

IMPROVED SCALABLE ARCHITECTURE OF SERVERS PROVIDING ACCESS TO DATA CONTENT

5

FIELD OF THE INVENTION

[0001] The present invention generally relates to the field of computing and communications. More specifically, the invention relates to the access and management
10 of resources using a plurality of servers.

BACKGROUND PRIOR ART

[0002] The access to resources and data stored in servers become nowadays more
15 and more critical, as the amount of data provided to users, and the number of applications using such data increase sharply. In computing, a server is a computer program or device that provides functionality for other programs or devices, called "clients". The computation of a server can be performed on a single device, or distributed across a plurality of devices.

20 [0003] A number of different kinds of server exist, such as database server allowing a client to perform requests and retrieve information from a database, file servers that are intended to store files, mail servers that allow receiving and sending mails, etc...

[0004] A number of servers are intended to provide to clients access to resources. A resource can be any data or information that is stored on a server, to be retrieved by a
25 client in order to be presented to a user. For example, a resource can be a picture that is stored in a server, in order to be sent upon request from a client. Such servers intended to provide access to resources to clients are used in a number of applications. For example, servers dedicated to social networks store large amounts of resources (pictures, videos, posts...) that are sent to clients upon request, to be displayed for
30 example in web browsers or mobile apps.

[0005] Such kinds of servers can also be used for professional applications. For example, the applicant has developed an innovative solution to perform interactive presentations wherein the user performing the presentation can insert interactive content (polls, games...) in a presentation. The content of the presentations can be

stored as a resource in servers, and be retrieved upon request by clients. Such content may comprise for example data to be presented/displayed by the dynamic presentation (images, videos, text...), and/or data collected based on the inputs of users during the execution of the dynamic presentation (e.g. statistics, scores, or the like).

- 5 **[0006]** As the number of clients increases, the amount of data stored in the servers for an application may also increase dramatically. The Quality of Service (QoS) offered by the servers may then get poorer, for a variety of reasons: the bandwidth and/or computing resources of the servers may become insufficient to manage the requests for an increasing number of clients, and the latency to manage the requests of the users
- 10 may increase; when the resources are stored in database that are getting larger, the response time to query a resource in the database may also increase; in case of worldwide clients, if all servers are located in the same location, the clients that are based in a different country, or continent than the servers may also experience high latencies due to the communication times across different countries or continents.
- 15 **[0007]** The term “scalability” designates the ability of a system, or service, to accommodate a growth in the demand, and to be able to preserve its QoS when responding to a higher demand (i.e an increasing number of clients, an increasing number of resources to provide, etc...).

- [0008]** Some server architectures are qualified as “single tenant”, when a specific
- 20 infrastructure is created for each client: for example, each client (or group of clients, for example a company) may be served by a dedicated infrastructure, for example servers and databases that are dedicated for its use only. This solution provides the advantage of ensuring that the data from a client will not be accessed by another client, and to precisely locate data. However, this solution does not achieve very good results in
- 25 terms of scalability. Indeed, the infrastructure related to each client need to be adapted separately, which in the same time hardly allows using quickly additional resource when the resource needs of a client increase, and may result into a waste of resources when the resource needs of a client decrease.

- [0009]** Other architectures of server applications are qualified as “multi tenant”. In such
- 30 architectures, the same infrastructures (servers, storage...) are used for a plurality of clients. This type of architecture is more efficient than single tenant architectures to achieve scalability, because the same resources are used for a plurality of clients, so resources can be allocated dynamically according to the needs of the client. However, in such architectures the data from all clients are stored in the same storage. Therefore,

it is much more difficult to ensure that data from a client will not be accessed by another. Moreover, if a large number of clients are located all over the world, different servers will usually be deployed in different countries/continents in order to serve all clients with a limited latency. In such a case, all data from all clients will be replicated in the different servers all over the world. This is an issue, because this does not allow a precise localization of the data, which is an issue because clients are getting more and more concerned about the physical localization of their data. This also wastes storage resources, because data belonging to a client that is based in a country may be replicated in other countries and continents, wherein they will not be used.

[0010] Therefore, none of existing solutions allows in the same time to provide a unique and universal access to a service, and a fine control of the access and localization of data for each client.

[0011] There is accordingly a need for a device that allows a unique and universal access to a service, while allowing clients to control the access and localizations of their data.

SUMMARY OF THE INVENTION

[0012] To this effect, the invention discloses a first device comprising: a first communication endpoint configured to establish a connection with a user device; an access to one or more first data storages storing: user credentials for a plurality of users; a set of identifiers of resources stored on two or more second data storages accessed respectively by two or more second devices, each identifier in the set having associated therewith access rights, and an identifier of a second communication endpoint of a second device having an access to a second data storage storing the resource; one or more first processing logics configured, upon receiving a request from the user device to access a said resource, said request comprising a said identifier of the resource, to: verify, based on access rights associated with the received resource identifier, if the user has the right to access the requested resource; if a said user associated with said user device has the right to access the requested resource, to send to the user device the identifier of the communication endpoint of the second device having an access to the second data storage storing the resource.

[0013] Advantageously, said one or more first processing logics are configured, upon an authentication request from the user device further comprising a user credential, to authenticate the user associated with said user device based on said user credential and user credentials for the plurality of users.

- 5 [0014] Advantageously, the first device further comprises a third communication endpoint configured to establish a connection with one or more fourth communication endpoints of the one or more second devices.

[0015] Advantageously, the first processing logic is further configured, upon the reception of a resource identifier creation request from one of the second devices, to:
10 create a unique identifier of a resource; associate to said unique identifier of the resource an identifier of said one the two or more second devices, or a second communication endpoint thereof; send to said one the two or more second devices the unique identifier of the resource.

[0016] Advantageously, the one or more first processing logics are further configured to:
15 generate identification data allowing the one or more second devices to identify the user and grant access to the resource, and identification validation data allowing the validation of the identification of the user; send to the user device the identification data.

[0017] Advantageously, the one or more first processing logics are configured, upon a reception, from said second device having an access to the second data storage storing
20 the resource, a request to identify the user comprising said identification data, to: validate the identification of the user based on said identification data and said identification validation data; if the identification is validated, send to said second device a validation of the identification of the user and the right of the user to access the resource.

25 [0018] Advantageously, the one or more first processing logics are configured, upon a reception, from said second device having an access to the second data storage storing the resource, of a request to identify the user comprising said identification data, to send to said second device having an access to the second data storage storing the resource said identification validation data.

30 [0019] Advantageously, the one or more first processing logics are configured, upon the generation of the user validation data, to send to the one or more second devices identification validation data.

[0020] Advantageously, the one or more first processing logics are configured to generate the identification validation data based on the identification data and shared secret keys that are common the first device and the one or more second devices.

5 [0021] Advantageously, the identification data is a token, and the identification validation data is a signature of the token.

[0022] The invention also discloses a method comprising: receiving a request from a user device to access a resource, said request comprising an identifier of the resource; accessing one or more first data storages storing: user credentials for a plurality of users; a set of identifiers of a set of resources comprising said requested resource, said
10 set of resources stored on two or more second data storages accessed respectively by two or more second devices, each identifier in the set having associated therewith access rights, and an identifier of a second communication endpoint of a second device having an access to a second data storage storing the resource; verifying, based on access rights associated with the resource identifier, if a user associated with said user
15 device has the right to access the resource; if the user associated with said user device has the right to access the resource, sending to the user device the identifier of the communication endpoint of the second device having an access to the second data storage storing the requested resource.

[0023] The invention also discloses a computer program product comprising: a non-
20 transitory computer-readable storage medium; and program code stored on the non-transitory computer-readable storage medium that, when executed by one or more processors, causes the one or more processors to: receive a request from a user device to access a resource, said request comprising an identifier of the resource; access one or more first data storages storing: user credentials for a plurality of users; a set of
25 identifiers of a set of resources comprising said requested resource, said set of resources stored on two or more second data storages accessed respectively by two or more second devices, each identifier in the set having associated therewith access rights, and an identifier of a second communication endpoint of a second device having an access to a second data storage storing the resource; verify, based on access rights
30 associated with the resource identifier, if a user associated with said user device has the right to access the resource; if the user associated with said user device has the right to access the resource, send to the user device the identifier of the communication endpoint of the second device having an access to the second data storage storing the requested resource.

[0024] The invention also discloses a first device comprising: an access to one or more first data storages storing: user credentials for a plurality of users; a set of identifiers of resources stored on two or more second data storages accessed respectively by two or more second devices, each identifier in the set having associated therewith access rights, and an identifier of a second communication endpoint of a second device having an access to a second data storage storing the resource; a third communication endpoint configured to establish a connection with one or more fourth communication endpoints of the one or more second devices; a first processing logic configured, upon the reception of a resource identifier creation request from one of the two or more second devices, to: create a unique identifier of a resource; associate to said unique identifier of the resource an identifier of said one the two or more second devices, or a second communication endpoint thereof; send to said one of the second devices the unique identifier of the resource.

[0025] The invention also discloses a method comprising: receiving a resource identifier creation request from one of two or more second devices; accessing one or more first data storages storing: user credentials for a plurality of users; a set of identifiers of a set of resources, said set of resources stored on two or more second data storages accessed respectively by said two or more second devices, each identifier in the set having associated therewith access rights, and an identifier of a second communication endpoint of a second device having an access to a second data storage storing the resource; creating a unique identifier of a resource; associating to said unique identifier of the resource an identifier of said one of the two or more second devices, or a second communication endpoint thereof; sending to said one of the two or more second devices the unique identifier of the resource.

[0026] The invention also discloses a computer program product comprising: a non-transitory computer-readable storage medium; and program code stored on the non-transitory computer-readable storage medium that, when executed by one or more processors, causes the one or more processors to: receive a resource identifier creation request from one of two or more second devices; access one or more first data storages storing: user credentials for a plurality of users; a set of identifiers of a set of resources, said set of resources stored on two or more second data storages accessed respectively by said two or more second devices, each identifier in the set having associated therewith access rights, and an identifier of a second communication endpoint of a second device having an access to a second data storage storing the

resource; create a unique identifier of a resource; associate to said unique identifier of the resource an identifier of said one of the two or more second devices, or a second communication endpoint thereof; send to said one of the two or more second devices the unique identifier of the resource.

5

[0027] The disclosure allows user devices to benefit from a universal and centralized access to a service.

[0028] The disclosure allows a strict separation between the resources belonging to different clients, as well as a strict control of the localization of data.

10 **[0029]** The disclosure allows the successful development of scalable applications.

[0030] The invention allows a reduction of bandwidth and storage needs, as well as a reduction of the latency to obtain a resource.

[0031] In certain aspects, the disclosure allows a reduction of the size of files that are shared between users.

15 **[0032]** In certain aspects, the disclosure allows the creation of new resources while strictly controlling resource access and localization of the newly created resource.

[0033] In certain aspects, the disclosure allows a management of the identification, authentication of users and the access rights of resources in a centralized way, in the universal access point, despite the repartition of the resources in large number of
20 different devices.

BRIEF DESCRIPTION OF THE DRAWINGS

25 **[0034]** The invention will be better understood and its various features and advantages will emerge from the following description of a number of exemplary embodiments and its appended figures in which:

- figure 1 depicts an example of a server configured to identify a user and deliver data upon a request to the user, in the prior art;
- 30 - figure 2 depicts an example of a device in a number of embodiments of the invention;
- figure 3 depicts an example of functional architecture of servers in a number of embodiments of the invention;

- figures 4a to 4c depict respectively 3 flowcharts of user interactions in a number of embodiments of the invention;
- figure 5a to 5e depict exemplary flowcharts for the creation and retrieval of a resource in a number of embodiments of the invention;
- 5 - figures 6a and 6b depict two examples of access to data through servers, in the prior art and in a number of embodiments of the invention respectively;
- figure 7 depicts an example of a method in a number of embodiments of the invention.

10

DETAILED DESCRIPTION OF THE INVENTION

[0035] Figure 1 depicts an example of a server configured to identify a user and deliver data upon a request to the user, in the prior art.

15 **[0036]** The server 100 is either a physical or a virtual machine 110, and is configured to identify a user to grant an access to resources.

[0037] To this effect, the server 100 has access to a database 140 that comprises both data relative to the identification of user, and resources to be accessed. The server runs an identification service that is configured to identify the user upon an identification request, based on relevant data, such as a login and password.

20 **[0038]** The server 100 also runs a manager that comprises user credentials including access rights to the resources. The server 100 is thus able, upon a resource request from the user, to validate if the user has the right to access the resource, and, if it is the case, send the resource back to the user.

25 **[0039]** The server 100 provides a universal access to all the resources for all the users/clients. However, all the resources from all the clients are accessed by the same server. Therefore, it is not possible to physically separate the data belonging to various clients. Moreover, if the service needs to be delivered worldwide, all the data of the database 140 will be replicated to a number of servers worldwide. This results in a waste of storage space, because data from given users that may be consumed in a single
30 country will be uselessly replicated worldwide. Meanwhile, this worldwide replication renders the control of the localization of the data impossible.

[0040] Figure 2 depicts an example of a device in a number of embodiments of the invention.

[0041] In a number of embodiments of the invention, a user device 240 sends requests to access resources. A user device may be any suitable kind of device having communication and processing capabilities. For example, the user device may be a smartphone, a tablet, a personal computer or a smart watch. The resources may be accessed for example using a web browser, or a computer application.

[0042] In the disclosure, the invention will be exemplified by an application, wherein the user device accesses resources allowing the execution of a dynamic presentation. For example, the resources may be pictures, videos, but also dynamic polls or scoring activities. Scoring activities are for example activities that allow obtaining scores based on inputs from the viewers of the dynamic presentation. For example, in the case of polls, the viewers can vote by selecting an item in a limited list, and the votes are collected. Any kind of activity that collects data from users in the course of a dynamic presentation can be inserted. However, the invention is not restricted to these examples, and the invention may be used for allowing a user device to access any kind of resource that may be displayed, played, executed, or more generally processed by a user device 240. For example, the resources may be office files, master files to be used for audio or video processing, etc... More generally, the invention is applicable to any data which is readable by a computer, and any data that can be stored in a binary form.

[0043] As will be explained in more details below, the user device first send a request to access a resource to a first device 200, that provides to the user device 240 the elements necessary to perform a second request to a second device 250 that actually has access to the resource.

[0044] In the disclosure, the resources are located on two or more data storages 280, 281, that are respectively accessed by two or more second devices 250, 251. For example the second device 250 has access to a second data storage 280 storing some of the resources, while the second device 251 has access to a second storage 281 storing other resources.

[0045] The first device 200, and the two or more second devices 250, 251 may be any suitable device comprising having computing and communication capabilities, and having access to storage capabilities. For example, the first device 200, and the two or more devices 250, 251 may be personal computers, or servers. Although only two devices are represented in the figure 2, the invention is applicable to a larger number of second devices. The number of second devices can thus be tailored according to the

resources needs of the users, but also according to operational needs. For example, the second devices may be set for users, and/or dedicated to a country or region.

[0046] The two or more second data storages 280, 281 may be any type of storage suitable to store and retrieve data. For example, the two or more second data 280, 281 storages may one or more of memories, hard drives, optical discs, etc... In the figure 2, the two or more second data storages 280, 281 are represented in the two or more second devices 250, 251 respectively. However, although the two or more second data storages 280, 281 may be located in the one or more second devices 250, 251, the invention is not restricted to this example. For example, some or all of the two or more second data storages 280, 281 may be shared hard drives to which the two or more second devices 250, 251 respectively have access, may belong to shared databases, or may be located in devices connected to the two or more or more second devices 250, 251. For example, the disclosure is applicable to server farms, wherein the data is stored on shared hard disks/database. However, this does not restrict the ability of the invention to define precisely the localization of data, and to strictly separate data belonging to different clients. Indeed, a set of devices associated to one or more second data storages, for example a server farm, can be dedicated to a single client.

[0047] The first device 200, and the second devices 250, 251 respectively comprise a first communication endpoint 210, and second communication endpoints 260, 261 adapted to establish a connection with the user device 240. The second communication endpoints 260, 261 may be for example a WAN connection or communication ports. According to various embodiments of the invention, the second communication endpoints 260, 261 may comprise any means allowing a communication with the user device 240, such as a TCP/IP port.

[0048] The first device 200, and the second devices 250, 251 also respectively comprise processing logics 230, 231, 270, 271. In the course of the disclosure, a processing logic may be a processor operating in accordance with software instructions, a hardware configuration of a processor, or a combination thereof. It should be understood that any or all of the functions discussed herein may be implemented in a pure hardware implementation and/or by a processor operating in accordance with software instructions. It should also be understood that any or all software instructions may be stored in a non-transitory computer-readable medium. Accordingly, a plurality of processing logics of the same device may be for example different processors, a same

processor configured to execute different instructions, or a plurality of computer instructions to configure one or more processors.

5 [0049] The repartition of the resources among the second data storages 280, 281 accessed by the second devices 250, 251 may be performed according to different rules. For example, each client or company may have its own second devices to store its resources; devices and storages may be defined for each country, etc... The disclosure thus advantageously allows a complete separation of the resources of each client, country, etc... into different storages accessed by different second devices, and thus ensures a complete separation of the resources of the different clients according to 10 the client needs. Moreover, since each client is able to precisely define the devices wherein its resources are stored, the disclosure allows a precise definition of the localization of data. For example, the disclosure allows each client to ensure that its resources are stored in its own country (i.e resources belonging to a French client in France, resources belonging to a German client in Germany, etc...).

15 [0050] This ability is very important for clients storing strategic or confidential data, as the concerns about data ownership and localization is growing. Moreover, the localization and protection of data is now also a legal issue, as exemplified by the European Regulation (EU) 2016/679 or General Data Protection Regulation. The disclosure, by allowing users and clients to efficiently control the localization and access 20 rights of resources may thus help them to comply with legal requirements relative to the protection of data.

[0051] The first device has also access to one or more first data storages 220. As already explained with reference to the second data storages 280, 281, the first data storages 220 may be located within the first device 200, or within a device in connection 25 with the first device.

[0052] The first data storages 220 store user credentials for a plurality of users. The user credentials may comprise a variety of data comprising personal data of users (name, mail address, etc...), data allowing the authentication of users, and data defining the resources the user are entitled to access. The data allowing the authentication of a 30 user can take any suitable form, such as hash allowing verification that the secret code entered by the user is correct. The data allowing the authentication can also be an access code. The access code is a secret code generated on demand to access a single resource, or a limited set of resources. The access code is useful when a registered user wishes to perform a dynamic presentation that requires resources to be

accessed by unregistered users: an access code can be generated that grants access only to a single resource, or a limited set of resources that are required by the dynamic presentation. Therefore the unregistered users can view the dynamic presentation successfully. The access code can have an expiration deadline in order to allow the
5 unregistered user to access the resources only when the dynamic presentation is intended to be performed (for example, for one day, one week, etc...).

[0053] As noted above, the first data storages 220 also store data defining the resources a user is entitled to access. This data can take different forms.. For example, it may be a list of identifiers of resources that the user has the right to access. According
10 to various embodiment of the invention, the access rights with respect to resources may be defined in different ways. For example, a user may be granted access to a defined resource through an access code. It is also possible to define environment that encompass a large number of resources. In the dynamic presentation framework of the applicant, such an environment is named a "universe". This naming will be adhered to in
15 the remaining of this disclosure, even though other names may be given to such kind of environments. For example, a company may define its own universe, and a user (for example an employee of the company) having access to the universe may have access to all the resources belonging to the universe.

[0054] The one or more first data storages 220 also store a set of identifiers of
20 resources: each resource is associated with a unique identifier that allows retrieving the resource unambiguously.

[0055] Each identifier of a resource has associated therewith access rights defining the users that are entitled to access the resource. The access rights can be defined in different ways. For example, the access right may explicitly define, for each resource, a
25 list of users having access to the resource. The access rights may also be associated indirectly to the resource: for example, a resource may be defined as belonging to the universe of a company, and access rights may be associated to this universe. For example, only the employee of a company may have access to the resource belonging to the universe of the company. More generally, access rights can be defined to groups
30 of resources.

[0056] Each identifier of a resource is also associated to an identifier of a second communication endpoint 260, 261 of a second device 250, 251 having an access to a second data storage 280, 281 storing the resource. According to various embodiments of the invention, such identifier may be any identifier allowing a user device 240 to

initiate a connection with the second device. For example, the identifier may be an URL or an IP address allowing the initiation of a connection to the second device. The identifier of the second communication endpoint of the second device therefore allows an identification, among all second devices, of the one that is able to grant access to the resource. As for the access rights, the identifiers of the second communication endpoints may be associated to the identifier of the second resource in different ways. For example, it can be associated directly by defining, for a given identifier of a resource, the identifier of the second communication endpoint 260, 261 of the second device 250, 251 having an access to a second data storage 280, 281 storing the resource. It may also be associated indirectly. For example, a second communication endpoint 260, 261 may be associated to a universe. Therefore, if a resource belongs to a universe, it is associated to the second communication endpoint 260, 261 associated with the universe. This allows defining a single communication endpoint for all resources belonging to a universe, for example of resources to be used by a company.

5 10 15 20 25 30

[0057] According to various embodiments of the invention, the resource identifiers can be stored in different ways. For example, a unique resource identifier can be stored for each resource, so that the one or more data storages 220 store an exhaustive list of all the resources. Alternatively, an identifier of a resource can be formed of a general identifier (for example an identifier of a second device, server, universe...), and a unique identifier of the resource depending on the general identifier. An example of such a kind of identifier may be an url comprising the address of one of the second devices, then a unique identifier of the resource. In such an example, the second communication endpoint 260, 261, and access rights may be associated to the general identifier.

[0058] In order to retrieve a resource, the user device 240 can perform a request to the first device 200. The request comprises the identifier of the resource to access.

[0059] Upon the reception of the request, the one or more first processing logics 230 are configured to verify, based on access rights associated with the resource identifier, if the user has the right to access the resource. This can be performed in any suitable way, such as a verification whether the user belongs to user accounts having access to the resource, or the user having access to the universe the resource belongs to.

[0060] If the user has the right to access the resource, one or more first processing logics 230 are configured to send to the user the identifier of the communication

endpoint of the second device having an access to the second data storage storing the resource.

[0061] For example, if the resource is located in the second storage 280, the one or more first processing logics 230 are configured to send to the user device 240 an identifier of the second communication endpoint 260 allowing the user device to connect to the second device 250. Respectively, if the resource is located in the second storage 281, the one or more first processing logics 230 are configured to send to the user device 240 an identifier of the second communication endpoint 261 allowing the user device to connect to the second device 251. This allows the user device to establish a communication with the second device that is able to deliver the desired resource.

[0062] In a number of embodiments of the invention, the user device 240 is directly redirected to the relevant second device, so that the user is not even aware that connections with different devices are used.

[0063] Therefore, the user device 240 communicates with a single entry point (in this example, the first user device 200) that provides access to the relevant second user device. This allows all the user devices to benefit from a universal and centralized access to a service.

[0064] Meanwhile, the allocation of resources across different second devices allows a strict separation between the resources belonging to different clients, as well as a strict control of the localization of data.

[0065] The storage and computation capabilities of the second devices can be tailored for each client according to its needs. This architecture therefore allows the successful development of scalable applications.

[0066] The localization of data among the second devices can also be set in order that the resources of each client are located as close as possible to the offices of the client, or more generally the places where they will be consumed. The closeness between the resources and the clients diminish the bandwidth needs, and the latency to obtain a resource. Meanwhile, it is not required to duplicate all the resources in multiple locations, if not all over the world, as in multi-tenant architectures. The architecture displayed in figure 2 therefore reduces the storage needs.

[0067] In a number of embodiments of the invention, the first device 200 comprises a processing logic 231 configured to authenticate a user upon an authentication request from the user device 240. Such authentication request may comprise user credential, and any suitable means to perform authentication can be used. For example,

authentication methods using a login and a password may be used. According to various embodiments of the invention, the processing logic 231 may be for example the same processor as the first processing logic 230, operating with different instructions, or another processor of the first device 200.

5 [0068] As will be explained in more details hereinafter, in a number of embodiments of the invention, the first device 200, and the one or more second devices 250, 251 need to communicate, for example exchange authentication information relative to a user. To this effect the first device 200 may comprise a third communication endpoint 211, and the one or more second devices 250, 251 may comprise respectively one or more fourth
10 communication endpoints 290, 291 that are configured to establish a connection with the third communication endpoint 211. Therefore, the first device 200, and the one or more second devices 250, 251 are able to communicate directly to exchange information relative to identification and/or authentication of user, as will be explained in grater details with reference to figures 5c to 5e.

15

[0069] Figure 3 depicts an example of functional architecture of servers in a number of embodiments of the invention.

[0070] A first server 300 may be the first device 200 acting as a physical server, or a virtual server running on a virtual machine (VM) 310 running on the first device 200. The
20 first server serves as a unique universal access point for users to identify themselves and request resources.

[0071] A second and third server 301 and 302 may be respectively either the second devices 250 and 251, or VMs 311, 312 running on the second devices 250 and 251 respectively. The second and third servers actually store and deliver resources to the
25 users. A larger number of servers may be used to store and deliver the resources, but only a single server, the first server 300, serves as a universal access point for the users to identify themselves and initially request resources.

[0072] The first server 300 has access to a database 340 that stores identification data for the user, resources identifiers, resource access rights, and data relative to the
30 servers storing the resources. The second server 301, and third server 302 have access respectively databases 341, 342 actually storing resources.

[0073] Upon a resource request from a user, the first server 300 redirects the user to the second server 301, or the third server 302, depending on the server that has access to the resource.

[0074] Therefore, contrarily to the prior art solutions as exemplified in figure 1, the resources owned by various users are located in different servers. Therefore, their location can be controlled, and there is no risk that the data belonging to a user is accessed by another. Meanwhile, the user benefit from a unique and universal access
5 to the service.

[0075] Figures 4a to 4c depict respectively 3 flowcharts of user interactions in a number of embodiments of the invention.

10 [0076] The figure 4a displays a flowchart of an example of an identification of a user, and access to a resource.

[0077] As noted above, a user may have access to a plurality of universes, or environments/platforms, each universe being controlled by at least one of the one or more second devices 250, 251. A universe may for example correspond to any
15 coherent group of resources, for example a company, an application, a country, etc...

[0078] In this example, the user (more specifically the user device 240) sends a connection request to the first device 200. The user is initially not identified. The first device 200 thus authenticates the user, and creates a cookie token of authentication of the user. The user is then redirected to the second device 250, that is the default
20 platform of the user.

[0079] The user device 240 then sends a request to access the platform of the second device 250. If it is not possible to identify the user based on the cookie, the user is redirected to the first device 200; if it is possible to identify the user, an environment of the user is displayed to the user, so that the user is able to request and display
25 resources.

[0080] The figure 4b displays a flowchart of an example of an access to a resource.

[0081] The user (more specifically the user device 240) first send a resource request to the first device 200 using the identifier of the resource. In this example, the first device
30 200 is a server running an access service. Once the existence of the resource, and the right of the user to access the resource is validated, the user is redirected to the platform having access to the resource, in this example the second device 250.

[0082] The user device 240 thus sends a resource request using the identifier of the resource to the second device 250. The second device 250 validates the access to the

resource, and sends the resource back to the user device 240, so the resource can be displayed to the user.

[0083] The figure 4c displays a flowchart of an example of platform switch.

5 **[0084]** In some cases a user may wish to access a platform that is different from the platform he/she is logged into. For example, the user may wish to access a platform having access to resources of another application, for example another second device 251 of the one or more second devices 250, 251. To this effect, the user device 240 sends a request to switch to another platform, for example the second device 251. The
10 request comprises the cookie, and the second device 251 performs an identification of the user from the cookie, and displays the content of the new platform.

[0085] Figures 5a to 5e depict exemplary flowcharts for the creation and retrieval of a resource in a number of embodiments of the invention.

15

[0086] The figures 5a to 5e represent the user device 240, first device 230, the second device 250, and, for the figures 5c to 5e, the second device 251. However these are represented by means of example only and the examples of figures 5a to 5e can be implemented with any device in which the invention may be implemented.

20 **[0087]** In the examples of figures 5a to 5e, the first device 240, and second devices 250 and 251 may be for example physical and/or virtual servers that are configured to provide to the user device resources needed by an application, for example and application to perform dynamic presentations.

25 **[0088]** Figure 5a depicts an exemplary flowchart of the creation of a resource in a number of embodiments of the invention.

[0089] As explained with reference to figures 4a to 4c, the user can be connected to a second device 250 that provides to the user an environment comprising the resources needed for a context, such environment being also called a "universe". According to
30 various embodiments of the invention, the user may have already been connected to the second device 250, because it requested a resource that the second device 250 has accessed to and/or because the second device 250 provides to the user his/her default universe. By means of example, the figure 5a will be exemplified with the second device

250. However this is provided by means of example only and this example may be implemented for any of the second devices of the invention.

[0090] The user of the user device 240 wishes to create a new resource. For example, the user may have created a dynamic content (ie. A poll, game, etc...) for a dynamic presentation, and wishes to store this content online for a future use, and/or allowing
5 other users to access the content when viewing the dynamic presentations.

[0091] To this effect, the user device 240 sends a resource creation request 510a to the first device 250. The resource creation request may contain for example the content that the user wants to convert into a resource.

10 [0092] Upon reception of the resource creation request 510a, the second processing logic 270 is configured to generate a resource identifier generation request 520a, that is sent to the first device 200 through the fourth communication endpoint 290. The resource identifier generation request is a request to generate a resource identifier (or id) for a newly created resource.

15 [0093] Upon reception of the resource communication request 520a, the first processing logic 230 creates the resource identifier corresponding to the content. The resource identifier needs to be unique. Provided that this requirement is fulfilled, a number of different methods may be used to generate a unique resource identifier: a resource identifier to attribute can be incremented at each resource identifier request;
20 the resource identifier may be created based on unique parameters such as an id of the second device 250, and the number of request that have been received from the second device 250, etc... Any suitable embodiment to generate a unique resource id is applicable to the invention. For example, the unique resource identifiers may be generated using random or pseudo-random generation methods using a limited set of
25 characters. The set of characters may comprise alphanumeric characters (letters + digits). In a number of embodiments of the invention, the set of characters does not comprise the alphanumeric characters that may are subject to errors of interpretation when read/entered by the users (for example 0 or O; 1 or l), in order to reduce the probability that a user enters an incorrect access code.

30 [0094] The identifier of the resource is then stored 530a on the one or more data storage 220. A data representative of the second device 250 which has access to the resource and/or the second communication endpoint 260 need also to be stored in the one or more data storage 220, and associated to the resource identifier. This data may have many different types (an id of the second device 250, a descriptor or identifier of

the second communication endpoint 260...). This allows a direct or indirect association between an identifier of the second communication endpoint 260 and the identifier of the resource. This identifier can be sent to user devices upon resource request, as will be explained in more details hereinafter. The storage and association of data in the one or more data storage 220 may be performed in many different ways, provided that the data can be stored and retrieved. For example, the data can be stored in files having a defined format (e.g. tables), or in databases. In a number of embodiments of the invention, the resource identifier is generated depending on an identifier of the second device 250, or second communication endpoint 260. For example, the resource identifier may be an url of the second communication endpoint 260, followed by a unique identifier of the resource. In such a case, the unique identifier of the resource does not need to be stored in the first data storages 220, because the first device 200 is able to redirect, based on the resource identifier, a user to the second device 250.

[0095] According to various embodiments of the invention, other data may be associated to the resource identifier, such as a descriptor of the resource, a resource type, of access rights to the resource, either directly or indirectly (for example if access rights are associated to all resources accessed by the second device 250).

[0096] The resource identifier is then sent back 540a to the second device 250, thereby acknowledging that the resource identifier has been successfully created.

[0097] Upon reception of the resource identifier, the second processing logic 270 is configured to store 550a the resource identifier, and the associated content to the one or more second data storages 280. Here again, any suitable means for storing the resource identifier and content, and associate them may be used within the invention.

[0098] The resource is therefore created, and the resource identifier is sent 560a to the user device 240. The user can thus use the resource freely, and share content comprising the resource easily. The resource can be simply added by specifying the unique resource identifier which, as will be explained below, will allow other users to retrieve the resource. For example, if the resource is a dynamic content in a dynamic presentation, a presentation file can be created in the user device 240 that comprises the corresponding unique resource identifier. When the user shares the dynamic presentation file to other users, the user devices of the user device can, using the unique resource identifier, retrieve the resource from the second device 250, as will be explained in more details below.

[0099] This example demonstrates the ability of the invention to create new content, and share easily the content with other users. As the content is stored in the one or more second data storage 280, only the resource identifier needs to be shared within user. This can advantageously reduce the size of files shared within user, if the resource represents large content (for example videos). Moreover, at each resource creation, the first device 200, that provides universal access, only knows that a new resource is created, but does not have any knowledge of the actual content of the resource. Meanwhile, the resource is actually created by the second device 250 that provides a secured access to a universe the user belongs to. The control of data access and data localization is therefore preserved at each resource creation.

[00100] Figure 5b depicts an exemplary flowchart of the retrieval of a resource in a number of embodiments of the invention.

[00101] In this example, a user device 240 performs a request to obtain a resource, without any a priori knowledge of the location of the resource. Such a case typically arises when a user device is using a file, or content sent by another device. For example, the user device 240 can be viewing a dynamic presentation created by another user, and comprising dynamic content. The dynamic presentation is read in the form of a dynamic presentation file, wherein the resources are identified by their identifier. The user device 240 therefore needs to retrieve the resource based only on the resource identifier, without any a priori knowledge of the location of the resource.

[00102] To this effect, the user devices sends to the first device 200 a resource access request 500b comprising the identifier of the resource.

[00103] Upon reception of the request, if the user is not already logged in, the processing logic 231 identifies the user. The invention allows different methods for identifying a user. For example, the user may be a registered user having a login and a password. The registered user may then be entitled to have access to certain resources. The access to resources may be granted in different ways. For example, it may be granted individually for certain resources and/or the user may have access to all or a part of the resources belonging to a universe.

[00104] Another option consists in generating an "access code" that allows an unregistered user to have access to one or more specific resources. The use of an access code provides a flexible option to grant access to specific resources to unregistered users. For example, if a registered user of a company wishes to perform a

dynamic presentation to unregistered user that belong to another company (for example, business clients, it may generate access codes granting to the unregistered users an access to the resources required by the dynamic presentation).

5 [00105] Upon reception of the resource access request 500b, the processing logic 231 identifies 510b the user, for example using a login and password, or an access code.

10 [00106] The request is then forwarded 520b to the processing logic 230, which retrieves from the one or more data storages 280, based on the identifier of the resource, the location of the resource, that is to say an information indicating the second device that has access to the resource. In this example, the resources can be retrieved by the second device 250. The processing logic 230 also verifies, based on the access rights associated with the identifier of the resource, and user credentials of the user, if the user has the right to access the resource.

15 [00107] If the user has the right to access the resource, an identifier of the second communication endpoint 260 of the second device is transmitted 540b to the user. As noted above, this identifier may be any information allowing the user device 240 to establish a connection with the second device 250: an IP address, and URL, a name of a server, etc... The user device may also be redirected to the second device 250. The redirection can be for example implemented if the resources is accessed through a web browser. The redirection allows the user to have access to information without even
20 knowing that he/she is now in connection with a new server.

[00108] The user device then sends a new request 550b to access the resource, to the second device 250.

[00109] The processing logic 270 locates the resource in the one or more data storage 280 based on the resource identifier, and returns 570b the resource to the user.

25 [00110] This example demonstrates the ability of the invention to deliver resources to users using a single access point for an application, even if the user only knows the resource identifier, and does not have any a priori knowledge about the actual location of the resource.

30 [00111] Figure 5c depicts an exemplary flowchart of the retrieval of a resource in a number of embodiments of the invention.

[00112] In this example, a user device 240 performs a request to obtain a resource, without any a priori knowledge of the location of the resource. In addition, in order to

secure the identification of the user by the second device, the first device delivers to the users a token that is used for the identification by the second device.

[00113] The user sends a resource request 500c to the first device 200.

5 **[00114]** The processing logic 231 fails to identify the user, for example because the user is not already connected/logged in when he/she is performing the resource request.

10 **[00115]** An identification request 520c is thus sent to the user device. The user device 240 sends 530c the user credentials accordingly. The processing logic 231 authenticates the user based on the credentials, and the credentials for all users stored in the one or more first data storages 220, and generates a unique token associated to the user, for future identification, as well as a token signature to validate the identification of the user. The token is sent 550c to the user device 240, as well as an identifier of the second communication endpoint 260 of the second device 250 that has access to the resource.

15 **[00116]** The user device 240 then sends a new resource request 560c to the second device 250, comprising the identifier of the resource, and the token. The processing logic 2100 of the second device 250 tries to identify the user based on the token, but does not have the information allowing it to identify the user.

20 **[00117]** The processing logic 2100 is then configured to send a request 580c to validate the identification of the user based on the token to the first device 200. The first device validates the identification of the user based on the token, and sends back to the second device 250 user credentials. Alternatively, the signature can be sent to the second device 250, so that the processing logic 2100 is able to validate the identification based on the token.

25 **[00118]** The user is then successfully identified by the second device, and the second device sends 590c the resource back to the user.

30 **[00119]** According to various embodiments of the invention, the second device 250 may request the first device to validate the identification of the user upon each resource request by the user device. It may also request the validation of the user identification once, and store data allowing it to identify the user directly at the next resource request from the user device 240.

[00120] In this example, the user is identified using a token. However, other identification data, such as cookies, may be used. More generally, the principle described in figure 5c is applicable to any identification system that rely on identification

data for each user (in this example, the token), and identification validation data that allows validating the identification (in this example, the signature of the token). The invention allows the first device 200 to send to the user device the identification data allowing it to identify itself to the second device, and, when receiving a request from the
5 second device comprising the same identification data, confirm to the second device 250 that the user is entitled to access the resources using the identification validation data, or send the identification validation data to the second device 250, so that the processing logic 2100 is able to validate the identification.

[00121] This example demonstrates the ability of the invention to manage the
10 identification, authentication of users and the access rights of resources in a centralized way, in the universal access point, despite the repartition of the resources in large number of different devices.

[00122] Figure 5d depicts an exemplary flowchart of the retrieval of a resource in a
15 number of embodiments of the invention.

[00123] The example of figure 5d is very similar to the example of figure 5c. The only difference is that, in order for the second device to validate the identification of the user, the first device sends 580d to the one or more second devices 250, 251 the identification validation data.

[00124] For example, if the user is identified using a token, the first device 200 sends to
20 the one or more second devices 250, 251 the signature of the token, so that the one or more second devices can validate the identification; if the user is identified using a cookie, the first device 200 sends to the one or more second devices 250, 251 any data necessary to validate that the session associated with the cookie is valid (i.e session id,
25 and, in some implementations, associated security data such as IP address of the user device 240). A man skilled in the art will easily identify the identification validation data depending on the identification technique used (for example token or cookie).

[00125] Therefore, the first device 200 sends to the one or more second devices 250,
251 all the information necessary to securely identify a user, without the one or more
30 second devices 250, 251 having to send a request to the first device 200. Therefore, the identification of the user by the one or more second devices 250, 251 becomes quicker.

[00126] According to various embodiments of the invention, the transmission 580d of the identification validation data may be performed in different ways. For example, the data can be sent for a user, each time a user is identified in the first device 200, and the

corresponding identification data is created. Therefore, the one or more second devices 250, 251 are virtually immediately able to identify the user.

[00127] The identification validation data may also be sent to the one or more second devices 250, 251 on a periodic basis, for a plurality of users, in order to limit the communication between the first device 200, and the one or more second devices 250, 251 and thus save bandwidth.

[00128] However, in this case, the second device 250 may not have identification validation data, when the user device 240 sends the resource request 560c. In order to solve this issue, the second device 250 can, in case it does not have the identification validation data, send a request to the first device to obtain this data. Therefore, this allows saving bandwidth while allowing, in all cases, the user to connect to the second device 250 to access the resource.

[00129] Figure 5e depicts an exemplary flowchart of the retrieval of a resource in a number of embodiments of the invention.

[00130] The example of figure 5e is very similar to the example of figure 5c. The only difference is that, in order that the second device validates the identification of the user, the identification validation data is packaged with the identification data. The identification validation data is generated using the identification data, and shared secret keys 500e that are shared between the first device 200 and the one or more second devices 250, 251. The secret keys 500e also allow the processing logics 2100, 2101 to validate that the identification validation data is correct, and therefore successfully identify the user. This can be performed for example using signed token, that comprise a token (identification data) and a signature (identification validation data) generated using the shared private keys 500e. Therefore, the validity of the signature can be verified using the same shared keys 500e. If the validity of the signature is correct, the user is identified.

[00131] This advantageously allows a secure identification, without needing to exchange data directly between the first and one or more second devices 200, 250, 251, once the shared keys 500e are known by the devices.

[00132] Figures 6a and 6b depict two examples of access to data through servers, in the prior art and in a number of embodiments of the invention respectively.

[00133] Figure 6a depicts an example of access to data through servers, in the prior art.

[00134] The users 610a, 611a, 612a, 613a and 614a, which are located all over the world, connect to the server 600a to obtain the resources they need for their applications. All the resources are stored on the server 600a, that sends back, upon the requests from the users, the resources they need. This solution suffers from a number of drawbacks: as depicted in figure 6a, the requests and data exchanges may be performed between very distant locations. This consumes bandwidth, and generates a high latency between the time a user sends his/her request, and the time the resource is received. Moreover, all the resources are located in the same server. This may cause a security issue, because it is very difficult to ensure that resources that belong to one of the users will not be accessed by others.

[00135] Figure 6b depicts an example of access to data through servers, in a number of embodiments of the invention.

[00136] The users 610b, 611b, 612b, 613b and 614b, which are located all over the world, connect to the server 600b, which serves as a universal access to the resources. However, the resources are not stored by the server 600b, but by servers 620b, 621b, 622b. The server 600b redirects the users to the servers storing the resource they need:

- the user 610b is redirected to the server 620b;
- the users 611b and 612b are redirected to the server 621b;
- the users 613b and 614b are redirected to the server 622b.

[00137] Therefore, the resources can be located in a location nearer to the user: the latency of exchanges to obtain the resources is reduced. Moreover, servers can be set up according to the needs of the users. For example, it is possible to set up a server for a single client, thereby allowing a strict enhancement of the security of the data.

[00138] Figure 7 depicts an example of a method in a number of embodiments of the invention.

[00139] The method 700 comprises a first step of receiving 710 a request from a user device to access a resource, said request comprising an identifier of the resource.

[00140] The method 700 further comprises a second step 720 of accessing one or more first data storages storing:

- user credentials for a plurality of users ;

- a set of identifiers of resources stored on two or more second data storages accessed respectively by two or more second devices, each identifier in the set having associated therewith access rights, and an identifier of a second communication endpoint of a second device having an access to a second data storage storing the resource.

[00141] The method further comprises a third step 730 of verifying, based on access rights associated with the resource identifier, if the user has the right to access the resource.

[00142] The method 700 further comprises, if the user has the right to access the resource, a fourth step 740 of sending to the user device the identifier of the communication endpoint of the second device having an access to the second data storage storing the resource.

[00143] All the embodiments discussed below are respectively applicable to the method 700.

[00144] The invention may be also implemented as a computer program configured to verify if a user has the right to access a resource, and send to a user device an identifier of a communication endpoint of a device that has access to the resources. Such a computer program may receive requests from a user device, and process the request accordingly. The embodiments described with reference to figures 2, 3 4a to 4c, and 5a to 5e are respectively implementable by such computer program, in order to grant access of resources to users.

[00145] The program code embodied in such computer program is capable of being individually or collectively distributed as a program product in a variety of different forms. In particular, the program code may be distributed using a computer-readable storage medium having computer-readable program instructions thereon for causing a processor to carry out aspects of the embodiments of the invention.

[00146] In certain alternative embodiments, the functions, acts, and/or operations specified in the flow charts, sequence diagrams, and/or block diagrams may be re-ordered, processed serially, and/or processed concurrently consistent with embodiments of the invention. Moreover, any of the flow charts, sequence diagrams, and/or block diagrams may include more or fewer blocks than those illustrated consistent with embodiments of the invention.

[00147] While all of the invention has been illustrated by a description of various embodiments and while these embodiments have been described in considerable detail, it is not the intention of the Applicant to restrict or in any way limit the scope of the appended claims to such detail. Additional advantages and modifications will readily appear to those skilled in the art.

5

CLAIMS

1. A first device (200) comprising:
- 5 - a first communication endpoint (210) configured to establish a connection with a user device (240);
- an access to one or more first data storages (220) storing:
- user credentials for a plurality of users;
- a set of identifiers of resources to be presented to one or more users
- 10 belonging to said plurality of users stored on two or more second data storages (280, 281) accessed respectively by two or more second devices (250, 251), each identifier in the set having associated therewith access rights, and an identifier of a second communication endpoint (260, 261) of a second device (250, 251) having an access to a second data storage (280,
- 15 281) storing the resource;
- one or more first processing logics (230, 231) configured, upon receiving a request (500b, 500c) from the user device (240) to access a said resource, said request comprising a said identifier of the resource, to:
- verify, based on access rights associated with the received resource
- 20 identifier, if the user has the right to access the requested resource;
- if a said user associated with said user device (240) has the right to access the requested resource, to send (540b, 560c) to the user device (240) the identifier of the communication endpoint (260) of the second device (250) having an access to the second data storage (280) storing the resource.
- 25
2. The first device (200) of claim 1, wherein said one or more first processing logics are configured (231), upon an authentication request from the user device further comprising a user credential, to authenticate the user associated with said user device based on said user credential and user credentials for the plurality of
- 30 users.
3. The first device of one of claims 1 or 2, further comprising a third communication endpoint (211) configured to establish a connection with one or more fourth

communication endpoints (290, 291) of the one or more second devices (250, 251).

- 5 4. The first device of claim 3, wherein the first processing logic (230) is further configured, upon the reception of a resource identifier creation request (520a) from one of the second devices (250), to:
- create a unique identifier of a resource;
 - associate to said unique identifier of the resource an identifier of said one the two or more second devices (250), or a second communication endpoint (260) thereof;
 - 10 - send (540a) to said one the two or more second devices (250) the unique identifier of the resource.
- 15 5. The first device of one of claims 2 to 4, depending upon claim 2, wherein the one or more first processing logics (230, 231) are further configured to:
- generate identification data allowing the one or more second devices (250, 251) to identify the user and grant access to the resource, and identification validation data allowing the validation of the identification of the user;
 - 20 - send to the user device (240) the identification data.
- 25 6. The first device of claim 5, depending upon claim 3, wherein the one or more first processing logics (231) are configured, upon a reception, from said second device (250) having an access to the second data storage (280) storing the resource, a request to identify the user comprising said identification data (580c), to:
- validate the identification of the user based on said identification data and said identification validation data;
 - if the identification is validated, send to said second device (250) a validation of the identification of the user and the right of the user to access the resource.
 - 30
7. The first device of claim 5, depending upon claim 3, wherein the one or more first processing logics (231) are configured, upon a reception, from said second

device (250) having an access to the second data storage (280) storing the resource, of a request to identify the user comprising said identification data (580c), to send to said second device (250) having an access to the second data storage (280) storing the resource said identification validation data.

5

8. The first device of claim 5, depending upon claim 3, wherein the one or more first processing logics (231) are configured, upon the generation of the user validation data, to send to the one or more second devices (250, 251) identification validation data.

10

9. The first device of claim 5, wherein the one or more first processing logics (231) are configured to generate the identification validation data based on the identification data and shared secret keys (500e) that are common the first device (200) and the one or more second devices (250, 251).

15

10. The first device of one of claims 5 to 9, wherein the identification data is a token, and the identification validation data is a signature of the token.

11. A method (700) comprising:

20

- receiving (710) a request (500b, 500c) from a user device (240) to access a resource, said request comprising an identifier of the resource;
- accessing (720) one or more first data storages (220) storing:

25

- user credentials for a plurality of users ;
- a set of identifiers of a set of resources to be presented to one or more users belonging to said plurality of users, comprising said requested resource, said set of resources stored on two or more second data storages (280, 281) accessed respectively by two or more second devices (250, 251), each identifier in the set having associated therewith access rights, and an identifier of a second communication endpoint (260, 261) of a second device (250, 251) having an access to a second data storage (280, 281) storing the resource ;

30

- verifying (730), based on access rights associated with the resource identifier, if a user associated with said user device (240) has the right to access the resource;

- if the user associated with said user device (240) has the right to access the resource, sending (740, 540b, 560c) to the user device (240) the identifier of the communication endpoint (260) of the second device (250) having an access to the second data storage (280) storing the requested resource.

5

12. A computer program product comprising:

a non-transitory computer-readable storage medium; and

program code stored on the non-transitory computer-readable storage medium that, when executed by one or more processors, causes the one or more processors to:

10

- receive a request (500b, 500c) from a user device (240) to access a resource, said request comprising an identifier of the resource;
- access one or more first data storages (220) storing:

15

- user credentials for a plurality of users ;
- a set of identifiers of a set of resources to be presented to one or more users belonging to said plurality of users, comprising said requested resource, said set of resources stored on two or more second data storages (280, 281) accessed respectively by two or more second devices (250, 251), each identifier in the set having associated therewith access rights, and an identifier of a second communication endpoint (260, 261) of a second device (250, 251) having an access to a second data storage (280, 281) storing the resource ;

20

- verify, based on access rights associated with the resource identifier, if a user associated with said user device (240) has the right to access the resource;

25

- if the user associated with said user device (240) has the right to access the resource, send to the user device (240) the identifier of the communication endpoint (260) of the second device (250) having an access to the second data storage (280) storing the requested resource.

30

13. A first device (200) comprising:

- an access to one or more first data storages (220) storing:
 - user credentials for a plurality of users;
 - a set of identifiers of resources stored on two or more second data storages (280, 281) accessed respectively by two or more second devices (250, 251),

each identifier in the set having associated therewith access rights, and an identifier of a second communication endpoint (260, 261) of a second device (250, 251) having an access to a second data storage (280, 281) storing the resource;

- 5 - a third communication endpoint (211) configured to establish a connection with one or more fourth communication endpoints (290, 291) of the one or more second devices (250, 251);
- a first processing logic (230) configured, upon the reception of a resource identifier creation request (520a) from one of the two or more second devices (250), to:
 - 10 - create a unique identifier of a resource;
 - associate to said unique identifier of the resource an identifier of said one the two or more second devices (250), or a second communication endpoint (260) thereof;
 - send (540a) to said one of the second devices (250) the unique identifier of
 - 15 the resource.

14. A method comprising:

- receiving a resource identifier creation request (520a) from one of two or more second devices (250);
- 20 - accessing one or more first data storages (220) storing:
 - user credentials for a plurality of users ;
 - a set of identifiers of a set of resources, said set of resources stored on two or more second data storages (280, 281) accessed respectively by
 - 25 said two or more second devices (250, 251), each identifier in the set having associated therewith access rights, and an identifier of a second communication endpoint (260, 261) of a second device (250, 251) having an access to a second data storage (280, 281) storing the resource ;
- creating a unique identifier of a resource;
- 30 - associating to said unique identifier of the resource an identifier of said one of the two or more second devices (250), or a second communication endpoint (260) thereof;
- sending (540a) to said one of the two or more second devices (250) the unique identifier of the resource.

15. A computer program product comprising:

a non-transitory computer-readable storage medium; and

program code stored on the non-transitory computer-readable storage medium that, when executed by one or more processors, causes the one or more processors to:

- receive a resource identifier creation request (520a) from one of two or more second devices (250);
- access one or more first data storages (220) storing:
 - user credentials for a plurality of users ;
 - a set of identifiers of a set of resources, said set of resources stored on two or more second data storages (280, 281) accessed respectively by said two or more second devices (250, 251), each identifier in the set having associated therewith access rights, and an identifier of a second communication endpoint (260, 261) of a second device (250, 251) having an access to a second data storage (280, 281) storing the resource ;
- create a unique identifier of a resource;
- associate to said unique identifier of the resource an identifier of said one of the two or more second devices (250), or a second communication endpoint (260) thereof;
- send (540a) to said one of the two or more second devices (250) the unique identifier of the resource.