(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 044 501**

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

(21) **N° d'enregistrement national :** **15 61439**

(51) Int Cl[8] : ***H 04 L 9/28*** *(2017.01), G 06 F 17/00, G 07 C 5/08*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 26.11.15.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 02.06.17 Bulletin 17/22.

(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) :** *PEUGEOT CITROEN AUTOMOBILES SA Société anonyme* — FR.

(72) **Inventeur(s) :** PATUREAU MIRAND SYLVAIN, FERNANDEZ ANTONIO EDUARDO et TRONCOSO CARMELA.

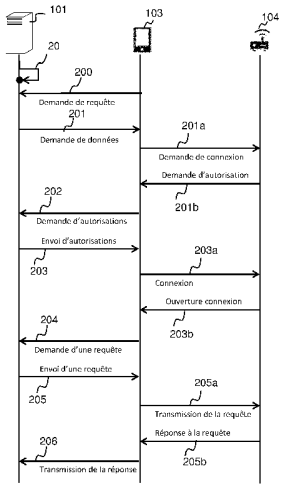
(73) **Titulaire(s) :** PEUGEOT CITROEN AUTOMOBILES SA Société anonyme.

(74) **Mandataire(s) :** PEUGEOT CITROEN AUTOMOBILES SA Société anonyme.

(54) PROCEDE DE TRANSMISSION, PAR UN TERMINAL, DE DONNEES CONFIDENTIELLES DEPUIS UN CALCULATEUR TELEMATIQUE DE VEHICULE VERS UN SERVEUR.

(57) L'invention concerne un procédé d'accès, par un serveur (101), à des données confidentielles disponibles auprès d'un calculateur télématique (104), par l'intermédiaire d'un terminal (103), ledit calculateur télématique (104) comportant une mémoire sécurisée dans laquelle est stockée une clé de chiffrement privée ledit procédé comportant des étapes de:

- Emission (201), par le serveur (101), à destination du terminal (103), d'une demande de données confidentielles disponibles auprès du calculateur télématique (104),
- Réception (202) d'une demande d'autorisation d'accès au calculateur télématique (104), provenant du terminal (103),
- En réponse à la demande, l'émission (203) d'autorisations permettant au terminal (103) de se connecter au calculateur télématique (104),
- Réception (204) d'une demande de requête, provenant du terminal (103),
- Emission (205) d'une requête portant sur les données confidentielles,
- Réception (206) des informations confidentielles demandées, signées par calculateur télématique (104), avec sa clé de chiffrement privée.



FR 3 044 501 - A1

PROCEDE DE TRANSMISSION, PAR UN TERMINAL, DE DONNEES CONFIDENTIELLES DEPUIS UN CALCULATEUR TELEMATIQUE DE VEHICULE VERS UN SERVEUR

L'invention concerne l'échange de données entre différents systèmes informatiques tel qu'un boitier électronique dans un véhicule, des équipements mobiles (Smartphones, tablettes, ordinateur portable…) et des systèmes débarqués (aussi appelé cloud en anglais) et, en particulier, l'échange de données confidentielles.

On connait, par le document US 2013/0190967, un procédé et un système permettant une supervision d'un véhicule à distance. Le système comprend un dispositif mobile communicant avec un serveur, d'une part, et avec le véhicule, d'autre part. Des données issues de capteurs peuvent être transmises du véhicule vers le serveur par l'intermédiaire du dispositif mobile. Cependant, rien n'est prévu pour assurer la sécurité et l'intégrité des données.

L'invention a donc pour but de remédier aux inconvénients précités en fournissant un procédé d'accès, par un serveur, à des données confidentielles disponibles auprès d'un calculateur télématique, par l'intermédiaire d'un dispositif mobile, le un dispositif mobile n'étant pas forcément pourvu d'un dispositif de sécurité.

Elle propose plus précisément à cet effet un procédé de transmission, par l'intermédiaire d'un terminal nomade, de données confidentielles disponibles auprès d'un calculateur télématique d'un véhicule, vers un serveur, ledit procédé mis en œuvre par le terminal nomade, comportant des étapes de :

- Réception d'une demande, provenant du serveur, de données confidentielles disponibles auprès du calculateur télématique,
- Emission d'une demande de requête, à destination du serveur,
- Réception d'une requête portant sur les données confidentielles,
- Transfert de la requête portant sur les données confidentielles vers le calculateur télématique du véhicule,
- Réception des informations confidentielles demandées,

- Transfert des informations confidentielles demandées, vers le serveur,

Caractérisé en ce que, ledit calculateur télématique comportant une mémoire sécurisée dans laquelle est stockée une clé de chiffrement privée, les informations confidentielles réceptionnées et transférées sont signées par le calculateur télématique du véhicule, avec sa clé de chiffrement privée, et en ce que ledit procédé comporte, en outre, en réponse à l'étape, une étape d'établissement d'une connexion sécurisée avec le calculateur télématique du véhicule.

L'invention permet à un serveur de récupérer, de façon sécurisée, des données disponibles auprès d'un calculateur télématique. L'invention trouve son application dans le cas où le calculateur télématique ne dispose de moyen de communication direct avec le serveur. L'échange de données se fait alors par l'intermédiaire d'un terminal dont le niveau de sécurité n'est pas garanti. L'invention permet de garantir la confidentialité des échanges par le chiffrement des messages et l'intégrité des données. Les données envoyées au serveur sont signées par le calculateur télématique.

L'invention permet de garantir l'intégrité de l'information échangée entre le serveur et le calculateur télématique indépendamment de la fiabilité de la chaine de communication (en particulier le terminal).

Le procédé selon l'invention fonctionne de façon asynchrone, celui-ci peut être mis en œuvre même si la connexion de données entre le boitier télématique et le terminal mobile est établi de façon intermittente.

De façon avantageuse, le procédé de transmission de données confidentielles selon l'invention comporte, en outre, une étape d'émission auprès du serveur, d'une demande pour déterminer si le serveur dispose de requêtes confidentielles à traiter. Cette caractéristique permet au terminal d'avoir connaissance des requêtes disponibles auprès du serveur sans que le serveur lui envoie des notifications.

De façon avantageuse, le procédé de transmission de données confidentielles selon l'invention comporte, en outre, en l'absence de connexion sécurisée avec le calculateur télématique du véhicule, le stockage

dans une mémoire du terminal nomade de la demande de données confidentielles. Cette caractéristique permet au terminal mobile de procéder à directement une demande de requête suite à une connexion réussie avec un boitier télématique.

De façon avantageuse, l'étape d'établissement d'une connexion sécurisée avec le calculateur télématique du véhicule comporte des étapes de :

- Emission d'une demande de connexion à destination du calculateur télématique,
- Réception d'une demande d'autorisation d'accès au calculateur télématique, provenant du calculateur télématique,
- Emission de la demande d'autorisation d'accès au calculateur télématique, à destination du serveur,
- Réception d'autorisations permettant au terminal mobile de se connecter au calculateur télématique,
- Demande de connexion au auprès du calculateur télématique du véhicule avec les autorisations reçues,
- Réception d'un acquittement d'ouverture de connexion.

De façon avantageuse, les autorisations sont reçues sous la forme d'un jeton, ledit jeton étant signé par le serveur et chiffré avec la clé de chiffrement public associée à la clé de chiffrement privée du calculateur télématique.

De façon avantageuse, le procédé de transmission de données confidentielles selon l'invention comporte, en outre, après le transfert des informations confidentielles demandées, l'émission d'une demande au serveur, pour demander s'il a une autre demande de données confidentielles à traiter. Cette caractéristique permet le traitement de plusieurs requêtes consécutivement lors d'une même connexion entre le terminal mobile et le boitier télématique.

L'invention concerne aussi un terminal mobile apte à transmettre des données confidentielles disponibles auprès d'un calculateur télématique d'un

véhicule, à un serveur, caractérisé en ce qu'il comporte :

- des moyens de réception, d'une demande, provenant du serveur, de données confidentielles disponibles auprès du calculateur télématique,
- des moyens de d'émission d'une demande de requête, à destination du serveur,
- des moyens de réception d'une requête portant sur les données confidentielles,
- des moyens de transfert de la requête portant sur les données confidentielles vers le calculateur télématique du véhicule,
- des moyens de réception des informations confidentielles demandées, signées par le calculateur télématique du véhicule, avec sa clé de chiffrement privée,
- des moyens de transfert des informations confidentielles demandées, vers le serveur,

Caractérisé en ce que ledit calculateur télématique comportant une mémoire sécurisée dans laquelle est stockée une clé de chiffrement privée, les informations confidentielles réceptionnées et transférées sont signées par le calculateur télématique du véhicule, avec sa clé de chiffrement privée, et en ce que le terminal nomade comporte, en outre, des moyens d'établissement d'une connexion sécurisée avec le calculateur télématique du véhicule.

D'autres caractéristiques et avantages de l'invention apparaîtront à l'examen de la description détaillée ci-après, et des dessins annexés, sur lesquels:

- la figure 1 illustre une vue schématique du système selon l'invention ;
- la figure 2 illustre un diagramme représentant des étapes du procédé selon l'invention.

Les dessins annexés pourront non seulement servir à compléter l'invention, mais aussi contribuer à sa définition, le cas échéant.

En référence à la figure 1, le système d'échange de données selon l'invention comporte au moins un terminal 103, un calculateur télématique 104 et un serveur 101. L'invention permet de transmettre de façon sécurisée des données confidentielles depuis le calculateur télématique 104 vers le serveur

101 par l'intermédiaire du terminal 103.

Pour ce faire, le serveur 101 (agissant comme une autorité d'authentification) délivre les authentifications et des autorisations au terminal 103. La transmission de ces authentifications et de ces autorisations est assurée au moyen de jetons d'autorisation aussi appelés token ou encore « identity credentials » en anglais.

Dans ce qui suit, on considère à titre d'exemple non limitatif que le terminal 103 est un téléphone mobile intelligent (aussi appelé smartphone en anglais). Mais l'invention n'est pas limitée à cet exemple. En effet, le terminal 103 peut être un ordinateur portable, une tablette tactile ou tout autre objet connecté (i.e. susceptible d'échanger des données via une connexion sans fils). Cet équipement mobile (ou objet connecté) appartient, par exemple, au conducteur d'un véhicule ou à l'un des passagers du véhicule.

Le terminal mobile 103 comporte en outre :

- des moyens de réception, d'une demande, provenant du serveur 101, de données confidentielles disponibles auprès du fournisseur de service 104,

- des moyens de d'émission d'une demande de requête, à destination du serveur 101,

- des moyens de réception d'une requête portant sur les données confidentielles,

- des moyens de transfert de la requête portant sur les données confidentielles vers le calculateur télématique 104 du véhicule,

- des moyens de réception des informations confidentielles demandées, signées par le calculateur télématique 104 du véhicule, avec sa clé de chiffrement privée,

- des moyens de transfert des informations confidentielles demandées, vers le serveur 101,

- ledit calculateur télématique 104 comportant une mémoire sécurisée dans laquelle est stockée une clé de chiffrement privée, les informations confidentielles réceptionnées et transférées sont signées par le

calculateur télématique 104 du véhicule, avec sa clé de chiffrement privée,

- des moyens d'établissement d'une connexion sécurisée avec le calculateur télématique 104 du véhicule,
- Et une mémoire destinée à stocker en l'absence de connexion sécurisée avec le calculateur télématique 104 du véhicule la demande de données confidentielles.

Ces moyens sont réalisés de façon matérielle, logicielle ou selon une combinaison des deux.

Le calculateur télématique 104 est une ressource informatique, contrôlant l'accès à des données ou à des commandes permettant de réaliser une activité. Le calculateur télématique 104 protège l'accès aux données et aux applications. Il refuse tout accès sans authentification préalable. De façon avantageuse, il redirige l'utilisateur non authentifié vers un fournisseur d'identité (par exemple le serveur 101). L'accès au service est donc restreint. Les utilisateurs doivent être identifiés avant de pouvoir accéder à une donnée ou lancer l'exécution d'une commande.

Les jetons, utilisés pour transmettre les autorisations, sont chiffrés (ou cryptés) selon un mécanisme de cryptographie asymétrique (aussi appelé cryptographie à clé publique). Dans un tel système, on utilise une paire de clés : une clé publique pour le chiffrement et une clé privée pour le déchiffrement. Lorsqu'une ressource envoie un jeton à une autre ressource informatique, il lui suffit de chiffrer le jeton à envoyer au moyen de la clé publique du destinataire. Ce dernier sera en mesure de déchiffrer le message à l'aide de sa clé privée (qu'il est seul à connaître).

Les jetons sont, en outre, signés par une autorité de confiance (par exemple le serveur 101) pour garantir qu'ils sont bien conformes et qu'ils proviennent bien d'une source autorisée.

Les jetons intègrent les autorisations qui permettent de donner les accès à des fonctions ou des données sur les services hébergés sur les infrastructures, chez des partenaires ou sur les boitiers connectés.

Selon une caractéristique de l'invention, le calculateur télématique 104 comporte un espace de stockage sécurisé apte à stocker une clé privée

utilisée pour déchiffrer les jetons d'autorisation. L'espace de stockage sécurisé est par exemple une puce TPM (pour Trusted Platform Module), qui est un composant cryptographique matériel permettant de stocker des secrets (tels que des clefs de chiffrement) de manière sécurisée.

Dans ce qui suit, on considère à titre d'exemple non limitatif que le calculateur télématique 104 est un boitier électronique d'un véhicule automobile 105. Le boitier électronique est un organe embarqué du véhicule qui est la frontière des données véhicule vers l'extérieur au travers de différents moyens : câble, protocoles sans fils (wifi, bluetooth,3G, etc.).

Mais l'invention n'est pas limitée à cet exemple. En effet, le calculateur télématique peut être un système d'information de gestion ou le système qui pilote une machine à commande numérique ou plus généralement n'importe quel objet connecté (i.e. susceptible d'échanger des données via une connexion sans fil) et comprenant un espace de stockage sécurisé susceptible de stocker une clé privée.

Le serveur 101 (ou IdP pour Identity Provider) s'occupe notamment d'authentifier l'utilisateur ainsi que de récupérer des informations additionnelles associées à son identité. Le serveur comporte aussi des moyens pour récupérer des informations confidentielles auprès d'un ou plusieurs calculateurs télématiques 104.

Le serveur 101 comporte des moyens pour signer, de façon électronique, des jetons d'autorisation. La signature électronique permet de garantir l'intégrité d'un jeton et d'en authentifier l'auteur. Le système de signature électronique utilise une paire de clés. Une clé privée utilisée pour signer un jeton et une clé publique permettant de lire le jeton signé.

Le serveur 101 comporte des moyens pour chiffrer le jeton. Le jeton est chiffré à l'aide d'une clé publique associée au calculateur télématique 104 auquel est destiné le jeton.

De la sorte, le jeton chiffré est uniquement lisible par le calculateur télématique 104 auquel il est destiné.

Le système peut aussi comporter une infrastructure à clés publiques (ou PKI pour Public Key Infrastructure en anglais), non représentée. Une PKI est une ressource informatique permettant de générer, de distribuer et de

publier des certificats aux différents composants nécessaires (fournisseur de service 104, serveur 101). Le serveur 101 et les différents calculateurs télématiques 104 disposent chacun d'un certificat qui leur est propre.

On rappelle qu'un certificat (ou certificat électronique) est un ensemble de données contenant au moins une clé publique, au moins une information d'identification (par exemple : un nom, généralement stocké dans un champ de données dit CN pour « Common Name ») et au moins une clé privée pour signer.

La figure 2 montre un diagramme illustrant les différentes étapes du procédé selon l'invention.

Le procédé comporte tout d'abord l'émission 200, par le terminal nomade 103, auprès du serveur 101 d'une demande pour déterminer si le serveur 101 dispose de requêtes confidentielles à traiter. De façon avantageuse, la demande comporte au moins un identifiant de véhicule (par exemple, un VIN pour Vehicle Identification Number), et/ou du calculateur télématique 104, de sorte que le serveur 101 est en mesure de répondre si des requêtes spécifiques au véhicule sont disponibles. Le ou les identifiants envoyés correspondent à des véhicules avec lesquels le terminal 103 s'est connecté au moins une fois.

De façon préférentielle, cette étape est exécutée à l'initialisation d'une application logicielle mettant en œuvre le procédé sur le terminal nomade et/ou de façon périodique si l'application tourne en tache en fond sur terminal nomade 103.

Le procédé comporte ensuite la réception 201, par le terminal nomade 103, provenant du serveur 101, d'une demande de données confidentielles disponibles auprès du calculateur télématique 104. La demande de données confidentielles est émise par le serveur 101 en réponse à la demande précédente 200, en particulier lorsque le serveur 101 a préalablement préparé et mis en attente 20 une demande de données confidentielles. De façon avantageuse, cette demande indique l'identifiant de véhicule.

Lorsque le terminal 103 reçoit la demande du serveur 101, celui-ci

103 essaie de se connecter 201a de façon sécurisée au calculateur télématique 104. Le calculateur télématique 104, en réponse, réclame une autorisation 201b pour la connexion. Le terminal transmet 202 alors la demande d'autorisation au serveur 101.

Ensuite, le serveur reçoit la demande d'autorisation d'accès au calculateur télématique 104, provenant du terminal 103.

La réponse du terminal 103 est immédiate si celui-ci est en mesure de se connecter au fournisseur de ressource 104, ce qui est le cas par exemple si l'utilisateur est dans son véhicule.

Cependant, dans le cas où le terminal 103 n'est pas en mesure de se connecter avec le calculateur télématique 104, alors le terminal 103 stocke la demande du serveur 101 dans une mémoire. La demande du serveur 101 est traitée quand le terminal 103 est en mesure de se connecter au calculateur télématique 104, par exemple lorsque le terminal 103 est à une portée suffisante du calculateur télématique 104 pour établir une connexion par Bluetooth.

La connexion du téléphone 103 au boitier électronique 104 du véhicule est une connexion par exemple sans fil (par exemple wifi, Bluetooth ou 3G).

L'étape suivante est la réception 203, par le terminal 103, des autorisations nécessaires pour avoir accès aux données confidentielles. Comme expliqué précédemment ces autorisations sont transportées par des jetons.

Lorsque le terminal 103 reçoit les autorisations nécessaires, il se connecte 203a au calculateur télématique 104. Le calculateur télématique 104 vérifie les autorisations, ouvre une connexion et envoie 203b au terminal 103 un acquittement d'ouverture de connexion.

Le terminal 103 est alors prêt à transmettre les données confidentielles. Le terminal 103 ayant reçu une demande de remontée de données confidentielles émet 204 une demande de création de requête vers le serveur 101 en rapport de l'identifiant du calculateur télématique 104.

Le serveur 101 réceptionne la demande de requête, provenant du terminal 103. Le serveur 101 génère une clé à usage unique et un identifiant

de requête associé et les conserve jusqu'au retour de la requête. Le serveur 101 crée la requête pour le calculateur télématique 104. La requête comporte notamment un identifiant de requête et la clé de chiffrement de la réponse. La requête est, de façon avantageuse, chiffrée avec la clé publique du calculateur télématique 104 et signé par le serveur 101. La requête est transmise 205 au terminal 103.

Une fois reçue par le terminal 103, la requête est relayée 205a au calculateur télématique 104.

La signature de la requête est validée par le calculateur télématique 104 puis la requête est déchiffrée avec la clé privée du calculateur télématique. La réponse est construite avec les données demandées ainsi qu'avec l'identifiant de la requête puis chiffrées avec la clé symétrique trouvée dans la requête. La réponse est envoyée 205b au terminal 103.

Le terminal 103 transfert 206 la réponse au serveur 101.

De façon avantageuse, le terminal 103 demande aussi s'il y a une autre requête confidentielle à traiter.

Le serveur 101 déchiffre la réponse avec la clé symétrique à usage unique associée à la requête. Le serveur 101 vérifie aussi la signature du calculateur télématique 104.

De façon avantageuse, le serveur 101 répond avec une autre requête de donnée confidentielle si celle-ci est demandée.

REVENDICATIONS

1. Procédé de transmission, par l'intermédiaire d'un terminal nomade (103), de données confidentielles disponibles auprès d'un calculateur télématique (104) d'un véhicule (105), vers un serveur (101), ledit procédé mis en œuvre par le terminal nomade (103), comportant des étapes de :

- Réception (201) d'une demande, provenant du serveur (101), de données confidentielles disponibles auprès du calculateur télématique (104),
- Emission (204) d'une demande de requête, à destination du serveur (101),
- Réception (205) d'une requête portant sur les données confidentielles,
- Transfert (205a) de la requête portant sur les données confidentielles vers le calculateur télématique (104) du véhicule,
- Réception (205b) des informations confidentielles demandées,
- Transfert (206) des informations confidentielles demandées, vers le serveur (101),

Caractérisé en ce que, ledit calculateur télématique (104) comportant une mémoire sécurisée dans laquelle est stockée une clé de chiffrement privée, les informations confidentielles réceptionnées (205b) et transférées (206) sont signées par le calculateur télématique (104) du véhicule, avec sa clé de chiffrement privée, et en ce que ledit procédé comporte, en outre, en réponse à l'étape (201), une étape d'établissement d'une connexion sécurisée avec le calculateur télématique (104) du véhicule.

2. Procédé de transmission de données confidentielles selon la revendication 1, caractérisé qu'il comporte, en outre, une étape d'émission (200), auprès du serveur (101), d'une demande pour déterminer si le serveur (101) dispose de requêtes confidentielles à traiter.

3. Procédé de transmission de données confidentielles selon l'une des revendications 1 ou 2, caractérisé en ce qu'il comporte en outre, en

l'absence de connexion sécurisée avec le calculateur télématique (104) du véhicule, le stockage dans une mémoire du terminal nomade (103) de la demande de données confidentielles.

4. Procédé de transmission de données confidentielles selon l'une des revendications précédentes, caractérisé que l'étape d'établissement d'une connexion sécurisée avec le calculateur télématique (104) du véhicule comporte des étapes de :

- Emission (201a) d'une demande de connexion à destination du calculateur télématique (104),
- Réception (201b) d'une demande d'autorisation d'accès au calculateur télématique (104), provenant du calculateur télématique (104),
- Emission (202) de la demande d'autorisation d'accès au calculateur télématique (104), à destination du serveur (101),
- Réception (203) d'autorisations permettant au terminal mobile (103) de se connecter au calculateur télématique (104),
- Demande (203a) de connexion au auprès du calculateur télématique (104) du véhicule avec les autorisations reçues,
- Réception (203b) d'un acquittement d'ouverture de connexion.

5. Procédé de transmission de données confidentielles selon l'une des revendications précédentes, caractérisé en ce que les autorisations sont émises (203) sous la forme d'un jeton, ledit jeton étant signé par le serveur (101) et chiffré avec la clé de chiffrement public associée à la clé de chiffrement privée du calculateur télématique (104).

6. Procédé de transmission de données confidentielles selon l'une des revendications précédentes, caractérisé en ce qu'il comporte en outre après le transfert (206) des informations confidentielles demandées, l'émission d'une demande au serveur (101), pour demander s'il a une autre demande de données confidentielles à traiter.

7. Terminal mobile (103) apte à transmettre des données confidentielles disponibles auprès d'un calculateur télématique (104) d'un véhicule, à un serveur (101), caractérisé en ce qu'il comporte :

- des moyens de réception (201), d'une demande, provenant du serveur (101), de données confidentielles disponibles auprès du calculateur télématique (104),
- des moyens de d'émission (204) d'une demande de requête, à destination du serveur (101),
- des moyens de réception (205) d'une requête portant sur les données confidentielles,
- des moyens de transfert de la requête portant sur les données confidentielles vers le calculateur télématique (104) du véhicule,
- des moyens de réception des informations confidentielles demandées, signées par le calculateur télématique (104) du véhicule, avec sa clé de chiffrement privée,
- des moyens de transfert des informations confidentielles demandées, vers le serveur (101),
- Caractérisé en ce que ledit calculateur télématique (104) comportant une mémoire sécurisée dans laquelle est stockée une clé de chiffrement privée, les informations confidentielles réceptionnées et transférées sont signées par le calculateur télématique (104) du véhicule, avec sa clé de chiffrement privée, et en ce que le terminal nomade (103) comporte, en outre, des moyens d'établissement d'une connexion sécurisée avec le calculateur télématique (104) du véhicule.

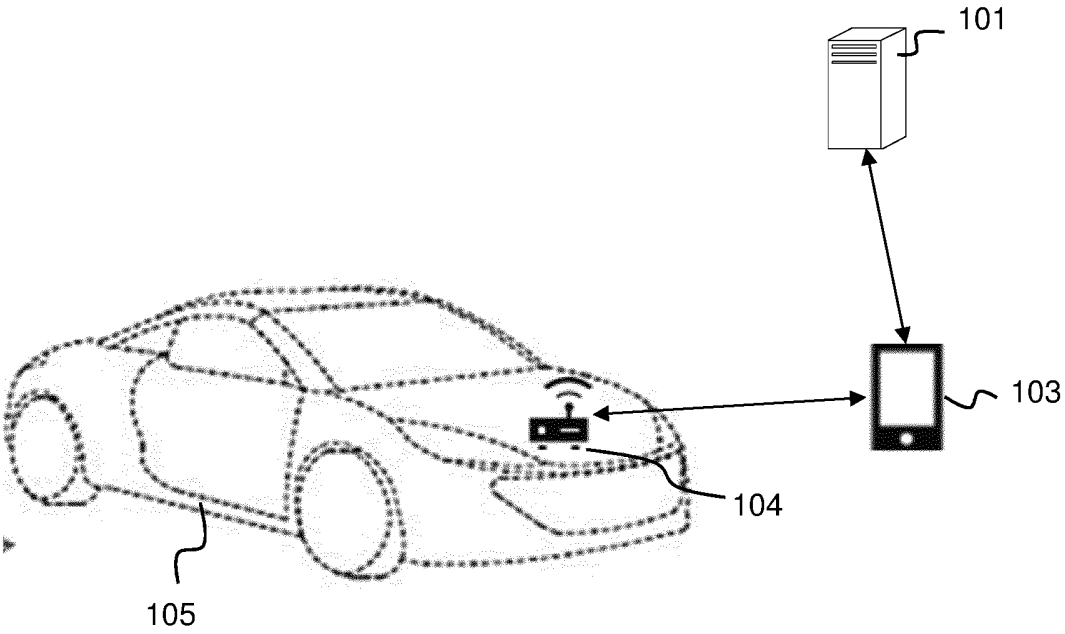


Fig. 1

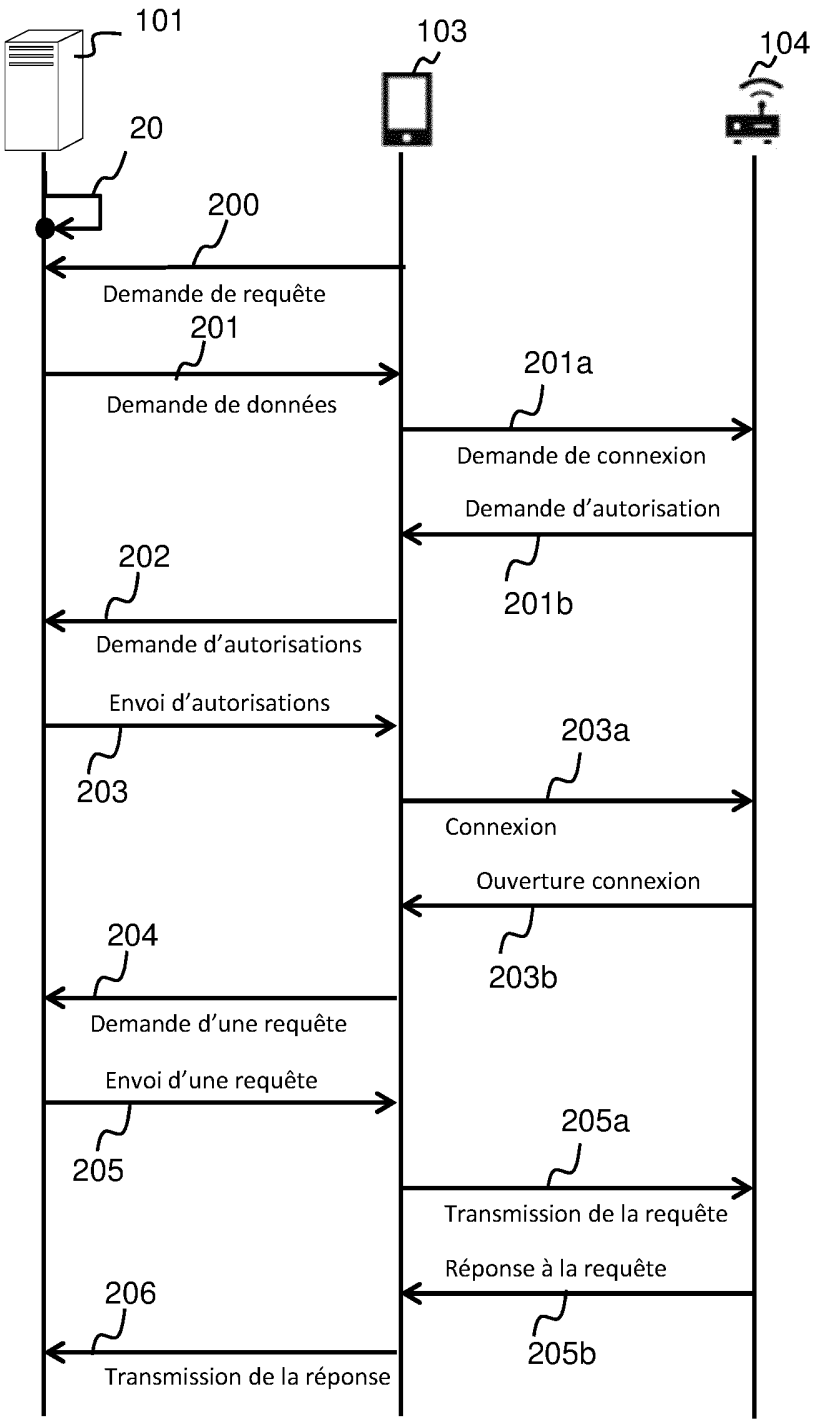

101
103
104
20
200
Demande de requête
201
Demande de données
201a
Demande de connexion
Demande d'autorisation
201b
202
Demande d'autorisations
Envoi d'autorisations
203
203a
Connexion
Ouverture connexion
203b
204
Demande d'une requête
Envoi d'une requête
205
205a
Transmission de la requête
Réponse à la requête
205b
206
Transmission de la réponse

Fig. 2

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 819526
FR 1561439

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		
Y	US 2015/312655 A1 (BALAKRISHNAN HARI [US] ET AL) 29 octobre 2015 (2015-10-29) * alinéas [0001], [0014], [0027] * * alinéas [0046] - [0057] * * alinéas [0089] - [0097] * * alinéas [0118] - [0127] * * figures 1-9 * -----	1-7	H04L9/28 G06F17/00 G07C5/08
Y	US 2015/005984 A1 (DE LOS SANTOS HANLY [US] ET AL) 1 janvier 2015 (2015-01-01) * alinéa [0015] * * alinéa [0050] - alinéa [0056] * * figures 1,2 * -----	1-7	
X	US 6 490 513 B1 (FISH ROBERT [US] ET AL) 3 décembre 2002 (2002-12-03) * colonne 2, ligne 25 - colonne 12, ligne 12 * * figures 1-4 * -----	1-7	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			H04W G07C

Date d'achèvement de la recherche	Examinateur
22 juillet 2016	Ghomrasseni, Z

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)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1561439 FA 819526

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 22-07-2016
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2015312655 A1	29-10-2015	AU 2014331637 A1	12-11-2015
		US 2015312655 A1	29-10-2015
		WO 2015166314 A1	05-11-2015
US 2015005984 A1	01-01-2015	AUCUN	
US 6490513 B1	03-12-2002	CN 1402135 A	12-03-2003
		EP 1286312 A2	26-02-2003
		JP 2003186748 A	04-07-2003
		KR 20030017334 A	03-03-2003
		US 6490513 B1	03-12-2002

EPO FORM P0465