(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 146 219**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **23 01862**

(51) Int Cl[8] : ***G 06 F 21/45*** *(2023.01), G 06 F 21/30, H 04 L 9/30*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 28.02.23.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 30.08.24 Bulletin 24/35.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *IDAKTO Société par actions simplifiée* — FR.

(72) **Inventeur(s) :** BOUAN Yann, BERTHIER Paul Edmond et CAUCHIE Stéphane.

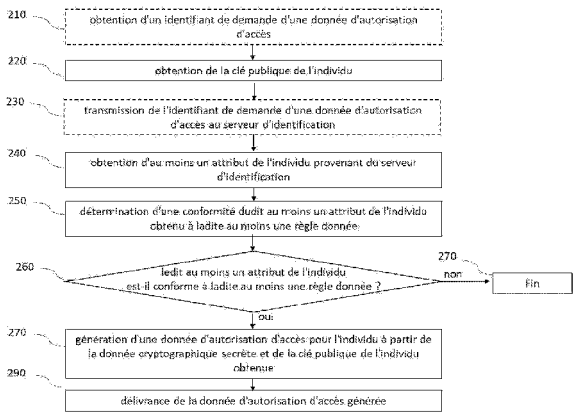
(73) **Titulaire(s) :** IDAKTO Société par actions simplifiée.

(74) **Mandataire(s) :** WR Europe SNC.

(54) Procédé de délivrance d'une autorisation d'accès pour un individu et procédé de vérification.

(57) L'invention concerne un procédé de délivrance d'une donnée d'autorisation d'accès pour un individu ayant une clé publique et un attribut donné, mis en œuvre dans un serveur d'autorisation d'accès apte à communiquer avec un serveur d'identification et un dispositif client. Le serveur d'autorisation d'accès a une règle et une donnée cryptographique secrète, la donnée cryptographique secrète étant spécifique pour un groupe d'individus ayant un attribut conforme à la règle. Le procédé comprend notamment une étape d'obtention d'un attribut de l'individu, une étape de détermination d'une conformité de l'attribut de l'individu à la règle. Si l'attribut de l'individu est conforme à la règle alors le procédé comprend une étape de génération d'une donnée d'autorisation d'accès pour l'individu à partir de la donnée cryptographique secrète et de la clé publique de l'individu et une étape de délivrance de la donnée d'autorisation d'accès au dispositif client. L'invention concerne également un procédé de vérification d'une autorisation d'accès d'un individu.

[figure 2]



FR 3 146 219 - A1

Description

Titre de l'invention : Procédé de délivrance d'une autorisation d'accès pour un individu et procédé de vérification

[0001] L'invention concerne un procédé et un dispositif de délivrance d'une donnée d'autorisation d'accès pour un individu et un procédé et un dispositif de vérification d'une autorisation d'accès d'un individu associés.

[0002] L'accès à des contenus, des services, des applications, des ressources ou des serveurs d'un fournisseur de services est très souvent contrôlé. En particulier, l'accès au fournisseur de services peut être autorisé pour une ou plusieurs catégories de personnes en fonction de caractéristiques propres à la personne ou en fonction de capacités de la personne. Autrement dit, si la personne possède une (ou plusieurs) caractéristique donnée ou une (ou plusieurs) capacité particulière, il dispose d'une autorisation d'accès. Dans le cas contraire, l'accès est refusé à la personne.

[0003] Le contrôle d'accès au fournisseur de services peut être réalisé de manière rudimentaire. Par exemple, avant d'entrer sur un site web spécifique, la personne doit simplement déclarer qu'elle est majeure, saisir une date de naissance ou cliquer sur un bouton du type "j'ai plus de 18 ans". Ce contrôle d'accès est donc soumis à une vérification qui est basée uniquement sur une déclaration de la personne. Ce contrôle est très souvent anonyme et peut être basé sur des informations erronées.

[0004] A l'inverse, le contrôle de l'accès au fournisseur de services peut être réalisé d'une manière très élaborée. Par exemple, avant de se connecter sur une site web d'un fournisseur de services, la personne doit s'enregistrer auprès de celui-ci et fournir ses informations personnelles telles que son nom, son prénom, son âge, son adresse et fournir des informations bancaires ou de carte d'identité. Il obtient alors un identifiant et un mot de passe permettant un accès ultérieur au site web du fournisseur de services. Dans ce cas, l'accès n'est pas anonyme et chaque connexion au site web peut être tracée.

[0005] Une autre solution consiste à utiliser une identité numérique. Cette dernière permet de réduire la divulgation d'informations d'identité de la personne et d'atteindre l'objectif de prouver que la personne possède une ou plusieurs caractéristiques propres ou des capacités particulières.

[0006] Toutefois, ces solutions ne sont pas satisfaisantes pour plusieurs raisons. Le contrôle d'accès à un fournisseur de services en fonction de caractéristiques propres à la personne est réalisé soit en fonction d'informations déclaratives pouvant être erronées soit suite à un enregistrement auprès de ce fournisseur de services avec la fourniture à ce dernier d'informations relatives à la personne. Ainsi, les solutions actuellement dis-

ponibles ne permettent pas un accès au fournisseur de services fiable au regard des caractéristiques de la personne, anonyme et non traçable.

[0007] Le but de l'invention est de remédier à ces inconvénients et de permettre d'une part la délivrance d'une donnée d'autorisation d'accès pour un individu en fonction d'au moins un de ses attributs par un serveur d'autorisation d'accès afin que ce dernier apporte ensuite la preuve à un fournisseur de services qu'il possède au moins un attribut qui satisfasse le fournisseur de services.

[0008] D'autre part, l'invention permet une vérification d'une autorisation d'accès d'un individu, la vérification étant réalisée de manière anonyme et sans traçabilité des différents accès.

[0009] Ainsi, l'invention a pour objet un procédé de délivrance d'une donnée d'autorisation d'accès pour un individu ayant une clé publique et au moins un attribut donné, le procédé étant mis en œuvre dans un serveur d'autorisation d'accès apte à communiquer avec un serveur d'identification et un dispositif client, le serveur d'autorisation d'accès ayant au moins une règle donnée et une donnée cryptographique secrète, la donnée cryptographique secrète étant spécifique pour un groupe d'individus ayant au moins un attribut conforme à ladite au moins une règle donnée. Le procédé comprenant les étapes suivantes :

- obtention de la clé publique de l'individu ;
- obtention dudit moins un attribut de l'individu provenant du serveur d'identification ;
- détermination d'une conformité dudit au moins un attribut de l'individu obtenu à ladite au moins une règle donnée ;
- si ledit au moins un attribut de l'individu est conforme à ladite au moins une règle donnée, génération d'une donnée d'autorisation d'accès pour l'individu à partir de la donnée cryptographique secrète et de la clé publique de l'individu obtenue ;
- délivrance de la donnée d'autorisation d'accès générée au dispositif client.

[0010] Le procédé conforme à l'invention permet la délivrance d'une information d'autorisation d'accès à un individu si ce dernier possède un ou plusieurs attributs conformes à une ou plusieurs règles. L'information d'autorisation d'accès permettra ultérieurement à l'individu de prouver à un fournisseur de services qu'il possède un ou plusieurs attributs, de manière fiable et anonyme.

[0011] Le serveur d'autorisation d'accès peut comprendre en outre une donnée cryptographique publique associée à ladite donnée cryptographique secrète, le procédé peut comprendre alors en outre une étape de transmission de la donnée cryptographique publique au dispositif client.

[0012] Le procédé peut comprendre en outre une étape de vérification de la possession d'une

clé privée de l'individu par le dispositif client associée à la clé publique de l'individu obtenue, préalablement à la délivrance de la donnée d'autorisation d'accès.

[0013] Le procédé peut comprendre en outre une étape d'obtention d'un identifiant de demande d'une donnée d'autorisation d'accès et une étape de transmission de l'identifiant de demande d'une donnée d'autorisation d'accès au serveur d'identification.

[0014] L'identifiant de demande d'une donnée d'autorisation d'accès peut dans ce cas comprendre un identifiant de l'individu.

[0015] Alternativement, le procédé peut comprendre en outre, une étape d'obtention d'un identifiant de l'individu provenant du serveur d'identification ou du dispositif client.

[0016] L'invention a également pour objet un procédé de vérification d'une autorisation d'accès d'un individu ayant une donnée d'autorisation d'accès, la donnée d'autorisation d'accès ayant été délivrée conformément au procédé décrit précédemment. Le procédé est mis en œuvre dans un serveur d'autorisation d'accès apte à communiquer avec un fournisseur de services, le fournisseur de services mettant en œuvre un contrôle d'accès en fonction d'au moins un attribut de l'individu. Le serveur d'autorisation d'accès a une donnée cryptographique publique, la donnée cryptographique publique étant spécifique pour un groupe d'individus ayant au moins un attribut conforme à au moins une règle donnée, ladite donnée cryptographique publique étant associée à une donnée cryptographique secrète, ladite donnée cryptographique secrète ayant été utilisée pour générer la donnée d'autorisation d'accès. Le procédé comprend les étapes suivantes :

- réception d'une information de preuve d'autorisation d'accès, l'information de preuve d'autorisation d'accès ayant été générée au moyen de la donnée d'autorisation d'accès de l'individu ;
- vérification de l'information de preuve d'autorisation d'accès reçue en utilisant la donnée cryptographique publique ;
- si l'information de preuve d'autorisation d'accès est vérifiée, envoi au fournisseur de services d'une information de validation de l'information de preuve d'autorisation d'accès, sans vérification de la conformité d'au moins un attribut de l'individu à ladite au moins une règle donnée lors de la vérification de l'autorisation d'accès.

[0017] La donnée cryptographique publique peut être reçue du fournisseur de services ou d'un dispositif client.

[0018] L'information de preuve d'autorisation d'accès peut être reçue du fournisseur de services ou d'un dispositif client.

[0019] Le serveur d'autorisation d'accès peut en outre être apte à communiquer avec un dispositif client. Le procédé peut alors comprendre en outre, les étapes suivantes :

- réception d'un identifiant de demande de vérification provenant du fournisseur de services ;

- génération d'une information de connexion à partir de l'identifiant de demande de vérification reçu ;
- transmission au fournisseur de services de l'information de connexion générée ;
- création d'un canal de communication entre le serveur d'autorisation d'accès et le dispositif client au moyen de l'information de connexion ;
- réception de l'information de preuve d'autorisation d'accès du dispositif client via le canal de communication créé.

[0020] Le serveur d'autorisation d'accès peut en outre être apte à communiquer avec un dispositif client. Le procédé peut alors comprendre en outre les étapes suivantes :

- génération d'une donnée de vérification ;
- transmission de la donnée de vérification générée au dispositif client ;
- l'information de preuve d'autorisation d'accès reçue étant en outre générée à partir de la donnée de vérification.

[0021] Le serveur d'autorisation d'accès peut être apte à communiquer avec une base de données de preuves, et le procédé peut alors comprendre en outre, une étape de transmission à ladite base de données de preuves de l'information de preuve d'autorisation d'accès reçue.

[0022] Le serveur d'autorisation d'accès peut comprendre en outre une donnée identifiant le groupe d'individus ayant au moins un attribut conforme à ladite au moins une règle donnée, et l'étape d'envoi au fournisseur de services d'une information de validation de l'information de preuve d'autorisation d'accès peut alors comprendre en outre l'envoi de la donnée identifiant le groupe d'individus.

[0023] L'invention a également pour objet un dispositif configuré pour mettre en œuvre au moins l'un des procédés précédemment décrits.

[0024] On va maintenant décrire des exemples de réalisation de la présente invention en référence aux figures annexées où les mêmes références désignent d'une figure à l'autre des éléments identiques ou fonctionnellement semblables :

[0025] [Fig.1] illustre un exemple d'un système dans lequel un procédé de délivrance d'une donnée d'autorisation d'accès pour un individu conformément à l'invention et un procédé de vérification d'une autorisation d'accès d'un individu conformément à l'invention peuvent être mis en œuvre.

[0026] [Fig.2] illustre un mode de réalisation du procédé de délivrance d'une donnée d'autorisation d'accès pour un individu conformément à l'invention.

[0027] [Fig.3] illustre un premier exemple de système dans lequel un serveur d'autorisation d'accès met en œuvre un mode de réalisation du procédé de délivrance d'une donnée d'autorisation d'accès pour un individu conformément à l'invention.

[0028] [Fig.4] illustre un deuxième exemple de système dans lequel un serveur

d'autorisation d'accès met en œuvre un autre mode de réalisation du procédé de délivrance d'une donnée d'autorisation d'accès pour un individu conformément à l'invention.

[0029] [Fig.5] illustre un mode de réalisation du procédé de vérification d'une autorisation d'accès d'un individu conformément à l'invention.

[0030] [Fig.6] illustre un premier exemple de système dans lequel un serveur d'autorisation d'accès met en œuvre un mode de réalisation du procédé de vérification d'une autorisation d'accès d'un individu conformément à l'invention.

[0031] [Fig.7] illustre un deuxième exemple de système dans lequel un serveur d'autorisation d'accès met en œuvre un autre mode de réalisation du procédé de vérification d'une autorisation d'accès d'un individu conformément à l'invention.

[0032] [Fig.8] illustre un premier exemple de système dans lequel un serveur de contrôle met en œuvre un mode de réalisation d'un procédé de détermination de l'identité de l'individu ayant demandé une vérification d'une autorisation d'accès.

[0033] [Fig.9] illustre un deuxième exemple de système dans lequel un serveur de contrôle met en œuvre un mode de réalisation d'un procédé de détermination de l'identité de l'individu ayant demandé une vérification d'une autorisation d'accès.

[0034] La présente invention concerne selon un premier aspect, une manière sûre et fiable, de délivrer une donnée d'autorisation d'accès pour un individu ayant une clé publique et au moins un attribut donné permettant ultérieurement un accès anonyme et non-traçable de l'individu auprès d'un fournisseur de services disposant d'un contrôle d'accès en fonction d'attributs de l'individu.

[0035] Un contrôle d'accès en fonction d'un ou plusieurs attributs de l'individu autorise l'accès de l'individu uniquement si celui-ci est capable d'apporter la preuve qu'un ou plusieurs de ses attributs sont conformes à une ou plusieurs règles. Un tel contrôle d'accès permet de filtrer l'accès de l'individu à un contenu, des services, des applications, des ressources ou des serveurs d'un fournisseur de services. La délivrance d'une donnée d'autorisation d'accès est fonction d'au moins un attribut donné de l'individu.

[0036] La donnée d'autorisation d'accès est générée pour un individu de sorte à permettre ultérieurement à ce dernier un accès anonyme, donc sans avoir à divulguer son identité et ses attributs. La donnée d'autorisation d'accès a un rôle d'attestation numérique anonyme certifiant que l'individu a au moins un attribut conforme à une règle donnée. En particulier, l'invention concerne un procédé de délivrance d'une donnée d'autorisation d'accès pour un individu ayant une clé publique et au moins un attribut donné, mis en œuvre dans un serveur d'autorisation d'accès.

[0037] La présente invention concerne selon un deuxième aspect une manière sûre et fiable de réaliser une vérification d'autorisation d'accès d'un individu souhaitant accéder à un

fournisseur de services mettant en œuvre un contrôle d'accès en fonction d'au moins un attribut de l'individu. La vérification est réalisée au moyen d'une information de preuve d'autorisation d'accès générée à partir de la donnée d'autorisation d'accès préalablement générée pour l'individu. Une telle vérification d'autorisation d'accès permet de s'assurer que l'individu a effectivement au moins un attribut conforme à au moins une règle donnée et donc qu'il est légitime pour accéder au fournisseur de services. Toutefois, la vérification est réalisée sans avoir à vérifier effectivement la conformité du ou des attributs de l'individu à une ou des règles données, la conformité ayant été réalisée précédemment par la délivrance de la donnée d'autorisation d'accès.

[0038] Ainsi, il est rendu possible de vérifier une autorisation d'accès d'un individu à un fournisseur de services au moyen d'une information de preuve d'autorisation d'accès générée à partir de la donnée d'autorisation d'accès de l'individu, de manière anonyme et sans pouvoir tracer les connexions de l'individu. En particulier, l'invention concerne un procédé de vérification d'une autorisation d'accès d'un individu ayant une donnée d'autorisation d'accès mis en œuvre dans un serveur d'autorisation d'accès.

[0039] Un attribut d'un individu est une caractéristique d'un individu, telle que son âge, sa région de domiciliation, son pays de domiciliation, etc., ou une capacité de l'individu, telle que la possession du permis de conduire ou d'un permis de travail. L'attribut peut également comprendre le fait pour un individu de disposer d'un compte d'accès auprès d'un organisme, tel qu'un organisme public, une banque, etc.

[0040] Conformément à l'invention, une donnée d'autorisation d'accès est délivrée à un individu, si un attribut de ce dernier est conforme à une règle donnée ou si des attributs de l'individu sont conformes respectivement à des règles données. Une règle a pour but de définir un critère d'accès. Par exemple, une règle relative à l'attribut "âge" peut être "avoir plus de 18 ans", une règle relative aux capacités de l'individu peut être "avoir un permis de conduire".

[0041] En référence à la [Fig.1], il est décrit un exemple d'un système dans lequel peut être mis en œuvre un procédé de délivrance d'une donnée d'autorisation d'accès pour un individu conformément à l'invention et un procédé de vérification d'une autorisation d'accès d'un individu conformément à l'invention.

[0042] Le système comprend un individu INDIV, au moins un dispositif client à la disposition de l'individu DEV, un serveur d'autorisation d'accès SERV-AUTO, un fournisseur de services FRS-SERV et un serveur d'identification IDP. Il peut comprendre en outre un support d'identité CAP de l'individu INDIV et un dispositif de contrôle CONTROL.

[0043] Un individu INDIV est un utilisateur qui souhaite accéder à un contenu, une application, un service, un serveur, etc. d'un fournisseur de services en utilisant un dispositif client DEV. Il a un identifiant ID_u, au moins un attribut donné ATT, une clé

publique pk_u et une clé secrète sk_u associée. Pour prouver qu'il possède l'attribut ou les attributs nécessaires à la connexion au fournisseur de services, il va tout d'abord obtenir une donnée d'autorisation d'accès qui peut être mémorisée dans un espace sécurisé du dispositif client. Ensuite, il va générer une information de preuve afin de prouver qu'il dispose d'une autorisation d'accès pour une connexion au fournisseur de services, sans toutefois divulguer à ce dernier son identité et ses attributs ATT. Autrement dit, il va générer une information de preuve qui devra être vérifiée permettant de certifier au fournisseur de services qu'il dispose du ou des attributs lui permettant une connexion à ce dernier sans toutefois que le fournisseur de services n'est accès à l'identité et aux attributs ATT de l'individu.

[0044] Le dispositif client DEV peut être tout type de dispositif, tel qu'un téléphone portable, une tablette, un ordinateur, etc., comprenant une plateforme matérielle et logicielle sur laquelle s'exécutent des logiciels, ces logiciels étant soit directement exécutables soit interprétés sur une machine virtuelle. Le dispositif client DEV comprend en particulier une interface de communication homme-machine permettant d'afficher des données et de recevoir des données provenant de l'individu INDIV. Cette interface de communication homme-machine comprend par exemple un écran et un clavier, ou un écran tactile. Le dispositif client DEV peut comprendre un navigateur Internet s'exécutant sur l'interface de communication homme-machine. Le dispositif client est apte à communiquer avec le serveur d'autorisation d'accès SERV-AUTO, le fournisseur de services FRS-SERV et le serveur d'identification IDP. Il peut aussi communiquer avec le support d'identité CAP. Pour cela, le dispositif client DEV est muni de moyens de communication (filaire ou sans fil). Par exemple, le dispositif client DEV peut comprendre une connectivité de type réseau, soit via une connexion filaire soit via une connexion sans fil (par exemple, conforme à la norme Bluetooth, à la norme NFC, à la norme WIFI ou à la norme PC/SC) pour une communication avec le support d'identité CAP et peut comprendre des moyens de communication réseau conformes à l'une quelconques des normes Ethernet, et/ou conformes à l'une quelconque des normes IEEE 802.11 (Wifi), et/ou conformes à une ou plusieurs normes de téléphonie mobile (2G, 3G, 4G, etc.) pour une communication avec le serveur d'autorisation d'accès SERV-AUTO, le fournisseur de services FRS-SERV et le serveur d'identification IDP.

[0045] Le support d'identité CAP est un moyen mémorisant des informations propres à l'individu INDIV. Il peut comprendre notamment un identifiant de l'individu ID_u, le ou les attributs ATT de ce dernier et/ou une clé privée sk_u et une clé publique pk_u de l'individu. Il peut s'agir par exemple, d'une carte d'identité électronique, d'un passeport électronique ou d'une carte bancaire. Il comprend des moyens de connectivité, notamment des moyens de communication sans fil (par exemple, conforme à la norme

Bluetooth, à la norme NFC ou à la norme PC/SC) afin d'être apte à communiquer avec un dispositif client DEV. Le support d'identité CAP peut comprendre en outre, une fonction d'établissement d'un canal de communication sécurisé permettant la création d'un canal de communication sécurisé entre le support d'identité CAP et le dispositif client DEV. L'établissement d'un canal de communication sécurisé s'appuie sur l'utilisation de protocoles de sécurité. Le dispositif client DEV peut également comprendre en outre, une fonction d'établissement d'un canal de communication sécurisé permettant la création d'un canal sécurisé entre le dispositif client DEV et le support d'identité CAP. L'établissement d'un canal de communication sécurisé s'appuie sur l'utilisation de protocoles de sécurité.

[0046] Selon un mode de réalisation dans lequel le système ne comprend pas de support d'identité CAP, l'identifiant de l'individu ID_u, le ou les attributs ATT de ce dernier et/ou une clé privée sk_u et une clé publique pk_u de l'individu INDIV peuvent être mémorisés dans le dispositif client DEV, notamment dans un espace mémoire sécurisé.

[0047] Le serveur d'identification IDP comprend une plateforme matérielle et logicielle sur laquelle s'exécutent des logiciels. Il peut être utilisé pour authentifier un individu, notamment à partir de l'identifiant de ce dernier ID_u, et il peut fournir, notamment au serveur d'autorisation d'accès, le ou les attributs ATT de l'individu INDIV dont il a eu régulièrement la connaissance. En particulier, le serveur d'identification IDP mémorise pour un ensemble d'individus, leur identifiant ID_u et un ou plusieurs attributs ATT de ces individus. Un serveur d'identification IDP est, par exemple un fournisseur d'identité gouvernemental, une banque ou un espace sécurisé de données. Le serveur d'identification IDP peut comprendre une fonction d'établissement d'un canal de communication sécurisé permettant la création d'un canal sécurisé entre le serveur d'identification IDP et le dispositif client DEV ou entre le serveur d'identification IDP et le serveur d'autorisation d'accès SERV-AUTO. L'établissement d'un canal de communication sécurisé s'appuie sur l'utilisation de protocoles de sécurité La connexion au serveur d'identification IDP nécessite une authentification sévère. Pour cela, différentes technologies peuvent être utilisées telles que OpenID, SAML, ISO18013 ou ISO2020.

[0048] Le fournisseur de services FRS-SERV est par exemple un fournisseur de services d'applications ou un fournisseur d'applications en ligne. Autrement dit, il peut s'agir d'un fournisseur d'applications hébergées qui fournit des logiciels, des contenus ou des services informatiques à ses clients au travers d'un réseau Internet par exemple. L'accès à ces applications est notamment réalisé à travers un navigateur web et en utilisant un protocole standard comme le protocole http. Ainsi, le fournisseur de services FRS-SERV comprend une plateforme matérielle et logicielle sur laquelle s'exécutent des applications afin de fournir des logiciels, des services ou des contenus. Selon le cas, le fournisseur de services peut vouloir ou a une obligation de s'assurer que l'individu qui

souhaite accéder à ces services, applications ou contenus appartienne à une certaine catégorie de personnes, par exemple que l'individu soit majeur. En d'autres termes, dans ce cas, le fournisseur de services met en œuvre un contrôle d'accès en fonction d'au moins un attribut de l'individu. Pour ce faire, le fournisseur de services communique avec le serveur d'autorisation d'accès SERV-AUTO.

[0049] Le serveur d'autorisation d'accès SERV-AUTO fournit un service qui délivre une donnée d'autorisation d'accès à un individu et qui vérifie une autorisation d'accès d'un individu pour prouver la légitimité d'un individu à accéder à un service, un contenu, une application, etc. d'un fournisseur de services. Le serveur d'autorisation d'accès est apte à mettre en œuvre tout ou partie du procédé de délivrance d'une donnée d'autorisation d'accès pour un individu ou du procédé de vérification d'une autorisation d'accès d'un individu conformément à l'invention. Tout ou partie du procédé de délivrance d'une donnée d'autorisation d'accès pour un individu et/ou tout ou partie du procédé de vérification d'une autorisation d'accès d'un individu peuvent être mis en œuvre sous forme logicielle et/ou sous forme de dispositif(s). Les modes de réalisation du serveur d'autorisation d'accès SERV-AUTO décrits ci-après sont tels que le serveur d'autorisation d'accès SERV-AUTO est apte à mettre en œuvre tout ou partie du précédé de délivrance d'une information d'autorisation d'accès pour un individu et du procédé de vérification d'une autorisation d'accès d'un individu. Cependant, selon d'autres modes de réalisation, le procédé de délivrance d'une donnée d'autorisation d'accès pour un individu et le procédé de vérification d'une autorisation d'accès d'un individu peuvent être mis en œuvre dans des serveurs distincts.

[0050] Le serveur d'autorisation d'accès SERV-AUTO est apte à communiquer avec le fournisseur de services FRS-SERV et le serveur d'identification IDP en utilisant des moyens de connectivité dont est pourvu le serveur d'autorisation d'accès SERV-AUTO. Les moyens de connectivité du serveur d'autorisation d'accès SERV-AUTO peuvent comprendre des moyens des communication réseau conformes à l'une quelconques des normes Ethernet, et/ou conformes à l'une quelconque des normes IEEE 802.11 (Wifi), et/ou conformes à une ou plusieurs normes de téléphonie mobile (2G, 3G, 4G, etc.). Il peut en outre communiquer avec le dispositif client DEV et le serveur de contrôle CONTROL.

[0051] Le serveur d'autorisation d'accès SERV-AUTO comprend en outre, des moyens d'exécution d'un algorithme de calcul et d'échange de clés cryptographiques.

[0052] Un serveur de contrôle CONTROL peut être mis en œuvre pour révéler l'identité de l'individu qui a soumis une information de preuve d'autorisation d'accès au fournisseur de services. Toutefois, ce serveur est mis en œuvre notamment dans les modes de réalisation dans lesquels il est nécessaire de pouvoir retrouver l'identité de l'individu ayant soumis une information de preuve d'autorisation d'accès au fournisseur de services.

[0053] La [Fig.2] illustre un mode de réalisation du procédé de délivrance d'une donnée d'autorisation d'accès pour un individu INDIV ayant une clé publique pk_u et au moins un attribut donné ATT conformément à l'invention. Les étapes en pointillées sur la figure sont optionnelles.

[0054] Le procédé est mis en œuvre dans un serveur d'autorisation d'accès SERV-AUTO apte à communiquer avec un serveur d'identification IDP et un dispositif client DEV.

[0055] Le serveur d'autorisation d'accès SERV-AUTO comprend au moins une règle donnée. Il comprend en outre une paire de données cryptographiques spécifiques pour un groupe d'individus ayant au moins un attribut conforme à ladite au moins une règle donnée. La paire de données cryptographiques comprend une donnée cryptographique secrète et une donnée cryptographique publique. Un groupe d'individus comprend un ensemble d'individus ayant obtenu une information d'autorisation d'accès car le ou les attributs de ces individus sont conformes à ladite au moins une règle donnée.

[0056] Le procédé peut débuter par une étape d'obtention d'un identifiant de demande d'une donnée d'autorisation d'accès (étape 210). Cette étape peut résulter de la génération de l'identifiant de la demande par le dispositif client DEV et le service d'autorisation d'accès SERV-AUTO.

[0057] L'identifiant de demande d'une donnée d'autorisation d'accès est par exemple un identifiant de session établi entre le dispositif client et le serveur d'autorisation d'accès ou un code d'authentification.

[0058] Selon un mode de réalisation, l'identifiant de demande d'une donnée d'autorisation d'accès est obtenu par la génération d'un identifiant par le dispositif client et le serveur d'autorisation d'accès suite, par exemple, à l'échange de messages pour la création d'un canal de communication.

[0059] Selon un mode de réalisation particulier, l'identifiant de demande d'une donnée d'autorisation d'accès peut comprendre un identifiant de l'individu ID_u.

[0060] L'identifiant de l'individu ID_u est par exemple un identifiant personnel de cet individu. Il peut s'agir d'un identifiant attribué par un organisme spécifique (par exemple, un fournisseur d'identité gouvernemental, une banque, etc.). Ainsi, l'identifiant de l'individu ID_u peut être un numéro d'identification ou des données personnelles comme un nom, un numéro de téléphone et/ou une date de naissance.

[0061] L'étape 210 est suivie d'une étape d'obtention de la clé publique de l'individu pk_u (étape 220). Selon un mode de réalisation particulier, l'étape 220 peut également comprendre l'obtention d'un identifiant de l'individu ID_u associé à la clé publique de l'individu pk_u.

[0062] L'étape 220 peut être suivie d'une étape 230 de transmission de l'identifiant de demande d'une donnée d'autorisation d'accès au serveur d'identification IDP (étape optionnelle) Cette étape peut permettre au serveur d'identification IDP d'initier un

processus d'authentification avec l'individu notamment au moyen du dispositif client DEV (via ou non le serveur d'autorisation d'accès).

[0063] Le procédé se poursuit par une étape 240 d'obtention d'au moins un attribut ATT de l'individu INDIV. L'étape 240 d'obtention d'au moins un attribut ATT est réalisée par la réception dudit au moins un attribut de l'individu INDIV transmis directement ou indirectement par le serveur d'identification IDP au serveur d'autorisation d'accès SERV-AUTO. Le ou les attributs d'un individu sont déterminées par le serveur d'identification IDP par exemple après l'authentification de l'individu auprès du serveur d'identification IDP ou à partir de l'identifiant de l'individu ID_u.

[0064] Selon un mode de réalisation particulier, le procédé peut également comprendre une étape d'obtention d'un identifiant de l'individu ID_u provenant du serveur d'identification IDP, notamment dans le cas où l'identifiant de l'individu ID_u n'a pas été transmis par le dispositif client. L'identifiant de l'individu ID_u est alors associée à la clé publique de l'individu reçue.

[0065] L'étape 240 est suivie d'une étape 250 de détermination d'une conformité dudit au moins un attribut ATT de l'individu obtenu à ladite au moins une règle donnée du serveur d'autorisation d'accès.

[0066] Selon un exemple particulier, l'attribut de l'individu comprend la donnée selon laquelle l'individu est en possession d'un permis de conduire et la règle définit un critère relatif à la possession du permis de conduire. Dans le présent exemple, l'attribut de l'individu est conforme à la règle puisque l'attribut est conforme au critère.

[0067] L'étape 250 est suivie d'une étape 260 de test relatif à la conformité dudit au moins un attribut ATT de l'individu à ladite au moins une règle donnée. Si le test est négatif, l'étape 260 est suivie d'une étape 270 de fin du procédé et aucune donnée d'autorisation d'accès n'est générée et délivrée à l'individu. Si, au contraire, le test de l'étape 260 est positif, alors l'étape 260 est suivie d'une étape 280 de génération d'une donnée d'autorisation d'accès pour l'individu à partir de la donnée cryptographique secrète et de la clé publique de l'individu pk_u obtenue.

[0068] Dans le mode de réalisation dans lequel le serveur d'autorisation d'accès a obtenu l'identifiant de l'individu ID_u, la donnée d'autorisation d'accès pour l'individu est en outre générée à partir de l'identifiant de l'individu ID_u.

[0069] L'étape 280 est ensuite suivie d'une étape 290 de délivrance de la donnée d'autorisation d'accès générée au dispositif client DEV. Cette étape comprend par exemple l'envoi de la donnée d'autorisation d'accès générée au dispositif client.

[0070] Le procédé de délivrance peut en outre comprendre une étape de transmission de la donnée cryptographique publique au dispositif client DEV.

[0071] Selon un mode de réalisation, préalablement à l'étape de délivrance de la donnée d'autorisation d'accès générée, le procédé peut comprendre en outre une étape de véri-

fication de la possession de la clé privée sk_u par l'individu, en particulier par le dispositif client de l'individu, associée à la clé publique de l'individu pk_u obtenue et utilisée pour la génération de la donnée d'autorisation d'accès. Cette étape permet au serveur d'autorisation d'accès de s'assurer que la donnée d'autorisation d'accès générée est délivrée à l'individu possédant la clé publique utilisée pour la génération de la donnée d'autorisation d'accès.

[0072] Selon un mode de réalisation particulier dans lequel le serveur d'autorisation d'accès a obtenu l'identifiant de l'individu ID_u, le procédé comprend en outre une étape de mémorisation dans une base de données d'individus BD-INDIV, de l'identifiant de l'individu ID_u et de la clé publique pk_u de cet individu. La base de données d'individus peut être mémorisées sur un serveur distinct du serveur d'autorisation d'accès.

[0073] Selon un autre mode de réalisation particulier du procédé de délivrance d'une donnée d'autorisation d'accès pour un individu, l'identifiant de l'individu ID_u n'est pas fourni au serveur d'autorisation d'accès.

[0074] La [Fig.3] illustre un premier exemple d'un système comprenant un serveur d'autorisation d'accès SERV-AUTO lequel met en œuvre un mode de réalisation particulier du procédé de délivrance d'une donnée d'autorisation d'accès pour un individu ayant une clé publique pk_u et au moins un attribut donné ATT conformément à l'invention.

[0075] Le système illustré en [Fig.3] comprend en plus du serveur d'autorisation d'accès SERV-AUTO, un dispositif client DEV et un serveur d'identification IDP.

[0076] Le serveur d'autorisation d'accès SERV-AUTO comprend au moins une règle donnée. Il comprend en outre une paire de données cryptographiques spécifiques pour un groupe d'individus ayant au moins un attribut conforme à ladite au moins une règle donnée. La paire de données cryptographiques comprend une donnée cryptographique secrète et une donnée cryptographique publique. Un groupe d'individus comprend un ensemble d'individus ayant obtenu une information d'autorisation d'accès car le ou les attributs de ces individus sont conformes à ladite au moins une règle donnée.

[0077] Le dispositif client DEV est par exemple un téléphone portable. L'individu INDIV peut en outre être muni d'un support d'identité CAP comprenant notamment la clé publique pk_u de l'individu. Le support d'identité CAP peut également comprendre un identifiant de l'individu ID_u associé à la clé publique pk_u de l'individu. Le dispositif client DEV comprend des moyens de communication avec le support d'identité CAP.

[0078] Selon un autre mode de réalisation, la clé publique pk_u de l'individu peut être mémorisée sur le dispositif client DEV.

[0079] Selon le système illustré, le serveur d'autorisation d'accès obtient un identifiant de demande d'une donnée d'autorisation d'accès (étape 310). Cette étape peut comprendre l'échange de messages entre le serveur d'autorisation d'accès SERV-AUTO et le

dispositif client DEV permettant la génération et l'obtention d'un identifiant de demande d'une donnée d'autorisation d'accès. Cette étape aboutit à l'obtention par le serveur d'autorisation d'accès SERV-AUTO d'un identifiant de demande d'une donnée d'autorisation d'accès conformément à l'étape 210 précédemment décrite au support de la [Fig.2].

[0080] Selon un mode de réalisation particulier, l'identifiant de demande d'une donnée d'autorisation d'accès comprend en outre un identifiant de l'individu ID_u.

[0081] Lors de l'étape 310, le serveur d'autorisation d'accès SERV-AUTO obtient la clé publique de l'individu pk_u (conformément à l'étape 220 décrite précédemment au support de la [Fig.2]). En particulier, le dispositif client peut envoyer la clé publique de l'individu pk_u au serveur d'autorisation d'accès SERV-AUTO.

[0082] Selon un mode de réalisation particulier, lors de l'étape 310, le serveur d'autorisation d'accès SERV-AUTO peut également obtenir l'identifiant de l'individu ID_u.

[0083] L'étape 310 peut être suivie d'une étape de transmission par le serveur d'autorisation d'accès SERV-AUTO de l'identifiant de demande d'une donnée d'autorisation d'accès au serveur d'identification IDP (étape 320 qui conforme à l'étape 210 précédemment décrite au support de la [Fig.2]).

[0084] Selon un autre mode de réalisation, l'étape 320 est une étape de création d'un canal de communication sécurisé entre le serveur d'autorisation d'accès SERV-AUTO et le serveur d'identification IDP.

[0085] Selon le mode de réalisation illustré, l'étape 320 est suivie d'une phase d'authentification par l'individu auprès du serveur d'identification IDP, par exemple au moyen du dispositif client.

[0086] Pour cela, selon un premier mode de réalisation illustré à la [Fig.3], le serveur d'identification IDP communique avec le dispositif client DEV afin que l'individu s'authentifie (étape 330). Cela est possible notamment lorsque l'identifiant de demande d'une donnée d'autorisation d'accès reçu par le serveur d'identification IDP comprend l'identifiant de l'individu ID_u.

[0087] Selon un autre mode de réalisation, l'authentification de l'individu peut être réalisée via le serveur d'autorisation d'accès, ce dernier ayant alors un rôle de proxy.

[0088] Selon encore un autre mode de réalisation, l'individu s'authentifie auprès du serveur d'identification IDP au moyen de son dispositif client DEV préalablement à l'étape 310 puis le dispositif client transmet au serveur d'autorisation d'accès, l'identifiant de l'individu ID_u authentifié.

[0089] Suite à l'authentification de l'individu auprès du serveur d'identification IDP, ce dernier transmet au serveur d'autorisation d'accès SERV-AUTO au moins un attribut ATT de l'individu (étape 340). Ainsi, le service d'autorisation d'accès SERV-AUTO obtient au moins un attribut ATT de l'individu provenant du serveur d'identification

IDP conformément à l'étape 240 précédemment décrite au support de la [Fig.2].

[0090] Selon un mode de réalisation particulier, le serveur d'identification IDP transmet au serveur d'autorisation d'accès SERV-AUTO au moins un attribut ATT de l'individu via le dispositif client DEV.

[0091] Selon un mode de réalisation particulier, le serveur d'autorisation d'accès peut en outre obtenir du serveur d'identification un identifiant de l'individu ID_u.

[0092] L'étape 340 est suivie d'une étape 350 au cours de laquelle le serveur d'autorisation d'accès SERV-AUTO va déterminer la conformité dudit au moins un attribut ATT de l'individu obtenu à ladite au moins une règle donnée conformément à l'étape 250 décrit au support de la [Fig.2]. Si ledit au moins un attribut ATT de l'individu est conforme à ladite au moins une règle donnée, le serveur d'autorisation d'accès SERV-AUTO génère une donnée d'autorisation d'accès pour l'individu à partir de la donnée cryptographique secrète et de la clé publique de l'individu pk_u obtenue, conformément aux étapes 260 et 280 précédemment décrites au support de la [Fig.2].

[0093] Dans le mode de réalisation dans lequel le serveur d'autorisation d'accès a obtenu l'identifiant de l'individu ID_u, la donnée d'autorisation d'accès pour l'individu est en outre générée à partir de l'identifiant de l'individu ID_u.

[0094] L'étape 350 est suivie d'une étape 360 de délivrance par le serveur d'autorisation d'accès SERV-AUTO de la donnée d'autorisation d'accès générée au dispositif client DEV conformément à l'étape 290 précédemment décrite au support de la [Fig.2]. Pour cela, le serveur d'autorisation d'accès SERV-AUTO envoie un message au dispositif client DEV contenant la donnée d'autorisation d'accès générée.

[0095] Selon un mode de réalisation particulier, l'étape de délivrance de la donnée d'autorisation d'accès est précédée d'une étape de vérification de la possession de la clé privée sk_u par l'individu, en particulier par le dispositif client de l'individu, associée à la clé publique de l'individu pk_u obtenue. Cette étape permet au serveur d'autorisation d'accès de vérifier avant de communiquer la donnée d'autorisation d'accès au dispositif client, que ce dernier dispose de la clé secrète de l'individu.

[0096] Dans le mode de réalisation particulier dans lequel le serveur d'autorisation d'accès a obtenu l'identifiant de l'individu ID_u, le serveur d'autorisation d'accès peut comprendre en outre une étape de mémorisation dans une base de données d'individus BD-INDIV, de l'identifiant de l'individu ID_u et de la clé publique de cet individu pk_u. D'autres informations additionnelles relatives à l'individu peuvent également être mémorisées dans la base de données d'individus BD-INDIV. La base de données d'individus BD-INDIV peut être mémorisée sur un serveur distinct du serveur d'autorisation d'accès.

[0097] La [Fig.4] illustre un deuxième exemple d'un système comprenant un serveur d'autorisation d'accès SERV-AUTO lequel met en œuvre un autre mode de réalisation du procédé de délivrance d'une donnée d'autorisation d'accès pour un individu

conformément à l'invention et décrit au support de la [Fig.2].

[0098] On ne décrira en détail ci-après que les étapes qui diffèrent de celles du premier exemple de système décrit au support de la [Fig.3]. Pour le reste, il est renvoyé au premier exemple décrit au support de la [Fig.3].

[0099] Le serveur d'autorisation d'accès comprend au moins une règle donnée.

[0100] Dans cet exemple de système, l'individu comprend une paire de clés, à savoir une clé privée sk_u et une clé publique pk_u mémorisées par exemple sur un dispositif client DEV ou dans un support d'identité CAP et le serveur de contrôle CONTROL comprend une clé de divulgation secrète sk_o et une clé de divulgation publique pk_o.

[0101] La clé de divulgation publique pk_o du serveur de contrôle CONTROL est transmise au serveur d'autorisation d'accès SERV-AUTO (étape 400).

[0102] Suite à la réception de la clé de divulgation publique pk_o provenant du serveur de contrôle CONTROL, le serveur d'autorisation d'accès SERV-AUTO va générer une paire de données cryptographique spécifique pour un groupe d'individus ayant au moins un attribut conforme à ladite au moins une règle donnée. La paire de données cryptographique comprend une donnée cryptographique publique Gpk et une donnée cryptographique secrète sk_m.

[0103] Dans l'exemple de réalisation illustré en [Fig.4], la donnée cryptographique publique Gpk comprend au moins une clé maitre publique pk_m et la clé de divulgation publique pk_o reçue du serveur de contrôle CONTROL.

[0104] Selon un autre mode de réalisation dans lequel le système ne comprend pas de serveur de contrôle CONTROL, le serveur d'autorisation d'accès comprend une paire de données cryptographique spécifique pour un groupe d'individus ayant au moins un attribut conforme à ladite au moins une règle donnée. La paire de données cryptographique comprend d'une part, une donnée cryptographique publique Gpk composée d'une clé maitre publique pk_m et d'autre part, une donnée cryptographique secrète sk_m.

[0105] La donnée cryptographique publique Gpk peut ensuite être transmise au dispositif client DEV.

[0106] Selon le système illustré, le serveur d'autorisation d'accès obtient un identifiant de demande d'une donnée d'autorisation d'accès (étape 410) conformément à l'étape 210 précédemment décrite au support de la [Fig.2].

[0107] Selon un mode de réalisation particulier, l'identifiant de demande d'une donnée d'autorisation d'accès (étape 410) peut être déterminé par le dispositif client à partir notamment de la clé secrète sk_u de l'individu et de la donnée cryptographique publique Gpk reçue. Il peut en outre être déterminé à partir de l'identifiant de l'individu ID_u. L'identifiant de demande d'une donnée d'autorisation d'accès est ensuite transmis par le dispositif client et reçu par le serveur d'autorisation d'accès.

[0108] Lors de l'étape 410, le serveur d'autorisation d'accès SERV-AUTO obtient la clé

publique de l'individu pk_u (conformément à l'étape 220 décrite précédemment au support de la [Fig.2]). En particulier, le dispositif client peut envoyer la clé publique de l'individu pk_u au serveur d'autorisation d'accès SERV-AUTO.

[0109] L'étape 410 est ensuite suivie des étapes 320 à 340 précédemment décrites.

[0110] A l'issue de l'étape 340, le serveur d'autorisation d'accès SERV-AUTO va déterminer la conformité dudit au moins un attribut ATT de l'individu obtenu à ladite au moins une règle donnée conformément à l'étape 240 décrite précédemment au support de la [Fig.2]. Si ledit au moins un attribut ATT de l'individu est conforme à ladite au moins une règle donnée, le serveur d'autorisation d'accès SERV-AUTO génère une donnée d'autorisation d'accès pour l'individu gsk_u à partir de la donnée cryptographique secrète sk_m et de la clé publique de l'individu pk_u obtenue, conformément aux étapes 260 et 280 précédemment décrites au support de la [Fig.2].

[0111] L'étape 450 est suivie d'une étape 460.a de délivrance de la donnée d'autorisation d'accès gsk_u générée, au dispositif client DEV.

[0112] Dans le mode de réalisation dans lequel le serveur d'autorisation d'accès a reçu l'identifiant de l'individu ID_u l'étape 450 peut également être suivie d'une étape 460.b de mémorisation par le serveur d'autorisation d'accès, dans une base de données d'individus BD-INDIV de l'identifiant de l'individu ID_u et de la clé d'individu publique pk_u de cet individu. D'autres informations additionnelles relatives à l'individu peuvent également être mémorisées dans la base de données d'individus BD-INDIV. La base de données d'individus BD-INDIV peut être stockée sur un serveur distinct du serveur d'autorisation d'accès.

[0113] La [Fig.5] illustre un mode de réalisation d'un procédé de vérification d'une autorisation d'accès d'un individu ayant une donnée d'autorisation d'accès mis en œuvre dans un serveur d'autorisation d'accès SERV-AUTO conformément à l'invention. La donnée d'autorisation d'accès a été délivrée conformément au procédé de délivrance d'une donnée d'autorisation d'accès précédemment décrit.

[0114] Le serveur d'autorisation d'accès SERV-AUTO est apte à communiquer avec un fournisseur de services FRS-SERV mettant en œuvre un contrôle d'accès en fonction d'au moins un attribut de l'individu.

[0115] Le serveur d'autorisation d'accès SERV-AUTO comprend une donnée cryptographique publique, la donnée cryptographique publique étant spécifique pour un groupe d'individus ayant au moins un attribut conforme à au moins une règle donnée. La donnée cryptographique publique est associée à une donnée cryptographique secrète, ladite donnée cryptographique secrète ayant été utilisée pour générer la donnée d'autorisation d'accès de l'individu.

[0116] Selon un mode de réalisation particulier, la donnée cryptographique publique peut être reçue par le serveur d'autorisation d'accès et provenir du fournisseur de services

FRS-SERV. Selon un autre mode de réalisation dans lequel le serveur d'autorisation d'accès SERV-AUTO est apte à communiquer avec un dispositif client DEV de l'individu, la donnée cryptographique publique peut être reçue par le serveur d'autorisation d'accès et provenir du dispositif client DEV.

[0117] Le serveur d'autorisation d'accès SERV-AUTO mettant en œuvre le procédé de vérification d'une autorisation d'accès peut être le même serveur que celui mettant en œuvre le procédé de délivrance d'une information d'autorisation d'accès ou un serveur distinct.

[0118] Le procédé de vérification d'une autorisation d'accès peut faire suite au procédé de délivrance d'une donnée d'autorisation d'accès précédemment décrit au support de la [Fig.2] et des figures suivantes.

[0119] L'objet du procédé de vérification d'une autorisation d'accès est de vérifier que l'individu dispose de l'autorisation d'accès pour accéder à un fournisseur de services mettant en œuvre un contrôle d'accès en fonction d'au moins un attribut de l'individu, sans vérification de la conformité du ou des attributs de l'individu à une ou plusieurs règles données lors de la vérification de l'autorisation d'accès. En outre, la vérification n'utilise pas non plus, un identifiant de l'individu.

[0120] Ainsi, ce procédé permet un contrôle d'accès d'un individu à un fournisseur de services mettant en œuvre un contrôle d'accès en fonction d'au moins un attribut de l'individu tout en garantissant un accès anonyme et non traçable de l'individu.

[0121] La non-traçabilité consiste à ne pas pouvoir identifier les différents accès d'un même individu au fournisseur de services. En d'autres termes, le système et le fournisseur de services ne peuvent pas déterminer si deux accès distincts appartiennent à un même individu (ou non).

[0122] Selon ce procédé, l'individu doit apporter une preuve qu'un ou plusieurs de ses attributs sont conformes à une ou plusieurs règles, les règles définissant les critères du contrôle d'accès du fournisseur de services. Pour cela, la preuve est une information de preuve d'autorisation d'accès générée par le dispositif client au moyen de la donnée d'autorisation d'accès qui lui a été précédemment délivrée.

[0123] En outre, selon le procédé de vérification conforme à l'invention, le ou les attributs ATT de l'individu ne sont pas communiquées au fournisseur de services. Toutefois, si l'information de preuve d'autorisation d'accès est validée par le procédé de vérification, le fournisseur de services mettant en œuvre un contrôle d'accès en fonction d'au moins un attribut de l'individu sait uniquement que la ou les règles relatives à un ou plusieurs attributs ATT de l'individu sont respectées.

[0124] Tel qu'illustré à la [Fig.5], le procédé de vérification d'une autorisation d'accès d'un individu ayant une donnée d'autorisation d'accès débute par une étape de réception d'une information de preuve d'autorisation d'accès (étape 510). L'information de preuve

d'autorisation d'accès a été générée au moyen de la donnée d'autorisation d'accès de l'individu, notamment par le dispositif client de l'individu. L'information de preuve d'autorisation d'accès peut parvenir au serveur d'autorisation d'accès à partir du fournisseur de services ou du dispositif client de l'individu.

[0125] Cette étape peut être précédée d'une étape de génération d'une donnée de vérification c par le serveur d'autorisation d'accès, d'une étape de transmission de la donnée de vérification générée au dispositif client DEV. Dans ce cas, l'information de preuve d'autorisation d'accès reçue peut être en outre générée à partir de la donnée de vérification.

[0126] L'étape 510 est suivie d'une étape 520 de vérification de l'information de preuve d'autorisation d'accès reçue en utilisant la donnée cryptographique publique.

[0127] L'étape 520 est suivie d'une étape 530 de test de la vérification de l'information de preuve d'autorisation d'accès. Si l'information de preuve d'autorisation d'accès n'a pas pu être vérifiée, alors l'étape 530 est suivie de l'étape 540 au cours de laquelle le serveur d'autorisation d'accès peut indiquer au fournisseur de services que l'information de preuve d'autorisation d'accès est non valide.

[0128] Si, au contraire, l'information de preuve d'autorisation d'accès a pu être vérifiée, autrement dit l'information de preuve d'autorisation d'accès est valide, alors l'étape 530 est suivie d'une étape 550 d'envoi au fournisseur de services FRS-SERV d'une information de validation de l'information de preuve d'autorisation d'accès. Ainsi, lors de la vérification de l'autorisation d'accès, le serveur d'autorisation d'accès ne réalise pas de vérification de la conformité du ou des attributs de l'individu à une ou plusieurs règles données. En outre, le serveur d'autorisation d'accès n'utilise pas un identifiant de l'individu pour réaliser la vérification de l'autorisation d'accès.

[0129] Selon un mode de réalisation particulier, le serveur d'autorisation d'accès comprend en outre une donnée identifiant le groupe d'individus ayant au moins un attribut conforme à ladite au moins une règle donnée IdToken. Selon ce mode de réalisation l'étape d'envoi au fournisseur de services FRS-SERV d'une information de validation de l'information de preuve d'autorisation d'accès comprend en outre l'envoi de la donnée identifiant le groupe d'individus IdToken.

[0130] La [Fig.6] illustre un premier exemple d'un système comprenant un serveur d'autorisation d'accès SERV-AUTO lequel met en œuvre un mode de réalisation particulier du procédé de vérification d'une autorisation d'accès d'un individu conformément à l'invention.

[0131] L'individu a une donnée d'autorisation d'accès précédemment délivrée conformément au procédé de délivrance d'une donnée d'autorisation d'accès décrit notamment au support de la [Fig.2].

[0132] Le serveur d'autorisation d'accès SERV-AUTO comprend une donnée crypto-

graphique publique, la donnée cryptographique publique étant spécifique pour un groupe d'individus ayant au moins un attribut conforme à au moins une règle donnée. La donnée cryptographique publique est associée à une donnée cryptographique secrète, ladite donnée cryptographique secrète spécifique ayant été utilisée pour générer la donnée d'autorisation d'accès de l'individu.

[0133] Selon un mode de réalisation particulier, la donnée cryptographique publique est mémorisée dans le serveur d'autorisation d'accès. Selon un autre mode de réalisation, la donnée cryptographique publique est reçue par le serveur d'autorisation d'accès du fournisseur de services FRS-SERV. Selon encore un autre mode de réalisation, la donnée cryptographique publique est reçue par le serveur d'autorisation d'accès du dispositif client DEV.

[0134] Le système illustré en [Fig.6] comprend en plus du serveur d'autorisation d'accès SERV-AUTO, un fournisseur de services FRS-SERV, un serveur d'identification IDP ou un serveur comprenant une base de données BD-PREUVES et un ou plusieurs dispositifs client DEV1, DEV2 d'un individu INDIV. La [Fig.6] illustre un système particulier dans lequel l'individu INDIV dispose d'un premier dispositif client DEV1 et d'un second dispositif client DEV2 qui peuvent être par exemple un ordinateur portable et un téléphone portable. Dans le système illustré, la donnée d'autorisation d'accès de l'individu est par exemple mémorisée dans le second dispositif client DEV2. Toutefois, selon un autre mode de réalisation du système, le premier dispositif client DEV1 et le second dispositif client DEV2 sont un même dispositif client.

[0135] Lorsque l'individu INDIV souhaite accéder par exemple à un contenu, une application ou un service, etc. d'un fournisseur de services mettant en œuvre un contrôle d'accès en fonction d'au moins un attribut de l'individu, il peut utiliser un navigateur internet pour réaliser un tel accès (étape 610).

[0136] Le fournisseur de services doit alors vérifier que l'individu dispose d'un ou plusieurs attributs lui permettant l'accès. Pour ce faire, le fournisseur de services FRS-SERV peut communiquer, notamment de manière sécurisée au moyen d'un canal de communication sécurisé créé par exemple au moyen du protocole OpenID CIBA, avec le serveur d'autorisation d'accès SERV-AUTO afin de vérifier que l'individu dispose d'une autorisation d'accès au fournisseur de services (étape 620).

[0137] Un identifiant de demande de vérification SessionID est alors reçu par le serveur d'autorisation d'accès SERV-AUTO lors de l'étape 620. La réception de l'identifiant de demande de vérification peut être précédée d'une étape de génération de l'identifiant de demande de vérification par le fournisseur de services et le serveur d'autorisation d'accès.

[0138] Le serveur d'autorisation d'accès peut ensuite générer une information de connexion à partir de l'identifiant de demande de vérification reçu et transmettre l'information de

connexion générée au fournisseur de services.

[0139] Selon le mode de réalisation illustré à la [Fig.6], le fournisseur de services transmet au dispositif client, par exemple au premier dispositif client DEV1, l'information de connexion qu'il a reçue (étape 630).

[0140] L'information de connexion peut être par exemple un QR Code qui va s'afficher sur l'écran d'affichage du premier dispositif client DEV1.

[0141] Selon un exemple de réalisation, l'individu scanne le QR Code s'affichant sur le premier dispositif client DEV1 au moyen du second dispositif client DEV2 (étape 640). Un canal de communication entre le serveur d'autorisation d'accès et le dispositif client, notamment le second dispositif client DEV2, est alors créé au moyen de l'information de connexion.

[0142] Le second dispositif client DEV2 génère ensuite une information de preuve d'autorisation d'accès, l'information de preuve d'autorisation d'accès étant générée au moyen de la donnée d'autorisation d'accès de l'individu mémorisée par exemple dans le second dispositif client DEV2.

[0143] Le serveur d'autorisation d'accès SERV-AUTO va alors recevoir l'information de preuve d'autorisation d'accès généré tel que précédemment décrit à l'étape 510 au support de la [Fig.5].

[0144] Le serveur d'autorisation d'accès reçoit l'information de preuve du second dispositif client de l'individu tel qu'illustré en [Fig.6] (étape 650) via le canal de communication créé.

[0145] Selon un autre mode de réalisation dans lequel aucun canal de communication entre le serveur d'autorisation d'accès SERV-AUTO et le dispositif client DEV n'est créé, le dispositif client, par exemple le premier dispositif client DEV 1, peut transmettre l'information de preuve d'autorisation d'accès au serveur d'autorisation d'accès via le fournisseur de services. Dans ce mode de réalisation, l'information de preuve d'autorisation d'accès est générée sur l'un des dispositifs client DEV1 ou DEV2 au moyen de la donnée d'autorisation d'accès de l'individu mémorisée par exemple sur le second dispositif client DEV2.

[0146] Selon un mode de réalisation particulier, le serveur d'autorisation d'accès peut envoyer l'information de preuve d'autorisation d'accès reçue au serveur d'identification IDP ou à une base de données de preuves BD-PREUVES afin de mémoriser l'information de preuve d'autorisation d'accès reçue (étape 650.a). Outre l'information de preuve, le serveur d'autorisation d'accès peut également envoyer l'identifiant de demande de vérification SessionID et/ou la date et l'heure de la réception de l'information de preuve d'autorisation d'accès afin d'être mémorisées. Des donnés additionnelles utilisées par exemple pour la génération de l'information de preuve d'autorisation d'accès peuvent également être mémorisées dans la base de données de

preuves.

[0147] Le serveur d'autorisation d'accès vérifie l'information de preuve d'autorisation d'accès reçue en utilisant la donnée cryptographique publique tel que précédemment décrit à l'étape 510.

[0148] Si l'information de preuve d'autorisation d'accès est vérifiée, alors le serveur d'autorisation d'accès envoie au fournisseur de services FRS-SERV une information de validation de l'information de preuve d'autorisation d'accès (étape 660) tel que précédemment décrit au regard de l'étape 530 de la [Fig.5]. Lors de la vérification de l'autorisation d'accès de l'individu, le serveur d'autorisation d'accès ne vérifie pas la conformité du ou des attributs de l'individu à une ou plusieurs règles données. En outre, le serveur d'autorisation d'accès n'utilise pas l'identifiant de l'individu.

[0149] Selon un mode de réalisation particulier, le serveur d'autorisation d'accès comprend en outre une donnée identifiant le groupe d'individus ayant au moins un attribut conforme à ladite au moins une règle donnée IdToken. Selon ce mode de réalisation l'étape d'envoi au fournisseur de services FRS-SERV d'une information de validation de l'information de preuve d'autorisation d'accès comprend en outre l'envoi de la donnée identifiant le groupe d'individus IdToken.

[0150] Suite à la réception de l'information de validation de l'information de preuve d'autorisation d'accès par le fournisseur de services, celui-ci permet l'accès au fournisseur de services (étape 670).

[0151] Selon un mode de réalisation particulier, le serveur d'autorisation d'accès peut recevoir la donnée cryptographique publique du fournisseur de services FRS-SERV ou du dispositif client DEV afin de réaliser la vérification de l'information de preuve d'autorisation d'accès.

[0152] La [Fig.7] illustre un deuxième exemple d'un système comprenant un serveur d'autorisation d'accès SERV-AUTO lequel met en œuvre un autre mode de réalisation du procédé de vérification d'une autorisation d'accès d'un individu ayant une donnée d'autorisation d'accès conformément à l'invention. La donnée d'autorisation d'accès gsk_u de cet exemple a été générée selon le mode de réalisation du procédé de délivrance décrit au support de la [Fig.4].

[0153] On ne décrira en détail ci-après que les étapes qui diffèrent de celles du premier exemple de système décrit à la [Fig.6]. Pour le reste, il est renvoyé au premier exemple décrit au support de la [Fig.6].

[0154] Dans cet exemple de réalisation, le serveur d'autorisation d'accès comprend une donnée cryptographique publique Gpk. La donnée cryptographique publique est spécifique pour un groupe d'individus ayant au moins un attribut conforme à au moins une règle donnée. La donnée cryptographique publique est associée à une donnée cryptographique secrète sk_m. Ladite donnée cryptographique secrète a été utilisée pour

générer la donnée d'autorisation d'accès tel que décrit dans le mode de réalisation illustré à la [Fig.4].

[0155] La donnée cryptographique publique Gpk comprend au moins une clé maitre publique pk_m. La donnée cryptographique publique Gpk peut en outre comprendre une clé de divulgation publique pk_o.

[0156] Selon un mode de réalisation particulier, la donnée cryptographique publique est mémorisée dans le serveur d'autorisation d'accès. Selon un autre mode de réalisation, la donnée cryptographique publique est reçue par le serveur d'autorisation d'accès du fournisseur de services FRS-SERV. Selon encore un autre mode de réalisation, la donnée cryptographique publique est reçue par le serveur d'autorisation d'accès du dispositif client DEV.

[0157] Tel qu'illustré à la [Fig.7], l'information de preuve d'autorisation d'accès σ est générée par le dispositif client au moyen d'un algorithme de signature ayant pour paramètre la donnée d'autorisation d'accès gsk_u et une donnée de vérification c à signer générée par le serveur d'autorisation d'accès et transmise au dispositif client. La donnée de vérification est par exemple un nombre aléatoire ou semi-aléatoire.

[0158] Dans le mode de réalisation illustré, l'information de preuve d'autorisation d'accès est générée sur l'un des dispositifs client DEV1 ou DEV2 au moyen de la donnée d'autorisation d'accès gsk_u l'individu mémorisée par exemple sur le second dispositif client DEV2.

[0159] L'information de preuve d'autorisation d'accès est ensuite vérifiée par le serveur d'autorisation d'accès au moyen d'un algorithme de vérification de signature ayant comme paramètres, l'information de preuve d'autorisation d'accès σ, la donnée de vérification c et la donnée cryptographique publique Gpk (étape 750).

[0160] Selon un mode de réalisation particulier, le serveur d'autorisation d'accès peut envoyer l'information de preuve d'autorisation d'accès σ reçue au serveur d'identification IDP ou à une base de données de preuves BD-PREUVES afin de mémoriser l'information de preuve d'autorisation d'accès σ reçue (étape 750.a). Outre l'information de preuve, le serveur d'autorisation d'accès peut également envoyer l'identifiant de demande de vérification SessionID, la date et l'heure de la réception de l'information de preuve d'autorisation d'accès σ afin d'être mémorisées. Des donnés additionnelles utilisées par exemple pour la génération de l'information de preuve d'autorisation d'accès peuvent également être mémorisées dans la base de données de preuves, tel que la donnée de vérification c.

[0161] Il est illustré à la [Fig.8] un premier exemple de système dans lequel un serveur de contrôle CONTROL détermine l'identité de l'individu ayant demandé une vérification d'une autorisation d'accès.

[0162] Le serveur de contrôle CONTROL peut en effet mettre en œuvre un procédé de dé-

termination de l'identifiant d'un individu à partir d'une information de preuve d'autorisation d'accès fournie au fournisseur de services et mémorisée dans une base de données de preuves BD-PREUVES. La base de données de preuves BD-PREUVES mémorise les différentes informations de preuve d'autorisation d'accès soumises par les individus au fournisseur de services pour montrer qu'ils sont légitimes à accéder au fournisseur de services. En outre pour chaque information de preuve σ mémorisée, sont associées l'identifiant de demande de vérification SessionID et la donnée de vérification c. La date et l'heure de la réception de l'information de preuve d'autorisation d'accès par le serveur d'autorisation d'accès peuvent également être mémorisées pour chaque information de preuve mémorisée.

[0163] La base de données de preuves BD-PREUVES peut être mémorisée sur le serveur d'identification IDP.

[0164] Le système comprend en outre une base de données d'individus BD-INDIV mémorisant l'identifiant ID_u des individus ayant demandé une donnée d'autorisation d'accès auprès du serveur d'autorisation d'accès. A chaque identifiant d'un individu est associée la clé publique pk_u de ce dernier.

[0165] Le procédé de détermination de l'identifiant d'un individu mis en œuvre dans le serveur de contrôle CONTROL a pour objectif de lever l'anonymat de l'individu ayant demandé une vérification d'une autorisation d'accès.

[0166] Le procédé de détermination de l'identifiant d'un individu débute par une étape de réception d'une demande de détermination de l'identifiant d'un individu (étape 810) et une étape de réception d'un identifiant de demande de vérification SessionID provenant du fournisseur de services FRS-SERV (étape 820). L'identifiant de demande de vérification SessionID identifie une session intervenue entre le fournisseur de services FRS-SERV et le serveur d'autorisation d'accès SERV-AUTO afin que ce dernier vérifie une information de preuve d'autorisation d'accès d'un individu.

[0167] A partir de l'identifiant de demande de vérification SessionID, le serveur de contrôle effectue une recherche dans la base de données de preuves BD-PREUVES afin d'identifier l'information de preuve d'autorisation d'accès σ mémorisée et la donnée de vérification c associées (étape 830).

[0168] L'étape 830 est suivie d'une étape 840 de détermination de l'identifiant de l'individu à partir de l'information de preuve d'autorisation d'accès σ et de la donnée de vérification c. Pour cela, le serveur de contrôle détermine tout d'abord la clé publique de l'individu pk_u. Ensuite, à partir de la clé publique déterminée pk_u, le serveur de contrôle effectue une recherche dans la base de données d'individus BD-INDIV de l'identifiant de l'individu ID_u ayant la clé publique pk_u déterminée.

[0169] L'étape 840 est suivie de l'étape 850 d'envoi de l'identifiant de l'individu ID_u déterminé.

[0170] Il est illustre à la [Fig.9] un deuxième exemple de système dans lequel un serveur de contrôle détermine l'identité de l'individu ayant demandé une vérification d'une autorisation d'accès.

[0171] On ne décrira en détail ci-après que les étapes qui diffèrent de celles du premier exemple de système décrit à la [Fig.8]. Pour le reste, il est renvoyé au premier exemple décrit au support de la [Fig.8].

[0172] Selon ce mode de réalisation, le serveur de contrôle CONTROL comprend une clé de divulgation secrète sk_o et une clé de divulgation publique pk_o. En outre, le serveur d'autorisation d'accès est tel que décrit à la [Fig.4] et à la [Fig.7] et comprend une donnée cryptographique publique Gpk. La donnée cryptographique publique Gpk est spécifique pour un groupe d'individus ayant au moins un attribut conforme à au moins une règle donnée. Ladite donnée cryptographique publique est associée à une donnée cryptographique secrète sk_m. La donnée cryptographique publique Gpk comprend une clé maitre publique pk_m et une clé de divulgation publique pk_o, la clé de divulgation publique étant la clé publique du serveur de contrôle CONTROL.

[0173] La base de données d'individus BD-INDIV mémorise l'identifiant ID_u des individus ayant demandé une donnée d'autorisation d'accès auprès du serveur d'autorisation d'accès selon le mode de réalisation décrit au support de la [Fig.4]. A chaque identifiant ID_u d'individu est associée la clé publique pk_u de ce dernier.

[0174] En outre, la base de données de preuves BD-PREUVES comprend les différentes informations de preuves d'autorisation d'accès σ soumises par les individus au fournisseur de services pour montrer qu'ils sont légitimes à accéder au fournisseur de services tel que décrit au support de la [Fig.7]. Dans la base de données de preuves BD-PREUVES, pour chaque information de preuve mémorisée σ, sont associées l'identifiant de demande de vérification SessionID et la donnée de vérification c. La date et l'heure de la réception de l'information de preuve d'autorisation d'accès par le serveur d'autorisation d'accès peuvent également être mémorisées pour chaque information de preuve mémorisée.

[0175] Le procédé de détermination de l'identifiant d'un individu mis en œuvre dans le serveur de contrôle CONTROL a pour objectif de lever l'anonymat de l'individu ayant demandé une vérification d'une autorisation d'accès.

[0176] Le procédé de détermination de l'identifiant d'un individu débute par les étapes 810 et 820 précédemment décrites au support de la [Fig.8]. En outre, le procédé se poursuit à l'étape 925 par l'obtention par le serveur de contrôle de la donnée cryptographique publique Gpk, provenant du serveur d'autorisation d'accès SERV-AUTO. Le procédé se poursuit à l'étape 830 précédemment décrite au support de la [Fig.8].

[0177] Selon ce mode de réalisation, à l'issue des étapes 820, 925 et 830, le serveur de contrôle CONTROL a obtenu la donnée cryptographique publique Gpk, la donnée de

vérification c, et l'information de preuve d'autorisation d'accès σ. A partir de la clé de divulgation secrète sk_o et des données et informations obtenues, le serveur de contrôle CONTROL détermine la clé publique de l'individu pk_u qui a généré l'information de preuve d'autorisation d'accès σ.

[0178] Le procédé se poursuit alors à l'étape 840 précédemment décrite au support de la [Fig.8] au cours de laquelle, à partir de la clé publique déterminée pk_u, le serveur de contrôle CONTROL va rechercher dans la base de données d'individus BD-INDIV l'identifiant de l'individu ID_u ayant la clé publique pk_u déterminée.

[0179] L'étape 840 est suivie de l'étape 850 d'envoi de l'identifiant de l'individu ID_u déterminé.

Revendications

[Revendication 1] Procédé de délivrance d'une donnée d'autorisation d'accès pour un individu ayant une clé publique (pk_u) et au moins un attribut donné (ATT),
le procédé étant mis en œuvre dans un serveur d'autorisation d'accès (SERV-AUTO) apte à communiquer avec un serveur d'identification (IDP) et un dispositif client (DEV),
le serveur d'autorisation d'accès (SERV-AUTO) ayant au moins une règle donnée et une donnée cryptographique secrète, la donnée cryptographique secrète étant spécifique pour un groupe d'individus ayant au moins un attribut conforme à ladite au moins une règle donnée,
le procédé comprenant les étapes suivantes :

- obtention de la clé publique de l'individu (pk_u) (étape 220) ;
- obtention dudit au moins un attribut (ATT) de l'individu provenant du serveur d'identification (IDP) (étape 240) ;
- détermination d'une conformité dudit au moins un attribut (ATT) de l'individu obtenu à ladite au moins une règle donnée (étape 250) ;
- si ledit au moins un attribut (ATT) de l'individu est conforme à ladite au moins une règle donnée, génération d'une donnée d'autorisation d'accès pour l'individu à partir de la donnée cryptographique secrète et de la clé publique de l'individu (pk_u) obtenue (étapes 260, 280) ;
- délivrance de la donnée d'autorisation d'accès générée au dispositif client (DEV) (étape 290).

[Revendication 2] Procédé selon la revendication précédente, caractérisé en ce que le serveur d'autorisation d'accès comprend en outre une donnée cryptographique publique associée à ladite donnée cryptographique secrète, et en ce que le procédé comprend en outre une étape de transmission de la donnée cryptographique publique au dispositif client (DEV).

[Revendication 3] Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le procédé comprend en outre une étape de vérification de la possession d'une clé privée de l'individu (sk_u) par le dispositif client associée à la clé publique de l'individu (pk_u) obtenue, préalablement à la délivrance de la donnée d'autorisation d'accès.

[Revendication 4] Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le procédé comprend en outre une étape d'obtention d'un identifiant de demande d'une donnée d'autorisation d'accès (étape 210) et une étape de transmission de l'identifiant de demande d'une donnée d'autorisation d'accès au serveur d'identification (IDP) (étape 230).

[Revendication 5] Procédé selon la revendication précédente, caractérisé en ce que l'identifiant de demande d'une donnée d'autorisation d'accès comprend un identifiant de l'individu (ID_u).

[Revendication 6] Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que le procédé comprend en outre, une étape d'obtention d'un identifiant de l'individu (ID_u) provenant du serveur d'identification (IDP) ou du dispositif client (DEV).

[Revendication 7] Procédé de vérification d'une autorisation d'accès d'un individu ayant une donnée d'autorisation d'accès,
la donnée d'autorisation d'accès ayant été délivrée conformément au procédé selon l'une quelconque des revendications 1 à 6,
le procédé étant mis en œuvre dans un serveur d'autorisation d'accès (SERV-AUTO) apte à communiquer avec un fournisseur de services (FRS-SERV), le fournisseur de services mettant en œuvre un contrôle d'accès en fonction d'au moins un attribut de l'individu,
le serveur d'autorisation d'accès (SERV-AUTO) ayant une donnée cryptographique publique, la donnée cryptographique publique étant spécifique pour un groupe d'individus ayant au moins un attribut conforme à au moins une règle donnée,
ladite donnée cryptographique publique étant associée à une donnée cryptographique secrète,
ladite donnée cryptographique secrète ayant été utilisée pour générer la donnée d'autorisation d'accès,
le procédé comprenant les étapes suivantes :

- réception d'une information de preuve d'autorisation d'accès, l'information de preuve d'autorisation d'accès ayant été générée au moyen de la donnée d'autorisation d'accès de l'individu (étape 510) ;
- vérification de l'information de preuve d'autorisation d'accès reçue en utilisant la donnée cryptographique publique (étape 520) ;

- si l'information de preuve d'autorisation d'accès est vérifiée, envoi au fournisseur de services (FRS-SERV) d'une information de validation de l'information de preuve d'autorisation d'accès, sans vérification de la conformité d'au moins un attribut de l'individu à ladite au moins une règle donnée lors de la vérification de l'autorisation d'accès (étapes 530, 550).

[Revendication 8] Procédé selon la revendication précédente, caractérisé en ce que la donnée cryptographique publique est reçue du fournisseur de services (FRS-SERV) ou d'un dispositif client (DEV).

[Revendication 9] Procédé selon la revendication 7 ou 8, caractérisé en ce que l'information de preuve d'autorisation d'accès est reçue du fournisseur de services (FRS-SERV) ou d'un dispositif client (DEV).

[Revendication 10] Procédé selon la revendication 7 ou 8, caractérisé en ce que le serveur d'autorisation d'accès est en outre apte à communiquer avec un dispositif client (DEV), et en ce que le procédé comprend en outre, les étapes suivantes :

- réception d'un identifiant de demande de vérification (SessionID) provenant du fournisseur de services (FRS-SERV) ;
- génération d'une information de connexion à partir de l'identifiant de demande de vérification reçu ;
- transmission au fournisseur de services (FRS-SERV) de l'information de connexion générée ;
- création d'un canal de communication entre le serveur d'autorisation d'accès (SERV-AUTO) et le dispositif client (DEV) au moyen de l'information de connexion ;
- réception de l'information de preuve d'autorisation d'accès du dispositif client (DEV) via le canal de communication créé.

[Revendication 11] Procédé selon l'une quelconque des revendications 7 à 10, caractérisé en ce que le serveur d'autorisation d'accès est en outre apte à communiquer avec un dispositif client (DEV), et en ce que le procédé comprend en outre les étapes suivantes :

- génération d'une donnée de vérification (c) ;

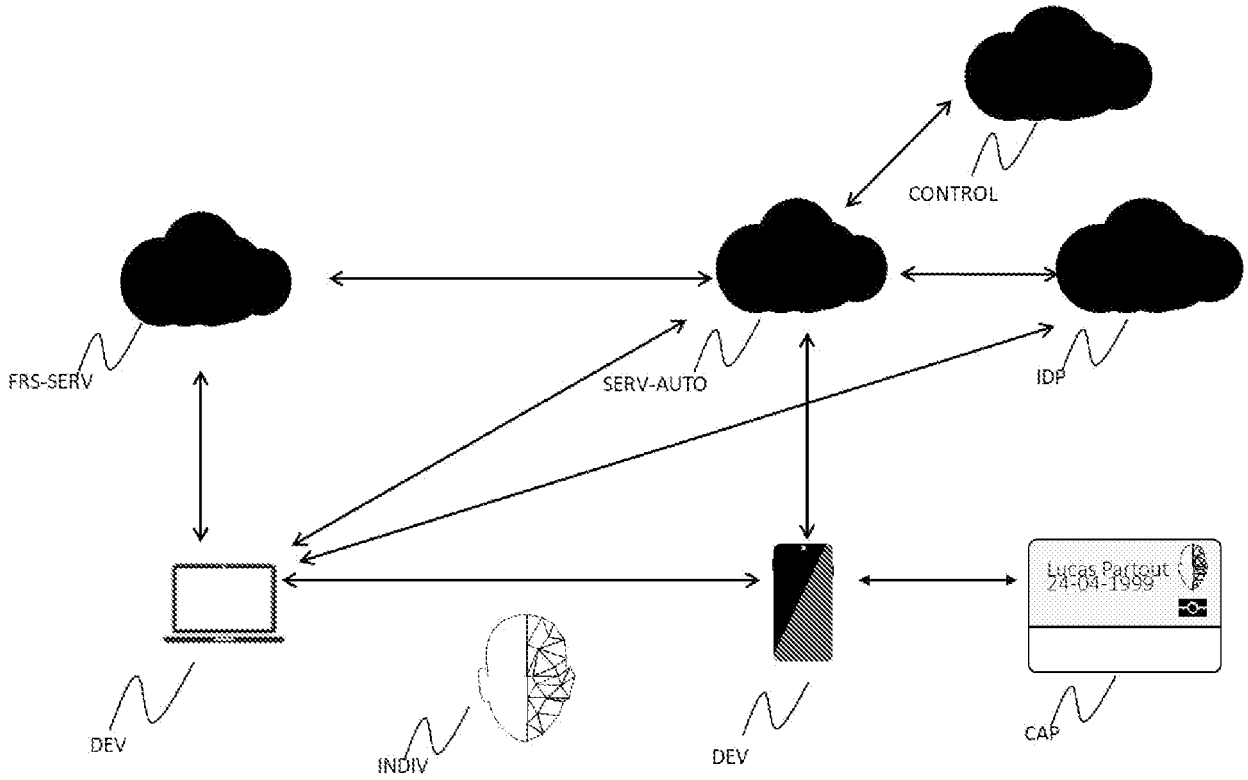
- transmission de la donnée de vérification générée au dispositif client (DEV) ;
- l'information de preuve d'autorisation d'accès reçue étant en outre générée à partir de la donnée de vérification.

[Revendication 12] Procédé selon l'une quelconque des revendications 7 à 11, caractérisé en ce que le serveur d'autorisation d'accès (SERV-AUTO) est apte à communiquer avec une base de données de preuves (BD-PREUVES), et en ce que le procédé comprend en outre, une étape de transmission à ladite base de données de preuves (BD-PREUVES) de l'information de preuve d'autorisation d'accès reçue.

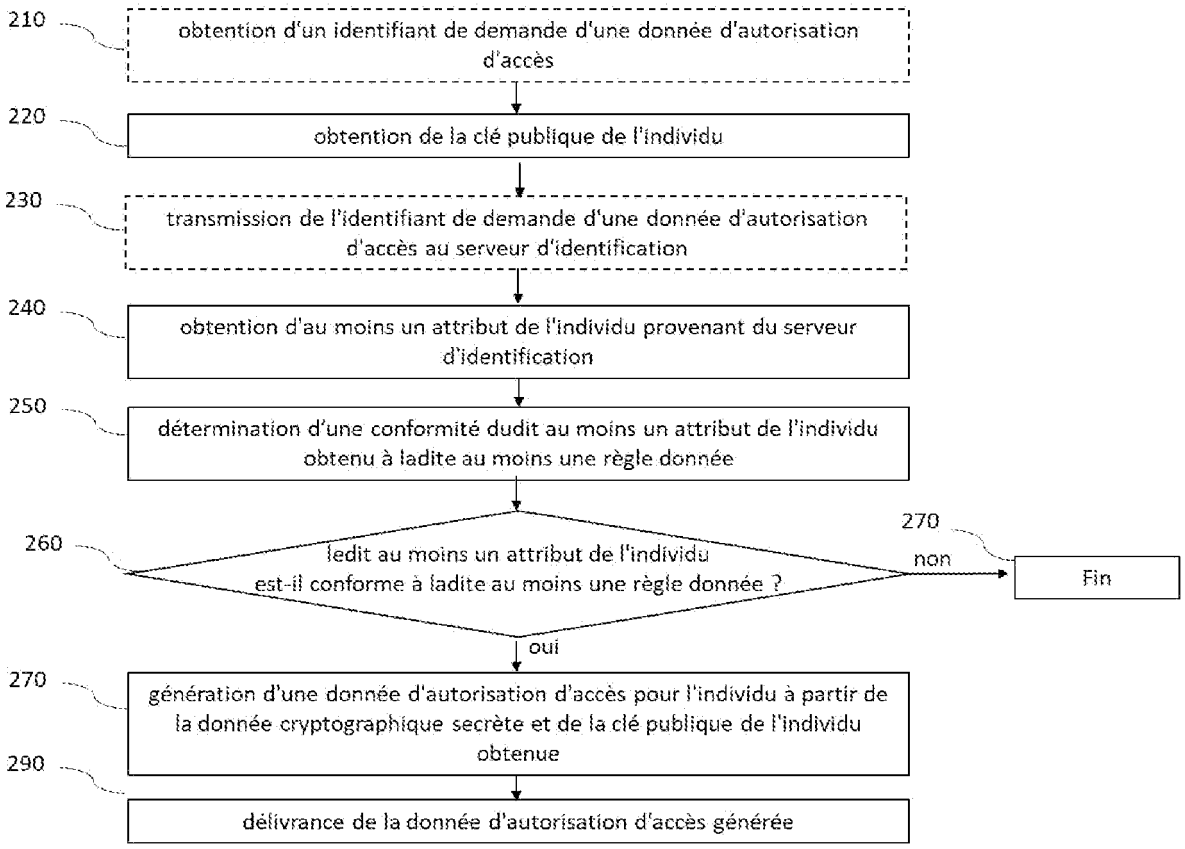
[Revendication 13] Procédé selon l'une quelconque des revendications 7 à 12, caractérisé en ce que le serveur d'autorisation d'accès comprend en outre une donnée identifiant le groupe d'individus ayant au moins un attribut conforme à ladite au moins une règle donnée (IdToken), et en ce que l'étape d'envoi au fournisseur de services (FRS-SERV) d'une information de validation de l'information de preuve d'autorisation d'accès comprend en outre l'envoi de la donnée identifiant le groupe d'individus (IdToken).

[Revendication 14] Dispositif configuré pour mettre en œuvre le procédé selon l'une quelconque des revendications 1 à 6 ou le procédé selon l'une quelconque des revendications 7 à 13.

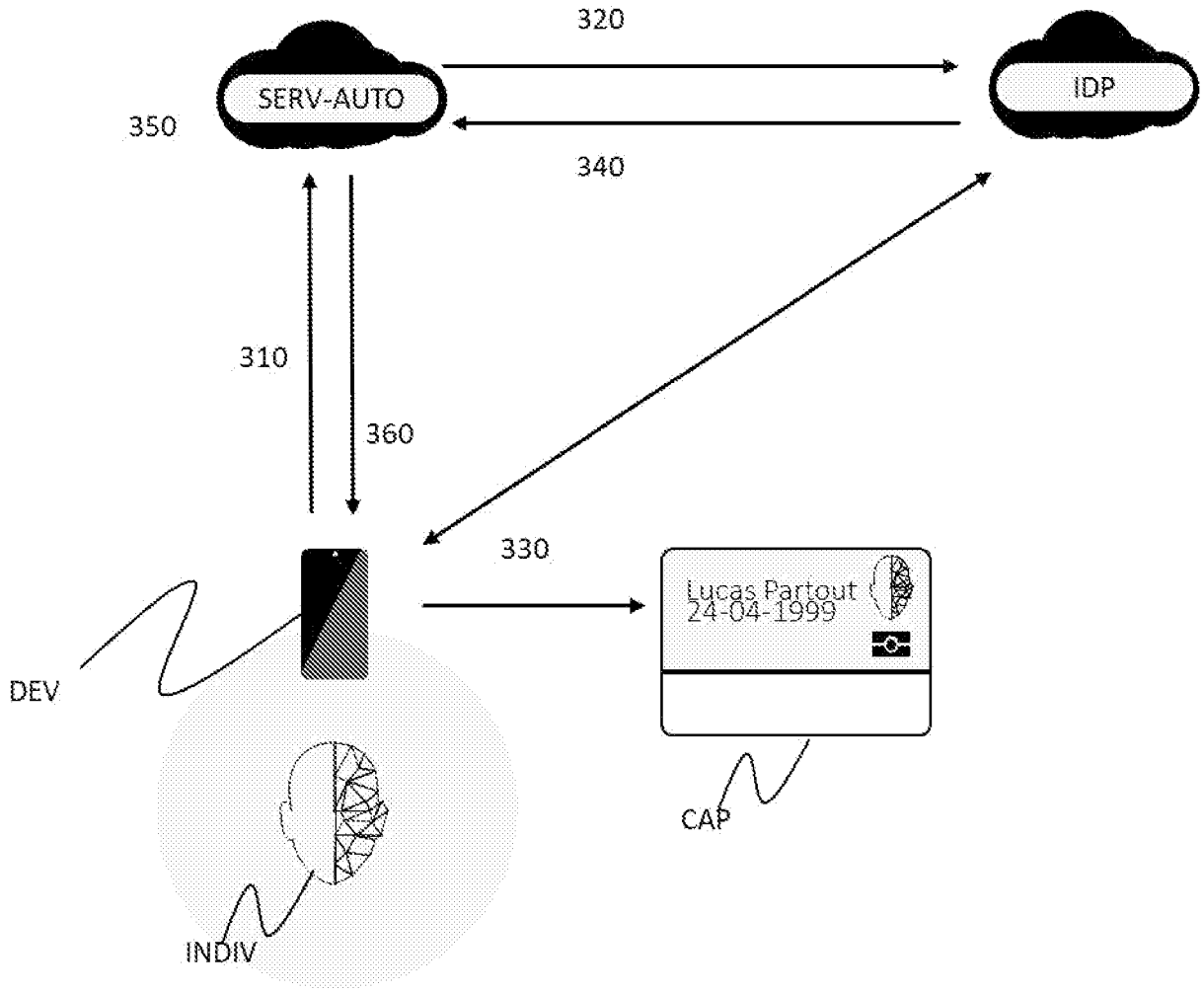
[Fig. 1]


CONTROL
FRS-SERV
SERV-AUTO
IDP
Lucas Partout
24-04-1999
DEV
INDIV
DEV
CAP

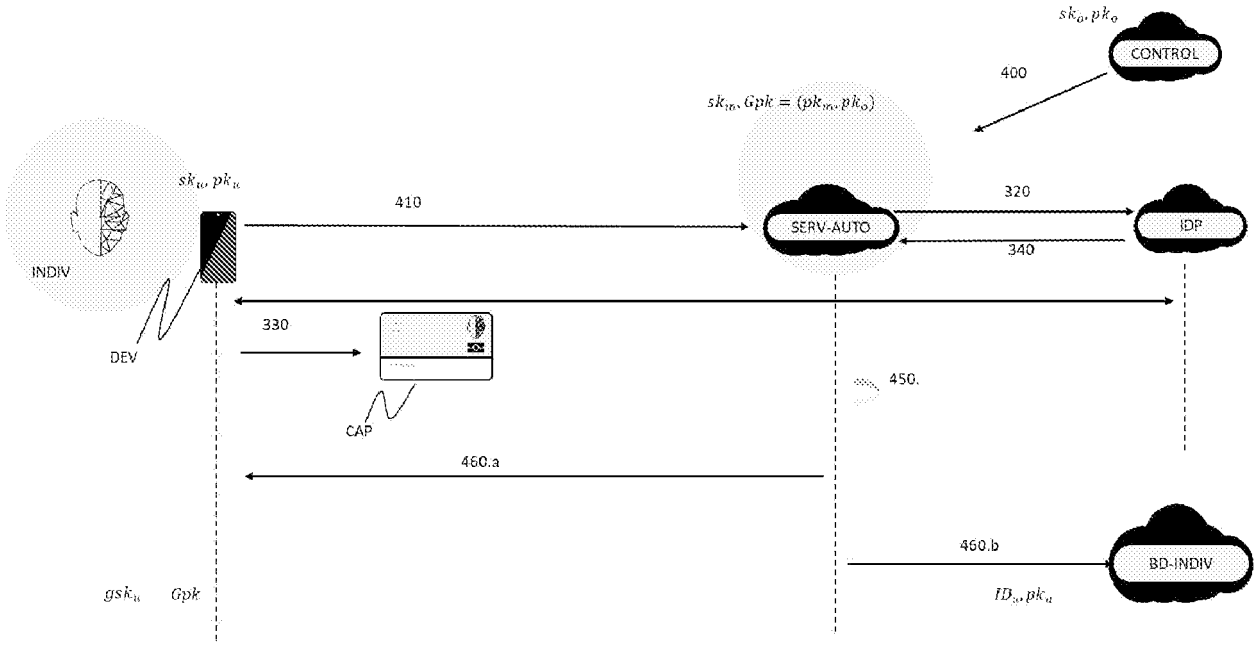
[Fig. 2]


210
obtention d'un identifiant de demande d'une donnée d'autorisation d'accès
220
obtention de la clé publique de l'individu
230
transmission de l'identifiant de demande d'une donnée d'autorisation d'accès au serveur d'identification
240
obtention d'au moins un attribut de l'individu provenant du serveur d'identification
250
détermination d'une conformité dudit au moins un attribut de l'individu obtenu à ladite au moins une règle donnée
260
ledit au moins un attribut de l'individu est-il conforme à ladite au moins une règle donnée ?
270
non
Fin
oui
270
génération d'une donnée d'autorisation d'accès pour l'individu à partir de la donnée cryptographique secrète et de la clé publique de l'individu obtenue
290
délivrance de la donnée d'autorisation d'accès générée

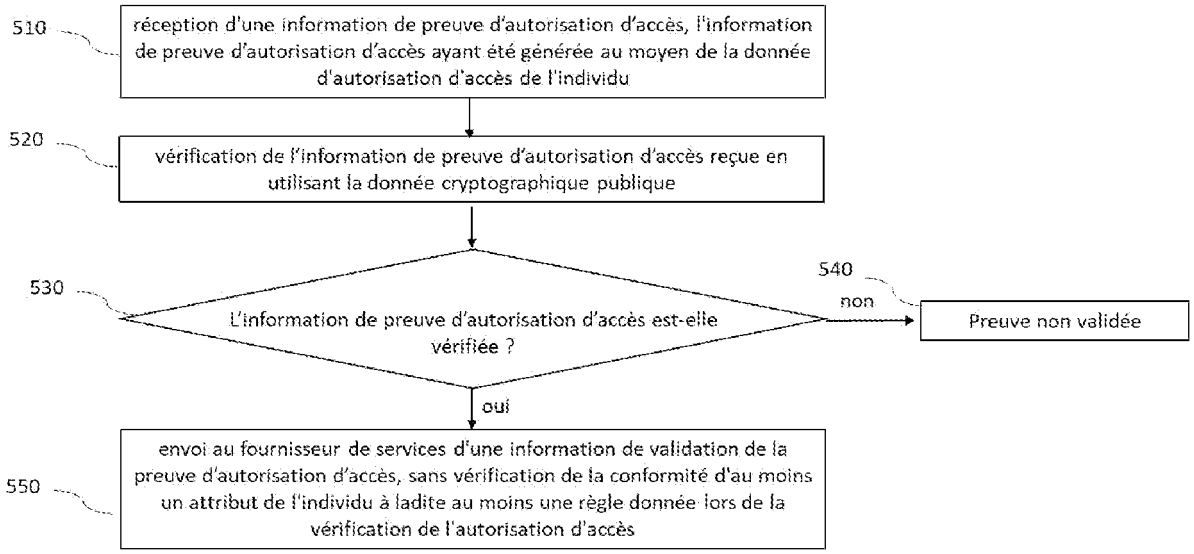
[Fig. 3]


320
SERV-AUTO
IDP
350
340
310
360
330
Lucas Partout
24-04-1999
DEV
CAP
INDIV

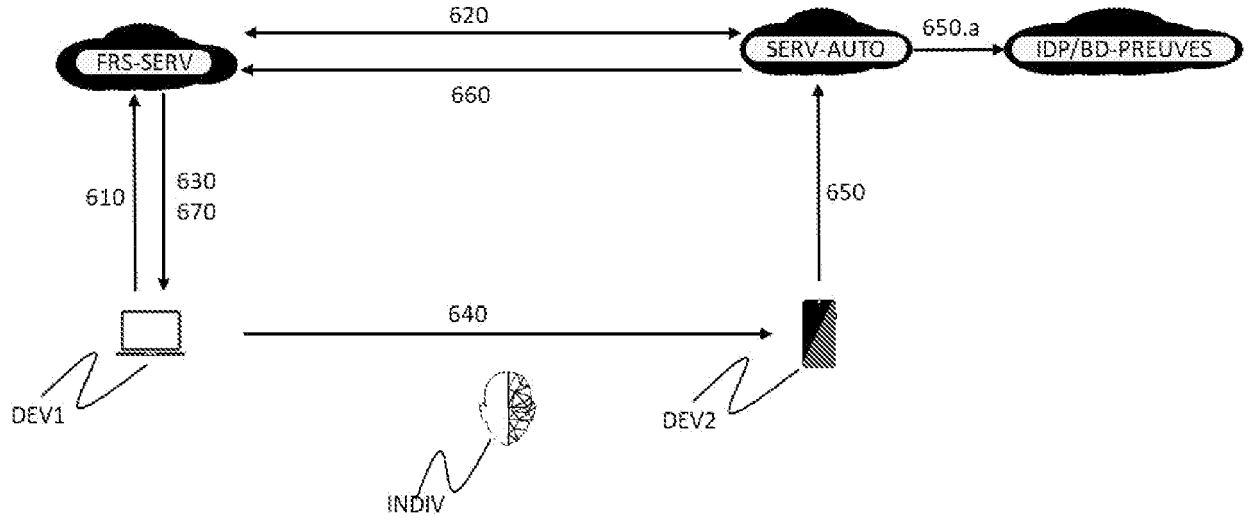
[Fig. 4]


sk_o, pk_o
CONTROL
400
$sk_m, Gpk = (pk_m, pk_o)$
sk_u, pk_u
410
320
SERV-AUTO
IDP
340
INDIV
DEV
330
CAP
450.
460.a
460.b
BD-INDIV
gsk_u
Gpk
ID_u, pk_u

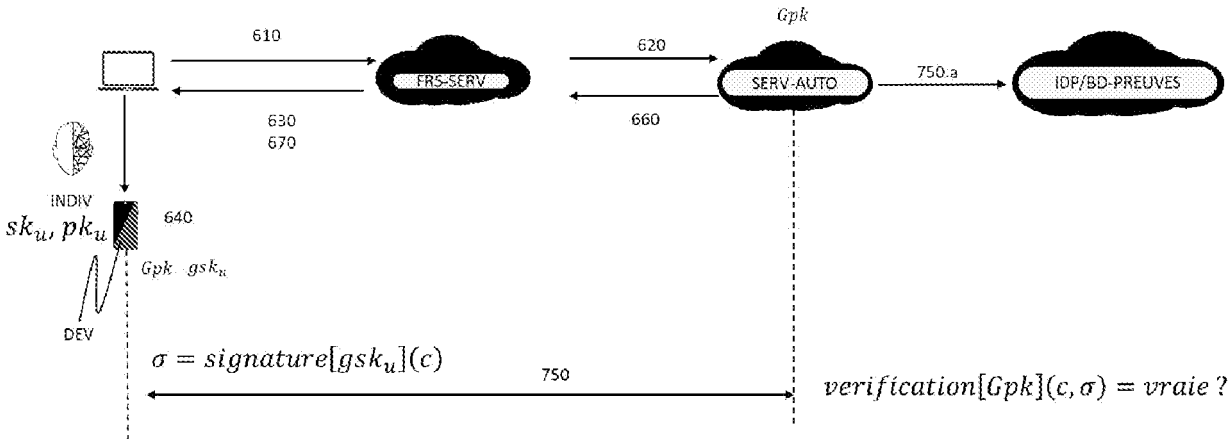
[Fig. 5]



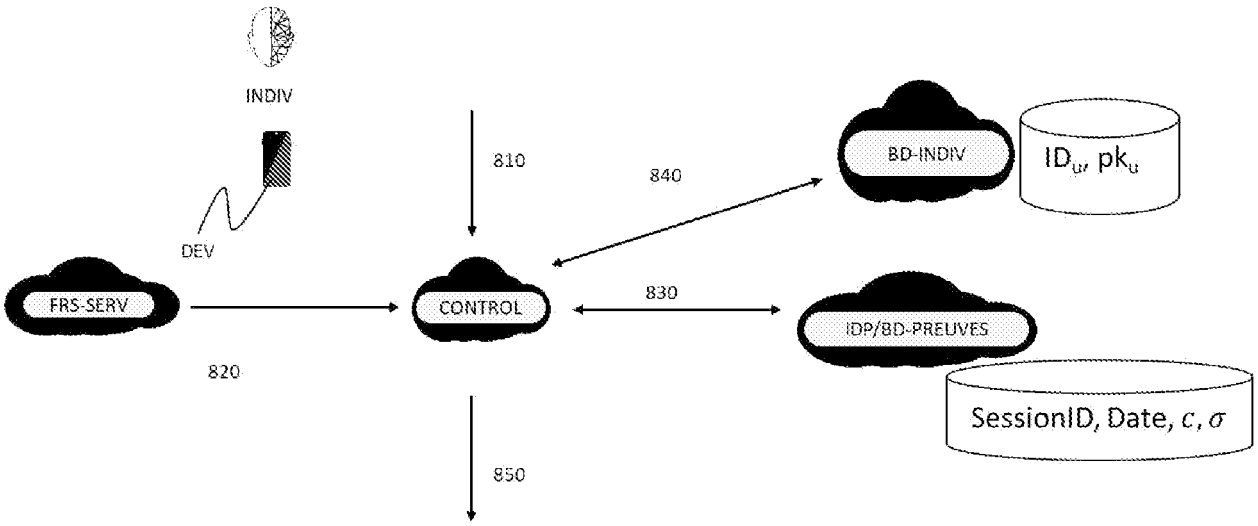
[Fig. 6]



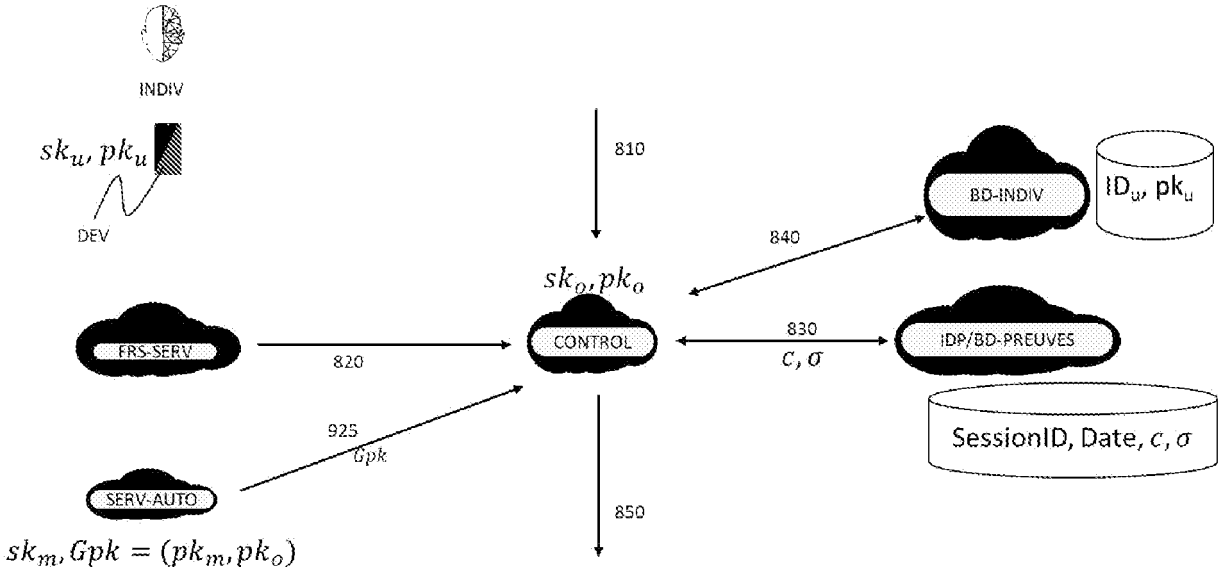
[Fig. 7]



[Fig. 8]


INDIV
DEV
FRS-SERV
CONTROL
BD-INDIV
ID_u, pk_u
IDP/BD-PREUVES
SessionID, Date, c, σ
810
820
830
840
850

[Fig. 9]


INDIV
sk_u, pk_u
DEV
FRS-SERV
CONTROL
sk_o, pk_o
BD-INDIV
ID_u, pk_u
IDP/BD-PREUVES
c, σ
SessionID, Date, c, σ
SERV-AUTO
$sk_m, Gpk = (pk_m, pk_o)$
Gpk
810
820
830
840
850
925

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 917171
FR 2301862

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	ASGHAR MUHAMMAD RIZWAN ET AL: "PRIMA: Privacy-Preserving Identity and Access Management at Internet-Scale", 2018 IEEE INTERNATIONAL CONFERENCE ON COMMUNICATIONS (ICC), IEEE, 20 mai 2018 (2018-05-20), pages 1-6, XP033378717, DOI: 10.1109/ICC.2018.8422732 [extrait le 2018-07-27]	1-12,14	G06F 21/30 G06F 21/45 H04L 9/30
Y	* figures 1,2 *	13	

Y	NABEEL MOHAMED ET AL: "Privacy Preserving Policy-Based Content Sharing in Public Clouds", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, IEEE SERVICE CENTRE , LOS ALAMITOS , CA, US, vol. 25, no. 11, 1 novembre 2013 (2013-11-01), pages 2602-2614, XP011527657, ISSN: 1041-4347, DOI: 10.1109/TKDE.2012.180 [extrait le 2013-09-19] * abrégé *	13	DOMAINES TECHNIQUES RECHERCHÉS (IPC) H04L H04W

A	ZÚQUETE ANDRÉ ET AL: "Personal Identification in the Web Using Electronic Identity Cards and a Personal Identity Provider", 2 juillet 2014 (2014-07-02), SAT 2015 18TH INTERNATIONAL CONFERENCE, AUSTIN, TX, USA, SEPTEMBER 24-27, 2015; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER, BERLIN, HEIDELBERG, PAGE(S) 160 - 169, XP047476688, ISBN: 978-3-540-74549-5 * figure 1 *	1-14	

Date d'achèvement de la recherche	Examinateur
7 septembre 2023	Padilla Serrano, M

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)