



- (51) Classification internationale des brevets :
H04L 9/08 (2006.01)
- (21) Numéro de la demande internationale :
PCT/FR2016/052713
- (22) Date de dépôt international :
20 octobre 2016 (20.10.2016)
- (25) Langue de dépôt : français
- (26) Langue de publication : français
- (30) Données relatives à la priorité :
1560565 4 novembre 2015 (04.11.2015) FR
- (71) Déposant : ORANGE [FR/FR]; 78 rue Olivier de Serres,
75015 Paris (FR).
- (72) Inventeurs : GRIMAULT, Jean-Luc; 7 impasse de l'Europe,
14120 Mondeville (FR). GRUPELLI, Franck; 15
boulevard de la Charité, Bâtiment A - Appartement 12,
14000 Caen (FR). MICHEL, Philip; 68 boulevard Lyau-
tey, 14000 Caen (FR).
- (74) Mandataire : ORANGE IMT/OLPS/IPL/PATENTS;
AMONOU Isabelle, ORANGE GARDENS -, 44 avenue de
la République - CS 50010, 92326 Chatillon Cedex (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, DJ, 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,
KW, 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,

[Suite sur la page suivante]

(54) Title : COMMUNICATION BETWEEN TWO SECURITY ELEMENTS INSERTED INTO TWO COMMUNICATING OBJECTS

(54) Titre : COMMUNICATION ENTRE DEUX ÉLÉMENTS DE SÉCURITÉ INSÉRÉS DANS DEUX OBJETS COMMUNICANTS

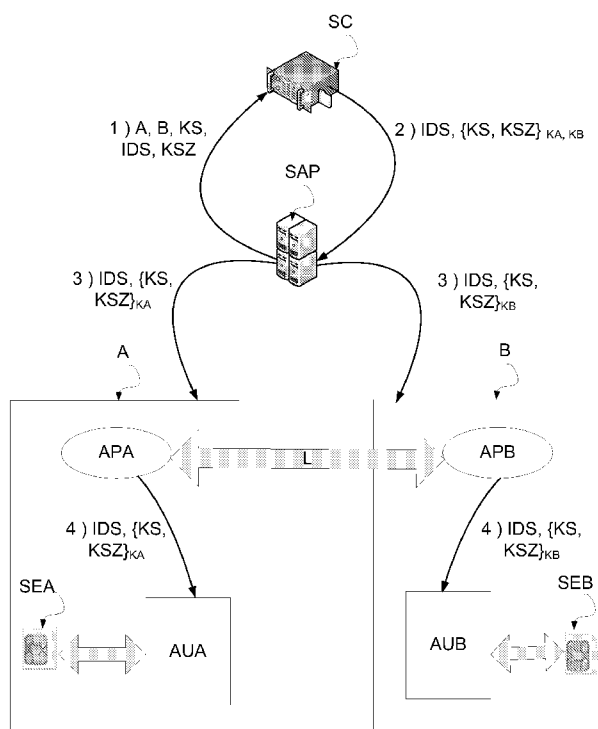


FIGURE 1

(57) Abstract : The invention relates to a method of communication between two devices (A, B), with which the following are associated: - two security elements (SEA, SEB, respectively) comprising respective secret security keys (KA, KB); - and two authenticators (AUA, AUB). The method includes a step of mutual authentication of the two devices (E10-E14, E20-25, E30-36, E40-E45), carried out by the two authenticators (AUA, AUB, respectively), which use their respective security elements (SEA, SEB) for decrypting a session key (KS).

(57) Abrégé : L'invention concerne un procédé de communication entre deux dispositifs (A,B) auxquels sont associés respectivement : - deux éléments de sécurité (SEA, SEB) comportant des clés secrètes de sécurité (KA,KB) respectives, - deux authenticateurs (AUA, AUB). Le procédé comporte une étape d'authentification mutuelle des deux dispositifs (E10-E14, E20-25, E30-36, E40-E45), mise en œuvre par les deux authenticateurs (AUA, AUB) faisant appel à leurs éléments de sécurité respectifs (SEA, SEB) pour déchiffrer une clé de session (KS).



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))

COMMUNICATION ENTRE DEUX ÉLÉMENTS DE SÉCURITÉ INSÉRÉS DANS DEUX OBJETS COMMUNICANTS

Domaine technique

L'invention se rapporte à un procédé de communication entre deux
5 objets de télécommunication. Elle concerne également un objet de
télécommunication destiné à la mise en œuvre dudit procédé.

L'invention s'applique à tout objet de communication équipé d'un
élément de sécurité. Elle trouve une application particulièrement avantageuse
dans le domaine de la sécurité des services de télécommunication entre objets,
10 éventuellement portables, munis d'un élément de sécurité.

Etat de la technique

Le mode de communication direct entre deux machines, dit M2M (de
l'anglais *Machine To Machine*), aussi appelé pair à pair (ou Peer to Peer en
anglais), devient de plus en plus fréquent, par exemple dans le contexte d'une
15 communication entre le téléphone portable et l'ordinateur de bord d'une
automobile d'un utilisateur. Ces communications sont aujourd'hui vulnérables aux
attaques de pirates qui pourraient prendre le contrôle d'un tel objet (dans cet
exemple, le véhicule). Un besoin existe donc de sécuriser les communications de
pair à pair entre machines.

20 A cet effet, certaines normes de communication radio de machine à
machine disposent de fonctionnalités de chiffrement et d'établissement de clés
entre les deux entités communicantes. Par exemple *ZigBee*, basé sur la norme
IEEE 802.15.4, définit un ensemble de protocoles de communications de haut
niveau utilisant des transmission radio à faible consommation. *ZigBee* propose
25 l'utilisation d'un algorithme de chiffrement symétrique des données. Ce type de
sécurité n'est cependant pas générique : elle reste liée à la technologie radio
utilisée, dans ce cas Zigbee. Par ailleurs ce type de sécurité est loin d'être aussi
élevé que celui offert par un élément de sécurité. Or il existe des cas d'usage

(dans les domaines de l'automobile, de la santé, etc.) où il est nécessaire d'assurer un fort niveau de sécurité.

L'intégration matérielle d'un module de communication (par exemple ZigBee, NFC, etc.) dans un élément de sécurité, par exemple une carte dite SIM
5 (de l'anglais Subscriber Identification Module), est connu. Ce type d'architecture offre une sécurité de haut niveau. Cependant, de tels éléments de sécurité incluant une technologie radio sont plus coûteux que des éléments de sécurité classiques. De plus, si plusieurs services sont visés, de tels éléments de sécurité, qui embarquent des éléments (hardware ou logiciels) propres à chaque service,
10 ne sont pas génériques et de ce fait difficiles à utiliser dans un contexte multi-applications.

Il est donc souhaitable de bénéficier d'une technologie à la fois générique et assurant le niveau de sécurité maximal, c'est-à-dire celui offert par un élément de sécurité.

Il est également connu un procédé d'authentification entre deux
15 dispositifs électroniques, munis ou non d'un élément de sécurité, basé sur la génération de deux nombres aléatoires, transmis sur les deux dispositifs et chiffrés sur chacun d'entre eux par une clé secrète connue des deux, de manière à ce que la comparaison des deux cryptogrammes assure l'identification mutuelle
20 des deux dispositifs. Le brevet européen EP0631408 donne un exemple d'un tel procédé.

Il est aussi connu du document « Survey on secure communication protocols for the Internet of Things » (Nguyen K.T. et al, Ad Hoc Networks, vol. 32, 01.09.2015, pages 17-31) un procédé de livraison sur deux dispositifs d'une
25 clé de session chiffrée par la clé secrète respective de chacun des deux dispositifs. Cependant un tel système n'est pas entièrement satisfaisant, car au-delà de l'authentification mutuelle, les deux dispositifs électroniques n'ont pas l'assurance de pouvoir échanger des données avec un haut niveau de sécurité. En outre, ces principes ne sont pas adaptés pour faire inter-fonctionner les deux

dispositifs dans un environnement multiservices, car la même clé secrète est utilisée pour tous les services mis en œuvre par les dispositifs.

L'invention offre une solution ne présentant pas les inconvénients de l'état de la technique.

5

L'invention

A cet effet, selon un aspect fonctionnel, l'invention a pour objet un procédé de communication entre deux dispositifs auxquels sont associés respectivement :

- 10 - deux éléments de sécurité comportant des clés secrètes de sécurité respectives,
 - deux authentificateurs,

le procédé comportant une étape d'authentification mutuelle des deux dispositifs, mise en œuvre par les deux authentificateurs faisant appel à
15 leurs éléments de sécurité respectifs pour déchiffrer une clé de session.

On entend par authentification mutuelle l'ensemble des étapes qui sont classiquement exécutées pour que la machine A authentifie la machine B et vice-versa. Avantageusement selon l'invention, chaque dispositif (A,B) dispose d'une clé de session (KS) chiffrée avec la clé de sécurité, ou clé secrète, de son propre
20 élément de sécurité, fournie par exemple par un serveur externe d'applications. Ainsi, seuls les dispositifs (A,B) visés initialement par le serveur pourront établir la session de communication, puisqu'ils seront les seuls à pouvoir déchiffrer la clé de session, au moyen de leur clé secrète, et donc utiliser cette clé de session.

Avantageusement, par rapport aux systèmes de l'état de l'art, seuls les
25 dispositifs autorisés, c'est-à-dire ceux qui ont reçu d'un serveur de service la clé de session chiffrée par la clé secrète de leur élément de sécurité, vont pouvoir utiliser le service entre eux. De surcroît, l'usage de la clé secrète propre à chaque dispositif permet de chiffrer des clés de session pour différents services. Ces principes sont utilisables quelle que soit la technologie radio et avantageusement

adaptables quant au niveau de sécurité réalisé : : l'élément de sécurité effectuant le déchiffrement peut être un microprocesseur de l'objet disposant de la clé secrète ou un élément de sécurité de type carte SIM, en passant par toutes les possibilités intermédiaires.

5 On notera notamment que cette solution surmonte avantageusement les inconvénients du document précité « Survey on secure communication protocols for the Internet of Things », car selon ce document :

10 - soit la clé de session chiffrée est livrée dans les deux dispositifs eux-mêmes et dans ce cas les deux dispositifs électroniques n'ont pas l'assurance de pouvoir échanger des données avec un haut niveau de sécurité, puisque les clés de session chiffrées sont déchiffrées et utilisées dans les dispositifs eux-mêmes,

15 - soit les clés de session chiffrées sont livrées dans les éléments de sécurité des dispositifs et dans ce cas, dans un environnement multiservices, ces éléments de sécurité sont obligés de stocker et de gérer ces clés de session chiffrées toute la durée où elles sont utilisables, ce qui complexifie les éléments de sécurité et ne permet pas leur l'indépendance vis-à-vis des services.

20 Selon un mode de mise en œuvre particulier de l'invention, un procédé tel que décrit ci-dessus est en outre caractérisé en ce l'étape d'authentification mutuelle comporte :

25 - une étape d'obtention, par les deux authenticateurs des deux dispositifs, de la clé de la session chiffrée par la clé secrète de leur élément de sécurité respectif.

 - une étape de transmission, par chaque authenticateur à son élément de sécurité respectif de la clé de session chiffrée par la clé secrète de l'élément de sécurité respectif ;

- une étape de déchiffrement, par les éléments de sécurité respectifs, de la clé de session.

Avantageusement par rapport au système de l'état de l'art précité, la présente invention sépare nettement la partie fonctionnelle du service (le dispositif et son authenticateur) de la partie sécurité générique, indépendante des services. En effet, la sécurité étant assurée par un élément de sécurité auquel fait appel l'authenticateur, les deux éléments étant indépendants, l'élément de sécurité n'est pas lié au service, c'est-à-dire que l'on peut adresser plusieurs services de fonctionnalités différentes tout en ayant un mécanisme unique et générique dans l'élément de sécurité.

Corrélativement, si le dispositif tombe en panne, l'élément de sécurité pourra avantageusement être porté sur un autre dispositif, et si inversement l'élément de sécurité tombe en panne, il pourra (à condition d'être amovible) être remplacé.

15

Selon un autre mode de mise en œuvre particulier de l'invention, qui pourra être mise en œuvre alternativement ou cumulativement avec le précédent, un procédé tel que décrit ci-dessus est en outre caractérisé en ce l'étape d'authentification mutuelle comporte :

- une étape d'obtention, par les deux authenticateurs des deux dispositifs, d'une clé initiale de chiffrement chiffrée par la clé secrète de sécurité de leur élément de sécurité respectif.

- une étape de transmission par chaque authenticateur à son élément de sécurité respectif, de la clé initiale de chiffrement chiffrée par la clé secrète de l'élément de sécurité respectif ;

- une étape de déchiffrement, par les éléments de sécurité respectifs, de la clé initiale de chiffrement.

Avantageusement selon ce mode, la clé de chiffrement est donc chiffrée avec la clé secrète de l'élément de sécurité propre à chaque dispositif. Ainsi, seuls les dispositifs visés initialement par le serveur pourront communiquer, puisqu'ils seront les seuls à pouvoir la déchiffrer. La clé initiale de chiffrement
5 peut être complètement indépendante de la clé de session qui sert à l'authentification, ce qui augmente la sécurité de la clé de session

Selon un autre mode de mise en œuvre particulier de l'invention, qui pourra être mise en œuvre alternativement ou cumulativement avec les
10 précédents, un procédé tel que décrit ci-dessus est en outre caractérisé en ce qu'il comporte les étapes suivantes :

- transmission, du premier dispositif au second dispositif, d'une première donnée de vérification générée par l'élément de sécurité du premier dispositif ;
- 15 - réception par le second dispositif de la première donnée de vérification ;
- transmission, du second dispositif au premier dispositif, d'une seconde donnée de vérification générée par l'élément de sécurité du second dispositif et de la première donnée de vérification chiffrée par l'élément de sécurité du second dispositif à l'aide d'une clé de session ;
- 20 - réception par le premier dispositif de la seconde donnée de vérification et de la première donnée de vérification chiffrée par l'élément de sécurité du second dispositif ;
- authentification du second dispositif par le premier dispositif à l'aide de la première donnée de vérification chiffrée ;
- 25 - génération par l'élément de sécurité du premier dispositif d'une première clé de chiffrement pour l'échange de données chiffrées entre les deux dispositifs sur la session ;

- transmission, du premier dispositif au second dispositif, de la seconde donnée de vérification chiffrée par l'élément de sécurité du premier dispositif à l'aide de ladite clé de session ;
- authentification du premier dispositif par le second dispositif à l'aide la
5 seconde donnée de vérification chiffrée ;
- génération, par l'élément de sécurité du second dispositif, d'une seconde clé de chiffrement pour l'échange de données chiffrées entre les deux dispositifs sur la session, ladite seconde clé de chiffrement étant identique à la première clé de chiffrement.

10

La clé de session est nécessaire, selon ce mode de réalisation, à l'authentification mutuelle des deux dispositifs : si le premier élément de sécurité (SEA) parvient à déchiffrer l'aléa qu'il a préalablement transmis, et qui a été chiffré par le second élément de sécurité ($\{A_{LEA_A}\}KS$ chiffré par B), il sait que
15 le second dispositif détient la bonne clé de session (KS) pour l'authentification et donc la bonne clé de chiffrement (KC). Il en déduit que le second dispositif (B) est bien celui visé par le service, puisque la clé de session (KS) chiffrée par KB et livrée par le service sur B ne pouvait être déchiffrée que par le dispositif B (contenant l'élément de sécurité de B avec la clé KB). Symétriquement, si le
20 second élément de sécurité (SEB) parvient à déchiffrer l'aléa qu'il a préalablement transmis, et qui a été chiffré par le premier élément de sécurité ($\{A_{LEA_B}\}KS$ chiffré par A), il sait que le premier dispositif détient la bonne clé de session (KS) pour l'authentification et donc la bonne clé de chiffrement (KC). Il en déduit que le premier dispositif (A) est bien celui visé par le service,
25 puisque la clé de session (KS) chiffrée par KA et livrée par le service sur A ne pouvait être déchiffrée que par le premier dispositif A (contenant l'élément de sécurité SEA avec la clé KA).

Selon une variante de ce mode de mise en œuvre particulier de
30 l'invention, un procédé tel que décrit ci-dessus est en outre caractérisé en ce que

la clé de chiffrement est générée par un élément de sécurité en utilisant les données de vérification et au moins une donnée secrète.

Selon cette variante, la clé de chiffrement (KC) est générée par l'élément de sécurité de chaque dispositif à partir des deux aléas ayant servi à l'authentification mutuelle et à partir d'une donnée secrète, c'est-à-dire connue 5 seulement des dispositifs autorisés à communiquer. Une telle donnée secrète, commune aux deux dispositifs, est nécessaire pour assurer la sécurité, faute de quoi la clé de chiffrement pourrait être devinée par un dispositif espion sur la session. De préférence, cette donnée secrète a été chiffrée par la clé secrète de 10 l'élément de sécurité de chaque dispositif.

Grâce à l'utilisation avantageuse des deux aléas et de la donnée secrète, la clé de chiffrement ne peut être générée que par les deux éléments de sécurité des dispositifs de la session, ce qui augmente considérablement la sécurité puisqu'un dispositif tiers ne peut la générer. De surcroît, il n'est pas 15 nécessaire de mettre en œuvre des échanges supplémentaires, en plus des échanges nécessaires à l'authentification préalable.

Selon encore une variante de cette variante, un procédé tel que décrit ci-dessus est en outre caractérisé en ce que la donnée secrète est la 20 clé de session.

Avantageusement selon ce mode, la clé de session est utilisée comme élément secret en combinaison avec les deux aléas pour générer la clé de chiffrement. La clé de session ayant été préalablement chiffrée par la clé secrète des éléments de sécurité des dispositifs, seuls les éléments de sécurité des 25 dispositifs en question peuvent la déchiffrer. L'utilisation de la clé de session et des deux aléas est particulièrement intéressante pour obtenir une construction robuste de la clé.

Selon encore une seconde variante, qui pourra être mise en œuvre alternativement ou cumulativement avec la précédente, un procédé tel que décrit plus haut est en outre caractérisé en ce que la donnée secrète est la clé initiale de chiffrement.

- 5 Selon cette variante, chaque dispositif (A,B) dispose d'une clé de chiffrement initiale (KSZ) fournie par exemple par un serveur externe d'applications, cette clé de chiffrement étant chiffrée avec la clé secrète de son propre élément de sécurité. Ainsi, seuls les dispositifs (A,B) visés initialement par le serveur pourront communiquer, puisqu'ils seront les seuls à pouvoir la
- 10 déchiffrer. Dans ce mode, la clé initiale de chiffrement KSZ est complètement indépendante de la clé de session KS qui sert à l'authentification, ce qui augmente la sécurité de la clé de session KS. Il est connu en effet, selon les règles de l'art en matière de cryptographie, qu'il est préférable de ne pas utiliser la même clé (ou une clé dérivée) pour le chiffrement et pour l'authentification, si
- 15 la clé d'authentification doit être utilisée plusieurs fois, par exemple si le service permet que les deux dispositifs (A et B) se reconnectent ensemble plusieurs fois en réutilisant la clé KS.

- Selon un autre mode de mise en œuvre particulier de l'invention, qui
- 20 pourra être mis en œuvre alternativement ou cumulativement avec les précédents, un procédé tel que décrit plus haut est en outre caractérisé en ce qu'il comporte en outre une étape d'obtention, respectivement, par chaque dispositif, d'un identifiant de la session correspondant à la clé de session.

- Ce mode de réalisation de l'invention permet de gérer simultanément
- 25 ou successivement plusieurs services sur des sessions distinctes en identifiant, pour le service et sa session courante, la bonne clé de session (KS) chiffrée, stockée sur le dispositif à utiliser, parmi l'ensemble de clés de sessions (KS) chiffrées, stockées sur le dispositif. On peut ainsi imaginer un premier service s'exécutant entre deux machines A et B sur une session Wi-Fi, un second service
- 30 s'exécutant entre les deux machines A et B en Zigbee, et un troisième service

s'exécutant en NFC entre les machines A et C. Dans ce cas, le dispositif A aura tout intérêt à mémoriser trois identifiants de session distincts.

Si le dispositif doit traiter en parallèle plusieurs établissements de session, l'identifiant de session peut servir avantageusement d'index dans un tableau mémorisé par exemple dans l'élément de sécurité, qui permet de repérer la session en cours d'établissement. Ainsi la machine ciblée (la machine A dans l'exemple ci-dessus) pourra-t-elle faire facilement la différence entre les différentes sessions des différents services en cours d'établissement. Cet identifiant de la session permet avantageusement aussi de référencer les clés de session chiffrées afin qu'elles puissent être accédées rapidement et de manière univoque par les deux machines au moment de l'établissement de la session.

Selon un aspect matériel, l'invention concerne également un système de communication comprenant :

- 15 - un serveur comprenant un module de fourniture, pour chaque dispositif, d'au moins la clé de session chiffrée par une clé secrète connue seulement de l'élément de sécurité du dispositif ;
- au moins deux dispositifs comportant respectivement :
 - un éléments de sécurité comportant une clé secrète de sécurité
 - 20 - un authentificateur comportant :
 - un module d'obtention de la clé de session chiffrée par la clé secrète de son élément de sécurité respectif ;
 - un module d'authentification mutuelle faisant appel à son élément de sécurité respectif pour déchiffrer la clé de session.

Le terme module peut correspondre aussi bien à un composant logiciel qu'à un composant matériel ou un ensemble de composants matériels et logiciels, un composant logiciel correspondant lui-même à un ou plusieurs programmes ou sous-programmes d'ordinateur ou de manière plus générale à

5 tout élément d'un programme apte à mettre en œuvre une fonction ou un ensemble de fonctions telles que décrites pour les modules concernés. De la même manière, un composant matériel correspond à tout élément d'un ensemble matériel (ou hardware) apte à mettre en œuvre une fonction ou un ensemble de fonctions pour le module concerné (circuit intégré, carte à puce, carte à mémoire, etc.).

L'élément de sécurité de ces dispositifs peut être une carte SIM.

10 On rappelle qu'une carte SIM (acronyme de l'anglais Subscriber Identity Module), est une puce électronique comportant un microcontrôleur et des mémoires. Elle est notamment apte à supporter des applications spécifiques appelées "applets", programmes logiciels spécifiés en particulier selon la recommandation ETSI TS 102 223 et qui permettent de réaliser certaines fonctions de manière sécurisée, car s'exécutant justement au sein de la carte SIM. Une carte SIM peut être incluse dans un téléphone mobile ou tout autre
15 dispositif communiquant.

L'élément de sécurité peut aussi être constitué d'un environnement d'exécution de confiance. Par « environnement de confiance » (en Anglais « TEE » pour *Trusted Execution Environment*), on se réfère ici à une zone sécurisée et isolée d'autres environnements d'exécutions, située dans un
20 dispositif (de type téléphone portable), garantissant que des données sensibles sont stockées, traitées et protégées dans un environnement de confiance. Les applications présentes dans le TEE, appelées Trusted Applications (TA), ou applications de confiance, bénéficient d'un ensemble de services de sécurité comme le stockage sécurisé des données, la gestion des clefs et d'algorithmes
25 cryptographiques, etc.

Selon un autre aspect matériel, l'invention concerne également un dispositif de communication tel que décrit ci-dessus, caractérisé en ce que le dispositif est un téléphone mobile.

30 Selon un autre aspect matériel, l'invention concerne également un programme d'ordinateur apte à être mis en œuvre dans un dispositif et dans un

élément de sécurité tels que définis ci-dessus, le programme comprenant des instructions de code qui, lorsque le programme est exécuté par un processeur, réalise les étapes du procédé d'établissement d'une session de communication.

- 5 Selon un autre aspect matériel, l'invention concerne également un programme d'ordinateur apte à être mis en œuvre dans un élément de sécurité tel que défini ci-dessus, le programme comprenant des instructions de code qui, lorsque le programme est exécuté par un processeur, réalise les étapes du procédé de génération de clé.

- 10 Selon un autre aspect matériel, l'invention concerne également un programme d'ordinateur apte à être mis en œuvre dans un serveur tel que défini ci-dessus, le programme comprenant des instructions de code qui, lorsque le programme est exécuté par un processeur, réalise les étapes du procédé de livraison des clés de session.

- 15 Ces dispositifs, serveur, système et programmes d'ordinateurs présentent des caractéristiques et avantages analogues à ceux décrits précédemment en relation avec le procédé de communication.

- 20 Selon encore un autre aspect matériel, l'invention a trait à un support d'enregistrement lisible par un processeur de données sur lequel est enregistré un programmes comprenant des instructions de code de programme pour l'exécution des étapes du procédé défini ci-dessus.

L'invention sera mieux comprise à la lecture de la description qui suit, donnée à titre d'exemple et faite en référence aux dessins annexés.

- 25 Les figures:

La figure 1 représente un système sur lequel est illustré un exemple de réalisation de l'invention pour la communication sécurisée entre deux dispositifs équipés d'un élément de sécurité.

La figure 2 représente un organigramme illustrant les différentes étapes d'un procédé selon l'invention.

Description détaillée d'un exemple de réalisation illustrant l'invention

La figure 1 représente un système sur lequel est illustré un exemple de réalisation de l'invention pour la communication sécurisée entre deux dispositifs équipés d'un élément de sécurité.

Selon cet exemple, les premier (A) et second (B) dispositifs sont les deux machines (ou objets communicants) qui vont être appelées à s'authentifier mutuellement, puis à échanger des données de manière confidentielle sur un lien de communication (L).

La machine A peut par exemple être un *smartphone* et la machine B l'ordinateur de bord d'une automobile. Par exemple, l'authentification mutuelle des deux machines va permettre à un *smartphone* Zigbee d'ouvrir les portes de la voiture, puis de transmettre ensuite des données confidentielles à l'ordinateur de bord. On notera que la machine pourrait être d'un autre type : borne de parking, serveur dans un réseau, etc.

Le lien de communication (L) peut être de tout type permettant l'établissement d'une communication, de préférence en point à point, entre les deux machines : communication en mode Wi-Fi, notamment «Wi-Fi Direct », une technologie développée par le consortium «Wi-Fi Alliance» permettant le partage de données entre différents périphériques via leur connexion Wi-Fi sans point d'accès Wi-Fi intermédiaire ; communication de type Bluetooth (BT), une technologie radio de courte distance destinée à simplifier les connexions entre les appareils électroniques, développée par l'association « Bluetooth SIG » ; communication en champ proche, par exemple de type NFC (Near Field

- Communication), une technologie basée principalement sur la norme ISO (International Standard Organisation) 14443, pour permettre un échange d'informations sans fil entre deux périphériques éloignés d'une courte distance, typiquement inférieure à dix centimètres ; communication basée sur le protocole
- 5 Zigbee (un protocole qui permet la communication dans des réseaux locaux, sur un lien radio, avec une consommation réduite), la norme «DECT», etc.

Chacune des deux machines ou objets communicants (A, B) dispose:

- d'une application correspondant au service à mettre en œuvre (resp. APA dans la machine A et APB dans la machine B) pour le ou les services
- 10 considérés.

- d'un authentificateur (resp. AUA et AUB), élément logiciel se trouvant typiquement dans un module de la machine moins falsifiable qu'une application normale ; l'authentificateur peut par exemple être un processus du système d'exploitation ou du modem de la machine.

- 15 - d'un élément de sécurité (resp. SEA et SEB). Par « élément de sécurité », on entend ici un élément de stockage et de manipulation des données permettant de garantir à un utilisateur du dispositif une sécurité élevée, puisque les données enregistrées dans l'élément de sécurité ne sont pas accessibles à un utilisateur non autorisé. Cet élément de sécurité peut par exemple être constitué
- 20 par une carte SIM (de l'anglais Subscriber Identity Module), utilisée notamment en téléphonie mobile pour stocker les informations spécifiques à l'abonné d'un réseau mobile et des applications de l'utilisateur, de son opérateur ou dans certains cas de tierces parties. Cet élément de sécurité peut encore être un support amovible de type "Secure SD Card" ou un élément de sécurité intégré au
- 25 terminal ("Embedded Secure Element") ou encore une zone sécurisée du processeur applicatif grâce à l'utilisation d'une technologie de sécurité intégrée dans le processeur et ses composants périphériques (par exemple la technologie « TrustZone », marque déposée de la société ARM). Dans le cas d'un terminal supportant des applications de type Android (on rappelle qu'une application
- 30 Android est une application mobile spécifiquement développée pour les

terminaux mobiles utilisant le système d'application Android développé par la société Google), des applications peuvent également s'exécuter avec une sécurité principalement basée sur du logiciel, dans le terminal Android lui-même (à partir de la version 4.4. "KitKat"), grâce à la technologie "HCE" ("Host Card Emulation")
5 qui permet la communication NFC avec d'autres équipements. De manière plus générale, ce type de sécurité principalement basé sur du logiciel peut aussi utiliser des technologies connues sous la dénomination *d'obfuscation* ; on se référera par exemple à la présentation donnée dans l'article « WHITE-BOX CRYPTOGRAPHY: HIDING KEYS IN SOFTWARE » accessible à l'adresse
10 http://www.whiteboxcrypto.com/files/2012_misc.pdf.

Par la suite, on utilisera indifféremment les termes « élément de sécurité » et « carte SIM ».

Les deux dispositifs sont connectés à un serveur applicatif (SAP) chargé de délivrer au coup par coup des clés de sessions afin que les deux machines
15 puissent ensuite s'authentifier par le procédé de l'invention. Ce serveur applicatif peut relever de toute sorte de service nécessitant de faire dialoguer deux machines. Il peut s'agir d'un serveur sur un réseau Internet, sur un réseau mobile, etc. Le droit d'utiliser le service est livré aux deux dispositifs à partir du serveur applicatif, qui a prévu que les deux machines se rencontrent ; ce serveur
20 applicatif a notamment pour rôle, comme il sera détaillé par la suite, de livrer les clés de session chiffrées dans les deux machines.

Le serveur de confiance (SC) a quant à lui la connaissance des clés secrètes installées dans les éléments de sécurité des deux dispositifs. Dans l'exemple décrit ici, les éléments de sécurité étant des cartes SIM, ce serveur de
25 confiance peut appartenir à l'opérateur mobile qui distribue et contrôle les cartes SIM des deux dispositifs. Il peut dans ce cas avoir la connaissance d'une clé secrète, ou clé de sécurité, installée dans chaque carte SIM (clé différente pour chaque carte SIM). Selon un autre exemple, le serveur de confiance pourrait être tenu par exemple par un loueur d'automobiles qui aurait fait installer une clé
30 secrète (différente pour chaque voiture) dans les cartes SIM (ou éléments de sécurité) contenues dans les équipements de communication de ses voitures.

Dans de tels cas, la même entité juridique peut tenir les rôles de serveur applicatif (SAP) et de serveur de confiance (SC).

Selon un mode de réalisation de l'invention, qui sera détaillé par la suite à l'appui de la figure 2, le serveur applicatif est en charge de la livraison des clés de session sur les deux dispositifs.

1) Le serveur applicatif transmet dans un premier temps au serveur de confiance un message comprenant les informations suivantes:

- l'identité de la machine A et l'identité de la machine B ;
- la clé de session (KS) qui servira ensuite aux deux machines pour s'authentifier mutuellement ;
- éventuellement un index (IDS) identifiant le service concerné et la session dans le service et qui sert ici de référence entre le serveur applicatif et le serveur de confiance pour l'échange de type requête/réponse entre les deux serveurs. On notera qu'une autre référence pourrait selon une variante être utilisée entre le serveur applicatif et le serveur de confiance, car le serveur de confiance n'a pas d'intérêt particulier à connaître l'identifiant de session qui sera utilisé ultérieurement entre les deux dispositifs.
- éventuellement une clé de chiffrement initiale (KSZ) qui servira pour générer la clé de chiffrement finale (KC) qui servira aux deux machines pour échanger des données de manière confidentielle sur la session.

2) Le serveur de confiance (SC) répond au serveur applicatif (SAP) par un message qui comprend :

- l'index (IDS) identifiant le service concerné pour que le serveur applicatif puisse savoir à quelle requête se réfère cette réponse ;
- des éléments chiffrés par la clé secrète (KA, KB) de l'élément de sécurité de chacune des machines (resp. A et B) ; selon un exemple, les deux données (KS et KSZ) sont concaténées et chiffrées par la clé secrète de la SIM de la machine A, KA (resp. la machine B, KB).

3) Le serveur applicatif délivre à la machine A (resp. B) ces données chiffrées par la clé secrète de son élément de sécurité SEA (resp. SEB). Tout

mode de communication est envisageable pour cette communication (SMS, HTTP sur 3G/4G, etc...).

- 4) L'application dans la machine A, APA (resp. B, APB) stocke
5 (préférentiellement selon ce mode de réalisation, dans son authenticateur), les éléments reçus précédemment.

A l'issue de cette étape, chaque machine dispose des éléments qui vont lui permettre de mettre en œuvre la suite du procédé selon l'invention, en particulier l'utilisation, par chacun des deux éléments de sécurité, de la clé de
10 session chiffrée par la clé secrète propre à chaque élément de sécurité.

La figure 2 représente un organigramme illustrant les différentes étapes du procédé de l'invention.

- 15 Lors d'une étape E0, comme expliqué auparavant à l'appui de la figure 1, le serveur applicatif délivre aux deux dispositifs que sont la machine A (A) et la machine B (B) la clé de session (KS) chiffrée respectivement par la clé secrète de leur élément de sécurité (KA, KB).

Selon ce mode de réalisation, le serveur applicatif délivre en même
20 temps que la clé de session KS une clé initiale pour le chiffage, KSZ, et un identificateur de session, IDS :

- l'identificateur de la session permet de distinguer la session de communication des autres sessions de communication susceptibles d'être établies entre les deux machines, et aussi de référencer les
25 clés de session chiffrées afin qu'elles puissent être accédées par les deux machines. Cet identificateur de session est donc assimilable à un index de session.
- la clé de chiffage KSZ est utilisée ultérieurement pour générer la clé de chiffage finale KC qui sera utilisée pour l'échange des données
30 chiffrées entre les deux machines. Il est préférable, pour des raisons

de sécurité, que cette clé soit indépendante de la clé de session, qui sert pour sa part à l'authentification.

Selon ce mode de réalisation, la machine A et la machine B disposent également d'un authentificateur, c'est-à-dire un élément logiciel privilégié pour la communication avec l'élément de sécurité, chargé notamment de stocker les clés
5 chiffrées. Sur l'exemple de la figure 2, l'authentificateur (AUTH) et l'application (AP) sont confondus.

Dans cet exemple, l'application A de la machine A prend l'initiative de contacter l'application B de la machine B. L'application A peut, par exemple, dans
10 le contexte d'un mode de communication en champ proche de type ZigBee, découvrir qu'une autre machine (la machine B) est à proximité.

Lors d'une étape E1, l'application APA transmet à son élément de sécurité SEA les clés KS de session et KSZ de chiffrement chiffrées par la clé
15 secrète KA de l'élément de sécurité ainsi que l'index IDS de session.

Selon une variante, l'application A envoie à son authentificateur l'index IDS de session et l'authentificateur A cherche dans la mémoire de la machine ce qu'il y a stocké précédemment et qui correspond à l'index IDS, à savoir les données (KS, KSZ) chiffrées par la clé secrète de l'élément de sécurité KA, puis il
20 envoie ces éléments à son élément de sécurité SEA.

Lors d'une étape E2 symétrique, l'application APB (ou l'authentificateur de la machine B) transmet à son élément de sécurité SEB les clés KS de session et KSZ de chiffrement chiffrées par la clé secrète KB de l'élément de sécurité ainsi que l'index de session IDS.

On notera que, dans un mode de réalisation où l'élément de sécurité ne
25 sait traiter qu'un seul établissement de session à la fois (et non plusieurs en parallèle), il est superflu de lui communiquer l'index de session IDS. Notamment si l'élément de sécurité est une carte SIM, celle-ci n'est pas multitâche dans son fonctionnement. Elle n'a donc pas besoin de recevoir IDS n'y de l'ajouter dans sa

réponse, car l'authentificateur sait que la réponse se réfère forcément à la dernière commande.

- Lors d'une étape E3, l'élément de sécurité SEA déchiffre avec sa clé secrète KA les données reçues, puis crée ou modifie dans sa mémoire un tableau dit de référencement des sessions en cours (TABSA):

<i>IDS</i>	<i>KS</i>	<i>KSZ</i>		
------------	-----------	------------	--	--

On notera qu'après authentification, cette table n'est plus utilisée.

- Selon une variante, s'il y avait plusieurs serveurs de confiance associés au serveur applicatif, il pourrait y avoir plusieurs clés KA, il faudrait alors passer un identifiant de clé secrète KA. Cette variante n'est pas décrite plus avant.

Lors d'une étape E4 similaire à l'étape E3, l'élément de sécurité SEB déchiffre avec sa clé secrète KB les données reçues, puis crée ou modifie dans sa mémoire un tableau dit de référencement des sessions en cours (TABSB) :

<i>IDS</i>	<i>KS</i>	<i>KSZ</i>		
------------	-----------	------------	--	--

- Lors d'une étape E10, l'élément de sécurité SEA génère un aléa pour cette session, AL_A. L'aléa est classiquement un nombre généré aléatoirement. Le fait d'avoir un nombre aléatoire différent à chaque fois permet d'éviter qu'une personne ayant réussi à récupérer une signature d'un ancien nombre aléatoire puisse la réutiliser. SEA ajoute cet aléa dans la ligne créée dans son tableau de référencement TABSA :

<i>IDS</i>	<i>KS</i>	<i>KSZ</i>	<i>AL_A</i>	
------------	-----------	------------	-------------	--

Puis l'élément de sécurité retourne l'aléa à l'application (ou authentificateur selon cet exemple) de la machine A, qui la reçoit lors d'une étape E20.

- Lors d'une étape E20, l'application (ou l'authentificateur) de la machine A envoie vers la machine B l'index IDS de session ainsi que l'aléa AL_A qui vient d'être généré.

Ces données sont reçues par l'application B de la machine B lors d'une étape E30, qui les retransmet à son élément de sécurité SEB.

- 5 Selon une variante, l'application B envoie l'index dans un premier temps à son authenticateur et ce dernier recherche en mémoire les éléments stockés précédemment en relation avec l'index IDS, c'est-à-dire (KS, KSZ) chiffrées par la clé secrète KB de l'élément de sécurité.

- 10 Lors d'une étape E40, l'élément de sécurité SEB reçoit les données IDS, et AL_A, et complète dans sa mémoire la ligne du tableau de référencement TABSB des sessions en cours en y ajoutant AL_A. L'état de son tableau est alors le suivant :

IDS	KS	KSZ		AL_A
-----	----	-----	--	------

Lors d'une étape E41, l'élément de sécurité de la machine B chiffre cet aléa avec la clé de session KS et le renvoie à l'application (ou à l'authentificateur).

- 15 Lors d'une étape E42, l'élément de sécurité SEB génère également un aléa pour cette session, AL_B. Il ajoute cet aléa dans son tableau de référencement TABSB, et le renvoie à l'application (ou à l'authentificateur). L'état de son tableau est alors le suivant :

IDS	KS	KSZ	AL_B	AL_A
-----	----	-----	------	------

- 20 Naturellement, selon une variante, les étapes E4 et E40 pourraient être avantageusement concaténées, ce qui permettrait notamment de gagner un échange avec l'élément de sécurité. Il en est de même des étapes E41 et E42.

Lors d'une étape E32, l'application B envoie les données IDS, AL_A chiffré par KS et AL_B à l'application A.

- 25 L'application A (via l'authentificateur) relaie ces données (IDS, {AL_A}_{KS}, AL_B) à son élément de sécurité SEA au cours d'une étape E21.

Au cours d'une étape E11, l'élément de sécurité de la machine A, SEA, consulte son tableau de référencement des sessions en cours (s'il y en a plusieurs) et détermine (via l'index IDS) la ligne de la session concernée, puis ajoute AL_B dans le tableau ; l'état de son tableau est alors le suivant :

IDS	KS	KSZ	AL_A	AL_B
-----	----	-----	------	------

5

Puis lors de l'étape E11, SEA déchiffre l'aléa chiffré reçu $\{AL_A\}_{KS}$; si le résultat trouvé est égal à AL_A dans le tableau, le procédé continue ; SEA retourne un message d'acquiescement au cours d'une étape E12 successive à l'authentificateur et/ou l'application A. Sinon le procédé est interrompu et les deux machines ne pourront pas s'authentifier mutuellement. Cet acquiescement de l'élément de sécurité SEA indique que la vérification de AL_A chiffré par la machine B est positive. A partir de ce moment, l'élément de sécurité SEA sait que la machine B détient la bonne clé de session KS de session pour l'authentification (et également, selon ce mode de réalisation, la bonne clé KSZ pour le chiffrement).

Lors d'une étape E13, l'élément de sécurité génère une clé de chiffrement KC qui est issu d'un traitement des données KSZ (donnée secrète), AL_A et AL_B (aléas); selon un mode de réalisation, la génération consiste à hacher AL_A concaténé avec AL_B puis chiffrer le résultat par KSZ, pour obtenir KC.

Selon une variante, moins sécurisée, la clé de session KS est utilisée comme donnée secrète au lieu de la clé KSZ.

Selon une variante, c'est l'authentificateur qui reçoit les données en provenance de l'élément de sécurité et retourne à l'application A l'acquiescement ainsi que IDS, KC, et AL_B chiffré par la clé de session. Dans ce cas, l'acquiescement de l'authentificateur A à l'application A lui indique que l'authentification de la machine B est positive. L'application A pourra par conséquent utiliser KC pour chiffrer les données vers l'application B.

25

Lors d'une étape E14, l'élément de sécurité SEA chiffre AL_B avec KS et renvoie le résultat à l'application (ou à l'authentificateur).

Naturellement, selon une variante, les étapes E12, E13 et E14 pourraient être concaténées, ce qui permettrait notamment de gagner deux
5 échanges avec l'élément de sécurité.

Lors d'une étape E24, l'application A transmet à l'application B les informations IDS , OK , $\{AL_B\}_{KS}$. L'application B interprète, au cours de l'étape E33 le champ "OK" comme indiquant que la machine A a bien authentifié la machine B. L'application B (ou l'authentificateur) relaie ensuite ces données
10 (IDS , $\{AL_B\}_{KS}$) à son élément de sécurité SEB.

Au cours d'une étape E43, l'élément de sécurité de la machine B, SEB, consulte son tableau de référencement des sessions en cours (s'il y en a plusieurs) et détermine (via l'index IDS) la ligne de la session concernée qui
15 prend la forme :

IDS	KS	KSZ	AL_A	AL_B
-------	------	-------	---------	---------

Puis SEB déchiffre l'aléa chiffré reçu $\{AL_B\}_{KS}$; si le résultat trouvé est égal à AL_B dans le tableau, le procédé continue : SEB retourne un message d'acquiescement au cours d'une étape E44 successive à l'authentificateur et/ou
20 l'application A. Sinon le procédé est interrompu et les deux machines ne pourront pas s'authentifier mutuellement. Cet acquiescement de SEB indique que la vérification de AL_B chiffré par la machine A est positive. A partir de ce moment, SEB sait que la machine A détient la bonne clé de session KS de session pour l'authentification (et selon ce mode de réalisation, la bonne clé de session KSZ
25 pour le chiffrement).

Lors d'une étape E45, l'élément de sécurité SEB génère une clé de chiffrement KC qui est issue d'un traitement des données KSZ , AL_A et AL_B ; selon un mode de réalisation, la génération consiste à hacher AL_A concaténé avec AL_B puis chiffrer le résultat par KSZ , pour obtenir KC . La clé KC obtenue à
30 cette étape est identique à celle obtenue à l'étape E13.

Selon une variante, c'est l'authentificateur de B qui reçoit les données en provenance de l'élément de sécurité et retourne à l'application B l'acquiescement ainsi que IDS et KC. L'acquiescement de l'authentificateur B à l'application B lui indique dans ce cas que l'authentification de la machine A est positive.

L'application B pourra par conséquent utiliser KC pour chiffrer les données vers l'application A sans avoir recours à l'élément de sécurité. En particulier, pour la session d'authentification qui vient de s'achever, l'élément de sécurité n'utilise plus le tableau de référencement des sessions en cours. En particulier, s'il n'y a pas d'autre session d'authentification en cours d'établissement, le tableau peut être effacé.

Naturellement, selon une variante, les étapes E44 et E45 pourraient être concaténées, ce qui permettrait notamment de gagner un échange avec l'élément de sécurité.

Au cours d'une étape E36, l'application B envoie un acquiescement sous la forme d'un message (IDS, OK) à l'application A. L'application A interprète le champ "OK" comme indiquant que la machine B a authentifié la machine A.

Optionnellement, l'application A (resp. B) relaie les informations (IDS, OK) à son authentificateur, pour qu'il mette à jour sa machine d'état.

20

Il va de soi que le mode de réalisation qui a été décrit ci-dessus a été donné à titre purement indicatif et nullement limitatif, et que de nombreuses modifications peuvent être facilement apportées par l'homme de l'art sans pour autant sortir du cadre de l'invention.

25

Revendications

1. Procédé de communication entre deux dispositifs (A,B) auxquels sont associés respectivement :

- 5 - deux éléments de sécurité (SEA, SEB) comportant des clés secrètes de sécurité (KA,KB) respectives,
- deux authenticateurs (AUA, AUB),

le procédé comportant une étape d'authentification mutuelle des deux dispositifs (E10-E14, E20-25, E30-36, E40-E45), mise en œuvre par les deux authenticateurs (AUA, AUB) faisant appel à leurs éléments de sécurité respectifs (SEA, SEB) pour déchiffrer une clé de session (KS)..

2. Procédé de communication selon la revendication 1, caractérisé en ce que l'étape d'authentification mutuelle comporte :

- 15 - une étape d'obtention (E0), par les deux authenticateurs (AUA, AUB) des deux dispositifs (A,B), de la clé de la session (KS) chiffrée par la clé secrète (KA, KB) de leur élément de sécurité respectif (SEA, SEB).
- une étape de transmission (E1, E2) par chaque authenticateur à son élément de sécurité respectif de la clé de session (KS) chiffrée par la clé secrète (KA, KB) de l'élément de sécurité respectif ;
- 20 - une étape de déchiffrement (E3, E4), par les éléments de sécurité respectifs, de la clé de session (KS).

3. Procédé de communication selon la revendication 1, caractérisé en ce que l'étape d'authentification mutuelle comporte en outre :

- 25 - une étape d'obtention (E0), par les deux authenticateurs (AUA, AUB) des deux dispositifs (A,B), d'une clé initiale de chiffrement (KSZ) chiffrée par la clé secrète de sécurité (KA, KB) de leurs éléments de sécurité respectifs (SEA, SEB).
- une étape de transmission (E1, E2) par chaque authenticateur à son élément de sécurité respectif, de la clé initiale de chiffrement (KSZ)
- 30 chiffrée par la clé secrète (KA, KB) de l'élément de sécurité respectif ;

- une étape de déchiffrement (E3, E4), par les éléments de sécurité respectifs, de la clé initiale de chiffrement (KSZ).

4. Procédé de communication selon la revendication 1, le procédé comportant
5 les étapes suivantes :

- transmission (E20), du premier dispositif (A) au second dispositif (B),
d'une première donnée de vérification (AL_A) générée (E10) par l'élément
de sécurité du premier dispositif (SEA) ;
- réception (E30) par le second dispositif (B) de la première donnée de
10 vérification (AL_A) ;
- transmission (E32), du second dispositif (B) au premier dispositif (A),
d'une seconde donnée de vérification (AL_B) générée (E42) par l'élément
de sécurité du second dispositif (SEB) et de la première donnée de
vérification ($\{AL_A\}_{KS}$) chiffrée (E41) par l'élément de sécurité du second
15 dispositif (SEB) à l'aide d'une clé de session (KS) ;
- réception (E21) par le premier dispositif (A) de la seconde donnée de
vérification (AL_B) et de la première donnée de vérification ($\{AL_A\}_{KS}$)
chiffrée par l'élément de sécurité du second dispositif ;
- authentification (E11, E12) du second dispositif (B) par le premier
20 dispositif (A) à l'aide de la première donnée de vérification ($\{AL_A\}_{KS}$)
chiffrée.
- génération (E13) par l'élément de sécurité du premier dispositif (A) d'une
première clé de chiffrement (KC) pour l'échange de données chiffrées
entre les deux dispositifs (A, B) sur la session ;
- transmission (E24), du premier dispositif au second dispositif, de la
25 seconde donnée de vérification ($\{AL_B\}_{KS}$) chiffrée (E14) par l'élément de
sécurité du premier dispositif à l'aide de ladite clé de session (KS);
- authentification (E43, E44) du premier dispositif (A) par le second
dispositif (B) à l'aide la seconde donnée de vérification ($\{AL_B\}_{KS}$)
30 chiffrée ;

- génération (E45), par l'élément de sécurité du second dispositif (B) d'une seconde clé de chiffrement (KC) pour l'échange de données chiffrées entre les deux dispositifs sur la session, ladite seconde clé de chiffrement étant identique à la première clé de chiffrement (KC).
- 5 5. Procédé de communication selon la revendication 4, caractérisé en ce que la clé de chiffrement (KC) est générée par un élément de sécurité en utilisant les données de vérification (AL_A, AL_B) et au moins une donnée secrète (KS, KSZ).
6. Procédé de communication selon la revendication 5, caractérisé en ce que la
10 donnée secrète est la clé de session (KS).
7. Procédé de communication selon la revendication 5, caractérisé en ce que la donnée secrète est la clé initiale de chiffrement (KSZ).
8. Procédé de communication selon la revendication 1, caractérisé en ce qu'il comporte en outre une étape d'obtention, respectivement, par chaque
15 dispositif (A,B), d'un identifiant de la session (IDS) correspondant à la clé de session (KS).
9. Système de communication comprenant :
- un serveur (SAP) comprenant un module de fourniture, pour chaque dispositif, d'au moins la clé de session (KS) chiffrée par une clé secrète
20 (KA, KB) connue seulement de l'élément de sécurité du dispositif;
 - au moins deux dispositifs (A,B) comportant respectivement :
 - un éléments de sécurité (SEA, SEB) comportant une clé secrète de sécurité (KA,KB),
 - un authentificateur (AUA, AUB) comportant
25
 - un module d'obtention (E1, E2, E3, E4) de la clé de session (KS) chiffrée par la clé secrète (KA, KB) de son élément de sécurité respectif (SEA, SEB)
 - un module d'authentification mutuelle (AUA, AUB) faisant appel à son élément de sécurité respectif (SEA, SEB) pour
30 déchiffrer la clé de session (KS).

10. Programme d'ordinateur comportant des instructions de code pour la mise en œuvre du procédé de communication conforme à la revendication 1, lorsque celle-ci est exécutée par un processeur.

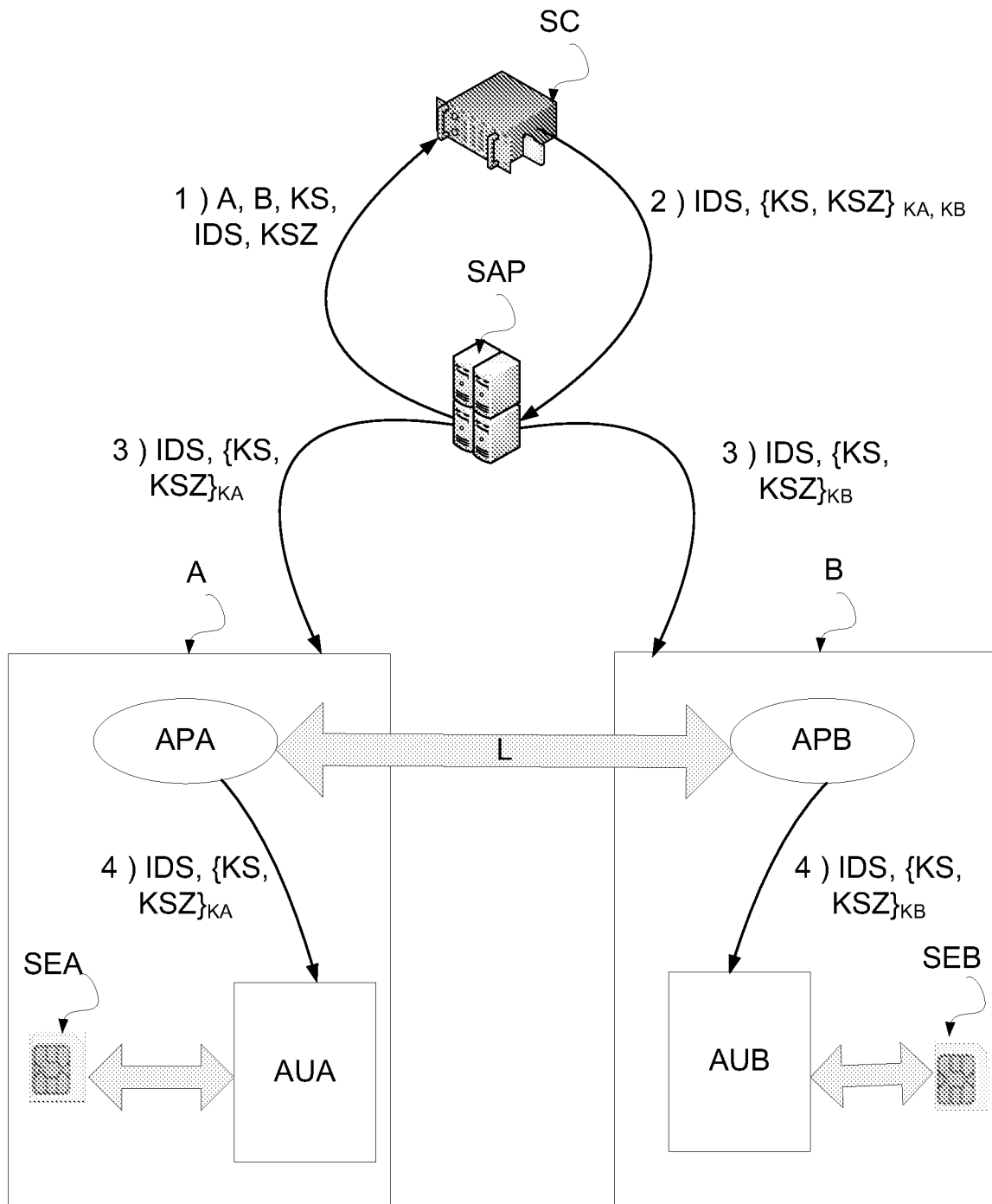


FIGURE 1

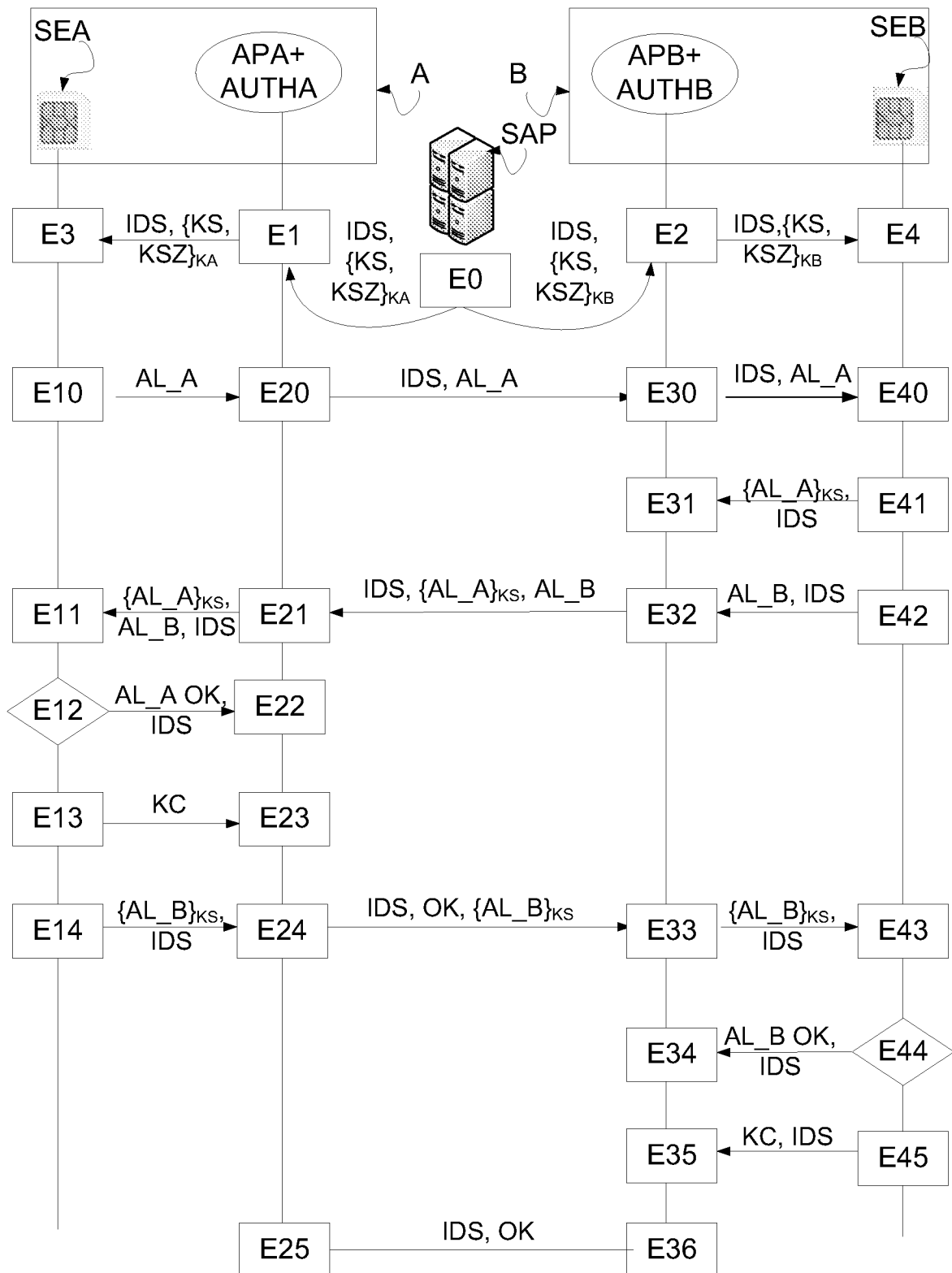


FIGURE 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2016/052713A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08
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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KIM THUAT NGUYEN ET AL: "Survey on secure communication protocols for the Internet of Things", AD HOC NETWORKS, vol. 32, 1 September 2015 (2015-09-01), pages 17-31, XP055288290, AMSTERDAM, NL ISSN: 1570-8705, DOI: 10.1016/j.adhoc.2015.01.006	1-3,8-10
Y	section 2.1 and 5.2.2 ----- -/--	4-7



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

7 February 2017

Date of mailing of the international search report

16/02/2017

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

Billet, Olivier

INTERNATIONAL SEARCH REPORT

International application No

PCT/FR2016/052713

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"Chapter 13: Key Management Techniques ED - Menezes A J; Van Oorschot P C; Vanstone S A", HANDBOOK OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, PAGE(S) 543 - 590 1 October 1996 (1996-10-01), XP001525013, ISBN: 978-0-8493-8523-0 Retrieved from the Internet: URL: http://www.cacr.math.uwaterloo.ca/hac/ section 13.2.3	1,3,8-10
Y	-----	4-7
X	ENDER YUKSEL ET AL: "A secure key establishment protocol for zigbee wireless sensor networks", COMPUTER AND INFORMATION SCIENCES, 2009. ISCIS 2009. 24TH INTERNATIONAL SYMPOSIUM ON, IEEE, PISCATAWAY, NJ, USA, 14 September 2009 (2009-09-14), pages 340-345, XP031549459, ISBN: 978-1-4244-5021-3 section II; figure 1; table 1	1-10
Y	"Chapter 12: Key Establishment Protocols ED - Menezes A J; Van Oorschot P C; Vanstone S A", HANDBOOK OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, PAGE(S) 489 - 541 1 October 1996 (1996-10-01), XP001525012, ISBN: 978-0-8493-8523-0 Retrieved from the Internet: URL: http://www.cacr.math.uwaterloo.ca/hac/ section 12.3.1	4-7

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/FR2016/052713

A. CLASSEMENT DE L'OBJET DE LA DEMANDE INV. H04L9/08 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		
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		
C. DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	KIM THUAT NGUYEN ET AL: "Survey on secure communication protocols for the Internet of Things", AD HOC NETWORKS, vol. 32, 1 septembre 2015 (2015-09-01), pages 17-31, XP055288290, AMSTERDAM, NL ISSN: 1570-8705, DOI: 10.1016/j.adhoc.2015.01.006	1-3,8-10
Y	section 2.1 and 5.2.2 ----- -/--	4-7
☒ 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 7 février 2017		Date d'expédition du présent rapport de recherche internationale 16/02/2017
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 Billet, Olivier

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	"Chapter 13: Key Management Techniques ED - Menezes A J; Van Oorschot P C; Vanstone S A", HANDBOOK OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, PAGE(S) 543 - 590 1^{er} octobre 1996 (1996-10-01), XP001525013, ISBN: 978-0-8493-8523-0 Extrait de l'Internet: URL:http://www.cacr.math.uwaterloo.ca/hac/section 13.2.3	1,3,8-10
Y	----- ENDER YUKSEL ET AL: "A secure key establishment protocol for zigbee wireless sensor networks", COMPUTER AND INFORMATION SCIENCES, 2009. ISCIS 2009. 24TH INTERNATIONAL SYMPOSIUM ON, IEEE, PISCATAWAY, NJ, USA, 14 septembre 2009 (2009-09-14), pages 340-345, XP031549459, ISBN: 978-1-4244-5021-3 section II; figure 1; tableau 1 -----	4-7
X	ENDER YUKSEL ET AL: "A secure key establishment protocol for zigbee wireless sensor networks", COMPUTER AND INFORMATION SCIENCES, 2009. ISCIS 2009. 24TH INTERNATIONAL SYMPOSIUM ON, IEEE, PISCATAWAY, NJ, USA, 14 septembre 2009 (2009-09-14), pages 340-345, XP031549459, ISBN: 978-1-4244-5021-3 section II; figure 1; tableau 1 -----	1-10
Y	"Chapter 12: Key Establishment Protocols ED - Menezes A J; Van Oorschot P C; Vanstone S A", HANDBOOK OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, PAGE(S) 489 - 541 1^{er} octobre 1996 (1996-10-01), XP001525012, ISBN: 978-0-8493-8523-0 Extrait de l'Internet: URL:http://www.cacr.math.uwaterloo.ca/hac/section 12.3.1 -----	4-7