Acknowledgement of receipt

We hereby acknowledge receipt of the following subsequently filed document(s):

Submission number	9563816
Application number	EP21382085.5
Date of receipt	04 March 2021
Receiving Office	European Patent Office, The Hague
Your reference	20-013-B
Applicant	All applicants as on file

Documents submitted		
	package-data.xml	ep-sfd-request.xml
	epf1038.pdf (1 p.)	TRANEAPP-1.pdf\English translation.pdf (22 p.)

Submitted by	CN=Miguel de Fuentes 68232
Method of submission	Online
Date and time receipt generated	04 March 2021, 12:02 (CET)
Message Digest	23:4E:A9:EF:06:12:34:52:9F:44:DB:77:58:7F:CF:0F:C4:0B:08:14

/European Patent Office/

Representative:

Isern Patents y Marcas, S.L.
838
Avda. Diagonal 463 Bis, 2 Planta
08036 Barcelona
Spain

Phone: +34 93 363 79 00
Fax: +34 93 363 79 02
E-mail: patent@isern.com

80298 Munich
Germany
Tel. +49(0)89 2399-0 | Fax -4465

P.O. Box 5818
2280 HV Rijswijk
Netherlands
Tel. +31(0)70 340-2040 | Fax -3016

10958 Berlin
Germany
Tel. +49(0)30 25901-0 | Fax -840

The document(s) listed below is (are) subsequently filed documents pertaining to the following application:

Application number	21382085.5

Applicant's or representative's reference	20-013-B

	Description of document	Original file name	Assigned file name
1	Translation of previously filed application	English translation.pdf	TRANEAPP-1.pdf

	Payment	
1	Method of payment	Not specified

Signatures

Place:	**Barcelona**
Date:	**04 March 2021**
Signed by:	**Miguel de Fuentes 68232**
Association:	**Isern Patents y Marcas, S.L.**
Representative name:	**Miguel de Fuentes**
Capacity:	**(Representative)**

METHOD, SYSTEM AND COMPUTER PROGRAM FOR MANAGING AND TRANSMITTING INFORMATION

TECHNICAL FIELD OF THE INVENTION

5   The present invention is related to the Internet of Things and communication systems for transmitting information that is stored and managed by means of a server, such as the cloud, wherein the information stored in said server is accessible by means of access links arranged in tags of the NFC, RFID, QR, or similar type, said tags being provided for establishing data

10   communication with a portable communication device, wherein, when communicating with the tag, the portable communication device can access the information stored in the server.

STATE OF THE ART

15   In today's world, almost all the information available is dumped on servers accessible by means of network links. The greater and more varied information that becomes available, the more effective the ability to share it with users should be.

        One example of sharing information dumped on the network has been

20   materialised in the so-called "Electronic business cards" wherein a bar code is arranged on a common business card, for example, a QR code (Quick Response code), which, when decrypted by a portable communication device, such as a smartphone, enables access in the web browser of said smartphone to information stored on a server related to the business card, in this case,

25   professional information about the carrier of the electronic business card.

        More recently, and taking advantage of NFC (Near Field Communication) secure wireless near field communication technology, NFC tags have been created that can be associated with a software or app, wherein a user acquires an NFC tag, creates a profile in the software or app to which it uploads

30   information in a database associated with the software of, for example, the social networks and contacts thereof. By means of the software or app, the user enters the profile information thereof on the NFC tag, linking up the software or app with the tag. Thus, by using NFC technology, social networks user profiles can be instantly shared between smartphones.

35   Notwithstanding the foregoing, in the present context it would be an

advance in the art to provide better ways of managing personal information on the Internet, or not just personal information, but, for example, business information. For example, improvements are needed to reduce the tedium of users, such as that which can occur when having to search the entire menu of a restaurant for the breakfast menu, increase the control of users over their private information, i.e., selecting the kind of information they want to share, and provide better ways to manage personal or business information according to the relationship of the parties involved.

DESCRIPTION

To respond to the required advance of the art, the present invention provides a computer-implemented method for managing and transmitting information in an information management system wherein the elements that compose said system are at least one server in which the information to be managed is stored. This server comprises processing means, such as a controller or processor, capable of processing and/or managing the data or information stored therein.

The system further comprises at least one tag, transponder or the like, provided with a tag code, a unique tag code, for uniquely identifying said tag, a portable communication device, such as a smartphone, tablet, laptop or similar, configured to establish a data connection with said tag.

Given that the portable communication device is used by a person, i.e., it is generally personalised, said portable communication device has associated with it a receiver profile indicative of the person who owns or is using the mobile terminal. This issuer profile may have an associated issuer code, a unique issuer code, which aims to identify the issuer profile by means of the server as will be seen below.

Taking into consideration the elements that compose the system, the computer-implemented method of the invention comprises the steps of storing at least one issuer profile on the server. This means that a user who intends to share information that, from now on, will be called "issuer" creates a profile that will be stored on the server, wherein the issuer profile provides a series of data owned by the issuer, such as their name or business name, location, etc.

The issuer profile comprises an issuer code, unique issuer code, which can be assigned by the server at the time of storing or loading the issuer profile,

which identifies the stored issuer profile, such that, as the next step of the method, the issuer code is linked up with the tag, associating or linking up the issuer code with the tag code, such that said tag is associated with the issuer profile on the server, i.e., the tag "belongs" to the issuer profile to which it has been associated.

Once the issuer profile has been linked up with the tag by means of the codes thereof, the server generates a link, a unique link, which is assigned to the tag, wherein this link is intended to provide a path that gives access to the issuer profile stored in the server, as is known in the state of the art.

The main feature of the user profile is that it comprises at least one subdirectory, preferably a plurality of subdirectories, so that the information that the issuer intends to share is conveniently distributed in the subdirectory or subdirectories, each of these subdirectories being able to be selected for access, either by the issuer, or by the server based on a protocol that will be detailed below.

The issuer profile, in addition to the subdirectory or the plurality of subdirectories, comprises at least one confidential subdirectory in which relevant or private information of the issuer can be arranged, wherein this confidential subdirectory will be able to be selected for access either by the issuer, or by the server based on a protocol analogous to the one that gives access to the subdirectories.

The objective of storing this issuer profile on the server is for said server to manage access to said issuer profile, so that, when the portable communication device establishes a data connection with the tag, said portable communication device interprets the link of the tag, opens said link in a web browser provided therein to access the issuer profile stored on the server, being able to further access the subdirectory or subdirectories or the confidential subdirectory or confidential subdirectories if said subdirectory or subdirectories have been selected for access.

The issuer will have the power to modify the information of the issuer profile, the subdirectories, and the confidential subdirectory at will and, as the tag comprises a link that, in principle, does not vary and that directs to said issuer profile on the server, the modifications do not affect the tag, i.e., by accessing the issuer profile by means of the tag link, changes in the issuer profile and/or in the subdirectories and/or in the confidential subdirectory can be

observed if said subdirectories are accessible.

As part of the method or protocol to enable access to the issuer profile, a receiver database comprising receiver profiles is stored on the server. This database can be completed with issuer profiles previously designated by the issuer and/or fed each time a portable communication device establishes data communication with one of the tags that compose the system, so that, when the connection between the portable communication device and the tag is established, said tag detects, reads or interprets, for example, by means of the receiver code identifying the receiver profile, the receiver profile associated with the portable communication device and transmits it to the server, so that the server compares said receiver profile with the receiver profiles stored in the receiver database and, based on the comparison, provides access to the issuer profile and/or to the subdirectory if said subdirectory has been selected for access, and/or to the confidential subdirectory if it has been selected for access.

Alternatively, the issuer profile is associated with the receiver profile, such that updates to said issuer profile are accessible by the associated receiver profile. That is, the server stores an access permission associated with a particular receiver profile, such that changes made by the issuer to the issuer profile can be notified by the server directly to the portable communication device, for example, by means of SMS instant messaging, email or similar, without the need for the portable communication device to establish data communication with the tag. In this case, the access permission can be given by the issuer, i.e., the issuer grants permission for a specific receiver profile to access the issuer profile, wherein this permission is stored on the server and verified by the latter, so that when the issuer profile is updated, a notification or link to the specific issuer profile is sent.

On the other hand, a tag database is available or linked up with the server, this base comprising the tag codes of each tag. It is important to highlight at this point that one same issuer profile can be associated with several tags, sharing the same subdirectories in each one of the tags, or selecting the subdirectories to be accessible by means of the link of each tag.

In alternative situations, the issuer profile is linked up with the tag receiving on the server, by means of SMS messaging, email, instant messaging or similar, the tag code to be linked up with the issuer profile. This is done in the event that, for example, the issuer does not physically have the tag to which it is

going to associate the issuer profile thereof, or, for example, to verify that the tag is one of the tags intended for being part of the system and/or for being able to associate with the issuer profile on the server.

5 Alternatively, the portable communication device comprises a plurality of receiver profiles associated with the portable communication device, each one of said receiver profiles having the issuer code thereof, and furthermore, the portable device has a device code, a unique device code, so that there is a portable communication device with a device code, with several receiver profiles, each one with the receiver code thereof, these issuer profiles being 10 able to be selected in the portable communication device, such that, prior to the connection between the portable communication device with the tag, a receiver profile is selected, in the portable communication device, and in the connection status between the tag and the portable device, both the device code and the receiver code selected on the portable communication device are transmitted to 15 the server.

Preferably, the information management carried out by the server is authenticated by means of blockchain; therefore, the creation and storage of the issuer profile, the subdirectories thereof and the confidential subdirectories and the information dumped therein are recorded in blockchain transactions by the 20 server. In the same way, the tags, in particular the tag codes, as well as the receiver profiles, the receiver codes and, optionally, the device code associated with the portable communication device are recorded in a blockchain transaction. The foregoing to give traceability to the information, as well as an added security value to the same. The person skilled in the art will see that 25 technologies analogous to blockchain are equally applicable without departing from the scope of the invention.

As part of the information management system, in preferred embodiments the tags are NFC (Near Field Communication) tags, which, as is known, comprise storage media in which, for example, the link that gives 30 access to the issuer profile is stored or, for example, the issuer profile, one or more subdirectories of said issuer profile are stored. Therefore, in this embodiment, the portable communication device is configured to establish an NFC data connection with the tag in the NFC mode thereof.

The tag can also take the form of other RFID devices known in the state 35 of the art.

Alternatively, the tag is a QR tag, wherein the portable communication device comprises a QR tag scanner application configured to generate a URL get request for a web page in a web browser of the portable communication device; in which the QR tag scanner application is configured to transmit the web page to the web browser of the portable communication device, to access the issuer profile stored in the server, and further access the subdirectory and/or the confidential subdirectory, if said subdirectories have been selected for access.

It is important to highlight that, in alternative embodiments, the creation and storage of the issuer profile on the server is carried out by means of identity verification methods such as OCR, document verification, biometric facial recognition technology, Artificial Intelligence and Machine Learning, Cloud computing, among others, which can be carried out by third parties and, when the identity of the issuer has been verified by means of any of these methods, the issuer profile is created. This is done in order to prevent the creation of fraudulent issuer profiles, identity theft and/or similar crimes.

In embodiments of the management system of the invention, a plurality of tags are arranged in particular spaces of an infrastructure, for example, if the issuer is a hotel and, therefore, has an issuer profile of this establishment, and it can arrange tags at the reception, the restaurant or the pool bar, wherein the issuer profile and/or each subdirectory of said issuer profile is associated with the arrangement of each tag in said particular space of the infrastructure.

Alternatively, an issuer creates and stores relevant information regarding himself in his issuer profile, for example, generally, his name and phone number, and then in a subdirectory his professional information (for example, a link to the LinkedIn profile or the professional website), in another subdirectory his social information (links to Instagram, Twitter, Facebook profiles, etc., respectively) and in the confidential subdirectory, confidential information of the issuer (identification document, bank accounts, passwords, etc.). At the same time, the issuer can choose which subdirectory will be accessible, or the server can, based on the detection of the receiver profile, give access to the appropriate subdirectory.

The computer-implemented method of the invention is implemented as a computer program, smartphone application or the like, which, when executed by the processing unit of the computer or smartphone, causes them to carry out

the method described so far.

The main advantage of the invention is that an issuer, by means of his issuer profile, can transmit information in a differentiated and adjusted way depending on a particular situation or the arrangement of the tag in a particular space of an infrastructure. That is, that the issuer can choose for himself what and with whom he shares information or, preferably, the server can give access to the information recorded in the issuer profile and the subdirectories thereof, based on the identification of the receiver profile that requires the information.

It is also very advantageous that an issuer can associate his issuer profile with multiple tags, it being possible to designate which subdirectory is shown in each tag. Likewise, it is an advantage that one same issuer can create multiple issuer profiles, linking up each issuer profile with one or more tags, being able to share information owned by each issuer profile by means of the tags.

Furthermore, based on the detection of the receiver profile associated with the portable communication device, the server can display personalised information related to the detected receiver profile. This results in an advantage that is reflected in more accurate and usable information on the part of the receiver.

BRIEF DESCRIPTION OF THE FIGURES

The foregoing and other advantages and features will be more fully understood from the following detailed description of some exemplary embodiments with reference to the attached drawings, which are to be considered by way of illustration and not limitation, wherein:

- Figure 1 is a schematic view of an information management system wherein the method of the invention is implemented.

DETAILED DESCRIPTION OF AN EXEMPLARY EMBODIMENT

Numerous specific details are set forth in the following detailed description in the form of examples to provide a thorough understanding of the relevant teachings. However, it will be apparent to those skilled in the art that the present teachings can be practiced without such details.

In a first exemplary embodiment, as seen in Figure 1, the invention, the computer-implemented method, is developed in an information management

system 1, with said system being composed of at least one server 2, one tag, transponder or similar 3, hereinafter tag 3, and one portable communication device 5.

5   The person skilled in the art will obviously see that the server 2 is provided with storage means (not shown) configured to store the information, processing means (not shown) configured to compute and process the information received and/or stored and communication means (not shown) configured to transmit and/or receive information.

10   In this first example, a particular user of information, hereinafter issuer, wishes to share information about himself, among which is without limitation, professional information, information from social networks, etc.

With this in mind, an issuer1 creates an issuer profile 4 that will be stored on the server 2, wherein in the root directory of the issuer profile 4 the most basic information of the issuer1 can be arranged, for example, his full name.
15   The information related to the professional profile of the issuer1, for example, a link to his LinkedIn profile or the website of the company for which he works, or the link to his profile in a job exchange, are stored in a subdirectory 41 of the issuer profile 4, and the information related to his social networks, links to the Facebook, Instagram, Tik Tok profile, etc., are stored in a subdirectory 42, or it
20   is even possible that, for each one of the professional or social profiles, there is a subdirectory, i.e., a subdirectory 41 for a link to LinkedIn, a subdirectory 42 for a link to the job exchange, a subdirectory 43 for the link to Facebook, a subdirectory for the link to Instagram 44, etc., there may be up to 4n subdirectories, wherein the "n" means there is no limitation on the number of
25   subdirectories.

The issuer profile 4 created with its subdirectories 41 to 4n is assigned a name, for example, "issuer1" and stored on the server 2. The issuer profile 4 is associated with an issuer code 40, which generally comprises a link (for example, www.server.co/issuer1) which gives access to the issuer profile 4 on
30   the server 2. The issuer1 can modify the information that he has in his issuer profile 4 at any time. The issuer1 can even create an additional issuer profile 4' with its own subdirectories 41' to 4n'.

Next, a tag 3 is associated, which has a tag code 31, a unique identifier code (for example, "045EDA4A656781"), wherein this tag code 31 generates a
35   unique tag code (for example, "k93kjrjrn334ndnj3") of the tag 3 associated with

the server 2 and it is linked up to a unique link 32, such as a URL link (for example, www.server.co/k93kjrjrn334ndnj3).

Next, the issuer profile 4 is linked up with the tag 3, linking up the issuer code 40, (for example, the link "www.server.co/issuer1") with the tag code 31 and/or with the unique tag code that generates the unique tag link 32 (for example, "www.server.co/k93kjrjrn334ndnj3") so that the issuer1 can decide what content from the issuer profile 4 will be displayed when the unique tag link 32 is accessed (for example, www.server.co/k93kjrjrn334ndnj3, wherein this link 32 can redirect to:

- Nothing: as the issuer1 does not want his issuer profile 4 to be shared at that time.

- To the root directory of the issuer profile 4, wherein there is only basic information.

- To all or a portion of the issuer profile 4: www.server.co/issuer1, the issuer1 may designate that a portion or all of the issuer profile 4, the root directory, and/or the different subdirectories be shown. At this point, and as mentioned in the previous section, the server 2 can also grant access to the issuer profile 4 and to the subdirectories (41... 4n) based on the detection of a portable communication device 5, by means of the tag 3, and the receiver profile 51 associated with said portable communication device 5.

- A link or application: for example, the unique tag link 32 of the tag 3 can be redirected to another app or specific link (for example, an Instagram page https://www.instagram.com/issuer1/?hl=en).

- It is also possible to configure the link 32 to redirect to a cloud storage, in which files and/or documents can be uploaded to be shared, so that a receiver receives a link that takes him to the storage to download the file or document.

Based on all the above, in a particular situation, the issuer1 has just met the receiver1, with whom he wants to share his issuer profile 4. The receiver1, which has a receiver profile 51 associated with a portable communication device 5, brings said portable communication device 5 closer to the tag 3 to establish a data connection with said tag 3, conveniently carried by the issuer1.

The unique tag link 32 opens in the web browser of the portable communication device 5 of the receiver1 (www.server.co/k93kjrjrn334ndnj3) and can access the issuer profile 4 and the subdirectories (41... 4n) previously selected by the issuer 1 for access. Thereby, the issuer1 has full control of the

information shared in the issuer profile 4 and its subdirectories (41... 4n).

Alternatively, for access to the information of the issuer profile 4 to be granted to the receiver1 by the server 2, a receiver database 50 is stored on the server 2 and comprises receiver profiles 51, 5m, 51', 5m', such that, when the data connection is established between the portable communication device 5 of the receiver1 and the tag 3, said tag 3 receives and transmits to the server 2 the associated receiver profile 51 (for example, by means of a receiver code) to the portable communication device 5, it compares said receiver profile 51 with the receiver profiles 51, 5m, 51', 5m' stored in the receiver database 50 and, based on the comparison, provides access to the issuer profile 4 and/or to the subdirectories 41... 4n.

The issuer can previously have receiver profiles 51... 5m in this receiver database 50, granting these receiver profiles 51... 5m from the database 50 access privileges or permissions, so that the server enables access without the need for the issuer's intervention. Furthermore, when the data connection is established with a portable communication device 5, whose receiver profile 51 is not in the receiver database 50, the server 2 stores said receiver profile 51 in the receiver database 50 to subsequently provide access to the issuer profile 4 when a new data connection is established.

In another exemplary embodiment, the issuer1 is a flower company, whose business name is Flowershop1.

Flowershop1 creates an issuer profile 4, entering their username, for example. "Flowershop1". This issuer profile 4 is stored in the link www.server.co/Flowershop1. Flowershop1 can modify the information in their issuer profile 4 at any time. The issuer profile 4 of Flowershop1 can create different subdirectories 41... 4n each one with different links, and even create other additional issuer profiles 4' with their own subdirectories 41'... 4n'. For example, to enter personalised information about each customer who has bought a bouquet, Flowershop1 can create different issuer profiles 4, 4', etc., wherein each one of said issuer profiles 4, 4' is focussed on a client (for example, issuer profile4 for receiver client 1, issuer profile 4' for receiver client 2).

Flowershop1 is going to link up with their issuer profile 4, for example 100 tags 3, 3', etc., where each tag 3, 3' has a unique tag code 31, 31', etc. Each tag 3, 3' has an associated link 32, 32', for example,

www.server.co/6ujgnnj4hsh328 or www.server.co/444gnffns767.

Next, Flowershop1 associates each of their issuer profiles 4, 4', etc., with the link 32, 32', etc., associated with each tag 3, 3', etc., so that Flowershop1 can decide which content each tag 3, 3' will display.

5   The receiver customer 1 has purchased a bouquet, and Flowershop1 attaches a tag 3 on the packaging with an associated link 32 (www.server.co/6ujgnnj4hsh328) which, when the receiver customer 1 establishes data communication with the tag 3, will direct him to an issuer profile 4 of Flowershop1 intended only for the receiver customer 1 to see.

10   The receiver customer 2 has purchased a bouquet, and Flowershop1 attaches a tag 3' on the packaging with an associated link 32' (www.server.co/444gnffns767) which will redirect to the issuer profile 4' of Flowershop1 designed only for the receiver customer 2 to see it.

Therefore, the receiver customers 1 and 2 will open the links 32, 32' that 15   will show different information simultaneously.

In another example, the company Restaurant1 creates an issuer profile 4, with the username "Restaurant1". This issuer profile 4 is saved in the link on the server 2 www.server.co/Restaurant1. Restaurant1 can modify the information of their issuer profile 4 at any time. The issuer profile 4 Restaurant1 20   comprises a plurality of subdirectories 41... 4n', each one provided with different links, and can even create other additional issuer profiles 4', etc.

For example, to enter lunch and dinner menu information, Restaurant1 can create different subdirectories 41... 4n within their issuer profile, wherein the lunch menu is arranged in the subdirectory 41, and the dinner menu in the 25   subdirectory 42.

Restaurant1 is going to link up with their issuer profile 4, for example 10 tags 3, 3', etc., wherein each tag 3, 3' has a unique tag code 31, 31', etc. Each tag 3, 3' has an associated link 32, 32', for example, www.server.co/6ujgnnj4hsh328 or www.server.co/444gnffns767.

30   Restaurant1 associates the ten tags with their issuer profile 4. In a particular arrangement, they place each tag on each one of the ten tables, so that Restaurant1 can decide what content from their issuer profile 4 they will show, for example, the subdirectory 41 will be accessible during the day and the subdirectory 42 will be accessible at night, but not the subdirectory 41.

35   The links 32, 32', etc., of each tag 3, 3' will open to the clients (receivers)

of Restaurant1, which will redirect to the issuer profile 4 of Restaurant1, and will show the information of the subdirectory that has been conceived for access by Restaurant1 according to schedule.

Additionally, Restaurant1 can create and store an additional issuer profile 4' on the server 2, with subdirectories 41'... 4n', wherein this additional issuer profile 4' is designed for another particular space of the infrastructure of Restaurant1. That is, if Restaurant1 is a hotel, the issuer profile 4 is associated with the restaurant, while the additional issuer profile 4' is associated with, for example, the pool bar. In this way, the tags linked up with the additional issuer profile 4' will show relevant information related to the pool bar to the customers.

It is important to highlight that, in any embodiment, the tags 3, 3', etc., comprise storage means 33, 33', etc., to directly provide a file able to be downloaded by the portable communication device 5 in the tag 3, 3', when establishing data communication with any of the tags 3, 3'.

Possible embodiments of the computer-implemented method for managing and transmitting information in an information management system are listed below:

1.   A computer-implemented method for managing and transmitting information in an information management system (1) composed of at least one server (2) provided for storing information, at least one tag (3) provided with a tag code (31), a portable communication device (5) configured to establish a connection with said tag (3), said portable communication device (5) having a receiver profile (51) associated thereto, the method comprising the steps of:

-      storing on the server (2) at least one issuer profile (4), wherein said issuer profile (4) comprises an issuer code (40); and

-      linking up the issuer profile (4) with the tag (3), associating the issuer code (40) with the tag code (31);

the method further comprising the steps of:

-      assigning to the tag (3) a link (32) associated with the tag code (31) which gives access to the issuer profile (4) stored in the server (2); and

-      the issuer profile (4) comprises at least one subdirectory (41), said subdirectory (41) being able to be selected for access;

wherein, in a connection status between the portable communication device (5) and the tag (3), said portable communication

device (5) is prepared to interpret the link (31) of the tag, open said link (31) to access the issuer profile (4) stored in the server (2), and further access the subdirectory (41).

2.   The method according to embodiment 1, comprising a step of:

5 -   storing on the server (4) a receiver database (50) comprising receiver profiles (51, 5m, 51', 5m'), such that, in the connection status between the portable communication device (5) and the tag (3), said tag (3) transmits to the server (2) the receiver profile (51) associated with the portable communication device (5), compares said receiver profile (51) with the receiver profiles (51, 5m, 10 51', 5m') stored in the receiver database (50) and, based on the comparison, provides access to the issuer profile (4) and/or the subdirectory (41).

3.   The method according to any of the preceding embodiments, wherein the issuer profile (4) is associated with the receiver profile (51), such that updates in said issuer profile (4) are accessible by the associated receiver profile (51).

15 4.   The method according to any of the preceding embodiments, wherein the server (2) comprises a tag database (30) in which the tag code (31) of each tag (3) is arranged, such that, in the step of linking up the issuer profile (4) with said tag (3), the issuer profile (4) is linked with the tag, receiving the tag code (31) on the server (2) by means of SMS messaging, email or security messaging 20 authentication.

5.   The method according to any of the preceding embodiments, wherein the portable communication device (5) comprises a plurality of receiver profiles (51 to 5m) associated with the portable communication device (5) and able to be selected in said portable communication device (5), such that, prior to the 25 connection between the portable communication device (5) with the tag (3), a receiver profile (51) is selected in the portable communication device (5).

6.   The method according to any of embodiments 2 to 5, wherein the issuer profile (4) further comprises at least one confidential subdirectory (41c), such that in the connection status between the portable communication device (5) 30 and the tag (3), said tag (3) transmits to the server the receiver profile (51) associated with the portable communication device (5), compares said receiver profile (51) with the receiver profiles (51, 5m, 51', 5m') stored in the receiver database (50) and, based on the comparison, provides access to the issuer profile (4) and/or the subdirectory (41) and/or the confidential subdirectory 35 (41c).

7.   The method according to any of the preceding embodiments, wherein the tag (3) comprises a configured storage means (33), such that in the step of linking up the issuer profile (4) with said tag (3), the issuer profile (4) or at least one subdirectory (41) of said issuer profile (4) are stored in said storage means (33) of the tag (3), wherein, in a connection status between the portable communication device (5) and the tag (3), said portable communication device (5) accesses the issuer profile (4) or the subdirectory (41) stored in the storage means (33) of the tag (3).

8.   The method according to any of the embodiments 1 to 7, wherein the issuer profile (4) and/or the subdirectories (41 to 4p) of said issuer profile (41) are authenticated by means of blockchain, the issuer profile (4) and/or the subdirectories (41 to 4p) being recorded in a transaction in a blockchain by the server (2), and wherein the receiver database (50) is authenticated by means of blockchain wherein each one of the plurality of receiver profiles (51, 5m, 51', 5m') is recorded in a transaction in a blockchain by the server (2).

Possible embodiments of the information management system are listed below:

9.   An information management system (1) comprising at least one tag (3) provided with a link (32) for access to a server (2), this link (32) being interpretable by a portable communication device (5) provided to establish a data connection with said tag (3), and said system comprising means for carrying out the method of embodiments 1 to 8.

10.   The system according to embodiment 9, wherein the tag (3) is an NFC tag and the portable communication device (5) is configured to establish an NFC data connection with said NFC tag.

11.   The system according to embodiments 9 or 10, wherein the link (32) assigned to the tag (3) comprises an encrypted URL code, readable by the portable communication device (5).

12.   The system according to embodiments 10 or 11, wherein the tag (5) is incorporated into a portable communication device.

13.   The system according to embodiment 10, wherein the tag is a QR tag, wherein the portable communication device (5) comprises a QR tag scanner application configured to generate a URL get request for a web page in a web browser of the portable communication device (5); in which the QR tag scanner application is configured to transmit the web page to the web browser of the

portable communication device (5), to access the issuer profile (4) stored in the server (2), and further access the subdirectory (41) and/or the confidential subdirectory (41p), if said subdirectories have been selected for access.

14.   The system according to any of embodiments 9 to 13, wherein a plurality

5   of tags (3, 3') is arranged in particular spaces of an infrastructure, each issuer profile (4, 4') and/or each subdirectory (41, 41') of each issuer profile (4, 4') being associated with the arrangement of each tag (3, 3') in said particular space of the infrastructure.

Next, a possible embodiment of a computer program is listed in which the

10   steps of the method for managing and transmitting information in an information management system are implemented:

15.   A computer program comprising instructions which, when the program is executed by a computer, smartphone, device equipped with processing means or the like, causes said computer to carry out the method of embodiments 1 to

15   8.

Likewise, the invention is envisaged so that more than one portable communication device 5, 5', etc., communicates with the tags 3, 3'. It is even possible that different receiver profiles 51... 5m, 51'... 5m' are configured on one same portable communication device 5, 5', for a receiver to conveniently select

20   the receiver profile 51... 5m, 51'... 5m' to interact with the system and access the issuer profiles 4, 4' stored on the server 2.

In alternative embodiments, each issuer profile 4, 4' has at least one confidential subdirectory 41c, 41c', in which the issuer stores confidential data such as, for example, the national identification document, bank account

25   numbers, passwords, etc., wherein to access this confidential subdirectory 41c, 41c', the issuer grants access permission to a particular receiver profile 51, 51', or the access permission to the confidential subdirectory 41c, 41c' can be done in combination, that is, because the issuer grants the access and, furthermore, the server 2 grants the access by verifying that the receiver profile 51, 51' is in

30   the receiver database 50 or a database provided for this purpose. For even greater security, the receiver profile 51, 51', by means of the portable communication device 5, 5', can send a request for access permission to the server 2, which in turn redirects it to the issuer, so that, if the issuer grants access, access to the confidential subdirectory 41c, 41c' is enabled. Therefore,

35   the confidential subdirectory 41c, 41c' can be accessed because the issuer

previously authorises it, the server authorises it, or the issuer and the server authorise it simultaneously, by means of the request for access by the receiver profile or combinations thereof. This access verification step may be applicable to the subdirectories 41, 41'.

5   Finally, the system 1 comprises a tag database 30, wherein the tag codes 31, 31', etc., of each tag 3, 3', etc. are stored, such that, in the step of linking up the issuer profile 4 with said tag 3, the issuer profile 4 is linked with the tag 3, 3' receiving on the server 2 the tag code 31 by means of SMS messaging, email or security messaging authentication.

10   This enables each tag 3, 3' to be associated with the issuer profile 4, 4' without the tag 3, 3' having to be physically present at the place of the issuer. This feature enables the information of the issuer profile to be shared without taking into account the geographic location of the issuer and/or the tag 3, since the link 32 can be linked up with the tag by means of this messaging, by means

15   of the tag code 31.

CLAIMS

1.   A computer-implemented method for managing and transmitting information in an information management system (1) composed of at least one server (2) provided for storing information, at least one tag (3) provided with a tag code (31), a portable communication device (5) configured to establish a connection with said tag (3), said portable communication device (5) having a receiver profile (51) associated thereto, the method comprising:

-       storing on the server (2) at least one issuer profile (4), wherein said issuer profile (4) comprises an issuer code (40); and

-       linking up the issuer profile (4) with the tag (3), associating the issuer code (40) with the tag code (31);

        the method being characterised by:

-       assigning to the tag (3) a link (32) associated with the tag code (31) which gives access to the issuer profile (4) stored in the server; and

-       the issuer profile (4) comprises at least one subdirectory (41), said subdirectory (41) being able to be selected for access;

        wherein, in a connection status between the portable communication device (5) and the tag (3), said portable communication device (5) is prepared to interpret the link (31) of the tag, open said link (31) to access the issuer profile (4) stored in the server (2), and further access the subdirectory (41).

2.   The method according to claim 1 comprising a step of:

-       storing on the server (2) a receiver database (50) comprising receiver profiles (51, 5m, 51', 5m'), such that, in the connection status between the portable communication device (5) and the tag (3), said tag (3) transmits to the server (2) the receiver profile (51) associated with the portable communication device (5), compares said receiver profile (51) with the receiver profiles (51, 5m, 51', 5m') stored in the receiver database (50) and, based on the comparison, provides access to the issuer profile (4) and/or the subdirectory (41).

3.   The method according to any of the preceding claims, wherein the issuer profile (4) is associated with the receiver profile (51), such that updates in said

issuer profile (4) are accessible by the associated receiver profile (51).

4.   The method according to any of the preceding claims, wherein the server (2) comprises a tag database (30) in which the tag code (31) of each tag (3) is arranged, such that, in the step of linking up the issuer profile (4) with said tag (3), the issuer profile (4) is linked with the tag, receiving the tag code (31) on the server (2) by means of SMS messaging, email or security messaging authentication.

5.   The method according to any of the preceding claims, wherein the portable communication device (5) comprises a plurality of receiver profiles (51 to 5m) associated with the portable communication device (5) and able to be selected in said portable communication device (5), such that, prior to the connection between the portable communication device (5) with the tag (3), a receiver profile (51) is selected in the portable communication device (5).

6.   The method according to any of claims 2 to 5, wherein the issuer profile (4) further comprises at least one confidential subdirectory (41c), such that in the connection status between the portable communication device (5) and the tag (3), said tag (3) transmits to the server the receiver profile (51) associated with the portable communication device (5), compares said receiver profile (51) with the receiver profiles (51, 5m, 51', 5m') stored in the receiver database (50) and, based on the comparison, provides access to the issuer profile (4) and/or the subdirectory (41) and/or the confidential subdirectory (41c).

7.   The method according to any of the preceding claims, wherein the tag (3) comprises a configured storage means (33), such that in the step of linking up the issuer profile (4) with said tag (3), the issuer profile (4) or at least one subdirectory (41) of said issuer profile (4) are stored in said storage means (33) of the tag (3), wherein, in a connection status between the portable communication device (5) and the tag (3), said portable communication device (5) accesses the issuer profile (4) or the subdirectory (41) stored in the storage means (33) of the tag (3).

8.   The method according to any of claims 1 to 7, wherein the issuer profile

(4) and/or the subdirectories (41 to 4p) of said issuer profile (41) are authenticated by means of blockchain, the issuer profile (4) and/or the subdirectories (41 to 4p) being recorded in a transaction in a blockchain by the server (2), and wherein the receiver database (50) is authenticated by means of

5   blockchain wherein each one of the plurality of receiver profiles (51, 5m, 51', 5m') is recorded in a transaction in a blockchain by the server (2).

9.   An information management system (1) comprising at least one tag (3) provided with a link (32) for access to a server (2), this link (32) being

10   interpretable by a portable communication device (5) provided to establish a data connection with said tag (3), and said system comprising means for carrying out the method of claims 1 to 8.

10.   The system according to claim 9, wherein the tag (3) is an NFC tag and

15   the portable communication device (5) is configured to establish an NFC data connection with said NFC tag.

11.   The system according to claims 9 or 10, wherein the link (32) assigned to the tag (3) comprises an encrypted URL code, readable by the portable

20   communication device (5).

12.   The system according to claims 10 or 11, wherein the tag (3) is incorporated into a portable communication device.

25   13.   The system according to claim 10, wherein the tag (3) is a QR tag, wherein the portable communication device (5) comprises a QR tag scanner application configured to generate a URL get request for a web page in a web browser of the portable communication device (5); in which the QR tag scanner application is configured to transmit the web page to the web browser of the

30   portable communication device (5), to access the issuer profile (4) stored in the server (2), and further access the subdirectory (41) and/or the confidential subdirectory (41p), if said subdirectories have been selected for access.

14.   The system according to any of claims 9 to 13, wherein a plurality of tags

35   (3, 3') is arranged in particular spaces of an infrastructure, each issuer profile

(4, 4') and/or each subdirectory (41, 41') of each issuer profile (4, 4') being associated with the arrangement of each tag (3, 3') in said particular space of the infrastructure.

5   15.   A computer program comprising instructions which, when the program is executed by a computer, causes said computer to carry out the method of claims 1 to 8.

ABSTRACT

METHOD, SYSTEM AND COMPUTER PROGRAM FOR MANAGING AND TRANSMITTING INFORMATION

5

The present invention relates to a computer-implemented method for managing and transmitting information in an information management system comprised by a server, at least one tag, a portable communication device that has a receiver profile associated thereto, the method comprising the steps of
10 storing on the server at least one issuer profile, wherein said issuer profile has an issuer code, and linking up the issuer profile with the tag, associating the issuer code with a tag code, the method comprising the additional steps of assigning to the tag a link associated with the tag code that gives access to the issuer profile stored on the server, and the issuer profile comprises at least one
15 subdirectory, said subdirectory being able to be selected for access, wherein the portable communication device visualises the issuer profile by reading the tag link.

FIG. 1