(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 155 672***

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

(21) **N° d'enregistrement national :** **23 12879**

(51) Int Cl[8] : ***H 04 L 9/08*** *(2024.01), H 04 L 9/16, G 06 F 21/60, H 04 W 12/069*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 22.11.23.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 23.05.25 Bulletin 25/21.

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

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

( ) **Demande(s) d'extension :** Polynésie-Fr

(71) **Demandeur(s) :** *IDAKTO SAS* — FR.

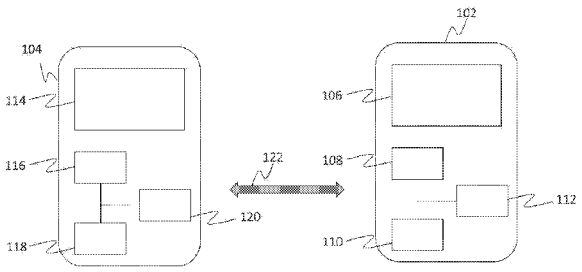
(72) **Inventeur(s) :** CAUCHIE Stéphane, MANGIN Lucas, CONDEMINE Thibault, BOUTHIER Clément et BERTHIER Paul-Edmond.

(73) **Titulaire(s) :** IDAKTO SAS.

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

(54) Procédés, dispositifs et système de transmission et d'acquisition d'une donnée.

(57) L'invention concerne un procédé d'échange d'une donnée entre un dispositif utilisateur (102) et un dispositif récepteur (104), le dispositif récepteur comprenant une information identifiant une donnée requise par le dispositif récepteur et le dispositif utilisateur ayant une donnée apte à être transmise.



FR 3 155 672 - A1

Description

Titre de l'invention : Procédés, dispositifs et système de transmission et d'acquisition d'une donnée

[0001] La présente invention concerne une manière sûre et fiable de réaliser une transmission d'une ou plusieurs données d'un dispositif utilisateur à un dispositif récepteur et une réception par le dispositif récepteur, de la donnée transmise par le dispositif utilisateur. En particulier, l'invention concerne un procédé de transmission d'une donnée d'un dispositif utilisateur à un dispositif récepteur mis en œuvre dans un dispositif utilisateur, un procédé de réception d'une donnée par un dispositif récepteur provenant d'un dispositif utilisateur, mis en œuvre dans un dispositif récepteur, le dispositif utilisateur et le dispositif récepteur associés ainsi que le système comprenant le dispositif utilisateur et le dispositif récepteur.

[0002] La transmission de données d'un dispositif utilisateur à un dispositif récepteur est critique, notamment lorsque les données sont des données personnelles ou confidentielles, pour plusieurs raisons. Tout d'abord, il est nécessaire que ces données ne puissent pas être acquises durant le transfert par un tiers, notamment un tiers malveillant. En outre, le dispositif récepteur doit être certain de la véracité des données reçues.

[0003] C'est particulièrement le cas, par exemple lorsque les données sont des données personnelles telles qu'une carte d'identité dématérialisée et que le dispositif récepteur est un dispositif apte à vérifier l'identité d'une personne porteuse d'un dispositif utilisateur mémorisant l'identité numérique.

[0004] Le but de l'invention est de permettre la transmission d'une donnée de manière fiable et sûre et de garantir au dispositif récepteur que les données reçues ne sont pas corrompues et sont les véritables données mémorisées dans le dispositif utilisateur.

[0005] Ce but est atteint par un procédé de transmission d'une donnée d'un dispositif utilisateur à un dispositif récepteur, le dispositif utilisateur ayant une donnée apte à être transmise. Le procédé mis en œuvre dans le dispositif utilisateur comprend les étapes suivantes :

- établissement d'un canal de communication sans fil entre le dispositif utilisateur et le dispositif récepteur ;
- envoi du dispositif utilisateur au dispositif récepteur via le canal de communication sans fil, d'une commande pour obtenir une information identifiant une donnée requise par le dispositif récepteur et obtention par le dispositif utilisateur de l'information identifiant une donnée requise ; et

- envoi du dispositif utilisateur au dispositif récepteur via le canal de communication sans fil, d'une commande comprenant la donnée apte à être transmise correspondant à l'information identifiant une donnée requise afin de transmettre la donnée apte à être transmise au dispositif récepteur.

[0006] L'information identifiant une donnée requise obtenue peut être signée, le procédé comprenant alors en outre, une étape de vérification de la signature de l'information identifiant une donnée requise obtenue signée.

[0007] Préalablement à l'envoi de la commande comprenant la donnée apte à être transmise, le procédé peut comprendre une étape de chiffrement de la donnée apte à être transmise.

[0008] Le dispositif utilisateur peut obtenir, en outre, une attestation de clés du dispositif récepteur.

[0009] L'attestation de clés du dispositif récepteur peut comprendre une clé cryptographique de signature publique du dispositif récepteur.

[0010] Le procédé peut comprendre en outre :

- une étape de génération d'un premier nombre aléatoire ;
- une étape d'envoi du dispositif utilisateur au dispositif récepteur, d'une commande comprenant le premier nombre aléatoire et d'obtention par le dispositif utilisateur d'une signature d'authentification du dispositif récepteur ;
- une étape de vérification de la signature d'authentification du dispositif récepteur obtenue au moyen de la clé cryptographique de signature publique du dispositif récepteur obtenue et du premier nombre aléatoire.

[0011] La vérification de la signature de l'information identifiant une donnée requise obtenue peut être réalisée au moyen de la clé cryptographique de signature publique du dispositif récepteur obtenue.

[0012] L'attestation de clés du dispositif récepteur peut comprendre une clé cryptographique de chiffrement publique du dispositif récepteur.

[0013] L'étape de chiffrement de la donnée apte à être transmise peut être réalisée au moyen de la clé cryptographique de chiffrement publique obtenue du dispositif récepteur.

[0014] L'information identifiant une donnée requise obtenue peut être chiffrée, et le procédé peut alors comprendre une étape de déchiffrement de l'information identifiant une donnée requise obtenue.

[0015] Préalablement à l'envoi de la donnée apte à être transmise, le procédé peut comprendre une étape de signature de la donnée apte à être transmise.

[0016] Le dispositif utilisateur peut comprendre une paire de clés cryptographiques de signature comprenant une clé cryptographique de signature privée et une clé cryptographique de signature publique, le procédé peut alors comprendre en outre, l'envoi du dispositif utilisateur au dispositif récepteur, d'une commande comprenant

une attestation de clés du dispositif utilisateur, l'attestation de clés du dispositif utilisateur comprenant la clé cryptographique de signature publique du dispositif utilisateur.

[0017] Le dispositif utilisateur peut obtenir, en outre, du dispositif récepteur, un deuxième nombre aléatoire. Le procédé peut alors comprendre une étape de génération d'une signature d'authentification du dispositif utilisateur à transmettre, la signature d'authentification étant générée à partir du deuxième nombre aléatoire obtenu et de la clé cryptographique de signature privée du dispositif utilisateur ; et l'envoi du dispositif utilisateur (102) au dispositif récepteur (104), d'une commande comprenant la signature d'authentification du dispositif utilisateur à transmettre générée.

[0018] Le déchiffrement de l'information identifiant une donnée requise obtenue peut être réalisée au moyen d'une clé cryptographique de chiffrement privée du dispositif utilisateur.

[0019] La signature de la donnée apte à être transmise peut être signée au moyen de la clé cryptographique de signature privée du dispositif utilisateur.

[0020] Le procédé peut comprendre en outre les étapes suivantes :

- envoi du dispositif utilisateur au dispositif récepteur, d'au moins un identifiant d'algorithme cryptographique supporté par le dispositif utilisateur et obtention d'au moins un identifiant d'algorithme cryptographique supporté par le dispositif récepteur;
- détermination d'un d'algorithme cryptographique supporté par le dispositif utilisateur et le dispositif récepteur et
- chiffrement de la donnée apte à être transmise correspondant à l'information identifiant une donnée requise obtenue en utilisation l'algorithme cryptographique déterminé.

[0021] L'étape d'envoi du dispositif utilisateur au dispositif récepteur d'une commande comprenant la donnée apte à être transmise correspondant à l'information identifiant une donnée requise peut être précédée d'une étape d'obtention d'un accord par l'utilisateur du dispositif utilisateur pour l'envoi de la donnée apte à être transmise.

[0022] Le canal de communication sans fil peut être un canal de communication conforme à la norme NFC, à la norme Bluetooth ou à la norme WiFi.

[0023] Le but est également atteint par un procédé de réception d'une donnée par un dispositif récepteur provenant d'un dispositif utilisateur, mis en œuvre dans le dispositif récepteur, le dispositif récepteur comprenant une information identifiant une donnée requise par le dispositif récepteur. Le procédé mis en œuvre dans le dispositif récepteur comprend les étapes suivantes :

- établissement d'un canal de communication sans fil entre le dispositif utilisateur et le dispositif récepteur ;

- réception via le canal de communication sans fil, d'une commande provenant du dispositif utilisateur, pour obtenir une information identifiant une donnée requise par le dispositif récepteur et réponse par la fourniture de l'information identifiant une donnée requise par le dispositif récepteur ; et
- réception via le canal de communication sans fil, d'une commande provenant du dispositif utilisateur, comprenant une donnée transmise correspondant à l'information identifiant une donnée requise par le dispositif récepteur.

[0024] Préalablement à la fourniture de l'information identifiant une donnée requise par le dispositif récepteur, le procédé peut comprendre en outre une étape de chiffrement de l'information identifiant une donnée requise par le dispositif récepteur.

[0025] La donnée transmise reçue peut être signée, le procédé peut alors comprendre en outre une étape de vérification de la signature de la donnée transmise reçue.

[0026] Le dispositif récepteur peut recevoir en outre, une attestation de clés du dispositif utilisateur.

[0027] L'attestation de clés du dispositif utilisateur peut comprendre une clé cryptographique de signature publique du dispositif utilisateur.

[0028] Le procédé peut comprendre en outre :

- une étape de génération d'un deuxième nombre aléatoire,
- une étape de mise à disposition au dispositif utilisateur du deuxième nombre aléatoire,
- une étape de réception d'une signature d'authentification du dispositif utilisateur,
- une étape de vérification de la signature d'authentification du dispositif utilisateur reçue au moyen de la clé cryptographique de signature publique du dispositif utilisateur obtenue et du deuxième nombre aléatoire.

[0029] La vérification de la signature de la donnée transmise reçue peut être réalisée au moyen de la clé cryptographique de signature publique du dispositif utilisateur obtenue.

[0030] L'attestation de clés du dispositif utilisateur peut comprendre une clé cryptographique de chiffrement publique du dispositif utilisateur.

[0031] L'étape de chiffrement de l'information identifiant une donnée requise par le dispositif récepteur peut être réalisée au moyen de la clé cryptographique de chiffrement publique du dispositif utilisateur.

[0032] La donnée transmise reçue peut être chiffrée, et le procédé peut comprendre alors une étape de déchiffrement de la donnée transmise reçue.

[0033] Le procédé peut comprendre en outre une étape de signature de l'information identifiant une donnée requise par le dispositif récepteur.

[0034] Le dispositif récepteur peut comprendre une paire de clés cryptographiques de signature comprenant une clé cryptographique de signature privée et une clé cryptographique de signature publique. Le procédé peut alors comprendre en outre, la mise à disposition du dispositif récepteur au dispositif utilisateur, d'une attestation de clés du dispositif récepteur, l'attestation de clés du dispositif récepteur comprenant la clé cryptographique de signature publique du dispositif récepteur.

[0035] Le dispositif récepteur peut recevoir, en outre, du dispositif utilisateur, un premier nombre aléatoire. Le procédé peut alors comprendre une étape de génération d'une signature d'authentification du dispositif récepteur à mettre à disposition du dispositif utilisateur, la signature d'authentification étant générée à partir du premier nombre aléatoire reçu et de la clé cryptographique de signature privée du dispositif récepteur ; et la mise à disposition du dispositif récepteur au dispositif utilisateur, de la signature d'authentification du dispositif récepteur à transmettre générée.

[0036] Le déchiffrement de la donnée transmise peut être réalisée au moyen d'une clé cryptographique de chiffrement privée du dispositif récepteur.

[0037] L'information identifiant une donnée requise obtenue peut être signée au moyen de la clé cryptographique de signature privée du dispositif récepteur.

[0038] Le procédé peut comprendre en outre les étapes suivantes :

- réception du dispositif utilisateur, d'au moins un identifiant d'algorithme cryptographique supporté par le dispositif utilisateur et réponse en fournissant au moins un identifiant d'algorithme cryptographique supporté par le dispositif récepteur ;
- détermination d'un d'algorithme cryptographique supporté par le dispositif utilisateur et le dispositif récepteur et
- déchiffrement de la donnée transmise correspondant à l'information identifiant une donnée requise par le dispositif récepteur en utilisation l'algorithme cryptographique déterminé.

[0039] Le canal de communication sans fil peut être un canal de communication conforme à la norme NFC, à la norme Bluetooth ou à la norme WiFi.

[0040] L'invention a également pour objet un dispositif configuré pour mettre en œuvre l'un des procédés précédemment décrit.

[0041] L'invention a également pour objet un système comprenant un dispositif utilisateur et un dispositif récepteur, le dispositif utilisateur et le dispositif récepteur mettant en œuvre respectivement les procédés précédemment décrit.

[0042] On va maintenant décrire des exemples de réalisation de la présente invention en référence aux figures annexées où les mêmes références désignent d'une figure à l'autre des éléments identiques ou fonctionnellement semblables :

[0043] La [Fig.1] est un schéma fonctionnel d'un exemple de système conformément à l'invention.

[0044] La [Fig.2] illustre un mode de réalisation du procédé de transmission d'une donnée mis en œuvre dans le dispositif utilisateur et du procédé de réception d'une donnée mis en œuvre dans le dispositif récepteur conformément à l'invention.

[0045] Selon la présente invention, le dispositif utilisateur possède une donnée qu'il souhaite transmettre à un dispositif récepteur qui souhaite obtenir l'information du dispositif utilisateur, notamment via un canal de communication, par exemple de courte distance.

[0046] La présente invention concerne selon un premier aspect, une manière sûre et fiable, de transmettre une donnée d'un dispositif utilisateur à un dispositif récepteur, le dispositif utilisateur ayant une donnée apte à être transmise.

[0047] La présente invention concerne selon un deuxième aspect une manière sûre et fiable, de réceptionner une donnée entre un dispositif utilisateur et un dispositif récepteur, le dispositif récepteur ayant une information identifiant une donnée requise par le dispositif récepteur afin d'obtenir une donnée du dispositif utilisateur correspondant à l'information identifiant une donnée requise par le dispositif récepteur.

[0048] La [Fig.1] est un schéma fonctionnel d'un exemple de système 100 permettant une transmission d'une ou plusieurs données entre deux dispositifs de manière sûre et fiable tout en garantissant la véracité des informations transmises. Par exemple, le système 100 peut être un système comprenant deux dispositifs informatiques différents, y compris un dispositif utilisateur 102 et un dispositif récepteur 104. Ces dispositifs informatiques peuvent communiquer entre eux via un canal de communication sans fil 106. Le canal de communication est par exemple conforme à un protocole de communication de courte distance (par exemple, une connexion conforme à la norme NFC, une connexion conforme à la norme Wifi, une connexion conforme à la norme Bluetooth, etc.). Le canal de communication va permettre de transmettre et obtenir des données d'un dispositif à l'autre dispositif.

[0049] Le dispositif utilisateur 102 peut être un dispositif mobile, tel qu'un ordinateur portable, un smartphone, une tablette ou un dispositif portable. Les dispositifs portables peuvent inclure des montres intelligentes ou tout autre type de dispositif informatique portable. Dans certaines mises en œuvre, le dispositif utilisateur 102 peut être un ordinateur de bureau ou un autre type de dispositif non portable, tel qu'une borne.

[0050] Le dispositif utilisateur 102 comprend une plateforme matérielle et logicielle sur laquelle s'exécutent des logiciels, ces logiciels étant soit directement exécutables soit interprétés sur une machine virtuelle.

[0051] Le dispositif utilisateur comprend un dispositif d'affichage 106, une unité de traitement 108, tel qu'un processeur, apte à exécuter des instructions et une mémoire de stockage 110.

[0052] Le dispositif d'affichage 106 comprend en particulier une interface de communication homme-machine permettant d'afficher des données et de recevoir des données provenant de l'utilisateur. Cette interface de communication homme-machine comprend par exemple un écran et un clavier, ou un écran tactile.

[0053] L'unité de traitement 108 est apte à exécuter un système d'exploitation qui peut être par exemple tout type de système d'exploitation du marché. L'unité de traitement 108 peut comprendre des moyens d'exécution d'au moins un algorithme cryptographique.

[0054] La mémoire de stockage 110 est apte à mémoriser des données de l'utilisateur, notamment des données confidentielles ou des données personnelles de l'utilisateur. La mémoire de stockage 110 peut comprendre notamment une mémoire sécurisée pour mémoriser les données confidentielles ou personnelles de l'utilisateur. La mémoire de stockage, notamment la mémoire sécurisée, peut en outre être utilisée pour stocker des clés cryptographiques.

[0055] Les données de l'utilisateur comprennent par exemple des données de paiement, d'identité numérique, de billettique de spectacle ou de transport.

[0056] La mémoire de stockage 110 peut en outre mémoriser des applications aptes à être exécutées par l'unité de traitement 108 du dispositif utilisateur 102.

[0057] Le dispositif utilisateur 102 peut comprendre en outre, des moyens de communication 112 aptes à communiquer avec un autre dispositif, par exemple un dispositif récepteur 104. Les moyens de communication 112 comprennent notamment une fonction d'établissement d'un canal de communication sécurisé, permettant la création d'un canal sécurisé 122 entre le dispositif utilisateur 102 et un dispositif récepteur 104. Les moyens de communication 112 permettent une connectivité de type réseau, soit via une connexion filaire soit via une connexion sans fil (par exemple, conforme à la norme Bluetooth, à la norme NFC, à la norme WIFI (par exemple, Wi-Di (ou Wi-Fi Direct)) ou à la norme PC/SC). Les moyens de communication 112 comprennent notamment un module permettant une communication basée sur une connexion de proximité.

[0058] Le dispositif récepteur 104 peut être un dispositif mobile, tel qu'un ordinateur portable, un smartphone, une tablette ou un dispositif portable. Les dispositifs portables peuvent inclure des montres intelligentes ou tout autre type de dispositif informatique portable. Dans certaines mises en œuvre, le dispositif récepteur 104 peut être un ordinateur de bureau ou un autre type de dispositif non portable, tel qu'une borne.

[0059] Le dispositif récepteur 104 comprend une plateforme matérielle et logicielle sur laquelle s'exécutent des logiciels, ces logiciels étant soit directement exécutables soit interprétés sur une machine virtuelle.

[0060] Le dispositif récepteur comprend un dispositif d'affichage 114, une unité de traitement 116, tel qu'un processeur, apte à exécuter des instructions et une mémoire de stockage 118.

[0061] Le dispositif d'affichage 114 comprend en particulier une interface de communication homme-machine permettant d'afficher des données et de recevoir des données provenant de l'utilisateur. Cette interface de communication homme-machine comprend par exemple un écran et un clavier, ou un écran tactile.

[0062] L'unité de traitement 116 est apte à exécuter un système d'exploitation qui peut être par exemple tout type de système d'exploitation du marché. L'unité de traitement 116 peut comprendre des moyens d'exécution d'au moins un algorithme cryptographique.

[0063] La mémoire de stockage 118 peut en outre mémoriser des applications aptes à être exécutées par l'unité de traitement 116 du dispositif récepteur 104. La mémoire de stockage 118 peut comprendre notamment une mémoire sécurisée pour stocker des clés cryptographiques.

[0064] Le dispositif récepteur 104 peut comprendre en outre, des moyens de communication 120 aptes à communiquer avec un autre dispositif, par exemple un dispositif utilisateur 102. Les moyens de communication 120 comprennent notamment une fonction d'établissement d'un canal de communication sécurisé, permettant la création d'un canal sécurisé 122 entre le dispositif récepteur 104 et un dispositif utilisateur 102. Les moyens de communication 122 permettent une connectivité de type réseau, soit via une connexion filaire soit via une connexion sans fil (par exemple, conforme à la norme Bluetooth, à la norme NFC, à la norme RFID, à la norme WIFI (par exemple, Wi-Di (ou Wi-Fi Direct)) ou à la norme PC/SC). Les moyens de communication 120 comprennent notamment un module permettant une communication basée sur une connexion de proximité.

[0065] Selon un exemple particulier de mise en œuvre, le canal de communication 122 est conforme à la norme NFC. Selon cette norme, plusieurs modes de fonctionnement peuvent être utilisés, notamment le mode émulation de carte, le mode lecteur et le mode pair-à-pair.

[0066] Dans le mode émulation de carte, dit passif, le dispositif se comporte comme une carte à puce sans-contact. Dans le cas où le dispositif est par exemple un téléphone mobile, la carte SIM de l'opérateur peut être utilisée comme élément de sécurité en stockant des informations chiffrées. Dans le mode lecteur, le dispositif devient un lecteur de cartes sans-contacts (mode actif) ou de "radio-étiquettes" (étiquettes

électroniques). Le mode pair-à-pair, quant à lui, permet à deux dispositifs d'échanger de l'information.

[0067] Selon la présente invention, le dispositif récepteur 104 est utilisé en mode émulation de carte. En d'autres termes, le dispositif récepteur n'initie pas la communication relative à l'échange d'une ou plusieurs données avec le dispositif utilisateur alors qu'il souhaite obtenir une donnée du dispositif utilisateur. C'est le dispositif utilisateur qui va émettre les commandes au dispositif récepteur pour la transmission de données.

[0068] Il n'est donc pas nécessaire que le dispositif récepteur dispose de service particulier, simplifiant ainsi le dispositif récepteur. En outre, aucune permission spéciale n'est à déclarer par le dispositif récepteur. Ce mode de fonctionnement réduit également les attaques possibles sur le dispositif utilisateur car il n'y a pas de communication avec le système d'exploitation. En effet, aucun émulateur de carte dans le dispositif utilisateur pouvant être corrompu n'est utilisé.

[0069] La [Fig.2] illustre un mode de réalisation du procédé de transmission d'une donnée mis en œuvre dans le dispositif utilisateur 102 et du procédé de réception d'une donnée mis en œuvre dans le dispositif récepteur 104 conformément à l'invention.

[0070] Le dispositif utilisateur 102 comprend une donnée apte à être transmise et le dispositif récepteur 104 comprend une information identifiant une donnée requise par le dispositif récepteur.

[0071] L'information identifiant une donnée requise est par exemple une information relative à l'identité dématérialisée de l'utilisateur, ou une information relative à des données bancaires de l'utilisateur, des données de paiement, de billettique de spectacle ou de transport, ou une information relative à toute autre donnée, telle que le nom, le prénom, l'adresse, la date de naissance de l'utilisateur.

[0072] La donnée apte à être transmise est par exemple une carte d'identité numérique, une donnée relative à un compte bancaire, et toute autre donnée à caractère personnel, confidentiel ou non.

[0073] A titre d'exemple, il va être considéré dans la suite que l'information identifiant une donnée requise est l'information "carte d'identité numérique" et que la donnée apte à être transmise est la carte d'identité de l'utilisateur du dispositif utilisateur 102.

[0074] Le procédé illustré à la [Fig.2] débute par une première étape d'établissement d'un canal de communication sans fil 204 entre le dispositif utilisateur 102 et dispositif récepteur 104. Le canal de communication est notamment un canal de communication sécurisé conforme à la norme NFC, à la norme Bluetooth ou à la norme WiFi.

[0075] Le dispositif récepteur n'initiant pas la communication relative à l'échange de données alors qu'il souhaite obtenir une donnée du dispositif utilisateur, ce dernier va initier la communication pour transmettre au moins une donnée, par l'envoi d'une

commande 206 via le canal de communication sans fil établi au dispositif récepteur 104.

[0076] La commande 206 est émise au dispositif récepteur pour obtenir une information identifiant une donnée requise par ce dernier. La commande peut être émise pour obtenir plus d'une information relative à plus d'une donnée requise.

[0077] Le dispositif récepteur 104 étant, dans cet échange, un dispositif passif, la commande va consister, pour le dispositif utilisateur 102 d'une part à écrire, notamment dans un espace mémoire du dispositif récepteur la commande et d'autre part à lire, notamment dans un espace mémoire, dans le dispositif récepteur, l'information identifiant une donnée requise par ce dernier.

[0078] Le résultat de cette commande consiste en l'obtention par le dispositif utilisateur 102 de l'information identifiant une donnée requise 210 par le dispositif récepteur. Dans l'exemple de la [Fig.2], l'information identifiant une donnée requise 210 est l'information "carte d'identité numérique".

[0079] En effet, sur réception d'une commande provenant du dispositif utilisateur, pour obtenir une information identifiant une donnée requise par le dispositif récepteur, le dispositif récepteur va répondre par la fourniture de l'information identifiant une donnée requise par le dispositif récepteur.

[0080] Sur réception de la commande 206 provenant du dispositif utilisateur, le dispositif récepteur 104 va mettre à disposition l'information identifiant une donnée requise, à savoir selon cet exemple, l'information "carte d'identité numérique", lors de l'étape 208. Lors de cette étape, d'autres opérations peuvent être réalisées qui seront détaillées ci-dessous.

[0081] Suite à la réception par le dispositif utilisateur de l'information identifiant une donnée requise, celui-ci va déterminer la donnée apte à être transmise correspondant à l'information identifiant une donnée requise obtenue lors de l'étape 212. Selon l'exemple de la [Fig.2], la donnée apte à être transmise est la carte d'identité de l'utilisateur du dispositif utilisateur 102. Lors de cette étape, d'autres opérations peuvent être réalisées qui seront détaillées ci-dessous.

[0082] Le dispositif utilisateur 102 va ensuite envoyer au dispositif récepteur 104 via le canal de communication sans fil établi, une commande comprenant la donnée apte à être transmise correspondant à l'information identifiant une donnée requise obtenue afin de transmettre la donnée apte à être transmise au dispositif récepteur, lors de l'étape 216. Le dispositif récepteur va alors recevoir la commande provenant du dispositif utilisateur, comprenant la donnée transmise correspondant à l'information identifiant une donnée requise par le dispositif récepteur.

[0083] Cette commande va consister, pour le dispositif utilisateur à écrire dans le dispositif récepteur la donnée apte à être transmise correspondant à l'information identifiant une

donnée requise par le dispositif récepteur. Le dispositif récepteur va ainsi recevoir la donnée transmise par le dispositif utilisateur qu'il souhaite obtenir, à savoir, dans l'exemple de la [Fig.2], la carte d'identité de l'utilisateur du dispositif utilisateur 102.

[0084] L'étape 216 peut être précédée d'une étape 214 au cours de laquelle le dispositif utilisateur 102 va envoyer au dispositif récepteur 104 via le canal de communication sans fil établi, une commande afin d'informer le dispositif récepteur de la taille de la donnée apte à être transmise que le dispositif utilisateur va transmettre en dispositif récepteur.

[0085] L'étape 216 est suivie d'une étape 218 de traitement de la donnée reçue par le dispositif récepteur. Lors de cette étape, d'autres opérations peuvent être réalisées qui seront détaillées ci-dessous.

[0086] Le procédé de transmission d'une donnée mis en œuvre dans le dispositif utilisateur 102 et du procédé de réception d'une donnée mis en œuvre dans le dispositif récepteur 104 conformément à l'invention décrite à la [Fig.2] peuvent également comprendre une ou plusieurs caractéristiques décrites ci-après.

[0087] En particulier, le dispositif utilisateur 102 et le dispositif récepteur 104 peuvent s'exécuter sur un même type de système d'exploitation ou sur un système d'exploitation de type différent.

[0088] Le dispositif utilisateur 102 et le dispositif récepteur 104 peuvent comprendre respectivement une paire de clés cryptographiques de signature comprenant une clé cryptographique de signature privée et une clé cryptographique de signature publique et/ou une paire de clés cryptographiques de chiffrement comprenant une clé cryptographique de chiffrement privée et une clé cryptographique de chiffrement publique.

[0089] Le dispositif utilisateur 102 et le dispositif récepteur 104 peuvent en outre comprendre chacun un ensemble de paramètres. L'un des paramètres peut être le nom de l'application ayant besoin d'un échange de données entre le dispositif utilisateur et le dispositif récepteur. Le nom de l'application est par exemple unique.

[0090] L'un des paramètres peut comprendre le mode de fonctionnement du dispositif. Le mode de fonctionnement consiste par exemple à indiquer si l'échange de la ou des données va se faire sans le consentement de l'utilisateur ou avec le consentement de l'utilisateur. D'autres modes de fonctionnement peuvent être utilisés.

[0091] Le dispositif utilisateur 102 et le dispositif récepteur 104 peuvent également comprendre un paramètre indiquant s'ils souhaitent respectivement que les dispositifs soient authentifiés préalablement à l'échange de données. L'un des paramètres peut en outre comprendre la ou les algorithmes cryptographiques aptes à être mis en œuvre dans le dispositif.

[0092] En outre, l'un des paramètres du dispositif utilisateur 102 peut comprendre un premier nombre aléatoire, généré par exemple par le dispositif utilisateur. Le premier nombre aléatoire peut être un nombre aléatoire ou un nombre pseudo aléatoire. La longueur du premier nombre aléatoire est par exemple de 32 octets.

[0093] Selon un mode de réalisation particulier, le dispositif utilisateur 102 peut envoyer au dispositif récepteur, soit dans la commande pour obtenir une information identifiant une donnée requise lors de l'étape 206, soit dans une nouvelle commande au moins un paramètre du dispositif utilisateur 102. Ledit au moins un paramètre peut être le premier nombre aléatoire, le nom de l'application du dispositif utilisateur, le mode de fonctionnement du dispositif, l'information selon laquelle le dispositif utilisateur 102 souhaite que les dispositifs soient authentifiés préalablement à l'échange de données, et/ou la liste des algorithmes cryptographiques supportés par le dispositif utilisateur 102.

[0094] Suite à la réception de la commande par le dispositif récepteur, celui-ci peut générer une attestation, notamment à l'étape 208 qui précède l'étape 210. L'attestation peut comprendre une signature d'authentification du dispositif récepteur, la signature d'authentification du dispositif récepteur pouvant être générée par la signature du premier nombre aléatoire reçu (par exemple avec la commande envoyée lors de l'étape 206) du dispositif utilisateur avec la clé cryptographique de signature privée du dispositif récepteur.

[0095] L'attestation peut en outre comprendre une attestation de clés du dispositif récepteur afin de démontrer la provenance des clés du dispositif récepteur, l'attestation de clés du dispositif récepteur comprenant notamment la clé cryptographique de chiffrement publique du dispositif récepteur et/ou la clé cryptographique de signature publique du dispositif récepteur. L'attestation de clés du dispositif récepteur peut en outre comprendre un type d'attestation, permettant notamment d'identifier le format de l'attestation, et une durée de validité de l'attestation de clés.

[0096] L'attestation peut également comprendre un deuxième nombre aléatoire généré par le dispositif récepteur et/ou au moins un paramètre du dispositif récepteur, à savoir le nom de l'application du dispositif récepteur, le mode de fonctionnement du dispositif, l'information selon laquelle le dispositif récepteur 104 souhaite que les dispositifs soient authentifiés préalablement à l'échange de données, et/ou la liste des algorithmes cryptographiques supportés par le dispositif récepteur 104. La longueur du deuxième nombre aléatoire est par exemple de 32 octets.

[0097] Cette attestation est mise à disposition du dispositif utilisateur de sorte que celui-ci puisse l'obtenir en réponse à la commande émise.

[0098] Le dispositif utilisateur peut alors obtenir à l'étape 210, l'attestation du dispositif récepteur ainsi que l'information identifiant une donnée requise.

[0099] Après l'obtention de l'attestation du dispositif récepteur, le dispositif utilisateur peut vérifier l'attestation reçue. La vérification peut par exemple est réalisée lors de l'étape 212 illustrée à la [Fig.2]. La vérification peut consister à vérifier la signature d'authentification du dispositif récepteur. La vérification de la signature d'authentification est par exemple réalisée à partir de la clé cryptographique de signature publique du dispositif récepteur qui a été reçue notamment au moyen de l'attestation de clés du dispositif récepteur.

[0100] La vérification de l'attestation reçue peut également consister à vérifier l'attestation de clés du dispositif récepteur reçue permettant de vérifier la provenance de la ou des clés reçues ainsi que la légitimité de l'application communiquant avec le dispositif utilisateur et du dispositif récepteur. De même, la durée de validité de l'attestation de clés peut être vérifiée.

[0101] Selon un mode de réalisation particulier, préalablement à la mise à disposition de l'information identifiant une donnée requise par le dispositif récepteur au dispositif utilisateur, l'information peut être signée, par exemple lors de l'étape 208 par le dispositif récepteur avec la clé cryptographique de signature privée du dispositif récepteur et/ou chiffrée par le dispositif récepteur avec une clé cryptographique de chiffrement publique du dispositif utilisateur que le dispositif récepteur aura préalablement reçu.

[0102] Après l'obtention par le dispositif utilisateur de l'information identifiant une donnée requise signée, celui-ci va vérifier, par exemple lors de l'étape 212, la signature de l'information identifiant une donnée requise obtenue à partir de la clé cryptographique de chiffrement publique du dispositif récepteur qui a été reçue notamment au moyen de l'attestation de clés du dispositif récepteur.

[0103] Si l'information identifiant une donnée requise obtenue par le dispositif utilisateur a été chiffrée par le dispositif récepteur, l'information est alors déchiffrée à partir de la clé cryptographique de chiffrement privée du dispositif utilisateur.

[0104] Préalablement à l'envoi du dispositif utilisateur 102 au dispositif récepteur 104 via le canal de communication sans fil, d'une commande comprenant la donnée apte à être transmise correspondant à l'information identifiant une donnée requise obtenue, le dispositif utilisateur 102 peut générer une attestation, par exemple lors de l'étape 212.

[0105] L'attestation du dispositif utilisateur peut comprendre une signature d'authentification du dispositif utilisateur, la signature d'authentification du dispositif utilisateur pouvant être générée par la signature du deuxième nombre aléatoire reçu généré par le dispositif récepteur et obtenu par le dispositif utilisateur, avec la clé cryptographique de signature privée du dispositif utilisateur.

[0106] L'attestation peut en outre comprendre une attestation de clés du dispositif utilisateur afin de démontrer la provenance des clés du dispositif utilisateur, l'attestation de clés

du dispositif utilisateur comprenant notamment une clé cryptographique de chiffrement publique du dispositif utilisateur et/ou une clé cryptographique de signature publique du dispositif utilisateur. L'attestation de clés du dispositif utilisateur peut en outre comprendre un type d'attestation, permettant notamment d'identifier le format de l'attestation, et une durée de validité de l'attestation de clés.

[0107] La commande comprenant la donnée apte à être transmise correspondant à l'information identifiant une donnée requise obtenue peut également comprendre l'attestation générée par le dispositif utilisateur.

[0108] La donnée apte à être transmise correspondant à l'information identifiant une donnée requise obtenue peut être signée au moyen de la clé cryptographique de signature privée du dispositif utilisateur et/ou chiffrée au moyen de la clé cryptographique de chiffrement publique du dispositif récepteur précédemment obtenue au moyen de l'attestation de clés du dispositif récepteur, notamment lors de l'étape 212.

[0109] A partir de l'attestation envoyée par le dispositif utilisateur 102 au dispositif récepteur 104, ce dernier peut vérifier l'attestation reçue, notamment lors de l'étape 218.

[0110] La vérification peut consister à vérifier la signature d'authentification du dispositif utilisateur. La vérification de la signature d'authentification est par exemple réalisée à partir de la clé cryptographique de signature publique du dispositif utilisateur qui a été reçue notamment au moyen de l'attestation de clés du dispositif utilisateur.

[0111] La vérification de l'attestation reçue peut également consister à vérifier l'attestation de clés du dispositif utilisateur reçue permettant de vérifier la provenance de la ou des clés reçues. Cette dernière est réalisée au moins d'attestations de clés fournis par le système d'exploitation du dispositif utilisateur. De même, la durée de validité de l'attestation de clés peut être vérifiée.

[0112] Si la donnée transmise reçue par le dispositif récepteur correspondant à l'information identifiant une donnée requise a été signée, alors la signature est vérifiée par le dispositif récepteur au moyen de la clé cryptographique de signature publique du dispositif utilisateur préalablement obtenue, lors de l'étape 218.

[0113] En outre, si la donnée transmise reçue par le dispositif récepteur correspondant à l'information identifiant une donnée requise a été chiffrée, alors elle est déchiffrée au moyen de la clé cryptographique de chiffrement privée du dispositif récepteur, lors de l'étape 218.

[0114] Selon un mode de réalisation particulier, le dispositif utilisateur envoie au dispositif récepteur, au moins un identifiant d'algorithme cryptographique supportée par le dispositif utilisateur via par exemple la commande pour obtenir une information identifiant une donnée requise ou une nouvelle commande et obtient au moins un identifiant d'algorithme cryptographique supportée par le dispositif récepteur. Dans ce

mode de réalisation, le dispositif utilisateur détermine un algorithme cryptographique supportée par le dispositif utilisateur et le dispositif récepteur et chiffre la donnée apte à être transmise correspondant à l'information identifiant une donnée requise obtenue en utilisation l'algorithme cryptographique déterminé. L'algorithme est par exemple l'algorithme SHA256 avec ECDSA. Selon ce mode de réalisation, le dispositif récepteur reçoit du dispositif utilisateur, une commande comprenant au moins un identifiant d'algorithme cryptographique supportée par le dispositif utilisateur et répond en fournissant au moins un identifiant d'algorithme cryptographique supportée par le dispositif récepteur. En outre, le dispositif récepteur détermine un d'algorithme cryptographique supportée par le dispositif utilisateur et le dispositif récepteur et déchiffre la donnée transmise chiffrée reçue correspondant à l'information identifiant une donnée requise en utilisation l'algorithme cryptographique déterminé.

[0115] Selon un mode de réalisation particulier, le dispositif utilisateur informe le dispositif récepteur de son mode de fonctionnement, à savoir, si l'échange de la ou des données va se faire sans le consentement de l'utilisateur ou avec le consentement de l'utilisateur. D'autres modes de fonctionnement peuvent être utilisés.

[0116] Dans le cas où le mode de fonctionnement du dispositif utilisateur nécessite le consentement de l'utilisateur, préalablement à l'envoi de la commande comprenant la donnée apte à être transmise correspondant à l'information identifiant une donnée requise, l'obtention d'un accord par l'utilisateur du dispositif utilisateur pour l'envoi de la donnée apte à être transmise sera exécutée. L'obtention sera réalisée par l'affichage d'une demande de confirmation pour l'envoi de la donnée apte à être transmise sur le dispositif d'affichage du dispositif utilisateur. Après confirmation par l'utilisateur du dispositif utilisateur, la commande comprenant la donnée apte à être transmise correspondant à l'information identifiant une donnée requise sera envoyée.

[0117] La donnée apte à être transmise pouvant être d'une taille importante, préalablement à sa transmission, le dispositif utilisateur 102 peut envoyer une commande au dispositif récepteur 104 comprenant la taille de la donnée apte à être transmise, lors de l'étape 214 illustrée à la [Fig.2]. Ainsi, le dispositif récepteur peut afficher à l'écran du dispositif une animation montrant la durée pour l'obtention par ce dernier de la donnée transmise.

Revendications

[Revendication 1] Procédé de transmission d'une donnée d'un dispositif utilisateur (102) à un dispositif récepteur (104), le dispositif utilisateur (102) ayant une donnée apte à être transmise,
le procédé mis en œuvre dans le dispositif utilisateur (102) comprend les étapes suivantes :

- établissement d'un canal de communication sans fil entre le dispositif utilisateur (102) et le dispositif récepteur (104) ;
- envoi du dispositif utilisateur (102) au dispositif récepteur (104) via le canal de communication sans fil, d'une commande pour obtenir une information identifiant une donnée requise par le dispositif récepteur (104) et obtention par le dispositif utilisateur (102) de l'information identifiant une donnée requise par le dispositif récepteur ; et
- envoi du dispositif utilisateur (102) au dispositif récepteur (104) via le canal de communication sans fil, d'une commande comprenant la donnée apte à être transmise correspondant à l'information identifiant une donnée requise afin de transmettre la donnée apte à être transmise au dispositif récepteur.

[Revendication 2] Procédé selon la revendication précédente, dans lequel l'information identifiant une donnée requise obtenue est signée, le procédé comprenant en outre, une étape de vérification de la signature de l'information identifiant une donnée requise obtenue signée.

[Revendication 3] Procédé selon l'une quelconque des revendications précédentes, dans lequel préalablement à l'envoi de la commande comprenant la donnée apte à être transmise, le procédé comprend une étape de chiffrement de la donnée apte à être transmise.

[Revendication 4] Procédé selon l'une quelconque des revendications précédentes, dans lequel le dispositif utilisateur (102) obtient, en outre, une attestation de clés du dispositif récepteur.

[Revendication 5] Procédé selon la revendication précédente, dans lequel l'attestation de clés du dispositif récepteur comprend une clé cryptographique de signature publique du dispositif récepteur.

[Revendication 6] Procédé selon la revendication précédente, dans lequel le procédé comprend en outre :

- une étape de génération d'un premier nombre aléatoire ;
- une étape d'envoi du dispositif utilisateur (102) au dispositif récepteur (104), d'une commande comprenant le premier nombre aléatoire et d'obtention par le dispositif utilisateur (102) d'une signature d'authentification du dispositif récepteur ;
- une étape de vérification de la signature d'authentification du dispositif récepteur obtenue au moyen de la clé cryptographique de signature publique du dispositif récepteur obtenue et du premier nombre aléatoire.

[Revendication 7] Procédé selon la revendication 2 et la revendication 5, dans lequel la vérification de la signature de l'information identifiant une donnée requise obtenue est réalisée au moyen de la clé cryptographique de signature publique du dispositif récepteur obtenue.

[Revendication 8] Procédé selon l'une quelconque des revendications 4 à 7, dans lequel l'attestation de clés du dispositif récepteur comprend une clé cryptographique de chiffrement publique du dispositif récepteur.

[Revendication 9] Procédé selon la revendication 3 et la revendication 8, dans lequel l'étape de chiffrement de la donnée apte à être transmise est réalisée au moyen de la clé cryptographique de chiffrement publique obtenue du dispositif récepteur.

[Revendication 10] Procédé selon l'une quelconque des revendications précédentes, dans lequel l'information identifiant une donnée requise obtenue est chiffrée, et le procédé comprend une étape de déchiffrement de l'information identifiant une donnée requise obtenue.

[Revendication 11] Procédé selon l'une quelconque des revendications précédentes, dans lequel préalablement à l'envoi de la donnée apte à être transmise, le procédé comprend une étape de signature de la donnée apte à être transmise.

[Revendication 12] Procédé selon l'une quelconque des revendications précédentes, dans lequel le dispositif utilisateur (102) comprend une paire de clés cryptographiques de signature comprenant une clé cryptographique de signature privée et une clé cryptographique de signature publique, dans lequel le procédé comprend en outre, l'envoi du dispositif utilisateur (102) au dispositif récepteur (104), d'une commande comprenant une attestation de clés du dispositif utilisateur,

l'attestation de clés du dispositif utilisateur comprenant la clé cryptographique de signature publique du dispositif utilisateur (102).

[Revendication 13] Procédé selon la revendication précédente, dans lequel le dispositif utilisateur (102) obtient, en outre, du dispositif récepteur (104), un deuxième nombre aléatoire, et en ce que le procédé comprend une étape de génération d'une signature d'authentification du dispositif utilisateur à transmettre, la signature d'authentification étant générée à partir du deuxième nombre aléatoire obtenu et de la clé cryptographique de signature privée du dispositif utilisateur (102) ; et l'envoi du dispositif utilisateur (102) au dispositif récepteur (104), d'une commande comprenant la signature d'authentification du dispositif utilisateur à transmettre générée.

[Revendication 14] Procédé selon la revendication 10, dans lequel le déchiffrement de l'information identifiant une donnée requise obtenue est réalisée au moyen d'une clé cryptographique de chiffrement privée du dispositif utilisateur (102).

[Revendication 15] Procédé selon la revendication 11 et la revendication 12, dans lequel la signature de la donnée apte à être transmise est signée au moyen de la clé cryptographique de signature privée du dispositif utilisateur (102).

[Revendication 16] Procédé selon l'une quelconque des revendications précédentes, le procédé comprenant en outre les étapes suivantes :

- envoi du dispositif utilisateur (102) au dispositif récepteur, d'au moins un identifiant d'algorithme cryptographique supporté par le dispositif utilisateur et obtention d'au moins un identifiant d'algorithme cryptographique supporté par le dispositif récepteur;
- détermination d'un d'algorithme cryptographique supporté par le dispositif utilisateur et le dispositif récepteur et
- chiffrement de la donnée apte à être transmise correspondant à l'information identifiant une donnée requise obtenue en utilisation l'algorithme cryptographique déterminé.

[Revendication 17] Procédé selon l'une quelconque des revendications précédentes, dans lequel l'étape d'envoi du dispositif utilisateur (102) au dispositif récepteur (104) d'une commande comprenant la donnée apte à être transmise correspondant à l'information identifiant une

donnée requise est précédée d'une étape d'obtention d'un accord par l'utilisateur du dispositif utilisateur pour l'envoi de la donnée apte à être transmise.

[Revendication 18] Procédé selon l'une quelconque des revendications précédentes, dans lequel le canal de communication sans fil est un canal de communication conforme à la norme NFC, à la norme Bluetooth ou à la norme WiFi.

[Revendication 19] Procédé de réception d'une donnée par un dispositif récepteur (104) provenant d'un dispositif utilisateur (102), le dispositif récepteur (104) comprenant une information identifiant une donnée requise par le dispositif récepteur,
le procédé mis en œuvre dans le dispositif récepteur (104) comprend les étapes suivantes :

- établissement d'un canal de communication sans fil entre le dispositif utilisateur et le dispositif récepteur ;
- réception via le canal de communication sans fil, d'une commande provenant du dispositif utilisateur, pour obtenir une information identifiant une donnée requise par le dispositif récepteur et réponse par la fourniture de l'information identifiant une donnée requise par le dispositif récepteur ; et
- réception via le canal de communication sans fil, d'une commande provenant du dispositif utilisateur, comprenant une donnée transmise correspondant à l'information identifiant une donnée requise par le dispositif récepteur.

[Revendication 20] Procédé selon la revendication précédente, dans lequel préalablement à la fourniture de l'information identifiant une donnée requise par le dispositif récepteur, le procédé comprend en outre une étape de chiffrement de l'information identifiant une donnée requise par le dispositif récepteur.

[Revendication 21] Procédé selon l'une quelconque des revendications 19 à 20, dans lequel la donnée transmise reçue est signée, le procédé comprenant en outre une étape de vérification de la signature de la donnée transmise reçue.

[Revendication 22] Procédé selon l'une quelconque des revendications 19 à 21, dans lequel le dispositif récepteur (104) reçoit en outre, une attestation de clés du dispositif utilisateur.

[Revendication 23] Procédé selon la revendication précédente, dans lequel l'attestation de clés du dispositif utilisateur comprend une clé cryptographique de signature publique du dispositif utilisateur.

[Revendication 24] Procédé selon la revendication précédente, dans lequel le procédé comprend en outre :

- une étape de génération d'un deuxième nombre aléatoire,
- une étape de mise à disposition au dispositif utilisateur du deuxième nombre aléatoire,
- une étape de réception d'une signature d'authentification du dispositif utilisateur,
- une étape de vérification de la signature d'authentification du dispositif utilisateur reçue au moyen de la clé cryptographique de signature publique du dispositif utilisateur obtenue et du deuxième nombre aléatoire.

[Revendication 25] Procédé selon la revendication 21 et la revendication 23, dans lequel la vérification de la signature de la donnée transmise reçue est réalisée au moyen de la clé cryptographique de signature publique du dispositif utilisateur obtenue.

[Revendication 26] Procédé selon l'une quelconque des revendications 22 à 25, dans lequel l'attestation de clés du dispositif utilisateur comprend une clé cryptographique de chiffrement publique du dispositif utilisateur.

[Revendication 27] Procédé selon les revendications 20 et 26, dans lequel l'étape de chiffrement de l'information identifiant une donnée requise par le dispositif récepteur est réalisée au moyen de la clé cryptographique de chiffrement publique du dispositif utilisateur.

[Revendication 28] Procédé selon l'une quelconque des revendications 19 à 27, dans lequel la donnée transmise reçue est chiffrée, et le procédé comprend une étape de déchiffrement de la donnée transmise reçue.

[Revendication 29] Procédé selon l'une quelconque des revendications 19 à 28, dans lequel le procédé comprend en outre une étape de signature de l'information identifiant une donnée requise par le dispositif récepteur.

[Revendication 30] Procédé selon l'une quelconque des revendications 19 à 29, dans lequel le dispositif récepteur comprend une paire de clés cryptographiques de signature comprenant une clé cryptographique de signature privée et une clé cryptographique de signature publique, dans lequel le procédé comprend en outre, la mise à disposition

du dispositif récepteur au dispositif utilisateur, d'une attestation de clés du dispositif récepteur, l'attestation de clés du dispositif récepteur comprenant la clé cryptographique de signature publique du dispositif récepteur.

[Revendication 31] Procédé selon la revendication précédente, dans lequel le dispositif récepteur reçoit, en outre, du dispositif utilisateur, un premier nombre aléatoire, et en ce que le procédé comprend une étape de génération d'une signature d'authentification du dispositif récepteur à mettre à disposition du dispositif utilisateur, la signature d'authentification étant générée à partir du premier nombre aléatoire reçu et de la clé cryptographique de signature privée du dispositif récepteur ; et la mise à disposition du dispositif récepteur (104) au dispositif utilisateur (102), de la signature d'authentification du dispositif récepteur à transmettre générée.

[Revendication 32] Procédé selon la revendication 28, dans lequel le déchiffrement de la donnée transmise est réalisée au moyen d'une clé cryptographique de chiffrement privée du dispositif récepteur.

[Revendication 33] Procédé selon la revendication 29 et la revendication 30, dans lequel l'information identifiant une donnée requise obtenue est signée au moyen de la clé cryptographique de signature privée du dispositif récepteur.

[Revendication 34] Procédé selon l'une quelconque des revendications 19 à 33, le procédé comprenant en outre les étapes suivantes :

- réception du dispositif utilisateur (102), d'au moins un identifiant d'algorithme cryptographique supporté par le dispositif utilisateur et réponse en fournissant au moins un identifiant d'algorithme cryptographique supporté par le dispositif récepteur ;
- détermination d'un d'algorithme cryptographique supporté par le dispositif utilisateur et le dispositif récepteur et
- déchiffrement de la donnée transmise correspondant à l'information identifiant une donnée requise par le dispositif récepteur en utilisation l'algorithme cryptographique déterminé.

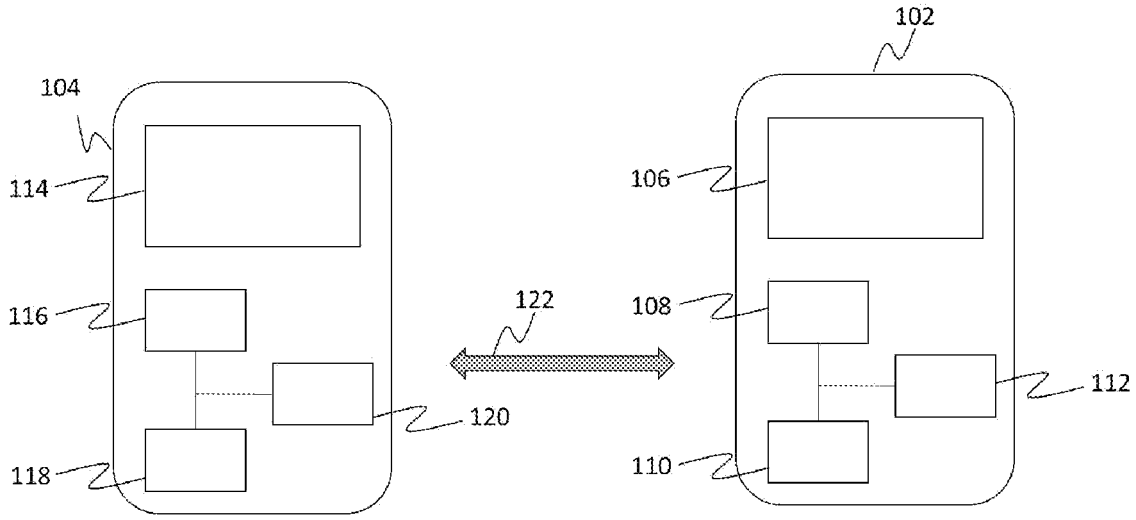
[Revendication 35] Procédé selon l'une quelconque des revendications 19 à 34, dans lequel le canal de communication sans fil est un canal de

communication conforme à la norme NFC, à la norme Bluetooth ou à la norme WiFi.

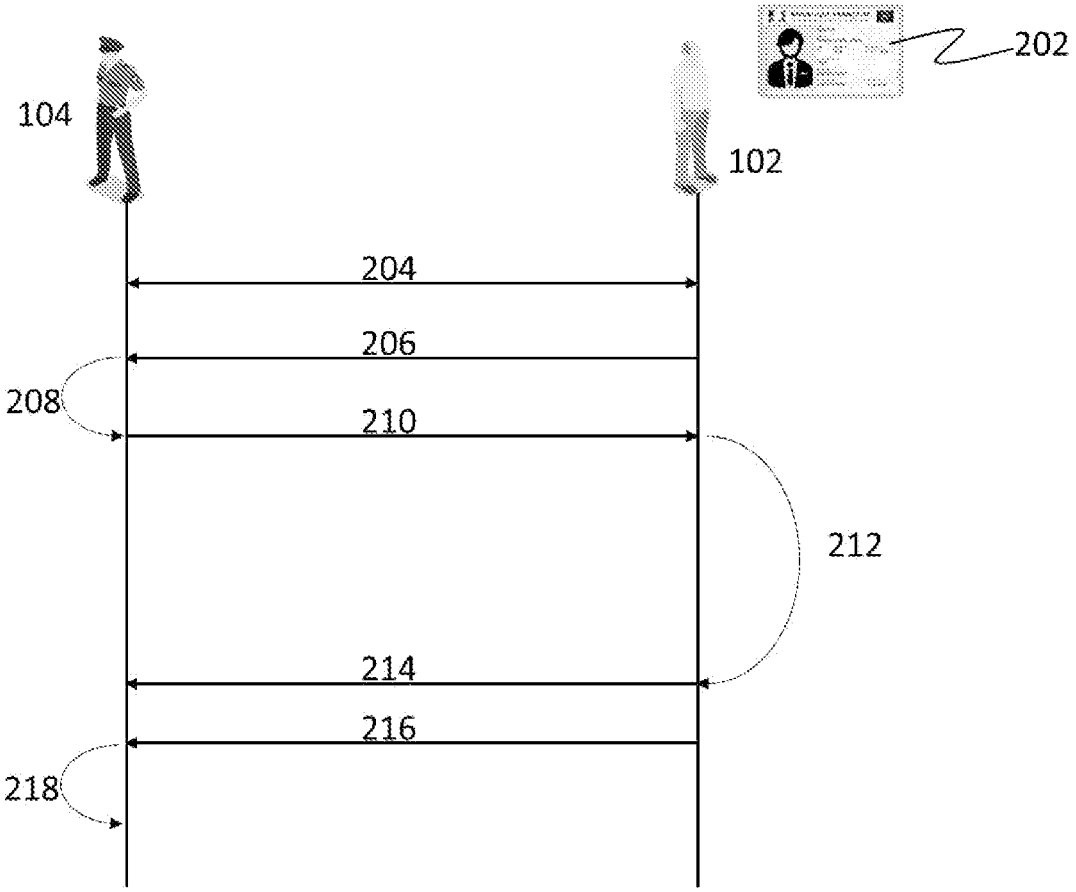
[Revendication 36] Dispositif configuré pour mettre en œuvre le procédé selon l'une quelconque des revendications 1 à 18 ou selon l'une quelconque des revendications 19 à 35.

[Revendication 37] Système comprenant un dispositif utilisateur et un dispositif récepteur, le dispositif utilisateur mettant en œuvre le procédé selon l'une quelconque des revendications 1 à 18 et le dispositif récepteur mettant en œuvre le procédé selon l'une quelconque des revendications 19 à 35.

[Fig. 1]


102
104
106
114
116
122
108
112
120
118
110

[Fig. 2]


202
104
102
204
206
208
210
212
214
216
218

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 930315
FR 2312879

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	EP 2 007 106 A1 (INSIDE CONTACTLESS [FR]) 24 décembre 2008 (2008-12-24) * abrégé * * alinéas [0002], [0003], [0005], [0010], [0011] * * alinéas [0052], [0055], [0057], [0060], [0069] * -----	1-37	G06F 21/60 H04L 9/08 H04L 9/16 H04W 12/069
A	WO 2018/160863 A1 (APPLE INC [US]) 7 septembre 2018 (2018-09-07) * abrégé * * alinéas [0052] - [0055], [0059] * * alinéas [0060], [0062], [0063], [0065], [0067] * -----	1-37	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			H04L H04W

Date d'achèvement de la recherche	Examinateur
11 septembre 2024	Adkhis, Franck

CATÉGORIE DES DOCUMENTS CITÉS

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

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

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 2312879 FA 930315

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 11-09-2024
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 2007106 A1	24-12-2008	CA 2623621 A1	07-09-2008
		CN 101261675 A	10-09-2008
		EP 2007106 A1	24-12-2008
		FR 2913549 A1	12-09-2008
		FR 2913550 A1	12-09-2008
		JP 2008252883 A	16-10-2008
		US 2008219444 A1	11-09-2008
WO 2018160863 A1	07-09-2018	AU 2018228890 A1	19-09-2019
		CN 110291754 A	27-09-2019
		CN 114584982 A	03-06-2022
		EP 3590225 A1	08-01-2020
		EP 3748900 A1	09-12-2020
		JP 6861292 B2	21-04-2021
		JP 2020511069 A	09-04-2020
		KR 20190104401 A	09-09-2019
		KR 20220069117 A	26-05-2022
		US 2020052905 A1	13-02-2020
		US 2022078029 A1	10-03-2022
		WO 2018160863 A1	07-09-2018

EPO FORM P0465