

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la
Propriété Intellectuelle
Bureau international



(43) Date de la publication internationale
11 juin 2015 (11.06.2015)

WIPO | PCT

(10) Numéro de publication internationale
WO 2015/082607 A1

(51) Classification internationale des brevets :
G01D 21/00 (2006.01) **H04L 29/06** (2006.01)
H04L 9/00 (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2014/076560

(22) Date de dépôt international :
4 décembre 2014 (04.12.2014)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
13 62108 4 décembre 2013 (04.12.2013) FR

(71) Déposant : **SCHNEIDER ELECTRIC INDUSTRIES SAS** [FR/FR]; 35 rue Joseph Monier, F-92500 Reuil-Malmaison (FR).

(72) Inventeurs : **CHICHE, Thierry**; 56 allée du fangeat, F-38330 Saint Ismier (FR). **PLATEL, Laurent**; 8 rue Alfred de Musset, F-38400 Saint Martin d'Heres (FR).

(74) Mandataires : **BLOT, Philippe** et al.; 2, place d'Estienne d'Orves, F-75009 Paris (FR).

(81) États désignés (sauf indication contraire, pour tout titre de protection nationale disponible) : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée :

— avec rapport de recherche internationale (Art. 21(3))

(54) Title : MEASUREMENT SENSOR, MEASUREMENT INSTALLATION COMPRISING SUCH A SENSOR AND A SERVER, METHOD OF EXCHANGING DATA AND COMPUTER PROGRAM PRODUCT ASSOCIATED THEREWITH

(54) Titre : CAPTEUR DE MESURE, INSTALLATION DE MESURE COMPRENANT UN TEL CAPTEUR ET UN SERVEUR, PROCÉDÉ D'ÉCHANGE DE DONNÉES ET PRODUIT PROGRAMME D'ORDINATEUR ASSOCIÉS

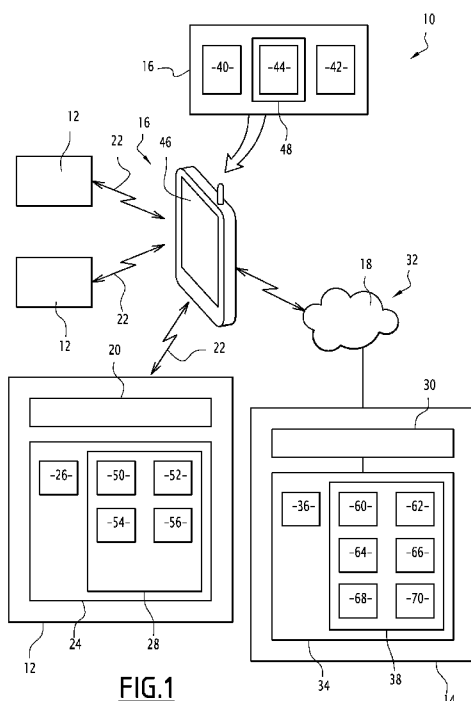


FIG.1

(57) Abstract : This sensor (12) for measuring a quantity, such as an electric quantity or a thermodynamic quantity, is intended to be linked to a computer server (14) via a communication gateway (16), the communication gateway (16) being linked to the computer server (14) via a communication network (18). The sensor (12) comprises an information processing unit (24) comprising a memory (28), radioelectric means (20) of communication with the gateway (16), and means (50) for exchanging data with the computer server (14), the means for exchanging data (50) being linked to the radioelectric means of communication (20). The memory (28) comprises information regarding secure connection to the computer server (14), said information regarding connection comprising a sensor authentication code (52).

(57) Abrégé : Ce capteur (12) de mesure d'une grandeur, telle qu'une grandeur électrique ou une grandeur thermodynamique, est destiné à être relié à un serveur informatique (14) via une passerelle de communication (16), la passerelle de communication (16) étant reliée au serveur informatique (14) via un réseau de communication (18). Le capteur (12) comprend une unité de traitement d'informations (24) comportant une mémoire (28), des moyens radioélectriques (20) de communication avec la passerelle (16), et des moyens (50) d'échange de données avec le

[Suite sur la page suivante]



serveur informatique (14), les moyens d'échange de données (50) étant reliés aux moyens radioélectriques de communication (20). La mémoire (28) comporte des informations de connexion sécurisée au serveur informatique (14), lesdites informations de connexion comportant un code (52) d'authentification du capteur.

Capteur de mesure, installation de mesure comprenant un tel capteur et un serveur, procédé d'échange de données et produit programme d'ordinateur associés

La présente invention concerne un capteur de mesure d'une grandeur, telle qu'une grandeur électrique ou une grandeur thermodynamique, destiné à être relié à un serveur informatique via une passerelle de communication. La passerelle de communication est reliée au serveur informatique via un réseau de communication, tel que le réseau Internet.

Le capteur comprend une unité de traitement d'informations comportant une mémoire, des moyens radioélectriques de communication avec la passerelle, et des moyens d'échange de données avec le serveur informatique, les moyens d'échange de données étant reliés aux moyens radioélectriques de communication.

L'invention concerne également une installation de mesure comprenant au moins un tel capteur de mesure et un serveur informatique relié à chaque capteur de mesure.

L'invention concerne également un procédé d'échange de données entre un tel capteur de mesure et le serveur informatique, via la passerelle de communication.

L'invention concerne également un produit programme d'ordinateur comportant des instructions logicielles qui, lorsque mis en œuvre par une unité de traitement d'informations, met en œuvre un tel procédé d'échange de données.

L'invention concerne le domaine de la transmission de données sécurisées entre le capteur de mesure, tel qu'un équipement industriel de mesure, et le serveur informatique via la passerelle de communication, celle-ci étant mobile, la passerelle de communication étant par exemple intégrée dans un appareil électronique mobile.

On connaît un capteur de mesure et une installation de mesure du type précité. Une passerelle de communication est reliée à un serveur informatique via le réseau Internet, et est chargée de se connecter de manière sécurisée au serveur informatique, par exemple via la mise en œuvre d'un réseau privé virtuel, également appelé VPN (de l'anglais *Virtual Private Network*), entre la passerelle et le serveur.

La passerelle de communication est par ailleurs connectée à chaque capteur de mesure. Elle recueille, auprès de chaque capteur de mesure, des informations relatives aux grandeurs mesurées, puis les transmet de manière sécurisée au serveur informatique.

Toutefois, dans ce type de communication sécurisée, la passerelle de communication est considérée comme étant un composant de confiance, connu par le serveur informatique et disposant des informations nécessaires à l'établissement de la communication sécurisée, telles qu'un identifiant unique, des clés de chiffrement

associées à la passerelle, permettant d'assurer la confidentialité et l'intégrité des échanges.

Le but de l'invention est donc de proposer un capteur de mesure permettant de s'affranchir de cette contrainte et d'autoriser l'emploi d'une ou plusieurs passerelles de communication sans que celles-ci ne soient connues au préalable par le serveur informatique en tant que composant de confiance.

À cet effet, l'invention a pour objet un capteur de mesure du type précité, dans lequel la mémoire comporte des informations de connexion sécurisée au serveur informatique, lesdites informations de connexion comportant un code d'authentification du capteur.

Suivant d'autres aspects avantageux de l'invention, le capteur de mesure comprend une ou plusieurs des caractéristiques suivantes, prises isolément ou suivant toutes les combinaisons techniquement possibles :

- le capteur comporte en outre des moyens d'élaboration d'une réponse à une requête du serveur informatique, la réponse étant élaborée en fonction du code d'authentification ;

- le capteur comporte en outre des moyens de chiffrement de données, les données chiffrées étant destinées à être transmises au serveur informatique par les moyens d'échange de données ; et

- les informations de connexion sont protégées par un mot de passe dans la mémoire.

L'invention a également pour objet une installation de mesure comprenant au moins un capteur de mesure d'une grandeur, telle qu'une grandeur électrique ou une grandeur thermodynamique, et un serveur informatique relié à chaque capteur de mesure, dans laquelle chaque capteur de mesure est tel que défini ci-dessus.

Suivant d'autres aspects avantageux de l'invention, l'installation de mesure comporte une ou plusieurs des caractéristiques suivantes, prises isolément ou suivant toutes les combinaisons techniquement possibles :

- le serveur informatique comporte des premiers moyens d'envoi d'une requête d'authentification à chaque capteur de mesure et des moyens d'authentification de la réponse élaborée par chaque capteur de mesure suite à la réception de ladite requête ;

- le serveur informatique comporte des deuxièmes moyens d'envoi, à chaque capteur authentifié, d'une clé de chiffrement adaptée pour le chiffrement de données échangées entre le serveur informatique et le capteur authentifié ;

- l'installation comprend en outre une passerelle de communication, la passerelle de communication étant reliée au serveur informatique via un réseau de communication,

tel que le réseau Internet, et chaque capteur de mesure étant relié au serveur informatique via la passerelle de communication ; et

- la passerelle de communication est intégrée dans un appareil électronique mobile, tel qu'un téléphone mobile, une tablette ou un ordinateur portable.

5 L'invention a également pour objet un procédé d'échange de données entre un capteur de mesure d'une grandeur, telle qu'une grandeur électrique ou une grandeur thermodynamique, et un serveur informatique via une passerelle de communication, la passerelle de communication étant reliée au serveur informatique via un réseau de communication,

10 le procédé étant mis en œuvre par le capteur de mesure, le capteur comprenant des moyens radioélectriques de communication avec la passerelle, et une unité de traitement d'informations comportant une mémoire,

le procédé comprenant l'échange de données avec le serveur informatique, via les moyens radioélectriques de communication,

15 dans lequel le procédé comprend en outre la connexion sécurisée au serveur informatique à l'aide d'un code d'authentification du capteur, ledit code d'authentification étant stocké dans la mémoire du capteur.

Suivant un autre aspect avantageux de l'invention, le procédé d'échange de données comprend la caractéristique suivante :

20 - l'étape de connexion sécurisée au serveur informatique comporte l'élaboration d'une réponse à une requête du serveur informatique, la réponse étant élaborée en fonction du code d'authentification.

L'invention a également pour objet un produit programme d'ordinateur comportant des instructions logicielles, qui, lorsque mis en œuvre par une unité de traitement d'informations, met en œuvre le procédé d'échange de données tel que défini ci-dessus.

25 Ces caractéristiques et avantages de l'invention apparaîtront à la lecture de la description qui va suivre, donnée uniquement à titre d'exemple non limitatif, et faite en référence aux dessins annexés, sur lesquels :

30 - la figure 1 est une représentation schématique d'une installation de mesure selon l'invention, comprenant plusieurs capteurs de mesure et un serveur informatique relié à chaque capteur de mesure via une passerelle mobile de communication, la passerelle de communication étant reliée au serveur via un réseau de communication, et

35 - la figure 2 est un organigramme d'un procédé d'échange sécurisé de données, conforme à l'invention, entre les capteurs de mesure et le serveur informatique, via la passerelle mobile de communication de la figure 1.

Sur la figure 1, une installation de mesure 10 comprend une pluralité de capteurs de mesure 12 et un serveur informatique 14 relié à chaque capteur de mesure 12 via une passerelle de communication 16. La passerelle de communication 16 est reliée au serveur informatique 14 via un réseau de communication 18.

5 L'installation de mesure 10 est adaptée pour effectuer des relevés automatiques de mesure, ces mesures étant réalisées par les capteurs de mesure 12.

Chaque capteur de mesure 12 est adapté pour mesurer une grandeur, telle qu'une grandeur électrique ou une grandeur thermodynamique. La grandeur électrique est par exemple la tension d'un conducteur électrique, respectivement l'intensité d'un courant
10 électrique, et le capteur de mesure 12 est alors appelé capteur de tension, respectivement capteur de courant.

En variante, la grandeur thermodynamique est par exemple une température, respectivement une pression, et le capteur de mesure 12 est alors appelé capteur de température, respectivement capteur de pression.

15 En variante encore, le capteur de mesure 12 est adapté pour mesurer une grandeur environnementale, tel qu'un pH, un taux d'oxygène, une densité de particules (monoxyde de carbone, dioxyde de carbone, poussière).

Chaque capteur de mesure 12 comprend un premier émetteur-récepteur radioélectrique 20 apte à communiquer avec la passerelle de communication 16 via une
20 première liaison de données 22.

Chaque capteur de mesure 12 comprend une première unité de traitement d'informations 24, formée par exemple d'un premier processeur 26 et d'une première mémoire 28 associée au premier processeur 26, comme représenté sur la figure 1 où un seul capteur de mesure 12 est représenté en détail par souci de simplification des
25 dessins. La première unité de traitement d'informations 24 est connectée au premier émetteur-récepteur radioélectrique 20.

Le serveur informatique 14 comprend un premier organe 30 de transmission de données apte à communiquer avec la passerelle de communication 16 via le réseau de communication 18 formant une deuxième liaison de données 32.

30 Le serveur informatique 14 comprend une deuxième unité de traitement d'informations 34, formée par exemple d'un deuxième processeur 36 et d'une deuxième mémoire 38 associée au deuxième processeur 36. La deuxième unité de traitement d'information 34 est connectée à l'organe de transmission 30.

Le serveur informatique 14 est propre à recevoir des données relatives aux
35 différentes grandeurs mesurées par chacun des capteurs de mesure 12. Autrement dit, le serveur informatique 14 permet de centraliser les différentes valeurs mesurées par les

capteurs 12, afin d'effectuer un suivi de manière centralisée de ces valeurs mesurées. Le serveur informatique 14 est par exemple un serveur Web. Les références du serveur informatique 14, telles que le nom ou l'adresse IP du serveur, sont par exemple stockées dans la première mémoire 28 du capteur, pour être transmises par le capteur 12 à la passerelle 16 lorsque le capteur 12 demande à la passerelle 16 d'établir une communication avec le serveur 14.

La passerelle de communication 16 est reliée, d'une part, à chacun des capteurs de mesure 12 via les premières liaisons de données 22 respectives, et d'autre part, au serveur informatique 14 via la deuxième liaison de données 32 formée par le réseau de communication. La passerelle de communication 16 forme fonctionnellement un routeur de communication entre un capteur de mesure 12 respectif et le serveur informatique 14, les données échangées entre le capteur de mesure 12 correspondant et le serveur informatique 14 ne faisant que transiter par la passerelle de communication 16, après établissement d'une communication entre la passerelle de communication 16 et le serveur informatique 14.

La passerelle de communication 16 comprend un deuxième émetteur-récepteur radioélectrique 40 apte à communiquer avec chaque capteur 12 via la première liaison de données 22 correspondante, en particulier avec le premier émetteur-récepteur radioélectrique 20 de chaque capteur de mesure. Autrement dit, la passerelle de communication 16 est reliée au capteur de mesure 12 via un réseau de communication local formé par le premier émetteur-récepteur 20, la première liaison 22 respective et le deuxième émetteur-récepteur 40. Le réseau local est, par exemple, conforme à la norme IEEE 802.15.1, également appelée norme Bluetooth, ou encore à la norme IEEE 802.15.4, également appelée norme ZigBee.

La passerelle de communication 16 comprend également un deuxième organe 42 de transmission de données apte à communiquer avec le serveur informatique 14, en particulier avec le premier organe de transmission 30 du serveur informatique. La passerelle de communication 16 est alors apte à communiquer de manière distante avec le serveur 14.

La passerelle de communication 16 comprend des moyens 44 de transfert de données entre le capteur 12 et le serveur informatique 14. La transmission de données entre la passerelle 16 et le serveur 14 s'effectue de manière préférentielle sur la base du protocole IP (de l'anglais *Internet Protocol*).

La transmission de données entre la passerelle 16 et le capteur 12 s'effectue de manière préférentielle sur la base d'un protocole de communication local, tel que les protocoles ZigBee ou ZigBee Green Power conformes à la norme IEEE 802.15.4, le

protocole MODBUS, le protocole CAN (de l'anglais *Controller Area Network*) conforme à la norme ISO 11898, le protocole BACnet, ou encore le protocole KNX.

Une fois la communication établie entre la passerelle 16 et le serveur 14, la passerelle 16 assure uniquement la transformation nécessaire entre les protocoles utilisés, d'une part entre le capteur 12 et la passerelle 16, et d'autre part entre la passerelle 16 et le serveur 14, et s'attache à transmettre l'information utile sans modification. Les modifications effectuées par la passerelle 16 concernent uniquement le passage d'un protocole à l'autre.

En complément, les moyens de transfert 44 sont également responsables de l'établissement d'une connexion initiale entre la passerelle 16 et le serveur 14 à l'initiative du capteur 12, afin de permettre la connexion sécurisée du capteur de mesure 12 au serveur informatique 14, l'ensemble de la chaîne de communication entre le capteur 12 et le serveur 14 via la passerelle 16 étant alors sécurisé.

La passerelle de communication 16 est, par exemple, intégrée dans un appareil électronique mobile 46, tel qu'un téléphone mobile, une tablette ou un ordinateur portable. Les moyens de transfert 44 sont alors de préférence en forme d'un logiciel apte à être stocké dans une mémoire 48 du téléphone mobile 46. Les références du serveur informatique 14, telles que l'adresse IP du serveur, sont en variante stockées dans la mémoire 48 du téléphone mobile

Le réseau de communication 18 est connu en soi. Le réseau de communication 18 est par exemple le réseau Internet.

La première liaison de données 22 est une liaison radioélectrique, de préférence une liaison radioélectrique à courte distance, c'est-à-dire pour des distances de l'ordre de quelques mètres ou quelques dizaines de mètres.

La première liaison de données 22 est, par exemple, conforme à la norme IEEE 802.15, également appelée norme Bluetooth®. En variante, la première liaison de données 22 est conforme à la norme IEEE 802.11, également appelée norme Wi-Fi, les capteurs de mesure 12 et la passerelle de communication 16 formant, par exemple, un réseau ad hoc. Les premier et deuxième émetteurs-récepteurs radioélectriques 20, 40 sont connus en soi, et sont conformes à la même norme radioélectrique que la première liaison de données 22.

La première mémoire 28 est apte à stocker un premier logiciel 50 d'échange de données avec le serveur informatique 14, de préférence via la passerelle 16, le logiciel d'échange de données 50 étant relié au premier émetteur-récepteur radioélectrique 20.

La première mémoire 28 comporte selon l'invention des informations de connexion sécurisée au serveur informatique 14, lesdites informations de connexion comportant un

code 52 d'authentification du capteur. Les informations de connexion sont de préférence protégées par un organe de contrôle d'accès, non représenté. L'organe de contrôle d'accès est apte à être stocké dans la première mémoire 28, et est par exemple apte à requérir la fourniture d'un mot de passe pour autoriser l'accès aux informations de connexion.

La première mémoire 28 est apte à stocker un logiciel 54 d'élaboration d'une réponse à une requête du serveur informatique 14, la réponse étant élaborée en fonction du code d'authentification 52.

En complément, la première mémoire 28 est apte à stocker un premier logiciel de cryptographie 56 apte à chiffrer des données destinées à être transmises au serveur informatique 14 par le logiciel d'échange de données 50 et/ou à déchiffrer des données chiffrées reçues depuis le serveur informatique 14.

En variante, les premiers moyens d'échange de données 50, les moyens d'élaboration de la réponse 54 et les premiers moyens de cryptographie 56 sont réalisés sous forme de composants logiques programmables, ou encore sous forme de circuits intégrés dédiés.

Le premier organe de transmission de données 30 est adapté pour recevoir des données de la part de chaque capteur de mesure 12 via la passerelle de communication 16 et le réseau de communication 18, et également pour envoyer des données à chaque capteur de mesure 12 via ladite passerelle 16 et ledit réseau 18.

Le premier organe de transmission de données 30 est adapté pour établir une connexion sécurisée avec la passerelle de communication 16 sur demande de la passerelle de communication 16 et sans que celle-ci soit authentifiée. La sécurisation de la connexion entre la passerelle 16 et le serveur 14 ne met pas en jeu d'information issue du capteur 12.

La deuxième mémoire 38 est apte à stocker un premier logiciel 60 d'envoi d'une requête d'authentification à chaque capteur de mesure 12, et un logiciel 62 d'authentification de la réponse élaborée par chaque capteur de mesure 12 suite à la réception de ladite requête.

En complément, la deuxième mémoire 38 est apte à stocker un deuxième logiciel 64 d'envoi, à chaque capteur authentifié 12, d'une clé de chiffrement adaptée pour le chiffrement ultérieur de données échangées entre le serveur informatique 14 et le capteur authentifié 12. En complément, le deuxième logiciel d'envoi 64 est apte à envoyer la clé de chiffrement à la passerelle 16 dès le début de la communication entre le capteur 12 et le serveur 14 pour le chiffrement ultérieur de données échangées entre le serveur informatique 14 et la passerelle 16.

La deuxième mémoire 38 est apte à stocker un deuxième logiciel de cryptographie 66 apte à chiffrer des données destinées à être transmises à un capteur de mesure 12 correspondant et/ou à déchiffrer des données chiffrées reçues depuis ledit capteur de mesure 12. La deuxième mémoire 38 est apte à stocker un deuxième logiciel 68 d'échange de données avec chaque capteur de mesure 12, le deuxième logiciel d'échange de données 68 étant relié au premier organe de transmission 30.

En variante, les premiers moyens d'envoi 60, les moyens d'authentification 62, les deuxièmes moyens d'envoi 64, les deuxièmes moyens de cryptographie 66 et les deuxièmes moyens d'échange de données 68 sont réalisés sous forme de composants logiques programmables, ou encore sous forme de circuits intégrés dédiés.

La deuxième mémoire 38 comporte une base de données 70 contenant des informations relatives à chacun des capteurs de mesure 12, notamment les codes d'authentification 52 des différents capteurs.

Le deuxième organe de transmission de données 42 est adapté pour recevoir des données de la part du serveur informatique 14 via le réseau de communication 18, et également pour envoyer des données au serveur 14 via ledit réseau 18. La passerelle de communication 16 est de préférence reliée au réseau de communication 18 par ondes radioélectriques, et le deuxième organe de transmission 42 est par exemple conforme à la norme IEEE 802.11 (norme Wi-Fi), ou à la norme UMTS (de l'anglais *Universal Mobile Telecommunications System*), également appelée norme 3G s'agissant de la norme de téléphonie mobile de troisième génération, ou encore à la norme LTE (de l'anglais *Long Term Evolution*), également appelée norme 4G s'agissant de la norme de téléphonie mobile de quatrième génération.

Le fonctionnement de l'installation de mesure 10 selon l'invention va être à présent décrit à l'aide de la figure 2 représentant un organigramme du procédé d'échange de données selon l'invention, entre un capteur de mesure 12 correspondant et le serveur informatique 14 via la passerelle de communication 16.

Initialement, le capteur 12 recherche si une passerelle 16 est disponible à proximité pour pouvoir envoyer ses données. Le capteur 12 envoie par exemple un message de recherche de passerelle de type « broadcast » pour déterminer les passerelles 16 disponibles. Ce message peut être envoyé à intervalles réguliers ou de manière aléatoire. Le capteur 12 a par exemple la faculté de mémoriser une plage horaire déterminée sur laquelle le capteur 12 a déjà transmis des données antérieurement et est à même d'envoyer un message de recherche sur cette plage horaire.

Lors d'une étape 90, le capteur de mesure 12 commence par requérir auprès de la passerelle 16 l'établissement d'une connexion entre le capteur 12 et la passerelle 16,

cette connexion pouvant ne pas être sécurisée. Lors de l'étape suivante 95, la passerelle de communication 16 valide que la communication est bien établie entre le capteur 12 et la passerelle 16.

Sur demande de communication du capteur 12 qui lui transmet à cette occasion le code d'authentification 52, la passerelle 16 va demander, lors d'une étape 96, l'établissement d'une communication sécurisée auprès du serveur 14 avec lequel le capteur 12 souhaite échanger des données. En variante, le nom et/ou l'adresse du serveur 14 sont fournis par la passerelle 16.

Lors de l'étape suivante 97, le serveur 14 valide la connexion sécurisée entre lui et la passerelle 16, et en informe la passerelle 16 à l'aide de son deuxième logiciel d'envoi 64.

Suite à la validation de l'établissement de la connexion sécurisée avec le serveur 14, la passerelle de communication 16 transmet, lors de l'étape 98 et au serveur 14, le code d'authentification 52 associé au capteur, celui-ci ayant été préalablement fourni à la passerelle 16 par le capteur 12.

Lors de l'étape suivante 99 et suite à la réception du code d'authentification 52 associé au capteur, le serveur 14 vérifie que le capteur 12 est bien connu et autorisé.

Suite à la réception de cette demande de connexion initiale de la part du capteur de mesure 12, le serveur 14 prépare lors de l'étape 110 une requête spécifique pour ce capteur 12 à l'aide des informations contenues dans sa base de données 70. Autrement dit, cette étape 110 correspond à la préparation d'un défi de la part du serveur 14 pour le capteur de mesure 12 concerné en vue du chiffrement des données qui seront ultérieurement échangées entre le capteur 12 et le serveur 14.

Le serveur 14 envoie alors, à l'aide de son premier logiciel d'envoi 60 et durant l'étape 120, la requête d'authentification créée lors de l'étape précédente, via la passerelle de communication 16 à destination du capteur de mesure 12 ayant envoyé sa demande de connexion. Cette étape 120 correspond en d'autres termes à l'envoi, par le serveur 14, du défi préparé lors de l'étape 110 au capteur 12 concerné.

Après réception de cette requête d'authentification de la part du serveur informatique 14, le capteur de mesure 12 élabore ensuite, à l'aide de son logiciel d'élaboration 54 et lors de l'étape 130, la réponse à ladite requête d'authentification, cette réponse étant élaborée en fonction du code d'authentification 52 associé à ce capteur 12. L'élaboration de la réponse consiste, par exemple, à chiffrer la requête d'authentification reçue avec ledit code d'authentification 52 en tant que clé de chiffrement. Autrement dit, cette étape 130 consiste, après réception du défi par le capteur 12, à la génération de la réponse et au chiffrement de celle-ci de la part du capteur 12.

Le capteur de mesure 12 transmet alors, à l'aide de son premier logiciel d'échange 50 et durant l'étape 140, la réponse élaborée lors de l'étape précédente, à destination du serveur informatique 14 et via la passerelle de communication 16. Cette étape 140 correspond en d'autres termes à l'envoi par le capteur 12, via la passerelle 16 et à destination du serveur informatique 14, de la réponse chiffrée au défi précédemment reçu.

Lorsque le serveur 14 reçoit cette réponse de la part du capteur 12 auquel la requête a été envoyée, le serveur 14 vérifie, lors de l'étape 150 et à l'aide de son logiciel d'authentification 62, si la réponse reçue est conforme ou non, en comparant le code d'authentification 52 ayant permis d'élaborer la réponse avec le code d'authentification contenu dans sa base de données 70 pour ce capteur 12. Autrement dit, l'étape 150 correspondant à la validation par le serveur 14 de la réponse au défi envoyée par le capteur 12, et dans le cas d'une validation positive au maintien d'une connexion sécurisée entre la passerelle 16 et le serveur 14 d'une part, et entre la passerelle 16 et le capteur 12 d'autre part.

La vérification de la réponse reçue consiste, par exemple, à déchiffrer la réponse reçue avec le code d'authentification contenu dans la base 70 en tant que clé de déchiffrement, puis à comparer la réponse déchiffrée avec la requête d'authentification envoyée. Dans ce cas, la vérification est positive lorsque la réponse déchiffrée est identique à la requête d'authentification précédemment envoyée.

En cas de vérification positive, une session d'échange de données est alors ouverte entre le serveur 14 et le capteur authentifié 12, et la connexion sécurisée entre la passerelle 16 et le serveur 14 est maintenue. En variante, le serveur 14 envoie, à destination du capteur 12 qui vient d'être authentifié, une clé de chiffrement spécifique dudit capteur authentifié, à l'aide de son deuxième logiciel d'envoi 64 et lors de l'étape 160.

À partir de cette étape 160, la passerelle 16 joue uniquement un rôle de transformation de protocoles de communication, entre le protocole de communication utilisé entre le capteur 12 et la passerelle 16 d'une part et le protocole de communication utilisé entre la passerelle 16 et le serveur 14 d'autre part.

Cette clé de chiffrement, également appelée clé de session, est par exemple une clé symétrique adaptée pour le chiffrement/déchiffrement des données qui vont être échangées lors de la session d'échange de données. La clé de session est de préférence envoyée sous forme chiffrée par le serveur 14, le chiffrement de la clé de session étant par exemple effectué à l'aide du code d'authentification 52.

Lors de l'étape suivante 170, le capteur authentifié 12 enregistre alors la clé de chiffrement reçue dans sa première mémoire 28, afin de l'utiliser ultérieurement lors de

l'envoi de données chiffrées à destination du serveur informatique 14. Le capteur de mesure 12 est connecté au serveur informatique 14, et est alors en mesure de transmettre régulièrement au serveur informatique 14 des valeurs successives de la grandeur mesurée, et ce de manière chiffrée en utilisant la clé de session.

5 Le capteur de mesure 12 envoie alors au serveur informatique 14, lors de l'étape 200 à l'aide de son premier logiciel d'échange 50 via la passerelle de communication 16, un message chiffré contenant une ou plusieurs valeurs de la grandeur mesurée, le message ayant été chiffré par le premier logiciel de cryptographie 56 avec la clé de session reçue précédemment.

10 Lors de l'étape 210, suite à la réception de ce message chiffré de la part du capteur authentifié 12, le serveur 14 commence par déchiffrer le message reçu à l'aide de son deuxième logiciel de cryptographie 66 et avec la clé de session précédemment envoyée audit capteur. Le serveur 14 enregistre ensuite, dans sa deuxième mémoire 38, la ou les valeurs de la grandeur mesurée contenues dans le message qui vient d'être
15 déchiffré.

Le serveur 14 envoie enfin, lors de l'étape 220, un message d'acquittement à destination du capteur 12 correspondant.

20 Suite à la réception de ce message d'acquittement, ledit capteur 12 retourne à l'étape 200 afin d'envoyer ultérieurement au moins une autre valeur de la grandeur mesurée.

En variante, suivant les technologies de chiffrements mises en œuvre, les étapes 110 et 150 sont regroupées, et les étapes 120 et 160 sont également regroupées. Selon cette variante, les étapes du procédé s'enchaînent alors de la manière suivante à partir de l'étape 110. L'étape 110, regroupée avec l'étape 150, comporte la vérification de l'identité
25 du capteur 12 et en la préparation du défi, ce défi comportant la clé de chiffrement à utiliser pour l'étape 200 ultérieure. L'étape 120, regroupée avec l'étape 160, comporte l'envoi du défi comportant la clé de chiffrement. L'étape 130 comporte la validation du défi par le capteur 12, ainsi que l'enregistrement, par le capteur 12 dans sa mémoire 28, de la clé de chiffrement contenue dans le défi reçu, et ce en vue des communications
30 ultérieures entre le capteur 12 et le serveur 14 à partir de l'étape 200.

Si le capteur de mesure 12 n'a plus de valeur mesurée à transmettre au serveur informatique 14, le capteur 12 clôt, lors de l'étape 230, la connexion avec la passerelle de communication 16 qui elle-même clôt sa connexion avec le serveur 14.

35 L'installation de mesure 10 selon l'invention et le procédé d'échange de données associé permettent ainsi un échange de données de manière sécurisée depuis le capteur de mesure 12 jusqu'au serveur informatique 14, et inversement depuis le serveur 14

jusqu'au capteur 12, ceci étant dû au fait que les informations de connexion, en particulier le code d'authentification 52, sont contenues directement dans la première mémoire 28 du capteur de mesure.

Avec l'installation de mesure de l'état de la technique, les échanges de données sont sécurisés seulement entre la passerelle de communication et le serveur, et les échanges de données ne sont pas protégés entre la passerelle de communication et le capteur de mesure.

L'installation de mesure 10 selon l'invention et le procédé d'échange de données associé permettent ainsi d'établir une communication sécurisée depuis le capteur 12 jusqu'au serveur 14, et pas seulement entre la passerelle 16 et le serveur 14. Ils permettent également de proposer cette communication sécurisée entre le capteur 12 et le serveur 14 via la passerelle de communication 16 qui n'est pas un composant de confiance, et de permettre à la passerelle de communication 16 d'établir la connexion sécurisée avec le serveur 14 en utilisant des paramètres de sécurité associés au capteur 12, c'est-à-dire les informations de connexion comportant le code d'authentification 52. La passerelle de communication 16 présente une aptitude à communiquer de manière locale avec le capteur 12, une aptitude à communiquer de manière distante avec le serveur informatique 14, une aptitude à exécuter une application propre à établir une communication sécurisée entre le capteur 12 et le serveur 14 suite à l'établissement d'une ou plusieurs connexions sécurisées. Dans l'exemple de réalisation de la figure 2, deux connexions sécurisées sont établies, une première entre le capteur 12 et la passerelle 16, et une seconde entre la passerelle 16 et le serveur 14 sur la base des informations de connexion stockées dans la première mémoire 28 du capteur.

L'homme du métier comprendra également que, pour un même capteur 12 ou un même groupe de capteurs 12, la passerelle de communication mobile 16 n'est pas nécessairement toujours la même, une nouvelle passerelle 16 étant susceptible d'être employée à chaque nouvelle émission de données par le ou les capteurs 12.

Le mécanisme d'authentification avec l'élaboration en fonction du code d'authentification 52 de la réponse à la requête d'authentification issue du serveur 14 permet en outre de faciliter la mise en œuvre de la sécurisation de cet échange de données, et il n'est notamment pas nécessaire de configurer un réseau privé virtuel entre la passerelle de communication 16 et le serveur informatique 14.

De manière générale, le procédé d'échange de données selon l'invention nécessite une interaction minimale entre le capteur de mesure 12 et la passerelle de communication 16, puisqu'il suffit seulement pour le capteur 12 d'ouvrir une connexion avec la passerelle de communication 16 préalablement à l'envoi de la demande de

connexion au serveur 14, puis de clore cette connexion avec la passerelle 16 lorsque l'échange de données avec le serveur 14 est terminé, les données ne faisant que transiter par la passerelle de communication 16 lors de cet échange de données.

On conçoit ainsi que le capteur de mesure 12 selon l'invention permet d'améliorer la sécurisation des données échangées avec le serveur informatique 14 via la passerelle de communication 16, tout en simplifiant la mise en œuvre de cette sécurisation de l'échange de données.

Comme décrit précédemment, la passerelle de communication 16 utilisée dans l'installation 10 n'est pas un composant de confiance. La passerelle 16 n'est donc connue ni du capteur 12, ni du serveur 14. La passerelle de communication 16 ne contient alors pas d'informations de connexion sécurisée au serveur 14. La passerelle 16 seule ne permet pas d'assurer la confidentialité et l'intégrité des échanges de données entre le serveur 14 et le capteur 12.

Lorsque plusieurs passerelles 16 sont présentes au voisinage du capteur 12, le choix de la passerelle 16 est effectué par le capteur 12, par exemple, en fonction de la proximité de la passerelle 16 par rapport au capteur 12.

En variante, le code d'authentification 52 comprend une clé privée de cryptage et un code d'identification.

La clé privée de cryptage a les mêmes fonctionnalités et caractéristiques que le code d'authentification 52 décrit dans le mode de réalisation précédent, à la différence que la clé privée de cryptage est conservée dans la mémoire 28 du capteur 12. La clé privée de cryptage n'est donc pas envoyée au serveur informatique 14 via la passerelle de communication 16.

La clé privée de cryptage permet de crypter, c'est-à-dire de chiffrer, les données sortant du capteur 12. En particulier, la clé privée de cryptage permet de crypter les données envoyées au serveur 14 depuis le capteur 12 via la passerelle 16.

Le code d'identification permet d'identifier le capteur 12. Le code d'identification est, par exemple, le nom du capteur 12, chaque capteur 12 ayant un nom spécifique, différent de celui des autres capteurs 12.

Le code d'identification est propre à être envoyé au serveur 14 via la passerelle de communication 16.

Dans ce qui suit, seules les différences de fonctionnement de l'installation 10 présentée selon cette variante par rapport au mode de réalisation précédent sont décrites.

Initialement, le capteur 12 envoie une requête pour identifier une passerelle de communication 16 située à proximité du capteur 12.

14

Puis, une fois que la passerelle 16 est identifiée, le capteur 12 utilise la passerelle 16 pour communiquer avec le serveur 14. Le capteur 12 envoie notamment son code d'identification au serveur 14 via la passerelle 16.

5 Ensuite, le serveur 14 identifie le capteur 12 grâce au code d'identification du capteur 12, et autorise alors les échanges de données avec le capteur 12.

La clé privée de cryptage du capteur 12 sert alors au chiffrement des données envoyées depuis le capteur 12 vers le serveur 14 via la passerelle de communication 16, le serveur 14 connaissant par ailleurs une clé de déchiffrement.

10 La clé de déchiffrement permet au serveur 14 de déchiffrer les données chiffrées reçues du capteur 12 via la passerelle de communication 16.

REVENDICATIONS

1.- Capteur (12) de mesure d'une grandeur, telle qu'une grandeur électrique ou une grandeur thermodynamique, destiné à être relié à un serveur informatique (14) via une passerelle de communication (16), la passerelle de communication (16) étant reliée au serveur informatique (14) via un réseau de communication (18),

le capteur (12) comprenant :

- une unité de traitement d'informations (24) comportant une mémoire (28),
- des moyens radioélectriques (20) de communication avec la passerelle (16), et
- des moyens (50) d'échange de données avec le serveur informatique (14) via la passerelle de communication (16), les moyens d'échange de données (50) étant reliés aux moyens radioélectriques de communication (20),

caractérisé en ce que la mémoire (28) comporte des informations de connexion sécurisée au serveur informatique (14), lesdites informations de connexion comportant un code (52) d'authentification du capteur.

2.- Capteur (12) selon la revendication 1, dans lequel le capteur (12) comporte en outre des moyens (54) d'élaboration d'une réponse à une requête du serveur informatique (14), la réponse étant élaborée en fonction du code d'authentification (52).

3.- Capteur (12) selon la revendication 1 ou 2, dans lequel le capteur (12) comporte en outre des moyens (56) de chiffrement de données, les données chiffrées étant destinées à être transmises au serveur informatique (14) par les moyens d'échange de données (50).

4.- Capteur (12) selon l'une quelconque des revendications précédentes, dans lequel les informations de connexion sont protégées par un organe de contrôle d'accès.

5.- Installation de mesure (10) comprenant au moins un capteur (12) de mesure d'une grandeur, telle qu'une grandeur électrique ou une grandeur thermodynamique, et un serveur informatique (14) relié à chaque capteur de mesure (12),

caractérisée en ce que chaque capteur de mesure (12) est conforme à l'une quelconque des revendications précédentes.

6.- Installation (10) selon la revendication 5, dans laquelle le serveur informatique (14) comporte des premiers moyens (60) d'envoi d'une requête d'authentification à

chaque capteur de mesure (12) et des moyens (62) d'authentification de la réponse élaborée par chaque capteur de mesure (12) suite à la réception de ladite requête.

5 7.- Installation (10) selon la revendication 6, dans laquelle le serveur informatique (14) comporte des deuxièmes moyens (64) d'envoi, à chaque capteur authentifié (12), d'une clé de chiffrement adaptée pour le chiffrement de données échangées entre le serveur informatique (14) et le capteur authentifié (12).

10 8.- Installation (10) selon l'une quelconque des revendications 5 à 7, dans laquelle l'installation (10) comprend en outre une passerelle de communication (16), la passerelle de communication (16) étant reliée au serveur informatique (14) via un réseau de communication (18), tel que le réseau Internet, et chaque capteur de mesure (12) étant relié au serveur informatique (14) via la passerelle de communication (16).

15 9.- Installation (10) selon la revendication 8, dans laquelle la passerelle de communication (16) est intégrée dans un appareil électronique mobile (46), tel qu'un téléphone mobile, une tablette ou un ordinateur portable.

20 10.- Procédé d'échange de données entre un capteur (12) de mesure d'une grandeur, telle qu'une grandeur électrique ou une grandeur thermodynamique, et un serveur informatique (14) via une passerelle de communication (16), la passerelle de communication (16) étant reliée au serveur informatique (14) via un réseau de communication (18),

25 le procédé étant mis en œuvre par le capteur de mesure (12), le capteur (12) comprenant des moyens radioélectriques (20) de communication avec la passerelle (16), et une unité de traitement d'informations (24) comportant une mémoire (28),

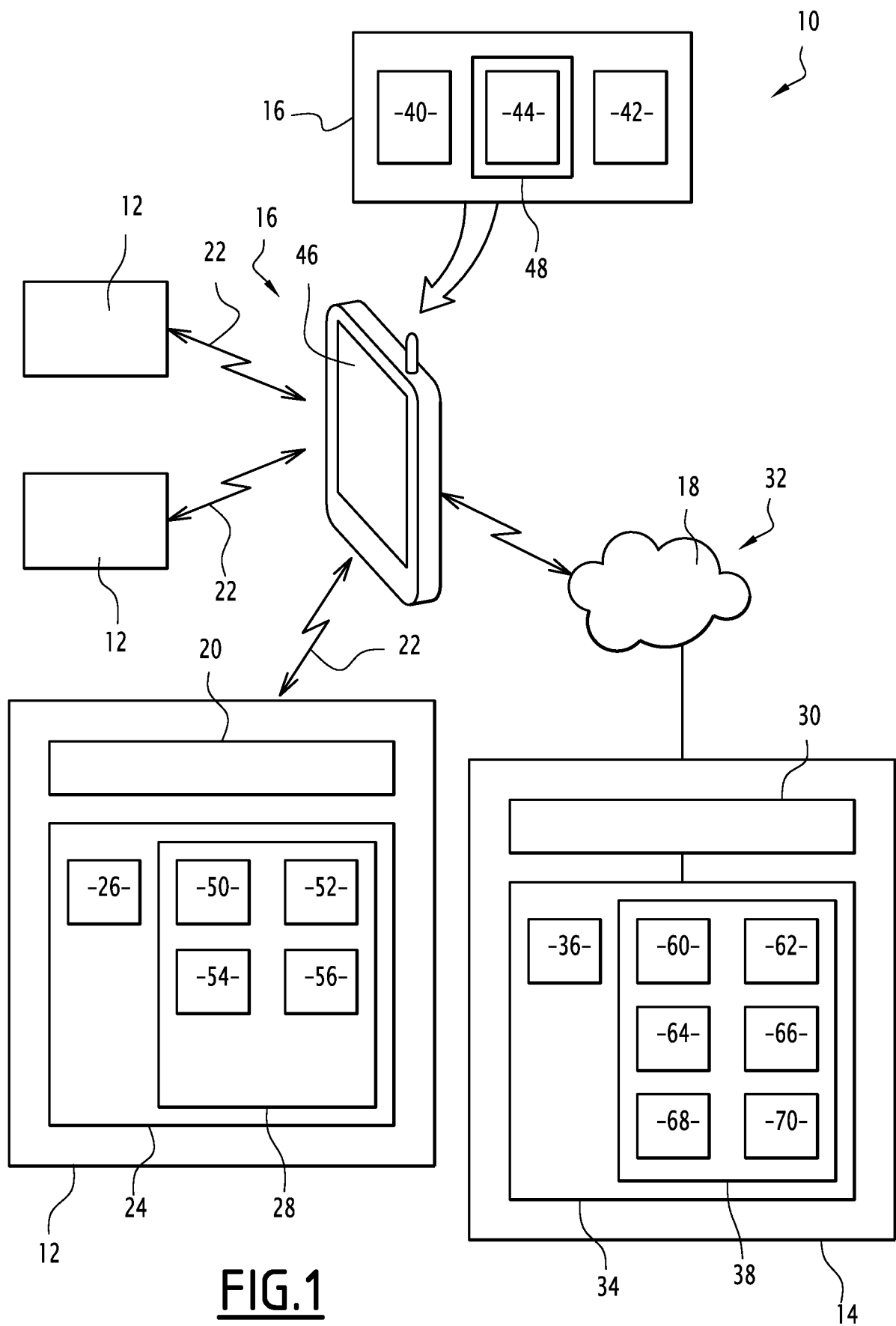
le procédé comprenant l'échange (200) de données avec le serveur informatique (14), via les moyens radioélectriques de communication (20),

30 le procédé étant caractérisé en ce qu'il comprend en outre la connexion sécurisée (130, 140) au serveur informatique (14) à l'aide d'un code (52) d'authentification du capteur, ledit code d'authentification (52) étant stocké dans la mémoire (28) du capteur.

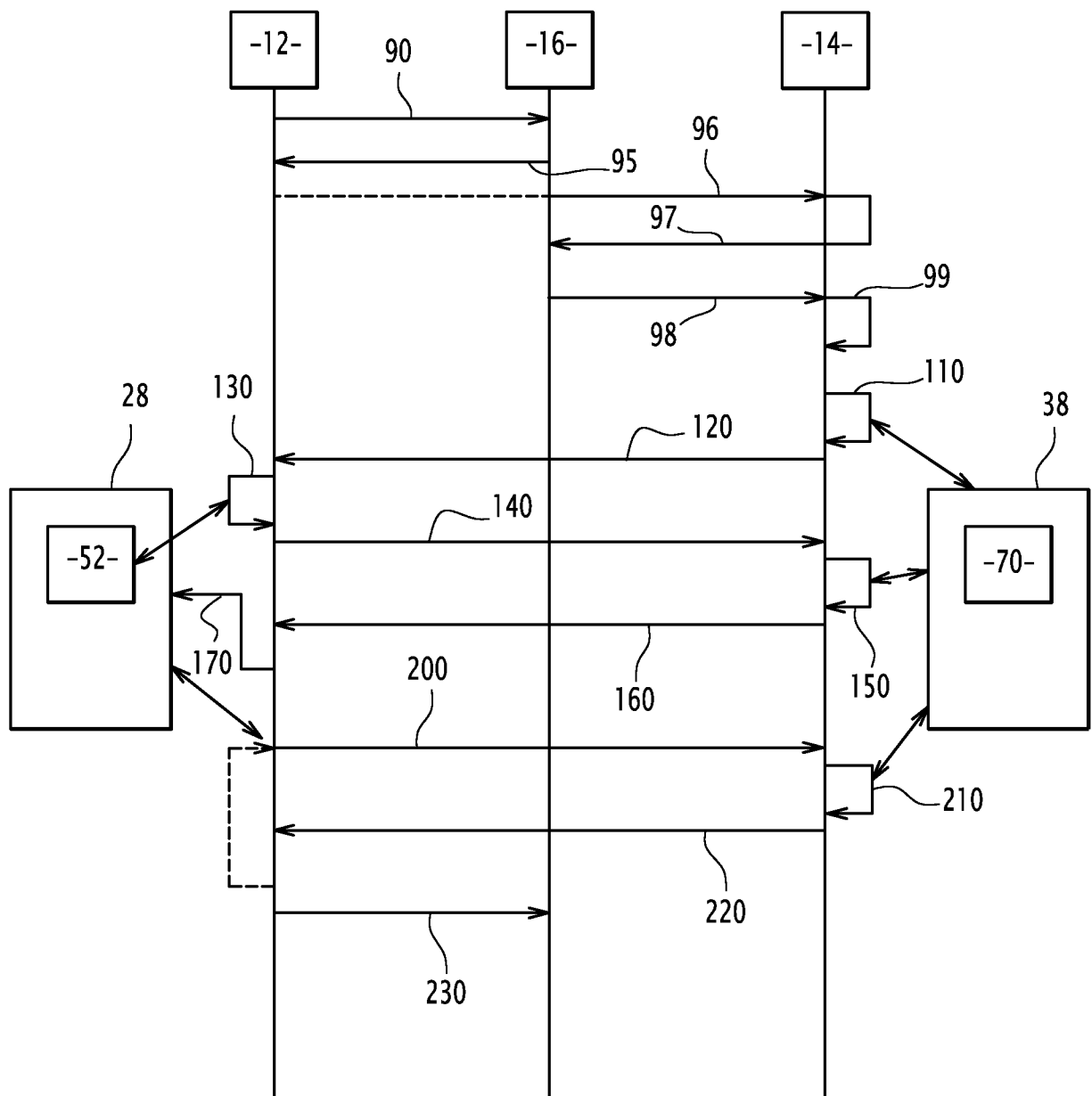
35 11.- Procédé selon la revendication 10, dans lequel l'étape de connexion sécurisée au serveur informatique (130, 140) comporte l'élaboration (130) d'une réponse à une requête du serveur informatique (14), la réponse étant élaborée en fonction du code d'authentification (52).

12.- Produit programme d'ordinateur comportant des instructions logicielles qui, lorsque mis en œuvre par une unité de traitement d'informations (24), met en œuvre le procédé d'échange de données selon la revendication 10 ou 11.

1/2



2/2

FIG.2

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2014/076560

A. CLASSIFICATION OF SUBJECT MATTER

INV. G01D21/00 H04L9/00 H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L G01D

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 506 392 A1 (TOSHIBA KK) 3 October 2012 (2012-10-03) abstract; figures 1-5,12,30 paragraphs [0011] - [0015], [0020], [0033], [0093] - [0103] -----	1-8, 10-12
X	GB 2 482 326 A (TOSHIBA RES EUROP LTD) 1 February 2012 (2012-02-01) abstract; figures pages 9-16 -----	1,3-5, 8-10,12



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

4 March 2015

Date of mailing of the international search report

13/03/2015

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Barthélemy, Matthieu

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2014/076560

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2506392	A1	03-10-2012	EP 2506392 A1 03-10-2012
			JP 5456058 B2 26-03-2014
			US 2012250864 A1 04-10-2012
			WO 2011064865 A1 03-06-2011

GB 2482326	A	01-02-2012	NONE

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/EP2014/076560

A. CLASSEMENT DE L'OBJET DE LA DEMANDE INV. G01D21/00 H04L9/00 H04L29/06 ADD.		
Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB		
B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE Documentation minimale consultée (système de classification suivi des symboles de classement) H04L G01D		
Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche		
Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 2 506 392 A1 (TOSHIBA KK) 3 octobre 2012 (2012-10-03) abrégé; figures 1-5,12,30 alinéas [0011] - [0015], [0020], [0033], [0093] - [0103]	1-8, 10-12
X	----- GB 2 482 326 A (TOSHIBA RES EUROP LTD) 1 février 2012 (2012-02-01) abrégé; figures pages 9-16 -----	1,3-5, 8-10,12
☐ Voir la suite du cadre C pour la fin de la liste des documents ☒ Les documents de familles de brevets sont indiqués en annexe		
* Catégories spéciales de documents cités: "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent "E" document antérieur, mais publié à la date de dépôt international ou après cette date "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée) "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée "T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention "X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément "Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier "&" document qui fait partie de la même famille de brevets		
Date à laquelle la recherche internationale a été effectivement achevée 4 mars 2015		Date d'expédition du présent rapport de recherche internationale 13/03/2015
Nom et adresse postale de l'administration chargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Fonctionnaire autorisé Barthélemy, Matthieu

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/EP2014/076560

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 2506392	A1	03-10-2012	EP 2506392 A1 03-10-2012
			JP 5456058 B2 26-03-2014
			US 2012250864 A1 04-10-2012
			WO 2011064865 A1 03-06-2011

GB 2482326	A	01-02-2012	AUCUN
