demandeur(s):

SKIDATA AG
Untersbergstrasse 40
5083 Grödig/Salzburg/AT

Bezeichnung der Erfindung / Title of the invention / Titre de l'invention:

(Falls die Bezeichnung der Erfindung nicht angegeben ist, oder falls die Anmeldung in einer Nicht-Amtssprache des EPA eingereicht wurde, siehe Beschreibung bezüglich ursprünglicher Bezeichnung.

If no title is shown, or if the application has been filed in a non-EPO language, please refer to the description for the original title.

Si aucun titre n'est indiqué, ou si la demande a été déposée dans une langue autre qu'une langue officielle de l'OEB, se référer à la description pour le titre original.)

Verfahren zur Vermeidung des Missbrauchs von in mobilen elektronischen Geräten mittels einer Wallet-Anwendung verwaltbaren elektronischen Zugangsberechtigungen, welche an die mobilen elektronischen Geräte von einem Server mittels jeweils eines Links zum Herunterladen der Zugangsberechtigung übermittelt werden

In Anspruch genommene Priorität(en) / Priority(Priorities) claimed / Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen / State/Date/File no. / Pays/Date/Numéro de dépôt:

Am Anmeldetag benannte Vertragstaaten / Contracting States designated at date of filing / Etats contractants désignés lors du dépôt:

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

Verfahren zur Vermeidung des Missbrauchs von in mobilen elektronischen Geräten
mittels einer Wallet-Anwendung verwaltbaren elektronischen Zugangs-
berechtigungen, welche an die mobilen elektronischen Geräte von einem Server
mittels jeweils eines Links zum Herunterladen der Zugangsberechtigung übermittelt
werden

Die vorliegende Erfindung bezieht sich auf ein Verfahren zum Vermeiden des Missbrauchs von in mobilen elektronischen Geräten mittels einer Wallet-Anwendung verwaltbaren elektronischen Zugangsberechtigungen, welche an die mobilen elektronischen Geräte von einem Server mittels jeweils eines Links zum Herunterladen der Zugangsberechtigung übermittelt werden, gemäß dem Oberbegriff des Patentanspruchs 1.

Aus dem Stand der Technik ist bekannt, elektronische Zugangsberechtigungen beispielsweise mittels sogenannter Wallet-Anwendungen auf mobilen elektronischen Geräten, wie beispielsweise Smartphones, Tablets zu speichern und zu verwalten. Hierbei ist es möglich, beispielsweise mittels der IOS-App „Wallet“ elektronische Zugangsberechtigungen an weitere mobile elektronische Geräte weiterzuleiten. Dies steigert zum einen den Komfort, für den Fall, dass eine berechtigte Person ein neues mobiles elektronisches Gerät verwenden möchte; andererseits können dadurch personenbezogene elektronische Zugangsberechtigungen „ausgeliehen“ werden, wodurch ein Missbrauch dieser Zugangsberechtigungen vorliegt.

Der vorliegenden Erfindung liegt die Aufgabe zugrunde, ein Verfahren zum Vermeiden des Missbrauchs von in mobilen elektronischen Geräten mittels einer Wallet- Anwendung verwaltbaren elektronischen Zugangsberechtigungen, welche an die mobilen elektronischen Geräte von einem Server mittels jeweils eines Links zum Herunterladen der Zugangsberechtigung übermittelt werden, anzugeben, durch dessen Durchführung ein Missbrauch einer Zugangsberechtigung bei gleichzeitiger Gewährleistung der Möglichkeit der Übertragung der elektronischen

Zugangsberechtigung auf ein weiteres mobiles elektronisches Gerät einer berechtigten Person ausgeschlossen wird.

Diese Aufgabe wird durch die Merkmale des Patentanspruchs 1 gelöst. Weitere erfindungsgemäße Ausgestaltungen und Vorteile gehen aus den Unteransprüchen hervor.

Demnach wird ein Verfahren zum Vermeiden des Missbrauchs von in mobilen elektronischen Geräten mittels einer Wallet- Anwendung verwaltbaren elektronischen Zugangsberechtigungen, welche an die mobilen elektronischen Geräte von einem Server mittels jeweils eines Links zum Herunterladen der Zugangsberechtigung übermittelt werden vorgeschlagen, im Rahmen dessen eine elektronische Zugangsberechtigung mittels einer Interaktion mit einem Server erworben wird, wobei beim Erwerb der elektronischen Zugangsberechtigung von einem Käufer ein Passwort oder Authentifizierungsdaten und ein mobiles elektronisches Gerät, an das die elektronische Zugangsberechtigung vom Server mittels eines Links zum Herunterladen der Zugangsberechtigung übermittelt wird, angegeben werden.

Erfindungsgemäß wird beim Ausführen des Links zum Herunterladen der erworbenen Zugangsberechtigung eine eindeutige ID des mobilen elektronischen Gerätes an den Server übermittelt, welche mit einer ID der erworbenen Zugangsberechtigung verknüpft wird, wobei eine Übertragung der elektronischen Zugangsberechtigung von dem ersten mobilen elektronischen Gerät auf ein weiteres mobiles elektronisches Gerät erst nach Eingabe des vom Käufer der Zugangsberechtigung angegebenen Passworts bzw. der vom Käufer der Zugangsberechtigung angegebenen Authentifizierungsdaten mittels einer Interaktion mit dem Server erfolgt, wobei bei erfolgter Übertragung im Server die Zugangsberechtigungs-ID mit der ID des weiteren mobilen elektronischen Gerätes verknüpft wird und vom Server die auf dem ersten mobilen elektronischen Gerät abgelegte Zugangsberechtigung als ungültig markiert wird.

Im Rahmen einer Ausgestaltung der Erfindung wird nach der Übermittlung des Links zum Herunterladen der Zugangsberechtigung an das mobile elektronische Gerät von einer Wallet- Anwendung, die auf dem mobilen Gerät installiert ist, der Link

ausgeführt und zum Herunterladen der erworbenen Zugangsberechtigung eine eindeutige ID des mobilen elektronischen Gerätes an den Server übermittelt, wobei im Server überprüft wird, ob eine ID der erworbenen Zugangsberechtigung mit der übermittelten eindeutigen ID des mobilen elektronischen Gerätes verknüpft ist, wobei, wenn dies nicht der Fall ist, die Zugangsberechtigungs-ID und die eindeutige ID des mobilen elektronischen Gerätes miteinander verknüpft werden und anschließend die elektronische Zugangsberechtigung heruntergeladen wird.

Für den Fall, dass die elektronische Zugangsberechtigung von einem mobilen elektronischen Gerät auf ein weiteres mobiles elektronisches Gerät übertragen werden soll, wird von der Wallet-Anwendung des mobilen elektronischen Gerätes, , mit dessen eindeutiger ID die Zugangsberechtigungs-ID verknüpft ist, ein Link zum Herunterladen der Zugangsberechtigung an das weitere mobile elektronische Gerät übermittelt, wobei die Wallet-Anwendung des weiteren mobilen elektronischen Gerätes den Link ausführt und eine eindeutige ID des weiteren mobilen elektronischen Gerätes an den Server übermittelt.

Erfindungsgemäß wird im Server überprüft, ob eine Verknüpfung der Zugangsberechtigungs-ID mit einer eindeutigen ID eines anderen mobilen elektronischen Gerätes existiert, wobei, wenn dies der Fall ist, vom Server ein Link auf das weitere mobile elektronische Gerät übermittelt wird, dessen Ausführung von der Wallet-Anwendung zu einer Eingabemaske für das vom Käufer der Zugangsberechtigung angegebene Passwort bzw. die vom Käufer der Zugangsberechtigung angegebenen Authentifizierungsdaten führt, wobei bei gültigem Passwort oder bei gültigen Authentifizierungsdaten, im Server die Zugangsberechtigungs-ID mit der ID des weiteren mobilen elektronischen Gerätes verknüpft wird und die elektronische Zugangsberechtigung auf das weitere mobile elektronische Gerät heruntergeladen wird.

Anschließend wird vom Server die auf dem ersten mobilen elektronischen Gerät abgelegte Zugangsberechtigung vorzugsweise mittels einer Push-Nachricht an die Wallet-Anwendung als ungültig markiert, wobei die Verknüpfung der ID des ersten mobilen elektronischen Gerätes mit der elektronischen Zugangsberechtigung gelöscht wird und die entsprechenden Daten im Server gespeichert werden.

Durch die erfindungsgemäß Konzeption wird ein Verfahren zum Vermeiden des Missbrauchs von in mobilen elektronischen Geräten mittels einer Wallet- Anwendung verwaltbaren elektronischen Zugangsberechtigungen, welche an die mobilen elektronischen Geräte von einem Server mittels jeweils eines Links zum Herunterladen der Zugangsberechtigung übermittelt werden zur Verfügung gestellt, durch dessen Durchführung gewährleistet wird, dass eine Zugangsberechtigung nur dann auf ein weiteres mobiles elektronisches Gerät übertragen werden kann, wenn dies ein mobiles elektronisches Gerät einer berechtigten Person ist.

Im Rahmen einer Weiterbildung der Erfindung wird, wenn eine Zugangsberechtigung von einem mobilen elektronischen Gerät auf ein weiteres mobiles elektronisches Gerät übertragen werden soll, d.h., wenn die Zugangsberechtigungs-ID bereits mit einer eindeutigen ID eines mobilen elektronischen Gerätes verknüpft ist, anhand der Anzahl der erfolgten Verknüpfungen der Zugangsberechtigungs-ID mit eindeutigen IDs mobiler elektronischer Geräte überprüft, wie oft die Zugangsberechtigung bereits übertragen worden ist, wobei, wenn die Anzahl der erfolgten Übertragungen einen vorgegebenen Schwellenwert erreicht hat, keine weitere Übertragung möglich ist.

Die Erfindung wird im Folgenden anhand der beigefügten Figur, welche ein Sequenzdiagramm zur Veranschaulichung der Hauptmerkmale des erfindungsgemäßen Verfahrens darstellt, beispielhaft näher erläutert.

Bezugnehmend auf die beigefügte Figur wird zu Beginn des Verfahrens von einem Käufer 1 mittels einer Interaktion mit einem Server 2 eine elektronische Zugangsberechtigung erworben (Schritt 1), wobei beim Erwerb der elektronischen Zugangsberechtigung vom Käufer ein Passwort oder Authentifizierungsdaten angegeben werden. Anschließend (Schritt 2) wird die elektronische Zugangsberechtigung vom Server 1 auf ein beim Erwerb der Zugangsberechtigung angegebenes mobiles elektronisches Gerät 3 mittels eines Links zum Herunterladen der Zugangsberechtigung übermittelt, wobei eine Wallet- Anwendung, die auf dem mobilen Gerät 3 installiert ist, den Link ausführt und zum Herunterladen der erworbenen Zugangsberechtigung eine eindeutige ID des mobilen elektronischen

Gerätes an den Server 2 übermittelt (Schritt 3), wobei im Server 2 überprüft wird, ob eine ID der erworbenen Zugangsberechtigung mit der übermittelten eindeutigen ID des mobilen elektronischen Gerätes 3 verknüpft ist, wobei, wenn dies nicht der Fall ist, die Zugangsberechtigungs-ID und die eindeutige ID des mobilen elektronischen Gerätes 3 miteinander verknüpft werden (Schritt 4) und anschließend die elektronische Zugangsberechtigung heruntergeladen wird.

Wenn die elektronische Zugangsberechtigung von einem mobilen elektronischen Gerät 3 auf ein weiteres mobiles elektronisches Gerät 4 übertragen werden soll, d.h., wenn die Zugangsberechtigungs-ID bereits mit einer eindeutigen ID eines mobilen elektronischen Gerätes 3 verknüpft ist, wird nach Initiierung des Vorgangs vom Besitzer des mobilen elektronischen Gerätes 3 (Schritt 5), mit dessen eindeutiger ID die Zugangsberechtigungs-ID verknüpft ist, von der Wallet-Anwendung des mobilen elektronischen Gerätes 3, mit dessen eindeutiger ID die Zugangsberechtigungs-ID verknüpft ist, ein Link zum Herunterladen der Zugangsberechtigung an das weitere mobile elektronische Gerät 4 übermittelt (Schritt 6), wobei die Wallet-Anwendung des weiteren mobilen elektronischen Gerätes 4 den Link ausführt (Schritt 7) und eine eindeutige ID des weiteren mobilen elektronischen Gerätes 4 an den Server 2 übermittelt.

Anschließend wird im Server 2 überprüft, ob eine Verknüpfung der ID der zu übertragenden Zugangsberechtigung mit einer eindeutigen ID eines anderen mobilen elektronischen Gerätes existiert, wobei, wenn dies der Fall ist, vom Server 2 ein Link auf das weitere mobile elektronische Gerät 4 übermittelt wird (Schritt 8), dessen Ausführung von der Wallet-Anwendung zu einer Eingabemaske für das vom Käufer der Zugangsberechtigung angegebene Passwort bzw. die vom Käufer der Zugangsberechtigung angegebenen Authentifizierungsdaten führt (Schritt 9), wobei bei gültigem Passwort oder bei gültigen Authentifizierungsdaten, im Server 2 die Zugangsberechtigungs-ID mit der ID des weiteren mobilen elektronischen Gerätes 4 verknüpft wird (Schritt 10) und die elektronische Zugangsberechtigung auf das weitere mobile elektronische Gerät 4 heruntergeladen wird.

Anschließend wird vom Server 2 die auf dem ersten mobilen elektronischen Gerät 3 abgelegte Zugangsberechtigung vorzugsweise mittels einer Push-Nachricht an die Wallet-Anwendung als ungültig markiert (Schritt 11).

Patentansprüche

1. Verfahren zum Vermeiden des Missbrauchs von in mobilen elektronischen Geräten mittels einer Wallet- Anwendung verwaltbaren elektronischen Zugangsberechtigungen, welche an die mobilen elektronischen Geräte von einem Server mittels jeweils eines Links zum Herunterladen der Zugangsberechtigung übermittelt werden, dadurch gekennzeichnet, dass eine elektronische Zugangsberechtigung mittels einer Interaktion mit einem dem Server (2) erworben wird, wobei beim Erwerb der elektronischen Zugangsberechtigung von einem Käufer (1) ein Passwort oder Authentifizierungsdaten und ein mobiles elektronisches Gerät, an das die elektronische Zugangsberechtigung vom Server (1) mittels eines Links zum Herunterladen der Zugangsberechtigung übermittelt wird, angegeben werden, wobei beim Ausführen des Links zum Herunterladen der erworbenen Zugangsberechtigung eine eindeutige ID des mobilen elektronischen Gerätes (3) an den Server (2) übermittelt wird, welche mit einer ID der erworbenen Zugangsberechtigung verknüpft wird, wobei eine Übertragung der elektronischen Zugangsberechtigung von dem mobilen elektronischen Gerät (3) auf ein weiteres mobiles elektronisches Gerät (4) erst nach Eingabe des vom Käufer der Zugangsberechtigung angegebenen Passworts bzw. der vom Käufer der Zugangsberechtigung angegebenen Authentifizierungsdaten mittels einer Interaktion mit dem Server (2) erfolgt, wobei bei erfolgter Übertragung im Server (2) die Zugangsberechtigungs-ID mit der ID des weiteren mobilen elektronischen Gerätes (4) verknüpft wird und vom Server (2) die auf dem mobilen elektronischen Gerät (3) abgelegte Zugangsberechtigung als ungültig markiert wird.

2. Verfahren zum Vermeiden des Missbrauchs von in mobilen elektronischen Geräten mittels einer Wallet- Anwendung verwaltbaren elektronischen Zugangsberechtigungen, welche an die mobilen elektronischen Geräte von einem Server mittels jeweils eines Links zum Herunterladen der Zugangsberechtigung übermittelt werden, nach Anspruch 1, dadurch gekennzeichnet, dass nach der Übermittlung des Links zum Herunterladen der Zugangsberechtigung an das mobile elektronische Gerät (3) eine Wallet- Anwendung, die auf dem mobilen Gerät (3) installiert ist, den Link ausführt und zum Herunterladen der erworbenen

Zugangsberechtigung eine eindeutige ID des mobilen elektronischen Gerätes an den Server (2) übermittelt, wobei im Server (2) überprüft wird, ob eine ID der erworbenen Zugangsberechtigung mit der übermittelten eindeutigen ID des mobilen elektronischen Gerätes (3) verknüpft ist, wobei, wenn dies nicht der Fall ist, die Zugangsberechtigungs-ID und die eindeutige ID des mobilen elektronischen Gerätes (3) miteinander verknüpft werden und anschließend die elektronische Zugangsberechtigung heruntergeladen wird und wobei, wenn eine elektronische Zugangsberechtigung von einem mobilen elektronischen Gerät (3) auf ein weiteres mobiles elektronisches Gerät (4) übertragen werden soll, nach Initiierung des Vorgangs vom Besitzer des mobilen elektronischen Gerätes (3), mit dessen eindeutiger ID die Zugangsberechtigungs-ID verknüpft ist, von der Wallet-Anwendung des mobilen elektronischen Gerätes (3), mit dessen eindeutiger ID die Zugangsberechtigungs-ID verknüpft ist, ein Link zum Herunterladen der Zugangsberechtigung an das weitere mobile elektronische Gerät (4) übermittelt wird, wobei die Wallet-Anwendung des weiteren mobilen elektronischen Gerätes (4) den Link ausführt und eine eindeutige ID des weiteren mobilen elektronischen Gerätes (4) an den Server (2) übermittelt, wobei anschließend im Server (2) überprüft wird, ob eine Verknüpfung der ID der zu übertragenden Zugangsberechtigung mit einer eindeutigen ID eines anderen mobilen elektronischen Gerätes existiert, wobei, wenn dies der Fall ist, vom Server (2) ein Link auf das weitere mobile elektronische Gerät (4) übermittelt wird, dessen Ausführung von der Wallet-Anwendung zu einer Eingabemaske für das vom Käufer der Zugangsberechtigung angegebene Passwort bzw. die vom Käufer der Zugangsberechtigung angegebenen Authentifizierungsdaten führt, wobei bei gültigem Passwort oder bei gültigen Authentifizierungsdaten, im Server (2) die Zugangsberechtigungs-ID mit der ID des weiteren mobilen elektronischen Gerätes (4) verknüpft wird und die elektronische Zugangsberechtigung auf das weitere mobile elektronische Gerät (4) heruntergeladen wird.

3. Verfahren zum Vermeiden des Missbrauchs von in mobilen elektronischen Geräten mittels einer Wallet- Anwendung verwaltbaren elektronischen Zugangsberechtigungen, welche an die mobilen elektronischen Geräte von einem Server mittels jeweils eines Links zum Herunterladen der Zugangsberechtigung übermittelt werden, nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass wenn

eine Zugangsberechtigung von einem mobilen elektronischen Gerät (3) auf ein weiteres mobiles elektronisches Gerät (4) übertragen werden soll, d.h., wenn die Zugangsberechtigungs-ID bereits mit einer eindeutigen ID eines mobilen elektronischen Gerätes (3) verknüpft ist, anhand der Anzahl der erfolgten Verknüpfungen der Zugangsberechtigungs-ID mit eindeutigen IDs mobiler elektronischer Geräte überprüft wird, wie oft die Zugangsberechtigung bereits übertragen worden ist, wobei, wenn die Anzahl der erfolgten Übertragungen einen vorgegebenen Schwellenwert erreicht hat, keine weitere Übertragung möglich ist.

Zusammenfassung

Im Rahmen des Verfahrens zum Vermeiden des Missbrauchs von in mobilen elektronischen Geräten mittels einer Wallet- Anwendung verwaltbaren elektronischen Zugangsberechtigungen, welche an die mobilen elektronischen Geräte von einem Server mittels jeweils eines Links zum Herunterladen der Zugangsberechtigung übermittelt werden, wird eine elektronische Zugangsberechtigung mittels einer Interaktion mit einem Server (2) erworben, wobei beim Erwerb der elektronischen Zugangsberechtigung vom Käufer (1) ein Passwort oder Authentifizierungsdaten und ein mobiles elektronisches Gerät, an das die elektronische Zugangsberechtigung vom Server (1) mittels eines Links zum Herunterladen der Zugangsberechtigung übermittelt wird, angegeben werden, wobei beim Ausführen des Links zum Herunterladen der erworbenen Zugangsberechtigung eine eindeutige ID des mobilen elektronischen Gerätes (3) an den Server (2) übermittelt wird, welche mit einer ID der erworbenen Zugangsberechtigung verknüpft wird, wobei eine Übertragung der elektronischen Zugangsberechtigung von dem mobilen elektronischen Gerät (3) auf ein weiteres mobiles elektronisches Gerät (4) erst nach Eingabe des vom Käufer der Zugangsberechtigung angegebenen Passworts bzw. der vom Käufer der Zugangsberechtigung angegebenen Authentifizierungsdaten mittels einer Interaktion mit dem Server (2) erfolgt, wobei bei erfolgter Übertragung im Server (2) die Zugangsberechtigungs-ID mit der ID des weiteren mobilen elektronischen Gerätes (4) verknüpft wird und vom Server (2) die auf dem ersten mobilen elektronischen Gerät (3) abgelegte Zugangsberechtigung als ungültig markiert wird.

Figur



